OXFORD CDE

Journal of Computational Design and Engineering, 2020, 7(3), 352–366

doi: 10.1093/jcde/qwaa029
Journal homepage: www.jcde.org
Advance Access Publication Date: 4 April 2020

RESEARCH ARTICLE

Modeling and assessing cyber resilience of smart grid using Bayesian network-based approach: a system of systems problem

Niamat Ullah Ibne Hossain[1,*], Morteza Nagahi[1], Raed Jaradat[1], Chiranjibi Shah[2], Randy Buchanan[3] and Michael Hamilton[4]

[1]Department of Industrial and Systems Engineering, Mississippi State University, PO Box 9542, Mississippi State, 39762; [2]Department of Electrical and Computer Engineering, Mississippi State University, PO Box 9542, Mississippi State, 39762; [3] Institute of Systems Engineering Research (ISER), U.S Army Engineer Research Development Center (ERDC), 3909 Halls Ferry Rd, Vicksburg, MS 39180 and [4]Institute of Systems Engineering Research (ISER), 3909 Halls Ferry Rd, Vicksburg, MS 39180.

*Corresponding author. E-mail: ni78@msstate.edu

Abstract

Due to the widespread of new technologies, the modern electric power system has become much more complex and uncertain. The Integration of technologies in the electric power system has increased the exposure of cyber threats and correlative susceptibilities from malicious cyber-attacks. To better address these cyber risks and minimize the effects of the power system outage, this research identifies the potential causes and mitigation techniques for the smart grid (SG) and assesses the overall cyber resilience of smart grid systems using a Bayesian network approach. Bayesian network is a powerful analytical tool predominantly used in risk, reliability, and resilience assessment under uncertainty. The quantification of the model is examined, and the results are analyzed through different advanced techniques such as predictive inference reasoning and sensitivity analysis. Different scenarios have been developed and analyzed to identify critical variables that are susceptible to the cyber resilience of a smart grid system of systems. Insight drawn from these analyses suggests that overall cyber resilience of the SG system of systems is dependent upon the status of identified factors, and more attention should be directed towards developing the countermeasures against access domain vulnerability. The research also shows the efficacy of a Bayesian network to assess and enhance the overall cyber resilience of the smart grid system of systems.

Keywords: cyber vulnerabilities; smart grid; power system; resilience; Bayesian network; system of systems

1. Introduction

The electric grid is the mainstay of power generation and is connected to many other critical infrastructures such as transportation, telecommunication, fuel distribution, and water supply. The entire electric grid network can be considered as a system of systems (SoS), where different constituents, legacies, or new systems integrate to accomplish an emergent mission or to produce new desirable goals that are beyond the individual systemic capabilities (Hossain & Jaradat, 2018; Hossain, Nagahi,

Received: 9 July 2019; **Revised:** 13 September 2019; **Accepted:** 10 December 2019

Jaradat, & Keating, 2019; Jaradat, Keating, & Bradley, 2014). Any failure of a grid infrastructure sub-system will ripple through and affect the electric grid system of systems. The underlying reasons for grid-disruptions are abundant, including natural disasters such as a hurricane, snowstorm, lightning as well as a course of events ranging from human errors to machinery failures to malicious cyber-attacks (Hossain, Jaradat, Hosseini, Marufuzzaman, & Buchanan, 2019). Concerning the smart grid (SG) system of systems, cyber-attack is the most common threat. A smart grid system of systems is comprised of heterogeneous distributed systems such as the metering system, SCADA system, microprocessors, wireless mesh networks, and remote terminal units (RTUs; Bojkovic & Bakmaz, 2012; Wadhawan, Al-Majali, & Neuman, 2018). For a better governance and information exchange, these individual systems and their components are interconnected through an advanced communications network (Nazir, Hamdoun, & Alzubi, 2015). Smart grid has gained increasing popularity due to its reliability and cost reduction power delivery. However, the interconnectivity nature of smart grids makes them more exposed to cyber threats.

Since cyber threats are complex, unpredictable, and persistent, cyber risks in smart grids cannot be readily predicted or even anticipated. Federal agencies and national security partners have emphasized on the development of subtle defense strategies and proper exercise control to keep the SoS grid system safe from cyber-intrusions. The losses due to the cyber threat depend on the type and severity of the attack, such as productivity loss, downtime, economic impact, loss of time, and business reputation (Cashell, Jackson, Jickling, & Webel, 2004). One of the recent reports claimed that cyber-attacks drop the stock value of many companies by 1–5% (Bryan, 2014). Also, on 15 December 2015, around 80,000 people suffered from the power outage due to a cyber-attack on an electrical power station in Europe. The hackers deleted the operational data, locked up the system, destroyed the hard drives, and took control over the infected computers. Homeland Security reported that there is an increasing trend in the total number of cyber-attack on electricity transmission networks, as evidenced by more than 4300 recent cyber-attack impacted the electrical grids in Europe. As the US electric grid relies more on internet operations, it is susceptible to serious cyber threats. To mitigate the impact of cyber-attack, several government agencies and private companies contribute to protecting smart grids. Baltimore gas and electric, as an example, shares data with industry and government partners to address issues related to cyber-attack. Law enforcement agencies and national and local institutions, such as Duke Energy, collaborate to develop rules and relegations of cyber protection (Bearingpoint, 2019). Based on these examples and others in the literature, the development of a safe smart grid system of systems has become a necessity and a research topic of paramount interest. The rationale for this research is to address the current gap in the literature—lack of studies dedicated to cyber resilience using advanced Bayesian analysis designed for the smart grid system of systems. The research attempts to help practitioners to withstand and recover from a grid disturbance due to a cyber-attack through the development of a robust smart grid resilience-based approaches. Cyber resilience is the ability of a system to absorb, adapt, and recover from cyber-intrusion (Biringer, Vugrin, & Warren, 2016). This research uses a Bayesian network (BN) to address a range of possible cyber risks to the SoS smart grid and to offer possible mitigation options to mitigate the consequences of a cyber-disruption.

Over the last several years, research on cybersecurity in the smart grid has received increased attention because of the vulnerable nature of the smart grid system to cyber-attacks. Some of the researchers characterized the severity of the attack, along with only a cursory discussion of mitigations by offering a wide gamut of analytical techniques. Other researchers developed theoretical frameworks to analyze the risks and validated their methodologies based on scenarios or case studies. For instance, Liang, Gao, Zheng, and Zhao (2013) proposed a reliable protection framework and provided some practical recommendations to mitigate the cyber risk of the smart grid. They developed 3-layer security protocols, namely the main station, communication network, and terminals of the smart grid. In another study, Shapsough, Qatan, Aburukba, Aloul, and Al Ali (2015) developed a 5-layer security smart grid conceptual model based on the Internet of Thing (IoT) platform and described some modern solutions to ensure seamless operations of smart grids. A somewhat comprehensive approach was followed by Wang and Lu (2013), who investigated the security requirements and network vulnerabilities of the smart grid from cyber-intrusion perspective. They classified the threats into three categories: people and policy, platform, and network threats and discussed the countermeasures for each category. Rana, Li, and Su (2016, 2018) adopted an advanced approach to mitigate and control the malicious cyber-attack on micro-grids. To maintain a safe cyber microgrid structure, they utilized a recursive systematic convolutional code and Kalman filter-based method. Numerical simulations were applied to verify the efficacy of the proposed approach. El Mrabet, Kaabouch, El Ghazi, and El Ghazi (2018) provided a detailed description of different cyber-attacks on the smart grid and recommended cutting-edge strategies to identify and counter these attacks. In another research, Saad, Faddel, and Mohammed (2019) modeled the physical and cyber system by applying the graph theory and consensus protocol for mitigating the cyber-attack, where the system can detect and mitigate the different kinds of attack such as replay, inception, and stealthy attack. By the same token, the security monitoring framework is analyzed as a tool for dealing with smart grid communication challenges by Parra, Rad, and Choo (2019). In this research, the network can be reconfigured in real-time to manage threats. The concept of dummy value for defense topology is introduced as an advanced technique by Shahid, Nawaz, Qureshi, and Mahmood (2018) to defense against cyber-intrusion related to the stealthy attack or false data injection in the smart grid. The authors also posited that all kinds of cyber-attacks could be detected using this technique to reduce the loss and damage of the entire network. Saleh, Khdour, Ferrah, Qasaymeh, and Togher (2019) proposed a mobile modular lab platform for cyber testing of the smart grid as one of the mitigation techniques to the vulnerabilities and threats of the ICT communication system, where the IP address of smart endpoint device can be used for analyzing cyber-threats and advocating proper solutions. Xia, Xiao, and Liang (2019) presented an adaptive algorithm as a scanning method to locate malicious users in the adjacent vicinity of a smart grid system within the shortest detection time. The authors also demonstrated the advantages of the adaptive algorithm over other techniques to detect and inspect malicious attackers in the smart grid. Rana, Xiang, and Choi (2018) developed a new algorithm using the Internet of things to estimate the states of smart grids. The Internet of things sensors was used to estimate the state of generator systems. The proposed algorithm showed a better performance in terms of time duration compared to conventional techniques. Similarly, Rana, Xiang, and Wang (2018) developed an algorithm based on a Bayesian filter concept to estimate the state of the smart grid system iteratively. The state of the smart grid system was balanced using

a semidefinite programming based optimal feedback controller. The simulation results showed the effectiveness of the proposed algorithm to stabilize the systems states within a small time duration. Rana (2017) also proposed a distributed state estimation and stabilization algorithm to protect smart electric vehicles from cyber-attack. Radoglou-Grammatikis, Sarigiannidis, Liatifis, Apostolakos, and Oikonomou (2018) presented the utility of the firewall system to deal with various cyber-attacks in the smart grid such that critical states and suitable specifications can be determined using appropriate protocols. Besides the development of conceptual approaches, Wadhawan et al. (2018) followed an analytical approach to compute the likelihood of cyber threats on the smart grid and provided a list of countermeasures. Table 1 provides a synthesis of the current themes of resilience in the smart grid cyber-attack literature. These general themes serve as a baseline snapshot in developing the proposed model.

Since the smart grid is comprised of a different set of systems, components, resources, and appliances, it requires a systemic integration approach of all these smart grid components to ensure seamless power transformation. For a better risk assessment, it is necessary to move from a reductionist paradigm toward a more "systemic paradigm" (Alfaqiri et al., 2019; Hossain, Nur, & Jaradat, 2016; Jaradat & Keating, 2014; Lawrence, Hossain, Nagahi, & Jaradat, 2019; Nagahi, Nagahisarchoghaei, Soleimani & Jaradat, 2018). The state-of-art literature review identified the main gap that needs to be addressed—lack of a framework that provides in-depth cyber resilience analysis of the smart grid system of systems. To address this gap, this research considers the smart grid cyber resilience as a system of systems and contributes towards developing a comprehensive resilience assessment and enhancement framework of the smart grid system of systems to ensure safe cyber synchronization of communication, data sensing, and information technology. This research commences by identifying the factors and subfactors that impact the cyber resilience of the smart grid. From this baseline, a comprehensive resilience model is designed and quantified based on the BN theory. The proposed model will assess the overall resilience of the smart grid system and evaluate the applicability of countermeasures based on the types of cyber-attack. The main contributions of this research are summarized as follows:

- Identification of potential factors that are responsible for the disruption of smart grid SoS under severe malicious cyber-intrusion.
- Development of a probabilistic graphical model, a BN, to visualize and quantify the potential cyber risks. This also allows offering mitigation techniques based on the types of attacks.
- Execution of a set of advanced analyses, such as predictive inference reasoning and sensitivity analysis, to provide meaningful insights based on proposed model results.
- Demonstration of the efficacy of the proposed model as a comprehensive cyber risk assessment tool to identify the smart grid cyber vulnerabilities that need to be prioritized to ensure cyber safe smart grid SoS.

A BN is an analytical tool that illustrates all the causal relationships among the different qualitative and quantitative variables and allows practitioners to understand the relative importance of independent variable(s) on a particular dependent variable for a given set of conditions. The BN aids in predicting interventions, handling missing data, and avoiding overfitting data (Fenton & Neil, 2012). Conventional techniques presented in literature lack an effective implementation of a Bayesian approach for enhancement of cyber resilience in a smart grid. To draw further insight from the proposed model, a set of advanced analysis techniques such as predictive inference reasoning and sensitivity analysis is conducted. One of the advantages of the BN over conventional techniques is that BN reduces the burden of parameter acquisition; thus, the elicitation of probabilities is easier, and the results of the model are self-explanatory. Moreover, irrespective of the size of the data, BN can accommodate both subjective beliefs and objective data, and overturn previous beliefs in light of new evidence. Thus, in the case of the proposed model, we can always update the prediction of the cyber vulnerability of a smart grid based on any new evidence or attacks.

The application of BN has been extended to across different domains, including but not limited to, risk and reliability evaluation, data classification, supply chain management, fault diagnosis, critical infrastructures, manufacturing system, safety management, the system of systems, project management, performance measurement, and many more. A sample summary is provided in Table 2 to demonstrate the efficacy of BN across different fields.

In what follows, Section 2 presents an overview of BNs. Section 3 presents the proposed framework for our study. In Section 4, we identified the potential causes of cyber risks that could impact the SoS smart grid, followed by an illustration of different control strategies against the backdrop of resilience capacities. Quantification of resilience contributors is discussed in Section 5. In Sections 6 and 7, we presented a set of advanced statistical techniques such as predictive inference reasoning and sensitivity analysis to provide better insight to enhance the overall resilience of the smart grid system of systems. The research will close with a discussion of the implications that the fundamental model has for the overall cyber resilience SG system of systems.

2. Bayesian Rule and Inference Algorithm

This section provides a background of the BN, which is a decision support tool widely used in risk and resilience engineering. BN is a Directed Acyclic Graph, which is comprised of nodes (variables) and edges (arcs). Nodes denote the variables and edges signify the relationship between the two variables in the underlying network. The interrelationships of the nodes are displayed through three levels of specification: graphical level, functional level, and numerical level (Laitila, 2013). The conditional interdependencies between nodes and edges are depicted through the graphical level specification. The functional level of specification states the conditional and joint probability distributions of the nodes through an algebraic manner, whereas the actual probability associated with a specific node is defined through the numerical level of specifications (Laitila, 2013). Equation (1) represents the generic rule of the Bayesian theorem.

$$P\,(H|e) = \frac{P\,(H|e) \times P\,(H)}{P\,(e)}, \tag{1}$$

where H is a hypothesis and e is evidence of an event. Bayes theorem revises the marginal probability associated with hypothesis H based on a given evidence e. The product of prior hypothesis probability $P(H)$ and a posterior probability $P(H|e)$ calculate the probability of H for given e.

To ground the functionality of BN, let us consider a BN structure with a set of variable $S = \{M_1, M_2, M_3, M_4, M_5\}$ and a set of edges to show the conditional interdependencies among the variables (see Fig. 1). A departing edge from M_i to M_j denotes the interrelationship between these two variables such that the value of M_j is conditioned on the value of M_i and M_i is the

Table 1: Current themes of resilience in smart grid.

Authors	Research theme	Approach
Nazir et al. (2015)	Vulnerabilities and resilience of smart grid	Macro and micromanagement technique
Liang et al. (2013)	Cybersecurity in smart grid	Protection framework and reliability
Shapsough et al. (2015)	Cybersecurity in smart grid	Information and communication technologies
Wang and Lu (2013)	Cybersecurity in smart grid	Cryptography
El Mrabet et al. (2018)	Cybersecurity in smart grid	Intrusion detection system
Wadhawan et al. (2018)	Cyber-physical system	Bayesian network
Saad et al. (2019)	Cybersecurity in smart grid	Graph theory
Parra et al. (2019)	Information and communication for smart grid	Software-defined network
Shahid et al. (2018)	False data injection attack in smart grid	Defenses topology
Saleh et al. (2019)	Cyber testing of smart grid	Setting up a mobile modular lab
Xia et al. (2019)	The malicious attack in smart grid	Adaptive algorithm
Radoglou-Grammatikis et al. (2018)	Cyber-attack in smart grid	Firewall system

Table 2: Application of BN across different domains.

Authors	Application area
Pérez-Miñana (2016)	Natural resource management
Arizmendi, Sierra, Vellido, and Romero (2014)	Data classification
Yet et al. (2016)	Project management
Han, Marais, and DeLaurentis (2012)	System of systems
Hänninen, Banda, and Kujala (2014)	Traffic accidents
Saini (2008)	Power system
Hossain, Nur, Hosseini, et al. (2019), Hossain, Nur, Jaradat, et al. (2019), Hossain et al. (2020)	Waterway port
Hosseini and Sarder (2019)	Electric vehicle
Zhou et al. (2018)	Safety management
Hossain, Jaradat, Hosseini et al. (2019)	Electrical infrastructure
Pascual, Miñana, and Giacomello (2016)	Biodiversity
Amundson, Faulkner, Sukumara, Seay, and Badurdeen (2012)	Supply chains
Hossain, Jaradat, Marufuzzaman, Buchanan, and Rinaudo (2019)	Oil and gas industry

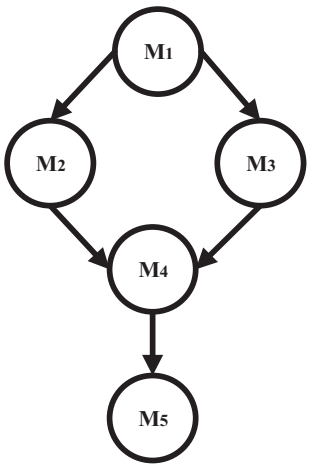

Figure 1: Diagrammatic depiction of a Bayesian model with five variables.

parent node of M_j and M_j is the child node of M_i. The corresponding decomposition of the joint distribution of variables can be expressed as follows [see equation (2)].

The equation can be streamlined as follows:

$$P(M_1, M_2, M_3, M_4, M_5)$$
$$= P(M_1)\, P(M_2|M_1)\, P(M_3|M_1)\, P(M_4|M_2,\ M_3)\, P(M_5|M_4)$$
$$= \prod_{i=1}^{n} P(M_i|Parents(M_i)). \quad (2)$$

3. Proposed Framework for Resilience Assessment

This section describes the proposed resilience assessment process of our research. The process is based on five phases, as presented below and depicted in Fig. 2.

- **Phase I** (Identification of factors and subfactors): To identify the factors and subfactors that can impact the cyber resilience of the smart grid, current research related to cybersecurity in the smart grid is studied, analyzed, and fundamental criteria are derived. Then, incorporating a view of experts, six main factors are considered to design the aspects of vulnerability and recoverability of SG.
- **Phase II** (Quantification of factors and subfactors): Based on subjective or frequentist approach, factors and subfactors are quantified in the second phase.
- **Phase III** (Construction of BN model): In the third phase, the fundamental BN model is developed and simulated.

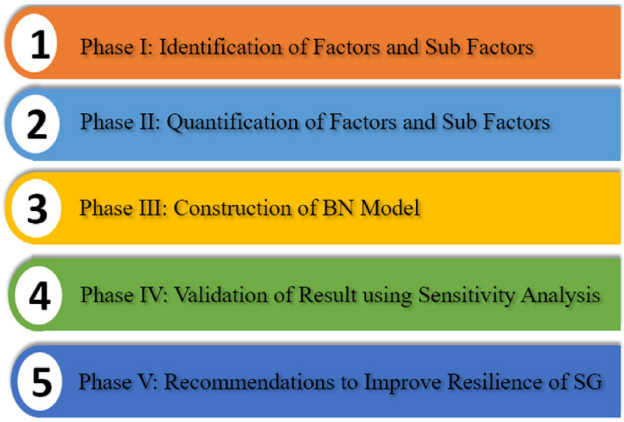

Figure 2: Proposed framework for resilience assessment using the BN approach.

- **Phase IV** (Validation of result): To illustrate the validation of the BN model, different approaches such as predictive inference reasoning and sensitivity analysis are conducted.
- **Phase V** (Recommendation to improve resilience performance of smart grid): Various recommendations are suggested to enhance the resilience of SG based on the outcomes obtained from the analyses.

4. Designing the Resilience Contributors of SG

Resilience is one of the salient features of a smart grid. Smart grid resilience defines how the efforts across the smart grid system resume the activity successfully after any disruption. Consistent with the recommendation of Henry and Ramirez-Marquez (2012), we calculated resilience as the ratio of restoration (recoverability) to vulnerability. Smart grid vulnerability is addressed through three domains of software, access, and network. Resilience capacities are the strategies to recover a region/entity from any shock or external perturbation due to disruption. The smart grid restoration (recoverability) can be expressed using absorptive capacity, adaptive capacity, and restorative capacity of the corresponding system (Hosseini, Al Khaled, & Sarder, 2016; Cai, Xie, Liu, Liu, & Feng, 2018; Hossain et al., 2019). The resilience method is generally designed based on meta-structure under internal deterioration and external perturbation (Feng, Fan, Cai, Liu, & Ren, 2019; Lawrence, Hossain, Rinaudo, Buchanan, & Jaradat, 2020). Thus, there are two contributing parent nodes for resilience: vulnerability and Restoration (recoverability). In this research, the parameters of the proposed scheme are designed based on the cyber resilience perspective. Identifying the main parameters (causes) plays a key role in the proper assessment of the cyber resilience of the smart grid system of systems. All the parameters associated with cyber vulnerability and recoverability are determined using the following procedure. First, an extensive literature review was conducted, analyzed, and then the main parameters are identified. Second, to finalize the salient set of parameters for the cyber vulnerability and recoverability of the smart grid, expert opinions are incorporated within the scope of the smart grid system of systems, and the less important parameters are removed. These parameters are further quantified based on historical data, frequentist approach, and expert elicitation techniques to measure the overall resilience of the smart grid system of systems. In the following subsection, we discuss the causes of vulnerability and different techniques of recoverability for the smart grid from cyber-intrusions.

4.1. Vulnerability

Generally, there are mainly three kinds of cyber vulnerabilities that impact the performance of the SoS smart grid, namely software, access, and network domain vulnerability (Polonetsky, 2009; Kundur, Feng, Liu, Zourntos, & Butler-Purry, 2010; Li et al., 2010; NISTIR, 2010; Line, Tøndel, & Jaatun, 2011; Nelso & Chaffin, 2011; Pallotti & Mangiatordi, 2011; Aloul, Al-Ali, Al-Dalky, Al-Mardini, & El-Hajj, 2012; Arghandeh, Von Meier, Mehrmanesh, & Mili, 2016). The description of these vulnerabilities, along with the causes, are presented below.

4.1.1. *Software domain vulnerability*

Several causes lead to software domain vulnerability. All these causes are liable to jeopardize the safety of the smart grid system. These causes are discussed below.

- Weak code: Weak code is the quality of code that was not precisely developed. These weak codes make the software system vulnerable to cyber-attacks and might be produced by the use of potentially dangerous functions or NULL pointer dereference (Aloul et al., 2012; NISTIR, 2010; Polonetsky, 2009; USDOE, 2009).
- Improper data validation: The improper data inputted to an application can provide an attacker with easy access to conduct cyber-intrusion. There are different improper data input validations approaches including, but not limited to, buffer overflow, lack of bounds checking, command injection, SQL injection, cross-site scripting, and path traversal makes the software system vulnerable (Aloul et al., 2012; Line et al., 2011; Nelso & Chaffin, 2011; NISTIR, 2010).
- Cryptographic issues: Issues related to transferring the credential across the network make the software system unprotected that allow the hacker to have unauthorized access to a computer system or its critical information. The cryptographic issues might be created by missing encryption of sensitive data or the use of broken/risky cryptographic algorithms (Arghandeh et al., 2016; Line et al., 2011; NISTIR, 2010; Pallotti & Mangiatordi, 2011).
- Untimely adoption of software: Flaws, misconfigurations, or poor maintenance of the smart grid might endanger the operating systems, applications patching, physical access control, and security concern of the SG system. These cyber-threats can be related to poor patch management during software development or improper security configuration (Arghandeh et al., 2016; NISTIR, 2010; Pallotti & Mangiatordi, 2011; Shah, Perrig, & Sinopoli, 2008).

4.1.2. *Access domain vulnerability*

Disability to detachment of duties through assigned access permissions, the deficiency to block system enforcement for failed login attempts, and end remote access sessions after a defined period are some common cyber vulnerabilities of the access control domain. Weak users, unauthorized protocols, or weak access policies may result in access domain vulnerability (Aloul et al., 2012; Arghandeh et al., 2016; Kundur et al., 2010; Li et al., 2010; Line et al., 2011; Nelso & Chaffin, 2011; NISTIR, 2010; Pallotti & Mangiatordi, 2011).

- Weak user: Attackers can capture and crack user credentials during the credential transfer through cleartext. Weak User password is another important vulnerability of the access

domain (Arghandeh et al., 2016; Line et al., 2011; Nelso & Chaffin, 2011; NISTIR, 2010).
- Unauthorized protocols: The disability to logging or poor logging practices as well as lack of security audits trigger protocol authorization (Kundur et al., 2010; Line et al., 2011; Nelso & Chaffin, 2011).
- Weak access policies: Lack of development of a formal business case documentation of SG security access policy threatens the resilience of the whole SG system (Kundur et al., 2010; Line et al., 2011; Nelso & Chaffin, 2011; Pallotti & Mangiatordi, 2011).

4.1.3. *Network domain vulnerability*

The threats on the network domain are associated with architectural design and its implementation technique. The proper network architecture can observe a process remotely and control the supply process data for a business function from the network domain. The major risks within the network domain discussed below (Aloul et al., 2012; Kundur et al., 2010; Li et al., 2010; Line et al., 2011; McDaniel & McLaughlin, 2009; Nelso & Chaffin, 2011; NISTIR, 2010; Pallotti & Mangiatordi, 2011; Polonetsky, 2009; USDOE, 2009).

- Network configuration: Lack of safe configuration of network devices, as well as lack of port security's implementation on network equipment, are major concerns regarding network configuration for SG system (Kundur et al., 2010; Li et al., 2010; Nelso & Chaffin, 2011; NISTIR, 2010; Pallotti & Mangiatordi, 2011).
- Network audit and monitoring: There is a common network weakness where the ongoing network diagram does not match the ongoing state of the smart grid network. This weakness might appear due to lack of understanding of network architecture, fragile support of remote login policies, fragile control of input and output media, and bad monitoring of intrusion detection systems (Li et al., 2010; Line et al., 2011; Nelso & Chaffin, 2011; NISTIR, 2010; Pallotti & Mangiatordi, 2011).
- Lack of security perimeter: One of the most important security network designs is a firewall policy, which regulates the transformation of network packets. The unrestricted access to certain ports on host based on IP addresses and a mismatch between firewall rules and network traffic are two major network security vulnerabilities for the smart grid (Kundur et al., 2010; Line et al., 2011; Nelso & Chaffin, 2011; NISTIR, 2010; Aloul et al., 2012).

4.2. Restoration (recoverability)

Restoration (recoverability) can be modeled through a unique set of resilience capacities, namely, absorptive capacity, adaptive capacity, and restorative capacity (Biringer et al., 2016). Resilience capacity is an endogenous feature of a system that enhances the capability of any system to absorb, adapt, and recover from any external attack or disruption (Hossain, Jaradat, Hosseini et al., 2019).

4.2.1. *Absorptive capacity*

Absorptive capacity is an endogenous feature of the system and is also considered to be the first course of defense to minimize the impacts of the disruption (Biringer et al., 2016; Hossain et al., 2019). The absorptive capacity of the system includes a set of intentional proactive measures by which a system can automatically cope with the exposure or sensitivity of the shock relatively with less effort. Following is a list of three key factors germane to the absorptive capacity of SG from cyber-attack.

Advanced metering infrastructure (AMI): Also known as "smart metering" is a critical component of smart grid system of systems that includes smart meters, concentrators, and the Meter Data Management System that together facilitate secured communication, power consumption measurements, communications with the outside nodes, data storage, management, and so on (Mohammadali, Haghighi, & Tadayon, Mohammadi-Nodooshan, 2016). Also, it can facilitate two-way communication between meter and distribution system operator that is difficult or impossible to implement without smart metering.

Visualization technology: To outperform the activities conducted by cyber hackers, experts need to incorporate cutting edge technologies within the structure of smart grid technology (Venugopalan & Rai, 2015). Tools associated with grid visualization can be used for real-time load monitoring and load-growth planning at the utility level. It may be challenging to understand and act on data when the demand response program for customers increases. Advantage of contents of Google earth can be taken into consideration due to its built-in platform of VERDE (Visualizing Energy Resources Dynamically on Earth). This technology facilitates wide-area grid awareness, integrating real-time sensor data, weather information, and grid modeling with geographical information to keep the smart grid system cyber safe. It can also provide instant information about blackouts and power quality to enhance the reliability of the system operation (Sadiku, Musa, & Nelatury, 2016).

Conditioning monitoring system (CMS): Operating characteristics of a smart grid can be monitored using a CMS so that the need for maintenance can be predicted before any serious breakdown or deterioration happens. CMS monitors the life mechanism of the individual components or whole equipment by acquiring the relevant data. This information is further analyzed and examined to predict the trend of failure (Han & Song, 2002).

- SCADA: The architecture of Supervisory control and data acquisition system (SCADA) includes programmable logic controllers or RTUs that communicate with an array of objects such as factory machines, HMIs, sensors, and end devices, and then route the information from those objects to computers with SCADA software. SCADA software processes, distributes, and displays the data and helps operators and other employees to analyze the data and make important decisions. SCADA systems are crucial for the smart grid system in terms of maintaining efficiency, data processing, smarter decision making, and communicating system issues to help mitigate downtime (Creery and Byres, 2005).
- *Phase measurement unit (PMU)* is used in the system control center for tracking the state of the system continuously, which enhances the security performance by anomaly detection using a dynamic state estimation process (Deng & Shukla, 2012). PMU measures current phasors, voltage phasors, and the frequency at 30, 60, or 120 times per second, and measurement from different PMU can be synchronized within 1 μs to facilitate accurate state estimation (Morris, Pan, & Adhikari, 2012). Equipped with smart grid technologies, it can ease the congestion and bottlenecks and mitigates or even prevent the blackouts by providing two-way visibility and control of energy usage (Sadiku et al., 2016).
- Wide area measurement system (WAMS): Power outage can impact hundreds of thousands of residences and industries as a result of a malicious attempt by cyber hackers. WAMS can provide real-time monitoring and control as an online

power system analysis tool for large scale implementation of the smart grid. More timely and accurate data can be obtained with a WAMS, which is crucial to protect the power system by defending against cyber-attacks (Liu, Fan, & Terzija, 2016). Out-step oscillation due to disturbance might impact the reliability of the smart grid system; WAMS can be used in such a situation to determine whether the system is stable or not, resulting in timely prevention by emergency control (Yang & Zhang, 2014).

- Wide area damping controller (WADC): WADC is used for small signal stability enhancement. WADC is an advanced technique that considers multiple operating points, time delays in communication channels, and track possible permanent loss of communication channel, which may occur due to the denial-of-service cyber-attack (Wang, Lu, & Tang, 2013).

4.2.2. *Adaptive capacity*

Adaptive capacity, which is considered to be the midline of defense, is described as the ability of a system to self-organizes itself and to provide immediate solutions to cope with the external perturbation without any recovery activity. Within the adaptive capacity of SG, three salient determinants are identified.

Grid partitioning: To minimize the impacts of cyber disturbances, grid partitioning allows the system operators to adjust voltage control inside each segment (microgrid) and minimize signal stability issues and cascading failures in the large complicated network during any perturbation (Arghandeh et al., 2016). Dynamic microgrid partition uses different kinds of advanced filters to manage the group information better and is substantially efficient compared to existing identity-based protocols to keep the SG system safe from large scale cyber threats (Wan, Phoha, Pei, & Chen, 2017).

Large capacity battery backup: Adaptive reconfigurable system can be deployed to address the real-time load requirement by adjusting to the desired system configurations (He et al., 2019). To avoid cyber-attacks, an energy management mechanism can be developed consisting of real-time measure on the state of charge (SOC) of the battery, power output of ultracapacitor, and the load profile (Kamal & Wei, 2017). For efficient management of a smart grid battery energy system, a high precision SOC of the battery can be considered as a viable technique.

Delay-adaptive control strategy: Power infrastructure is integrated with information technologies in the smart grid. To develop a resilient smart grid system, a delay-adaptive control strategy can be implemented so that the communication delay of the system can be reduced to a delay-free system. When large communication delay exists, distributed control mode can be converted into decentralized control mode (Wang & Wang, 2019). In the worst case, delay performance can be improved by increasing traffic to an adjustable amount as a means to combat jamming attacks (Lu, Wang, & Wang, 2015).

AI in cyber defense: Security operators often struggle to get access and deliver a prompt response to cyber-attacks. In such a case, the autonomous and intelligent cyber defense can be developed using interconnected systems, sensors, and effectors, defense vehicles, systems, and infrastructure, rendering high efficiency (Théron et al., 2018).

Intelligent power flow system: One of the imperative features of the smart grid is the intelligent power flow system. With the advanced computer, communication, and internet technologies, the intelligent power flow system significantly improves efficiency in all aspects of electricity generation, distribution, and processes by automatically regulating the flow of power (Wu, Varaiya, & Hui, 2015). This feature also identifies false data injection attacks by using default barrier conditions and blind identification techniques and data-driven approaches.

- Cooperative adaptive cruise control (CACC) can be used as a control scheme to mitigate the effect of cyber-attack, such as Denial of Service in smart grids. Since SG is a highly dynamic because of time reliant load and power generation, estimated states can be used in the algorithm to improve the security of SG under cyber-attack (Biron, Dey, & Pisu, 2017).
- Autonomous intelligent cyber defense agent (AICA) can work in cohorts that will be capable of detecting cyber-attack, devising appropriate countermeasures by running adaptive execution. AICA can detect enemy agents and can destroy or degrade malware in an autonomous manner (Théron et al., 2018). Without external intervention, such an intelligent autonomous system can perform well when uncertainties exist in the system for a more extended period (Antsaklis, Passino, & Wang, 1991).

4.2.3. *Restorative capacity*

Restorative capacity, considered to be the final line of defense, is the degree to which a system can efficiently repair or restore from the degraded state to retrieve its actual performance (Biringer et al., 2016). Restoration of cyber control is expected to go faster compared to other restoration activities. When the malevolent virus infects the entire SG system of systems, reinstallation might take more time than expected. It requires the dexterous team of experts who could work on an advanced decision support platform to ensure that every infected system will return to the initial service state quickly. Following is a list of salient factors about the restorative capacity of SG.

Restoration of control: In a smart grid, control architecture can be established as the restoration of control for fault location and power restoration (Bento, Kuiava, & Ramos, 2018).

Restorative self-healing: Fault may exist within internal switch breakers of a power system, which can be restored with restorative self-healing mechanism such as an artificial immune system as an optimization tool. For a complicated smart grid system, algorithms can be modified to achieve the restorative task within the stipulated time (Oliveira, Souza, Almeida, & Lima, 2015).

Restoration of service: Restoration of service can deal with restoring the maximum number of out-of-service loads. Various factors such as bus voltage violations, total operation cost, power flow violations, outage customer, power losses, the number of switching operation, customer minutes interruption, momentary average interruption frequency index, system average interruption frequency index, protection validation, and system average interruption duration needs to be considered for the restoration of service. To obtain high power quality and reliability in a smart grid, service restoration is required for users (Le, Bui, Ngo, & Le, 2018).

- Fault detection, location, isolation, and service restoration (FLISR) technology operates with line monitors, feeder switch and reclosers, outage management system, distribution management system, communication network and grid analytics. During the service restoration stage, FLISR can restore a maximum number of out-of-service loads and limit the number of switching operations for the smart grid. FLISR reduces the fault processing time and improves the power supply reliability (Le et al., 2018).
- Service restoration in distribution network: For resupplying in out-of-service areas, service restoration strategy to be considered as a feasible technology to avoid failure of any

component in the network, which will ultimately enhance the resilience of distribution network. Techniques such as heuristic algorithm, graph theory, mathematical programming can be implemented as a service restoration strategy in the distribution network (Shen et al., 2018).

5. Quantifying of Resilience Contributors

Developing a BN model is a complicated task. It can be split into two separate phases: modeling the underlying framework by showing the interdependencies among different variables, followed by the quantification of those corresponding variables. *AgenaRisk* software is used to quantify the variables and simulate the model. Quantification is conducted based on expert knowledge, statistical learning, historical data, and probabilistic estimations. Various kinds of statistical nodes, such as discrete, continuous, and label node, are generated based on statistical distribution. The base model of the BN network for assessing cyber resilience of the SG system of systems is illustrated in Fig. 3.

"Boolean node" is defined as a node that has exactly two states, "true" and "false" (Fenton & Neil, 2012). The true state is the counterpart of the false state, but it can be customized based on circumstance. However, any node that has exactly two states can be reported as a Boolean node. For instance, in Fig. 3, the node for SCADA shows True = 90% and False = 10%, which means that the SCADA is successful 90% of the time and fails 10% of the time. In other words, there is a 90% chance that the SCADA system may keep the network safe from the cyber incident based on the expert opinion, while there is a 10% chance that it may fail to perform. Along the same line, the node for weak user authentication shows the likelihood of 90% and 10% for the true and false state, respectively, which entails that there is a 90% chance that weak user authentication will lead to access domain failure. The same Boolean logic is applied to determine the posterior probability value for other Boolean variables under the "cyber vulnerability" and "restoration" node in Fig. 3.

Continuous variable (CV): Infinite number of possible values can be indexed by "continuous variables." In our study, the truncated normal distribution is used to model different continuous variables such as WAMS, WADC, massive battery packs, delay-adaptive control, FLISR, and service restoration. The normal distribution can be modified to obtain truncated normal distribution that confines the mean values between lower and upper bounds. For instance, the mean value of system outage for FLISR is found as 76.8 min with lower and upper bound 70 and 80 min, respectively. Hence, truncated normal distribution is found to be appropriate for the distribution of stated continuous variables in the proposed model. The Truncated normal distribution is defined in terms of four parameters: μ, mean (i.e. central tendency); σ^2, variance (i.e. confidence in the results); lower bound and upper bound (Perkusich, Soares, Almeida, & Perkusich, 2015).

When we compute the posterior probability of any child node in the BN structure, there might be some circumstance where we do not have the exact distribution of all parents nodes; other hidden factors may influence the child nodes. In these cases, the "Noisy-OR" assumption eases the situation. The noisy-OR functions describe the interdependencies between the parent and the child node in a simple way. It assumes that all parents' nodes are independent in terms of their influence on their child nodes (Mirarab, Hassouna, & Tahvildari, 2007) [28]. In the Noisy-OR function, hidden or missing parameters known as "leak parameters" can be estimated as in equation (3) below (Fenton & Neil, 2019).

$$N = NoisyOR\left(M_1, S_1, M_2, S_2, \ldots, M_n, S_n, l\right), \tag{3}$$

where $M_{i=1\ to\ n}$ are the causal factors and $S_{i=1\ to\ n}$ are the weights associated with corresponding causal factors, which ranges from 0 to 1. l is the leak parameter defined as nonzero probability for the effect to be triggered even if all the causes are false.

The conditional probability of N obtained with Noisy-OR function can be represented with equation (4) as follows (Fenton & Neil, 2019):

$$P\left(N = True|M_1, M_2, \ldots, M_n\right) = 1 - \prod_{i=1}^{n}\left[\left(1 - P\left(N = True|M_i = True\right)\left(1 - P\left(l\right)\right)\right)\right]. \tag{4}$$

The noisy-OR function has been used in modeling the parent nodes related to absorptive capacity, as shown in equation (5).

$$Absorptive\ Capacity \sim NoisyOR\left(AMI, 0.50, Visual.tech, 0.50, CMS, 0.50, 0.20\right). \tag{5}$$

The posterior probability of all vulnerabilities is also computed employing the Noisy-OR function.

In the proposed model, *resilience* is computed as the ratio of restoration (recoverability) to vulnerability (Henry & Ramirez-Marquez, 2012). Based on the calculation, expected resilience is 75% depicted in Fig. 3.

5.1. Modeling of absorptive capacity

As shown in Fig. 3, absorptive capacity mainly depends upon three variables, where its subfactor CMS reliant on four variables. To model the contributors of absorptive capacity, Boolean variables, continuous variable with truncated normal distribution, and discrete variables are used. In Table 3, it can be observed that AMI, visualization technology, SCADA are designed with Boolean logic, where WAMS and WADC are modeled as continuous variables described with TNORM distribution, and PMU is discrete variable with a constant value. Table 3 also provides a detailed description of the absorptive capacity and its contributors.

5.2. Modeling of adaptive capacity

It is apparent in Fig. 3 that adaptive capacity mainly conditioned upon four variables, where node AI in cyber defense is provisioned on three variables. Different Boolean and continuous variable with truncated normal distribution is used to design the adaptive capacity of SG. The detailed modeling procedure of adaptive capacity and its contributors are presented in the following Table 4.

5.3. Restorative capacity

From Fig. 3, it can be observed that there are mainly three contributors to restorative capacity, where restoration of service depends upon two variables, namely FLISR and service restoration in distributed networks. Different Boolean and truncated normal distributions that are used for contributors are presented in Table 5.

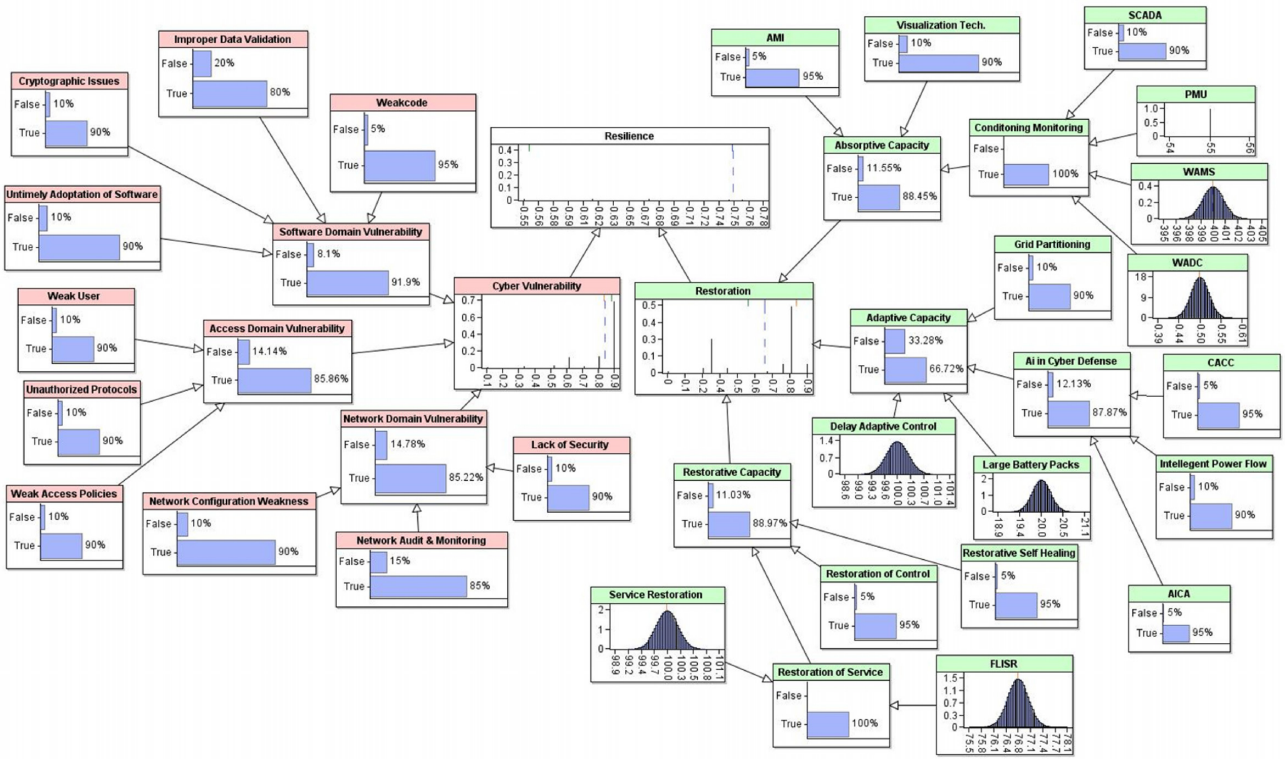

Figure 3: Base model of the BN for measuring cyber resilience of SG.

Table 3: Modeling of variables related to absorptive capacity.

Variable name	Modeling technique	Modeling description
AMI	*Boolean*	We assume that AMI is successful in preventing possible cyber-attack 95% of the time.
Visualization technology	*Boolean*	Visualization technology can be used as a tool to prevent possible failure of a smart grid system, which has a success rate of 90%, while there is a 10% chance that it may fail to perform.
SCADA	*Boolean*	There is a 90% chance that the SCADA system contributes to a secure SG system and a 10% chance that it may fail to provide appropriate prevention.
PMU	*Constant*	PMU can measure current, phasor, or voltage at rate of 60 samples/s (Morris et al., 2012).
WAMS	*TNORM*	For WAMS, communication delay ranges from 100 to 700 ms with an average of 400 ms (Naduvathuparambil, Valenti, & Feliachi, 2002).
WADC	*TNORM*	WADC can provide robustness to the system from possible permanent power failure when the damping ratio is more than 0.05 (Bento et al., 2018).
CMS	*Comparative expression*	The comparative expression is used for modeling and "conditioning monitoring" node. If the values of SCADA and PMU or WADC are greater than or equal to 90% and 55 or 0.05, respectively AND WAMS is lower than 400 ms, then the satisfactory level of CMS is achieved (true state), otherwise not (false state).
Absorptive capacity	*Noisy-OR*	A noisy-OR logic is used for modeling the "absorptive capacity" node. AMI, visualization technology, and conditioning monitoring are equally responsible, and other hidden factors are contributing remaining towards the absorptive capacity of SG.

6. Predictive Inference Reasoning

Based on the belief of the causal nodes in the BN, predictive inference reasoning, also known as forwarding belief propagation, updates the information about effect through the network (Ding, 2010). Predictive inference reasoning is conducted based on the message-passing algorithm to draw a probabilistic inference in a BN. In predictive inference reasoning, the probability distribution of any event N, which is resilience, in this case, can be predicted based on the evidence of its contributing factors $M_{i\ =\ 1\ to\ n}$. Considering the state of each factor as an input to the BN model, the probability distribution of N can be reported as follows (Zhou, Li, Zhou, & Luo, 2018).

$$P(N = S_k) = \sum_{1}^{m^n} P(N = S_k |\ M_1 = m_j, M_2 = m_j, \ldots, M_n = m_j) \times P\ (M_1 = m_j, M_2 = m_j, \ldots, M_n = m_j)\,, \quad (6)$$

where n is the numbers of root nodes, m_j is the jth state of a root node and $j = 1$ to m. S_k is the kth state of the leaf node when $k = 1$ to r. $P(N\ = S_k|M_1 = m_j,\ M_2 = m_j,\ \ldots,\ M_n = m_j)$ is the

Table 4: Modeling of adaptive capacity variable and its contributors.

Variable name	Modeling technique	Modeling description
Grid partitioning	*Boolean*	Grid partitioning can be successful 90% of the time such that it can prevent the system from the failure, and 10% is the chance it can fail.
Large capacity battery packs	*TNORM*	Truncated normal distribution with an average of 20 v is approximated for the large capacity battery packs (He et al., 2019).
Delay-adaptive control strategy	*TNORM*	Delay-adaptive control strategy is designed by a truncated normal distribution. It can be varied between 80 and 120 ms with a mean delay of 100 ms (Wang & Wang, 2019).
Intelligent power flow system	*Boolean*	There is a 90% probability that an intelligent power flow system contributes to adaptive measures of the SG system, whereas it may fail 10% of the time based on expert opinion.
CACC	*Boolean*	We assume that there is a 95% chance that CACC would devote to defend against cyber-attack in the SG system as an adaptive measure, while 5% of the time, it can be unsuccessful.
AICA	*Boolean*	Practitioners predict that 95% of the time, AICA is successful in defending against cyber-attack, and 5% of the time, it fails to contribute.
AI in comparative cyber defense	*Noisy-OR*	A noisy-OR logic is used for modeling the "AI in cyber defense" variable. For the successful implementation of AI in cyber defense, all the contributing factors including intelligent power flow system, CACC, and AICA are equally creditworthy.
Adaptive capacity	*Comparative expression*	An "IF" logic is used for modeling and "conditioning monitoring" node. If the values of grid partitioning and AI in cyber defense are greater than or equal to 90% and 95%, respectively, AND large battery packs or delay-adaptive control are less than 20 v or 100 ms, respectively, then the satisfactory level is achieved (true state), otherwise not (false state).

Table 5: Modeling of restorative capacity variable and its contributors.

Variable name	Modeling technique	Modeling description
Restoration of control	*Boolean*	After a malicious cyber-attack, 95% of the time, the SG system can retrieve its operational control within a stipulated period through its countermeasures and specialized cyber team.
Restorative self-healing	*Boolean*	By implementing advanced technologies, 95% of the time, restorative self-healing is achieved in a timely fashion.
FLISR	*TNORM*	Truncated normal distribution with mean SAIDI index of 76.8 min is applied to model FLISR (Creery & Byres, 2005; Terwilliger, Rosier, & DeBleeckere, 2017).
Service restoration in the distribution network	*TNORM*	Service restoration in the distribution network can be approximated using a truncated normal distribution with an average of 110 ms.
Restoration of comparative service	*Comparative expression*	Conceding that if the values of FLISR and service restoration distribution network are less than or equal to 78 min and 110 ms, respectively, then a satisfactory level of service restoration is achieved.
Restorative capacity	*Noisy-OR*	A noisy-OR logic is used for modeling the "restorative capacity" node. To meet the restorative capacity, all factors restorative self-healing, restoration of control, and restoration of service are equally responsible.

conditional probability distribution when $N = S_k$; In Fig. 3, network domain vulnerability → cyber vulnerability → resilience is an example of the predictive inference reasoning where marginal distributions of an ancestor node measure its influence on the connected descendant nodes.

$$P(M_i|e) \quad \forall \quad M_i \in M_l. \tag{7}$$

To conduct predictive inference analysis, we have generated and simulated a new scenario by setting the false state of three different variables, namely – "visualization technology, AI in cyber defense, restorative healing" for three capacities and true state for two variables: "cryptographic issues and access domain vulnerabilities" (see Fig. 4). This means that visualization technology, AI in cyber defense, restorative healing will entirely (100%) fail to perform to make the SG system cyber safe, and at the same time, cryptographic issues and access domain vulnerabilities will be 100% successful in impacting adversely on the overall cyber resilience of SG. These five decision variables were selected such that influences were believed to be significant to the overall cyber resilience of the SG system of systems. It is apparent from Fig. 4 that these observations together disseminate an adverse impact on the overall cyber resilience and subsequently reduces the cyber resilience of the SG system of systems from 75% to 55%. The comparative analysis between the new scenario and base case is summarized in Table 6.

7. Sensitivity Analysis

Sensitivity analysis (SA) is used for validating the structure of the BN model, which is a popular approach for examining the impact of the contributors on the target node within the same BN model and tells that which node has more influence on the target node. The outcome of the targeted node can be recalculated based on the different possible assumptions. For sensitivity analysis, the output can be represented based on input

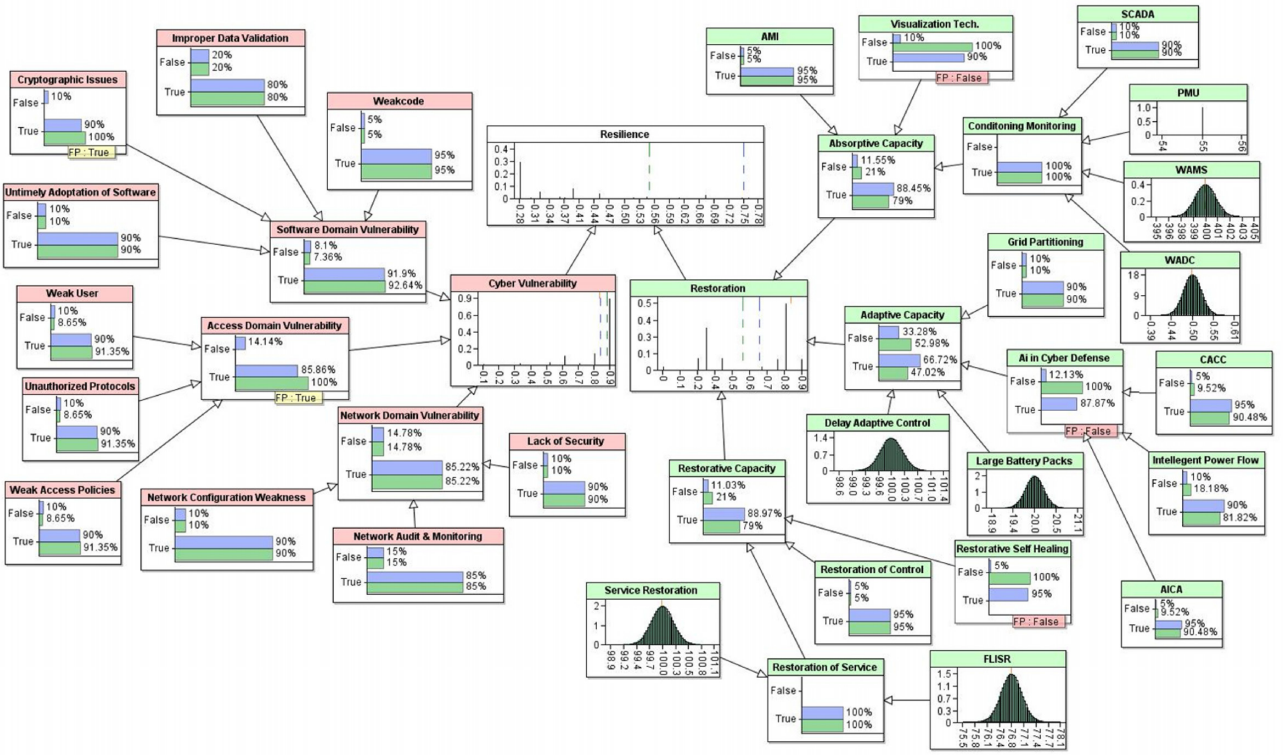

Figure 4: Predictive inference model of the BN for measuring the cyber resilience of SG.

Table 6: Comparative illustration of predictive inference reasoning.

Scenario	Cryptographic issue	Access domain vulnerability	Visualization tech	AI in cyber defense	Restorative self-healing	SG resilience
Base case	–	–	–	–	–	75%
Scenario 1 (FP)	True	True	False	False	False	55%

by equation (8) (Wang et al., 2013).

$$N(m) = N_0 + \sum_{i=1}^{n} N_i(m_i) + \sum_{1\le i<j\le n} N_{ij}(m_i, m_j) + \ldots + N_{1,2,\ldots,n}(m_1, m_2, \ldots, m_n), \quad (8)$$

where $N_0 = E(P_f)$

$$N_i = E(P_f|m_i) - E(P_f) \quad (9)$$

$$N_{ij} = E(P_f|m_i, m_j) - N_i - N_j - N_0, \quad (10)$$

$E(P_f)$ and $E(P_f|\bullet)$ are the expectation and conditional probability of failure probability, and $P_f = N(m)$ such that m is the input distribution for input M and P_f is the output failure probability.

Sensitivity measure can be defined as follows, where V is variance for the failure of output probability.

$$S_{m_i} = \frac{V(E(P_f|m_i))}{V(P_f)}. \quad (11)$$

To demonstrate the relative influence of the causal factors (i.e. access, software, and network domain vulnerability) of the "vulnerability," "cyber vulnerability" is set as a target node, and the impact of its causal factors are computed through conditional probability as stated in equations above. The sensitivity analysis of the "cyber vulnerability" of SG is shown in Fig. 5, in the form of a graphical bar, named as "tornado graph." Tornado graph entails the idea of the relative importance of each factor on its target node, respectively (Hossain, Jaradat, Hosseini et al., 2019, Hossain, Nur, Hosseini et al., 2019). The width of the bars corresponding to each sensitive node in the tornado graph represents a measurement of the impact from that corresponding node on the "overall cyber vulnerability of SG." The width of the bars is ranked based on the descending order so that it allows us to understand the relative importance of each factor (Hossain, Jaradat, Hosseini et al., 2019; Hossain, Nur, Hosseini et al., 2019). Figure 5 demonstrates the influence of a set of contributing factors (i.e. access, software, and network domain vulnerability) on the overall cyber vulnerability when it is "True." Figure 5 shows that the probability of access domain vulnerability changes from 0.559 (when a vulnerability is false) to 0.884 (when a vulnerability is true), whereas, the impact of software domain vulnerability is limited to a narrow range, which varies from 0.785 to 0.843. The formal representation of this figure shows that access domain vulnerability has the highest impact, and software domain vulnerability has the lowest influence on the cyber-attack of the SG system of systems. When compared to a real-world scenario, the results seem logical, as weak user policy, unauthorized protocols, access policy, and procedural issues are the prime reasons that lead to severe cyber vulnerability of the smart grid. In other words, the SG management authority should emphasize more

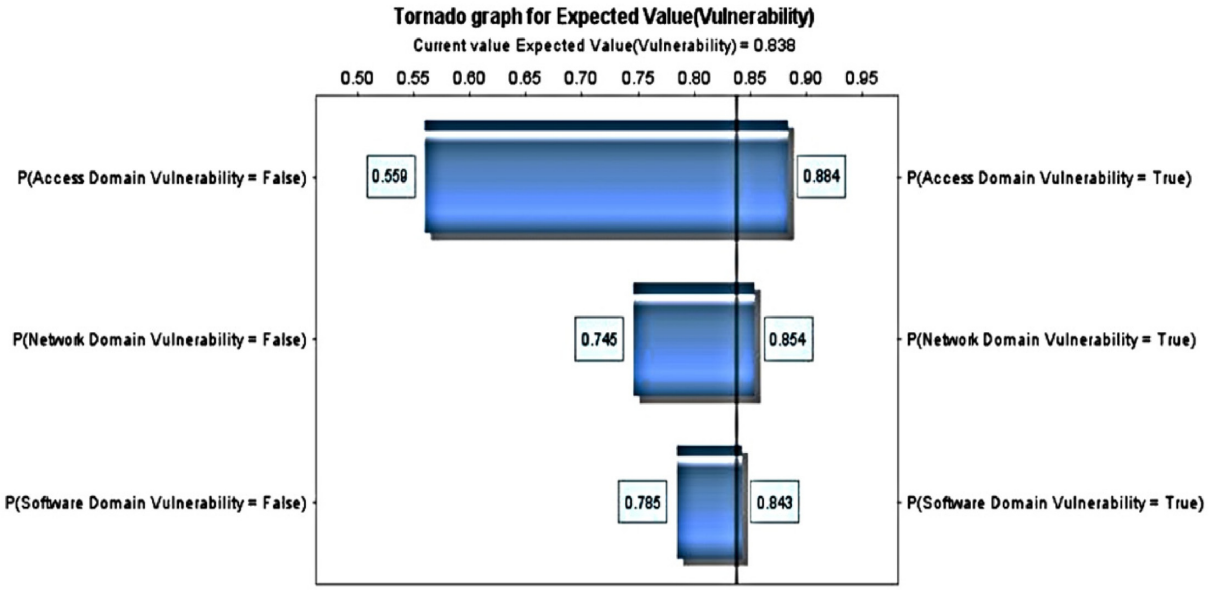

Figure 5: Sensitivity analysis of different vulnerabilities on SG.

on developing countermeasures against access domain vulnerabilities to improve the overall resilience of SG.

8. Conclusion

In this research, we presented a novel static Bayesian model to assess the resilience of SG. First, the principal causes of cyber-attack for SG are identified, and the related countermeasures are discussed subsequently. Then, the information extracted from the historical data and expert's opinion is fed into BN to measure the overall resilience of the SG system. The contribution of this research to the body of knowledge in a smart grid can be summarized as follows:

- The potential causes of cyber-attack for SG are recognized, and the underlying countermeasures are proposed concerning different resilience capacities such as absorptive, adaptive, and restorative capacities.
- Advanced analysis is performed to validate the effectiveness of the proposed model and generate new insights on how to improve the overall resilience of the SoS smart grid network.
- The use of BN as an effective tool in solving system of systems problems such as the grid system.

Although this framework is specifically developed for the smart grid, it can be tailored based on the structure and nature of any electrical network system to measure and enhance resilience. In future work, an extended dynamic Bayesian model can be developed, and advanced analysis such as information theory can be performed to provide more insights for the enhancement of the overall smart grid resilience system. The time-dependent dynamic Bayesian model will monitor the system performance and consistency of the model over time. Also, information theory will provide information about the state of uncertainty of the cyber vulnerability of the smart grid system of systems.

Another way of strengthening the actual model is by updating data/ prior belief through the Delphi technique. Delphi technique is based on the experts' judgment, and it can be used to prescribe the node probability table of BN variables. In determining the probabilities of the various node states, Sharma and Sharma (2015) recommended that if there are more than a few node states, expert judgment would be better replaced by using the Pairwise Comparison method developed by Wind and Saaty (1980) to determine weights that can be used as probabilities based on which state is more likely to happen. During the development of the model, less important factors were removed, and therefore, detailed attention could be directed towards what other factors can be included in the model.

Conflict of interest statement

Declarations of interest: none.

References

Alfaqiri, A., Hossain, N. U., Jaradat, R., Abutabenjeh, S., Keating, C., Khasawneh, M., & Pinto, A. (2019). A systemic approach for disruption risk assessment in oil and gas supply chains. *International Journal of Critical Infrastructures*, *15*(3), 230–259.

Aloul, F., Al-Ali, A. R., Al-Dalky, R., Al-Mardini, M., & El-Hajj, W. (2012). Smart grid security: Threats, vulnerabilities and solutions. *International Journal of Smart Grid and Clean Energy*, *1*(1), 1–6.

Amundson, J., Faulkner, W., Sukumara, S., Seay, J., & Badurdeen, F. (2012). A Bayesian network-based approach for risk modeling to aid in the development of sustainable biomass supply chains. In *Computer aided chemical engineering*(Vol. 30, pp. 152–156). Elsevier.

Antsaklis, P. J., Passino, K. M., & Wang, S. J. (1991). An introduction to autonomous control systems. *IEEE Control Systems Magazine*, *11*(4), 5–13.

Arghandeh, R., Von Meier, A., Mehrmanesh, L., & Mili, L. (2016). On the definition of cyber-physical resilience in power systems. *Renewable and Sustainable Energy Reviews*, *58*, 1060–1069.

Arizmendi, C., Sierra, D. A., Vellido, A., & Romero, E. (2014). Automated classification of brain tumors from short echo time in vivo MRS data using Gaussian decomposition and Bayesian neural networks. *Expert Systems With Applications*, *41*(11), 5296–5307.

Bearingpoint. (2019). Risk of cybersecurity attacks on the smart grid. Retrieved from: https://www.bearingpoint.com/fr-fr/blogs/blog-energie/risk-of-cyber-security-attacks-on-smart-grid/.

Bento, M. E., Kuiava, R., & Ramos, R. A. (2018). Design of wide-area damping controllers incorporating resiliency to permanent failure of remote communication links. *Journal of Control, Automation and Electrical Systems*, *29*(5), 541–550. https://doi.org/10.1007/s40313-018-0398-3.

Biringer, B., Vugrin, E., & Warren, D. (2016). *Critical infrastructure system security and resiliency*. Boca Raton: CRC Press.

Biron, Z. A., Dey, S., & Pisu, P. (2017). Resilient control strategy under Denial of Service in connected vehicles. In *2017 American Control Conference (ACC)*(pp. 4971–4976).

Bojkovic, Z., & Bakmaz, B. (2012). Smart grid communications architecture: A survey and challenges. In *Proceedings of the 11th international conference on applied computer and applied computational science (ACACOS)*(pp. 83–89).

Bryan, W. (2014). *Impact of cyber attacks on the private sector*. MidPoint Group.

Cai, B., Xie, M., Liu, Y., Liu, Y., & Feng, Q. (2018). Availability-based engineering resilience metric and its corresponding evaluation methodology. *Reliability Engineering & System Safety*, *172*, 216–224.

Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The economic impact of cyber-attacks. *Congressional research service documents, CRS RL32331 (Washington DC)*.

Creery, A., & Byres, E. J. (2005). Industrial cybersecurity for power system and SCADA networks. In *Record of Conference Papers Industry Applications Society 52nd annual petroleum and chemical industry conference*(pp. 303–309). IEEE.

Deng, Y., & Shukla, S. (2012). Vulnerabilities and countermeasures—A survey on the cyber security issues in the transmission subsystem of a smart grid, *Journal of Cyber Security and Mobility*, *1*, 251–276.

Ding, J. (2010). Probabilistic inferences in Bayesian networks. InA.Rebai (ed.), Bayesian Network, 39–53.

El Mrabet, Z., Kaabouch, N., El Ghazi, H., & El Ghazi, H. (2018). Cyber-security in smart grid: Survey and challenges. *Computers & Electrical Engineering*, *67*, 469–482.

Feng, Q., Fan, D., Cai, B., Liu, Y., & Ren, Y. (2019). Resilience design method based on meta-structure: A case study of an offshore wind farm. *Reliability Engineering & System Safety*, *186*, 232–244.

Fenton, N., & Neil, M. (2012). *Risk assessment and decision analysis with Bayesian networks*. Boca Raton: CRC Press.

Fenton, N., & Neil, M. (2019). *Risk assessment and decision analysis with bayesian networks*. Boca Raton: Chapman & Hall/CRC.

Han, S. Y., Marais, K., & DeLaurentis, D. (2012). Evaluating system of systems resilience using interdependency analysis. In *2012 IEEE international conference on systems, man, and cybernetics (SMC)*(pp. 1251–1256). IEEE.

Han, Y., & Song, Y. (2002). Condition monitoring techniques for electrical equipment: A literature survey. *IEEE Power Engineering Review*, *22*, 59–59.

He, L., Kong, L., Gu, Y., Liu, C., He, T., & Shin, K. G. (2019). Extending battery system operation via adaptive reconfiguration. *ACM Transactions on Sensor Networks*, *15*(1), 1–21.

Henry, D., & Ramirez-Marquez, J. E. (2012). Generic metrics and quantitative approaches for system resilience as a function of time. *Reliability Engineering & System Safety*, *99*, 114–122.

Hossain, N. U. I., El Amrani, S., Jaradat, R., Marufuzzaman, M., Buchanan, R., Rinaudo, C., & Hamilton, M. (2020). Modelling and Assessing Interdependencies between Critical Infrastructures using Bayesian Network: A Case Study of Inland Waterway Port and Surrounding Supply Chain Network, *Reliability Engineering & System Safety, 106898*.

Hossain, N. U. I., & Jaradat, R. (2018). A Synthesis of definitions for systems engineering. In *Proceedings of the international annual conference of the American Society for Engineering Management*. (pp. 1–10).American Society for Engineering Management (ASEM).

Hossain, N. U. I., Jaradat, R., Hosseini, S., Marufuzzaman, M., & Buchanan, R. K. (2019). A framework for modeling and assessing system resilience using a Bayesian network: A case study of an interdependent electrical infrastructure system. *International Journal of Critical Infrastructure Protection*, *25*, 62–83.

Hossain, N. U. I., Jaradat, R., Marufuzzaman, M., Buchanan, R. K., & Rinaudo, C. (2019). Assessing and enhancing oil and gas supply chain resilience: A Bayesian network-based approach. In *Proceedings of IISE annual conference and EXPO 2019, Orlando, FL*.

Hossain, N. U. I., Nagahi, M., Jaradat, R., & Keating, C. (2019) Development of an instrument to assess the performance of systems engineers. In *Proceedings of the international conference on industrial engineering and operations management, Toronto, Canada*, October 23–25, 2019.

Hossain, N. U. I., Nur, F., Hosseini, S., Jaradat, R., Marufuzzaman, M., & Puryear, S. M. (2019). A Bayesian network-based approach for modeling and assessing resilience: A case study of a full-service deepwater port. *Reliability Engineering & System Safety*, *189*, 378–396.

Hossain, N. U. I., Nur, F., Jaradat, R., Hosseini, S., Marufuzzaman, M., Puryear, S. M., & Buchanan, R. K. (2019). Metrics for assessing the overall performance of inland waterway ports: A Bayesian network-based approach. *Complexity*, Volume 2019, Article ID 3518705, Avaiable at https://doi.org/10.1155/2019/3518705.

Hossain, N. U. I., Nur, F., & Jaradat, R. M. (2016). An analytical study of hazards and risks in the shipbuilding industry. In *Proceedings of American Society for engineering management annual conference*(pp. 18–21).

Hosseini, S., Al Khaled, A., & Sarder, M. D. (2016). A general framework for assessing system resilience using Bayesian networks: A case study of the sulfuric acid manufacturer. *Journal of Manufacturing Systems*, *41*, 211–227.

Hosseini, S., & Sarder, M. D. (2019). Development of a Bayesian network model for optimal site selection of electric vehicle charging station. *International Journal of Electrical Power & Energy Systems*, *105*, 110–122.

Hänninen, M., Banda, O. A. V., & Kujala, P. (2014). Bayesian network model of maritime safety management. *Expert Systems with Applications*, *41*(17), 7837–7846.

Jaradat, R. M., & Keating, C. B. (2014). Fragility of oil as a critical infrastructure problem. *International Journal of Critical Infrastructure Protection*, *7*(2), 86–99.

Jaradat, R. M., Keating, C. B., & Bradley, J. M. (2014). A histogram analysis for system of systems. *International Journal of System of Systems Engineering*, *5*(3), 193–227.

Kamal, M. B., & Wei, J. (2017). Attack-resilient energy management architecture of hybrid emergency power system for more-electric aircrafts. In *2017 IEEE power & energy society innovative smart grid technologies conference (ISGT)*(pp. 1–5).

Kundur, D., Feng, X., Liu, S., Zourntos, T., & Butler-Purry, K. L. (2010). Towards a framework for cyber attack impact analysis of the electric smart grid. In *2010 First IEEE international conference on smart grid communications*(pp. 244–249). IEEE.

Laitila, P. (2013). *Improving the use of ranked nodes in the elicitation of conditional probabilities for Bayesian networks (Unpublished MSc Thesis)*. (Unpublished MSc Thesis). Aalto University, School of Science.

Lawrence, J. M., Hossain, N.U.I, Rinaudo, C., Buchanan, R., & Jaradat, R.M. (2020). An Approach to Improve Hurricane Disaster Logistics Using System Dynamics and Information Systems, *18th Annual Conference on Systems Engineering Research (CSER), CA, March 19-21*.

Lawrence, J. M., Hossain, N. U. I., Nagahi, M., & Jaradat, R. (2019). Impact of a cloud-based applied supply chain network simulation tool on developing systems thinking skills of undergraduate students. In *Proceedings of the international conference on industrial engineering and operations management, Toronto, Canada*.

Le, D., Bui, D., Ngo, C., & Le, A. (2018). FLISR approach for smart distribution networks using E-Terra Software—A case study. *Energies*, *11*(12), 3333. https://doi.org/10.3390/en11123333.

Liang, X., Gao, K., Zheng, X., & Zhao, T. (2013). A study on cyber security of smart grid on public networks. In *2013 IEEE green technologies conference (GreenTech)*(pp. 301–308). IEEE.

Li, F., Qiao, W., Sun, H., Wan, H., Wang, J., Xia, Y., Xu, Z., & Zhang, P. (2010). Smart transmission grid: Vision and framework. *IEEE Transactions on Smart Grid*, *1*, 168–177.

Line, M. B., Tøndel, I. A., & Jaatun, M. G. (2011). Cybersecurity challenges in smart grids. In *2011 2nd IEEE PES international conference and exhibition on innovative smart grid technologies*(pp. 1–8). IEEE.

Liu, Y., Fan, R., & Terzija, V. (2016). Power system restoration: A literature review from 2006 to 2016. *Journal of Modern Power Systems and Clean Energy*, *4*(3), 332–341.

Lu, Z., Wang, W., & Wang, C. (2015). Camouflage traffic: Minimizing message delay for smart grid applications under jamming. *IEEE Transactions on Dependable and Secure Computing*, *12*(1), 31–44. https://doi.org/10.1109/tdsc.2014.2316795.

McDaniel, P., & McLaughlin, S. (2009). Security and privacy challenges in the smart grid. *IEEE Security & Privacy*, *7*(3), 75–77.

Mirarab, S., Hassouna, A., & Tahvildari, L. (2007). Using Bayesian belief networks to predict change propagation in software systems. In *15th IEEE international conference on program comprehension (ICPC'07)*(pp. 177–188). IEEE.

Mohammadali, A., Haghighi, M. S., Tadayon, M. H., & Mohammadi-Nodooshan, A. (2016). A novel identity-based key establishment method for advanced metering infrastructure in smart grid. *IEEE Transactions on Smart Grid*, *9*(4), 2834–2842.

Morris, T. H., Pan, S., & Adhikari, U. (2012). Cybersecurity recommendations for wide-area monitoring, protection, and control systems. In *2012 IEEE power and energy society general meeting*(pp. 1–6).

Naduvathuparambil, B., Valenti, M., & Feliachi, A. (2002). Communication delays in wide-area measurement systems. In *Proceedings of the thirty-fourth southeastern symposium on system theory (Cat. No.02EX540)*. https://doi.org/10.1109/ssst.2002.1027017.

Nagahi, M., Nagahisarchoghaei, M., Soleimani, N., & Jaradat, R. M., (2018). Hedge strategies of corporate houses. *Journal of Business Administration Research*, *7*(1), 6–21.

Nazir, S., Hamdoun, H., & Alzubi, J. (2015). Cyber attack challenges and resilience for smart grids. *European Journal of Scientific Research*, *134*(1).

Nelso, T., & Chaffin, M. (2011). Common cybersecurity vulnerabilities in industrial control systems. In *Control systems security program*. Washington DC: Department of Homeland Security (DHS), National Cyber Security Division.

NISTIR. (2010). *Guidelines for smart grid cybersecurity*, v1.0.

Oliveira, D. Q., Souza, A. C., Almeida, A. B., & Lima, I. (2015). An artificial immune approach for service restoration in smart distribution systems. In *2015 IEEE PES innovative smart grid technologies Latin America (ISGT LATAM)*. https://doi.org/10.1109/isgt-la.2015.7381120.

Pallotti, E., & Mangiatordi, F. (2011). Smart grid cybersecurity requirements. In *2011 10th International conference on environment and electrical engineering* (pp. 1–4) IEEE.

Parra, G. D., Rad, P., & Choo, K. R. (2019). Implementation of deep packet inspection in smart grids and industrial Internet of things: Challenges and opportunities. *Journal of Network and Computer Applications*, *135*, 32–46. https://doi.org/10.1016/j.jnca.2019.02.022.

Pascual, M., Miñana, E. P., & Giacomello, E. (2016). Integrating knowledge on biodiversity and ecosystem services: Mind-mapping and Bayesian network modeling. *Ecosystem Services*, *17*, 112–122.

Perkusich, M., Soares, G., Almeida, H., & Perkusich, A. (2015). A procedure to detect problems of processes in software development projects using Bayesian networks. *Expert Systems with Applications*, *42*(1), 437–450.

Polonetsky, J. (2009). Privacy and the smart grid: New frontiers, new challenges. In *31st International conference of data protection and privacy commissioners*.

Pérez-Miñana, E. (2016). Improving ecosystem services modeling: Insights from a Bayesian network tools review. *Environmental Modeling & Software*, *85*, 184–201.

Radoglou-Grammatikis, P., Sarigiannidis, P., Liatifis, T., Apostolakos, T., & Oikonomou, S. (2018). An overview of the firewall systems in the smart grid paradigm. In *2018 Global information infrastructure and networking symposium (GIIS)*. https://doi.org/10.1109/giis.2018.8635747.

Rana, M. M. (2017). Attack resilient wireless sensor networks for smart electric vehicles. *IEEE Sensors Letters*, *1*(2), 1–4.

Rana, M. M., Li, L., & Su, S. W. (2016). Cyber-attack protection and control in microgrids using channel code and semidefinite programming. In *2016 IEEE power and energy society general meeting (PESGM)*(pp. 1–5). IEEE.

Rana, M. M., Li, L., & Su, S. W. (2018). Cyber-attack protection and control of microgrids. *IEEE/CAA Journal of Automatica Sinica*, *5*(2), 602–609.

Rana, M. M., Xiang, W., & Choi, B. J. (2018). Grid state estimation over unreliable channel using IoT networks. In *The 2018 15th international conference on control, automation, robotics, and vision (ICARCV)*(pp. 945–948). IEEE.

Rana, M. M., Xiang, W., & Wang, E. (2018). Smart grid state estimation and stabilization. *International Journal of Electrical Power & Energy Systems*, *102*, 152–159.

Saad, A. A., Faddel, S., & Mohammed, O. (2019). A secured distributed control system for future interconnected smart grids. *Applied Energy*, *243*, 57–70. https://doi.org/10.1016/j.apenergy.2019.03.185.

Sadiku, M. N. O., Musa, S. M., & Nelatury, S. R. (2016). Smart grid—An introduction. *International Journal of Electrical Engineering & Technology (IJEET)*, *7*(1), 45–49.

Saini, L. M. (2008). Peak load forecasting using Bayesian regularization, resilient, and adaptive back learning-based artificial neural networks. *Electric Power Systems Research*, *78*(7), 1302–1310.

Saleh, M., Khdour, T., Ferrah, A., Qasaymeh, M., & Togher, M. (2019). Analysis of digital utility endpoints in smart grid using modular computing platform. In *2019 Advances in science and engineering technology international conferences (ASET)*. https://doi.org/10.1109/icaset.2019.8714396.

Shah, A., Perrig, A., & Sinopoli, B. (2008). Mechanisms to provide integrity in SCADA and PCS devices. In *Proceedings of the international workshop on cyber-physical systems-challenges and applications (CPS-CA)*(p. 7).

Shahid, M. A., Nawaz, R., Qureshi, I. M., & Mahmood, M. H. (2018). Proposed defense topology against cyber attacks in smart grid. In *2018 International conference on power generation systems and renewable energy technologies (PGSRET)*. https://doi.org/10.1109/pgsret.2018.8685944.

Shapsough, S., Qatan, F., Aburukba, R., Aloul, F., & Al Ali, A. R. (2015). Smart grid cybersecurity: Challenges and solutions. In *2015 International conference on smart grid and clean energy technologies (ICSGCE)*(pp. 170–175). IEEE.

Sharma, S. K., & Sharma, S. (2015). Developing a Bayesian network model for supply chain risk assessment. *Supply Chain Forum: An International Journal*, *16*(4), 50–72.

Shen, F., Wu, Q., Huang, S., Lopez, J. C., Li, C., & Zhou, B. (2018). Review of service restoration methods in distribution networks. In *2018 IEEE PES innovative smart grid technologies conference Europe (ISGT-Europe)*. https://doi.org/10.1109/isgteurope.2018.8571821.

Terwilliger, H., Rosier, M., & DeBleeckere, T. (2017). Estimated SAIDI improvement—State of Minnesota. Available at: https://www.edockets.state.mn.us/EFiling/edockets/searchDocuments.do?method=showPoup&documentId={10281E61-0000-C21C-B3DE-AB6412DF5C2E}&documentTitle=20181-139141-01.

Théron, P., Kott, A., Drasar, M., Rzadca, K., Leblanc, B., Pihelgas, M., Mancini, L. V., & Panico, A. (2018). Towards an active, autonomous, and intelligent cyber defense of military systems: The NATO AICA reference architecture. In *2018 International conference on military communications and information systems (ICMCIS)*(pp. 1–9).

USDOE. (2009, *Smart grid system report—-Characteristics of the smart grid*.

Venugopalan, S., & Rai, V. (2015). Topic-based classification and pattern identification in patents. *Technological Forecasting and Social Change*, *94*, 236–250.

Wadhawan, Y., AlMajali, A., & Neuman, C. (2018). A comprehensive analysis of smart grid systems against cyber-physical attacks. *Electronics*, *7*(10), 249.

Wan, C., Phoha, V. V., Pei, B., & Chen, C. (2017). Securing dynamic microgrid partition in the smart grid. *International Journal of Distributed Sensor Networks*, *13*(5), 1550147717711136.

Wang, P., Lu, Z., & Tang, Z. (2013). An application of the Kriging method in global sensitivity analysis with parameter uncertainty. *Applied Mathematical Modelling*, *37*(9), 6543–6555. https://doi.org/10.1016/j.apm.2013.01.019.

Wang, W., & Lu, Z. (2013). Cybersecurity in the smart grid: Survey and challenges. *Computer networks*, *57*(5), 1344–1371.

Wang, Z., & Wang, J. (2019). A delay-adaptive control scheme for enhancing smart grid stability and resilience. *International Journal of Electrical Power & Energy Systems*, *110*, 477–486. https://doi.org/10.1016/j.ijepes.2019.03.030.

Wind, Y., & Saaty, T. L. (1980). Marketing applications of the analytic hierarchy process. *Management Science*, *26*(7), 641–658.

Wu, F. F., Varaiya, P. P., & Hui, R. S. (2015). Smart grids with intelligent periphery: An architecture for the energy internet. *Engineering*, *1*(4), 436–446.

Xia, X., Xiao, Y., & Liang, W. (2019). ABSI: An adaptive binary splitting algorithm for malicious meter inspection in smart grid. *IEEE Transactions on Information Forensics and Security*, *14*(2), 445–458. https://doi.org/10.1109/tifs.2018.2854703.

Yang, S., & Zhang, B. (2014). A real-time trajectory prediction scheme based on the WAMS information for a multi-machine system. In *12th IET international conference on developments in power system protection (DPSP 2014)*. https://doi.org/10.1049/cp.2014.0162.

Yet, B., Constantinou, A., Fenton, N., Neil, M., Luedeling, E., & Shepherd, K. (2016). A Bayesian network framework for project cost, benefit, and risk analysis with an agricultural development case study. *Expert Systems with Applications*, *60*, 141–155.

Zhou, Y., Li, C., Zhou, C., & Luo, H. (2018). Using Bayesian network for safety risk analysis of diaphragm wall deflection based on field data. *Reliability Engineering & System Safety*, *180*, 152–167. https://doi.org/10.1016/j.ress.2018.07.014.