IET Generation, Transmission & Distribution

Research Article

Framework for vulnerability assessment of communication systems for electric power grids

ISSN 1751-8687
Received on 13th July 2015
Revised on 15th September 2015
Accepted on 29th September 2015
doi: 10.1049/iet-gtd.2015.0857
www.ietdl.org

Qi Wang[1] ✉, Manisa Pipattanasomporn[2], Murat Kuzlu[2], Yi Tang[1], Yang Li[1], Saifur Rahman[2]

[1]School of Electrical Engineering, Southeast University, Nanjing, People's Republic of China
[2]Advanced Research Institute, Virginia Tech, Arlington, USA
✉ *E-mail: wangqi@seu.edu.cn*

Abstract: Communication systems serve as the key element in the smart grid as it supports observability and controllability of electric power systems. However, communication failures can lead to an electric power grid operating in an abnormal state causing cascading failures. It is therefore crucial to study adverse effects of communication system failures on power system operation. In this study, a vulnerability assessment framework is proposed to evaluate the role of communication networks on wide-area power system operation, in which the reliability is evaluated probabilistically considering both latency and communication interruptions; and impact of communication service interruption is evaluated using a multi-level analytic hierarchy process method. A case study of integrated power and communication systems is used to demonstrate the usefulness of the proposed framework. The proposed method can be used to evaluate the vulnerability of communication systems for electric power grids in both static and dynamic states.

Nomenclature

α	probability of successful auto-switching operation
C	the consequence of service failure
C_i	components in communication network
I_{PN_i}	importance index of node PN_i
I_{S_n}	importance degree of service S_n
k	standby path serial number
K	total number of the standby paths
L_{N_i}	the maximum loading level of the whole system without the power node N_i
P_{2_k}	probability of adopting the kth standby path
P_a	probability of service in state a
$Path_{\mathrm{P}}$	primary paths of service
$Path_{\mathrm{P}\_k-x}$	xth part of primary path which in interruption state
$Path_{\mathrm{S}}$	standby paths of service
$Path_{\mathrm{S}\_k}$	corresponding standby path of $Path_{\mathrm{P}\_k-x}$
P_C_i	unavailability of component C_i
$P_a^{\mathrm{C}_i}$	vulnerability *contribution* of component C_i in state a, where $a = 0$, 1, 2 and 3
$P_{\mathrm{LOL}}^{\mathrm{PN}_i}$	load loss (MW) in power node PN_i
P_{I}	unavailability of service caused by an interruption event
$P_{\mathrm{P}\_S_n^{mn}}$	distribution function of service latency when being transmitted in primary paths
$P_{\mathrm{S}\_k\_S_n^{mn}}$	distribution function of service latency when being transmitted in the kth standby path
P_{T}	unavailability of service caused by latency
P_{Total}	total system load (MW)
S_n	nth kind of communication service
S_n^{mn}	m_nth service of S_n
t	latency of service path
t_{switch}	switch time
$T_{\mathrm{S}_n^{mn}}$	threshold value of service S_n^{mn}
U	unavailability of service
$\mu(C_i)$	average latency of component C_i
μ_{T}	average latency in a given time interval T
V	vulnerability value of service
X	total number of interruption events occurred in *Path_k*

1 Introduction

Smart grid technologies and applications enable traditional electric power systems to operate more stably and economically. As the key component of the smart grid, a high-speed, reliable and secure data communication system provides support for observability and controllability of wide-area power systems [1, 2]. Classified by data rate and coverage range, a communication network can be divided into: premises area network, neighbourhood/field area networks and wide-area network (WAN) [1]. WAN is the focus in this paper.

With real-time protection, control and wide-area monitoring applications supported in WAN, early stage of cascading faults in electric power systems can be effectively detected and prevented [3, 4]. However, communication faults (e.g. interruptions, high latency and data error) may also cause power system to operate in a critical state that may propagate into cascading failures. In recent years, there have been several incidents in electric power systems that were caused or aggravated by communication faults. Examples include the malfunction of transmission system's relay protection devices caused by abnormally high latency and bit errors in communication channels in south China [5]; the blackout in south London in 2003 that was induced by erroneous alarm data [6]; and the propagation of the August 2003 blackout in USA and Canada for unobservable system status as a consequence of communication interruption [7].

Therefore, it is necessary to investigate negative impacts of communication system failures on electric power system operation. Previous work in this area addressed the following aspects:

(i) Focusing on the detailed model of communication infrastructure with simplified power grid model, Wang *et al.* [8] and Dai *et al.* [9] studied the reliability of communication systems based on the network structure and presented quantified reliability evaluation methods for wide-area measurement system and wide-area protection system. Fault tree analysis based on data of hardware failure probability was adopted in both researches. However, besides direct interruption of components in WAN, long latency can also prevent power systems from performing a required function. This has not been considered in the above-mentioned studies.

(ii) Looking at the detailed power system model with a simplified communication network, several studies pointed out negative impacts of communication network failures on power system operation [10–14], including inter-area oscillations, load scheduling and optimisations of power consumption. These researchers analysed the consequence of assumed specified communication failures including interruption and abnormal data transmission latency.
(iii) Considering both power and communication systems, Buldyrev *et al.* [15] treated power and communication systems as a coupled, interdependent system based on the complex network theory. This kind of research method can be used to reveal the cause of cascading failures at the macro level, while cannot be directly adopted to guide operation and control of power systems for excessively ignoring their physical characteristics. Ten *et al.* [16] proposed a vulnerability assessment method to systematically evaluate supervisory control and data acquisition systems in the cyber security layer. Falahati *et al.* [17] proposed an evaluation algorithm to assess the impact of cyber network failures on microgrid operation. However, these studies assumed that faults in communication networks cause a total failure of corresponding power nodes.

The power system is impacted by communication systems through their ability to provide communication services. To the best of authors' knowledge, there is no quantitative evaluation method for power systems with integrated communications that takes into account multiple communication services, for example, wide-area relay protection, load shedding and stability control. In this paper, we propose a vulnerability assessment framework to assess the impact of communication system failures on wide-area electric power system operation. The original research contributions of this paper are that: (i) both latency and interruption faults are considered probabilistically to assess the reliability of communication services; (ii) a multi-level analytic hierarchy process (AHP) structure is adopted to quantify different impacts of communication services; (iii) the communication network failure is quantified as the contribution of components to services failure, which is used to illustrate the weakest section of the whole network. Some other factors such as cyber-attacks, configuration/deployment issues, and user mistakes or sabotages, which can also introduce reliability problems into electric power and communication system, are not of focus in this paper.

2 Structure of wide-area communication system

A section of the real-world electric power and communication networks from an electric utility is shown in Fig. 1. For this system, the communication network has a typical hierarchical characteristic. The backbone is based on synchronous digital hierarchy (SDH) technology [18]. It comprises the control centre (CC), major communications hubs and multiple rings. The backbone supports wide-area monitoring, protection and control applications for the associated power network.

In general, most major physical electric power nodes (e.g. nodes power node (PN_1) and PN_3 in the electric power network level) usually have their corresponding communication facilities, which are shown as communication nodes (CNs) (e.g. nodes CN_1 and CN_3 in the communication network level). However, the connection between two nodes in each level may not be the same. For example, the power nodes PN_1 and PN_3 have a physical connection, whereas the information between their corresponding

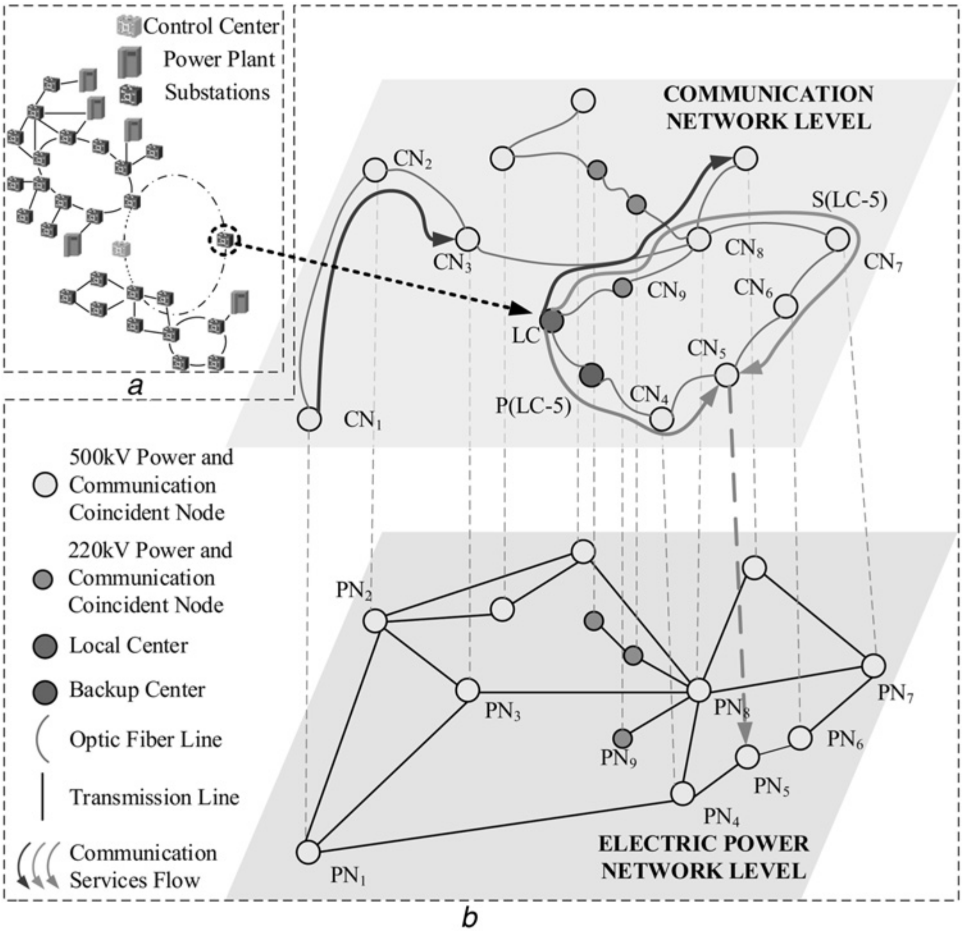
Control Center
Power Plant
Substations
a
COMMUNICATION NETWORK LEVEL
CN2
CN3
S(LC-5)
CN8
CN7
CN9
CN6
LC
CN5
P(LC-5)
CN4
CN1
500kV Power and Communication Coincident Node
220kV Power and Communication Coincident Node
Local Center
Backup Center
Optic Fiber Line
Transmission Line
Communication Services Flow
PN2
PN3
PN8
PN7
PN9
PN6
PN5
PN4
PN1
ELECTRIC POWER NETWORK LEVEL
b

Fig. 1 *Section of the real-world electric power and communication networks from an electric utility*

a Structure of the real-world power network from an electric utility
b Structure of a regional communication network (top) and its associated power network (bottom). Note: CN – communication node, PN – power node and LC – local centre

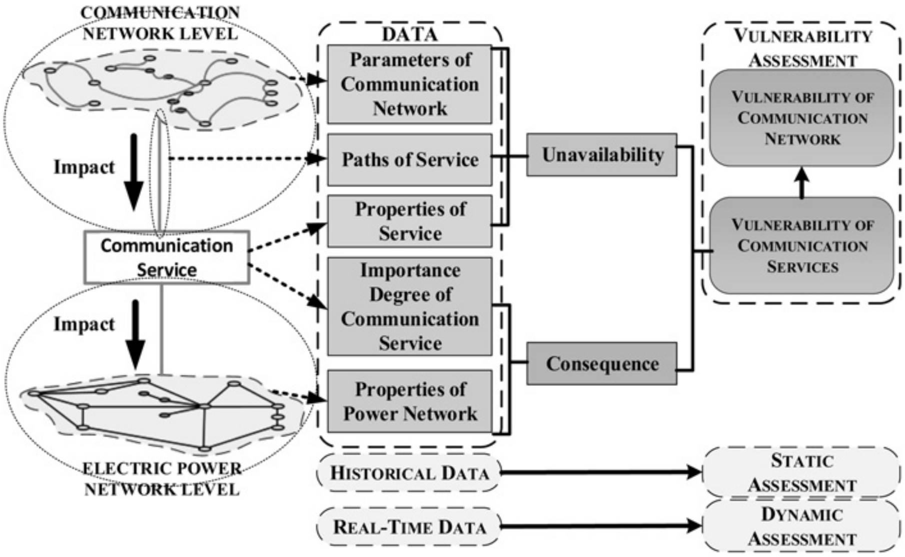
COMMUNICATION NETWORK LEVEL
Impact
Communication Service
Impact
ELECTRIC POWER NETWORK LEVEL
DATA
Parameters of Communication Network
Paths of Service
Properties of Service
Importance Degree of Communication Service
Properties of Power Network
Unavailability
Consequence
VULNERABILITY ASSESSMENT
VULNERABILITY OF COMMUNICATION NETWORK
VULNERABILITY OF COMMUNICATION SERVICES
HISTORICAL DATA
REAL-TIME DATA
STATIC ASSESSMENT
DYNAMIC ASSESSMENT

Fig. 2 *Proposed vulnerability assessment framework*

CNs should be transmitted through node CN_2. The local CC node and the backup CC node in the communication network level generally do not have corresponding power nodes.

For reliability and self-healing purposes, the structure of self-healing ring network (SHRN) is adopted [8]. In each SHRN, there are two fibre rings: primary optic fibre ring [e.g. line P(LC-5) in Fig. 1] and standby optic fibre ring [e.g. line S(LC-5) in Fig. 1]. In an emergency situation, the standby optic fibre ring is adopted through successful switching operation.

3 Vulnerability assessment approach for wide-area power system applications

There are three kinds of indices proposed by the previous work to assess the impact of communication system failures on power system operation: (i) reliability index of communication systems based on the network structure; (ii) vulnerability index based on complex network theory; and (iii) vulnerability index based on direct cyber power interdependencies, which means that faults in communication networks cause a total failure of corresponding power nodes.

In this paper, vulnerability assessment, which reflects the degree of reduced service performance, is chosen to measure system reliability. Vulnerability here is defined as the potential failure capability of a service or a system [19, 20]. The framework for vulnerability assessment proposed in this paper is illustrated in Fig. 2.

As shown, the communication system impacts electrical power system operation through its communication services. Therefore, under this framework, the vulnerability of communication service is first considered and the results are used in assessment of the communication network operation. To assess the vulnerability of a communication service, its unavailability and consequence of failures are taken into account.

In this paper, unavailability is defined as the probability of a communication service unable to perform a required function successfully under a given communication network structure and operating conditions. This unavailability is evaluated based on communication network parameters (i.e. latency and failure probability of communication components), paths of service (i.e. primary path or backup path) and the properties of service (i.e. data transmission latency requirement). Consequence of communication service failures can be evaluated based on the importance degree of each communication service and properties of a power network (i.e. importance index of power nodes). The proposed framework can be processed in both static assessments with historical data and dynamic assessment with real-time data.

Compared with previously proposed indices, the proposed vulnerability index has following three advantages: (i) both latency and interruption faults are considered; (ii) it has clear physical significance; and (iii) probabilistic method is adopted for accurate evaluation.

4 Vulnerability assessment of communication services

The vulnerability of each communication service can then be evaluated as the multiplication of its unavailability and failure consequence

$$V\left(S_n^{mn}\right) = U\left(S_n^{mn}\right) \times C\left(S_n^{mn}\right) \tag{1}$$

The proposed approach to perform unavailability and consequence assessment of communication service is discussed below. In this paper, power and communication networks as illustrated in Fig. 3 are used to demonstrate the methodology. It should be noted that the methodology presented in this section is applicable to any network structure.

4.1 Unavailability assessment

Main reasons for communication service failures include communication interruption and high latency. Other factors such as bit error, packet drop or denial of service, are not taken into account. This is because – based on real-world data obtained from an electric utility, it is found that communication service failures caused by bit error or packet drop can occur with extremely low probability in WAN.

In the proposed framework, the unavailability of a communication service is the sum of outage probability caused by interruption and latency of all available communication paths, as

$$U\left(S_n^{mn}\right) = P_{\mathrm{I}}\left(S_n^{mn}\right) + P_{\mathrm{T}}\left(S_n^{mn}\right) \tag{2}$$

Possible data transmission paths between the two CNs are shown in Fig. 3, assuming that the information is transmitted from the local centre (LC) to the destination node (YB). In this case, the primary data transmission path is P(LC-YB) as shown in State 0 and State 1; and the standby paths are S_1(LC-YB), S_2(LC-YB) and S_3 (LC-YB) as shown in State 2. Four possible states of communication paths are discussed below.

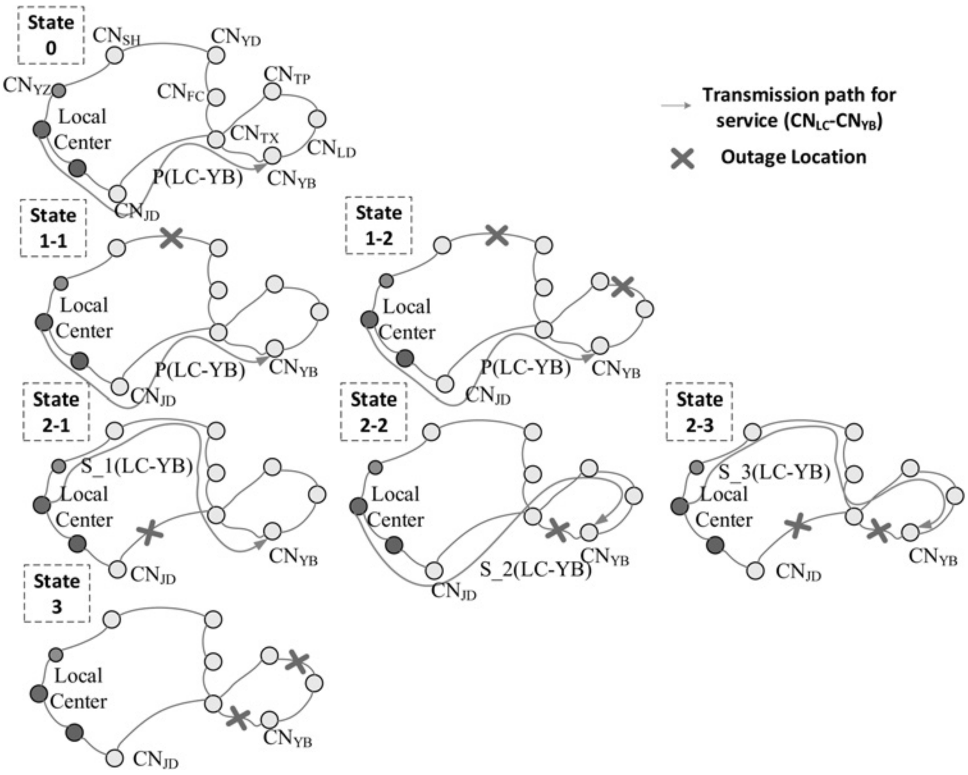

Fig. 3 *States of service between two CNs*

State 0 – Both primary and standby paths remain in their working state: This is a normal operating state when all components in both the primary and standby paths are available. The probability of adopting the primary path in this state is formulated as the product of component availability

$$P_0(S_n^{mn}) = \prod_{C_i \in Path_P(S_n^{mn}) \text{ or } Path_S(S_n^{mn})} (1 - P\_C_i) \tag{3}$$

Since only physical interruption of a component is considered, this paper assumes that the availability of each component is independent from each other.

State 1 – An outage occurs only in the standby path: This is shown as States 1–1 and 1–2 in Fig. 3. The probability of adopting the primary path in this state is formulated as the product of availability of components in the primary path and unavailability of the standby paths

$$P_1(S_n^{mn}) = \prod_{C_i \in Path_P(S_n^{mn})} (1 - P\_C_i) \left[1 - \prod_{C_i \in Path_S(S_n^{mn})} (1 - P\_C_i) \right] \tag{4}$$

State 2 – An outage occurs only in the primary path: This is shown as States 2–1, 2–2 and 2–3 in Fig. 3. The adoption of a standby path happens with the outage of a corresponding primary path in the same SHRN. For example, when an outage occurs in the path LC–CN$_{JD}$–CN$_{TX}$, only S_1(LC-YB) will be adopted although S_3 (LC-YB) is also available. A successful auto-switching operation is needed in this state. The probability of adopting each standby path is formulated as the product of component unavailability in the corresponding primary path and the availability of components in standby paths as

$$P_{2\_k}(S_n^{mn}) = \prod_{x=1}^{X} \left[1 - \prod_{C_i \in Path_{P\_k-x}(S_n^{mn})} (1 - P\_C_i) \right] \times \alpha^X \times \prod_{C_i \in Path_{S\_k}(S_n^{mn})} (1 - P\_C_i) \tag{5}$$

State 3 – An outage occurs in both primary and standby paths: This is illustrated as State 3 in Fig. 3. The interruption probability is calculated as

$$P_I(S_n^{mn}) = 1 - P_0(S_n^{mn}) - P_1(S_n^{mn}) - \sum P_{2\_k}(S_n^{mn}) \tag{6}$$

Interruption of all available paths will definitely cause the communication service to fail. Note that in States 0, 1 and 2, the communication service can also fail if high latency is experienced. Each communication service has different requirements of data transmission latency or a latency threshold value. When the data transmission latency of a communication path exceeds a threshold value, selected WAN services cannot be performed. For example, late receipt of a control signal at a relay can cause blocking of relay protection equipment. Higher latency is likely to cause more adverse effect to power system operation. To quantify this kind of impact, this paper considers latency of paths as a probability distribution function [21, 22], as shown in Fig. 4. Case 1 represents low latency, resulting in a small failure zone; Case 2 represents higher latency and a larger failure zone.

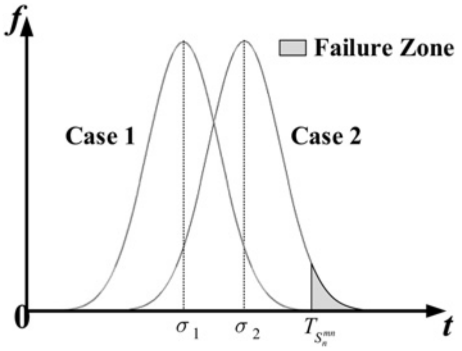

Fig. 4 *Probability distribution function of path latency with the threshold value (CT$_{Smmn}$)*

This probability distribution function can be obtained from the historical data of a communication network. In most cases, latency of a path is much less than the threshold value ($T_{S_n^{mn}}$); therefore, the outage probability is extremely low (e.g. Case 1 in Fig. 4). While in some particular situations, these two values can become close and the failure zone is likely to increase significantly (e.g. Case 2 in Fig. 4).

On the basis of path availability and factoring in the latency parameter, the outage probability of a communication service caused by high latency is calculated by summing the probabilities in States 0, 1 and 2 as follows

$$
\begin{aligned}
P_{\mathrm{T}}\left(S_n^{mn}\right) = {} & \left[P_0\left(S_n^{mn}\right) + P_1\left(S_n^{mn}\right)\right] \times P_{\mathrm{P\_S}_n^{mn}}\left(t > T_{\mathrm{S}_n^{mn}}\right) \\
& + \sum_{k=1}^{K} \left\{P_{2\_k}\left(S_n^{mn}\right) \times P_{\mathrm{S\_}k\mathrm{\_S}_n^{mn}}\left(\left(t + t_{\mathrm{switch}}\right) > T_{\mathrm{S}_n^{mn}}\right)\right\}
\end{aligned} \tag{7}
$$

The distribution function of path latency can be calculated using the distribution function of latency of components through which the service is transmitted. Latency of each component is described as a Gaussian distribution in this paper, and associated parameters have been derived using real data.

4.2 Consequence assessment

The impact of communication service failures on the operation of different wide-area applications is summarised in Table 1 [23].

Given the fact that not all communication service failures lead to loss of load, this paper considers that the consequence of a communication service failure is impacted by both the important level of the communication service and the important level of the power node in consideration. The highest consequence is expected with failures of both the communication service and the power node that are of highest importance.

Owing to the above consideration, in this paper, the consequence of each communication service failure is calculated by multiplying the importance index (I_{PN_i}) of a power node with the importance degree (I_{S_n}) of each kind of service as expressed in (8). It should be noted that when S_n^{mn} belongs to wide-area protection and control services, important indices of destination power nodes are adopted; while indices of measurement nodes are adopted with monitoring services

$$C\left(S_n^{mn}\right) = I_{\mathrm{PN}_i} \times I_{\mathrm{S}_n} \tag{8}$$

The method proposed in [16] is used to evaluate the importance index of a power node which is determined using both the loss of load ratio ($P_{\mathrm{LOL}}^{\mathrm{PN}_i}/P_{\mathrm{Total}}$) and loading level ($L_{\mathrm{N}_i}$), as shown in (9)

Table 1 Classification of communication services and consequence of failure

Application service	Consequence of failure
Wide-area protection service	
adaptive islanding	mal-operation
predictive under frequency load shedding	rejecting operation
Wide-area relay protection	
Wide-area control service	
wide-area voltage stability control	mal-operation
FACT and HVDC control	rejecting operation
cascading failure control	inaccurate operation
precalculation transient stability control	
closed-loop transient stability control	
wide-area power oscillation damping control	
Wide-area monitoring service	
wide-area power oscillation monitoring	declining objectivity
wide-area voltage stability monitoring	declining controllability
PMU-based state estimation	
dynamic state estimation	
PMU-assisted state estimation	

$$I_{\mathrm{PN}_i} = \left(\frac{P_{\mathrm{LOL}}^{\mathrm{PN}_i}}{P_{\mathrm{Total}}}\right)^{L_{\mathrm{N}_i}-1} \tag{9}$$

L_{N_i} is the maximum loading level of the whole system without the power node N_i. This is the loading level before the power flow diverges, which is an indication of a severe impact [16]. It should be noted that, in this paper, (9) is not used directly to evaluate the consequence of communication service failures. Rather, it is used to evaluate the importance degree of power node.

Importance degree I_{S_n} of each kind of service can be determined from communication system requirements and adequate level of reliability (ALR). In this paper, AHP method is adopted to quantify the importance degree of each kind of service [24–26]. A multi-level structure is proposed in this paper, as shown in Fig. 5. There are three levels of decision criteria, as explained below.

The first-level criteria are related to communication system requirements for each service. This level determines relative importance of different requirements.

The second-level criteria are different services, which determine relative weights of each service for each requirement.

The third-level criteria are requirements of the ALR matched with each service failure. The North American Electric Reliability Corporation (NERC) defined six requirements of ALR to help assessing performance of bulk electric system [27]. Here, the ALR index is used to assist the evaluation. Each communication service is evaluated using these requirements and the value of the highest requirement is adopted in the calculation of importance degree. The algorithm is presented as follows:

$$\boldsymbol{I}_{\mathrm{S}} = \left[\boldsymbol{W}_{1\times i}\right] \times \left[\boldsymbol{F}_{j\times i}\right]^{\mathrm{T}} \times \left[\boldsymbol{ALR}_{1\times j}\right] \tag{10}$$

where $\boldsymbol{I}_{\mathrm{s}}$ is a $1 \times j$ matrix, which represents the set of all I_{S_n}; and j is the number of services.

$\boldsymbol{W}$ is a set of communication system requirement weight (a $1 \times i$ matrix, i is the number of requirements being considered), which is used to show relative importance degree of different requirements. In this case, four requirements (i.e. latency, bit error, net bandwidth and protection channel) are considered. This weight can be obtained by using pairwise comparison matrix [28].

$\boldsymbol{F}$ is the services factor (a $j \times i$ matrix). To calculate $\boldsymbol{F}$, a table with actual data of four requirements of each service is obtained. For each requirement, a pairwise comparison matrix is created and an eigenvector is calculated with normalisation.

$\boldsymbol{ALR}$ is the ALR value for services (a $1 \times j$ matrix). The values in the matrix are obtained referencing the NERC report [27].

The detailed calculation of $\boldsymbol{W}$, $\boldsymbol{F}$ and $\boldsymbol{ALR}$ is given with an example in Section 7.

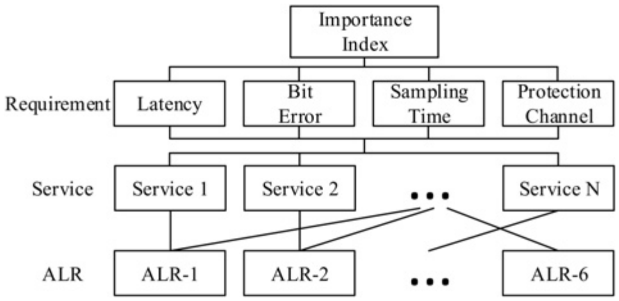

Fig. 5 *AHP structure to determine the importance degree of a communication service*

5 Vulnerability assessment of a communication component

On the basis of the vulnerability assessment results of communication services, the vulnerability of components in a communication network can be calculated as (11) (see (11))

Note that vulnerability of a communication network here is defined as the *contribution* of components to services failure, taking into account the aforementioned four states as follows.

In States 0, 1 and 2, latency is the main factor causing service failure since in these states there remain some available paths for services. Therefore, to each service, the vulnerability *contribution* of each component is determined by multiplication of probability of state, probability of service failure caused by high latency and the ratio of the component latency to the total path latency, as shown in (11) – i and ii.

While in State 3, an interruption event is the reason for service failures. As the outage of components causes a total service failure, the vulnerability *contribution* of components to service failure is determined by multiplying the outage probability of itself and that of the corresponding standby path, as shown in (11) – iii.

6 Dynamic vulnerability assessment of an integrated power-communication system

The vulnerability calculation above is based on static historical data, representing the static vulnerability of an integrated power and communication system. To explore dynamic vulnerability calculation where vulnerability values are calculated continuously over time, the same procedure can be used with only a little change.

First, check periodically if there is any primary or standby component in an overhaul or an interruption state and set its interruption probability to 1, then reset the paths of all services; Replace every component's distribution function of latency $t \sim N(\mu, \sigma^2)$ with $t \sim N(\mu_T, \sigma^2)$, where μ_T is the average latency value in a given time interval T; consider only available services in the time interval for S_n^{mn}. With the same calculation process, the vulnerability of communication services and communication network, which are represented as $V_D(S_n^{mn})$ and $V_D(C_i)$, respectively, can be calculated. This allows determination of the dynamic change of vulnerability to evaluate the performance of a communication system.

7 Case study

A case study based on the IEEE 30-bus test system is used to demonstrate the proposed vulnerability assessment approach, as shown in Fig. 6*a*. The corresponding communication network is modelled based on properties of the real-world WAN, as shown in Fig. 6*b*. Note that the similar design of a communication network can be found in [8].

7.1 Communication network model

The communication network model combines one backbone network (SDH-BN) and three regional networks (SDH-1, SDH-2 and SDH-3), all of which are of SHRN structure. Numbers on each communication paths represent distance of optical fibre lines in kilometres. The relationship between power and communication networks is referenced from [16], as shown by dashed arrows in Fig. 6*b*.

The data on interruption probability for communication components is obtained from [29], which is based on the SDH fibre optic technology. Characteristics of this technology are still valid in today's environment as it has long been in use to support backbone communications in power grids for several decades. The latency data is typical value obtained from an electric utility, as shown in Table 2.

Six WAN applications are selected to showcase the vulnerability assessment case study: wide-area relay protection (S_1), predictive under frequency load shedding (S_2), wide-area power oscillation damping control (S_3), closed-loop transient stability control service (S_4), wide-area voltage stability monitoring service (S_5) and PMU-based state estimation service (S_6). For this paper, it is assumed that number of services available are 64, 24, 16, 31, 24 and 17 for S_1, S_2, S_3, S_4, S_5 and S_6, respectively. It is also assumed that the threshold latency values of these services are 5, 20, 15, 20, 30 and 10 ms, respectively. It is necessary to mention that the threshold values considered here are transmission latency instead of the total time delay from a service being issued to a service being executed. All primary paths of services are designed based on the shortest route principle.

7.2 Vulnerability assessment result of communication services in a normal operating condition

The importance index of each power node (I_{PN_i}) is calculated using (9), as shown in Table 3.

Importance degree I_{S_n} of each kind of service is calculated using (10). The detailed process is given as follows.

To calculate the communication system requirement weight $\boldsymbol{W}$, the following pairwise comparison matrices $\boldsymbol{L}_1$ are constructed. $\boldsymbol{L}_1$ represents the importance comparison among four requirements, as shown in Fig. 5 – the first-level criteria, where 0.1–0.9 represent 'not important at all' to 'extremely important' and 0.5 represent 'equally importance' [28]. For example, $\boldsymbol{L}_1$ (1, 2) = 0.9 means latency is extremely more important than bit error in the assessment scope. On the basis of $\boldsymbol{L}_1$, the eigenvectors corresponding to the maximum eigenvalues are $\boldsymbol{W}$ = [0.3971, 0.1900, 0.1541, 0.2588].

$\boldsymbol{F}$ represents the services factor-based actual data of four requirements for each service (i.e. the second-level criteria). For each requirement, a pairwise comparison matrix is created and an eigenvector is calculated with normalisation. For latency, data of [5, 30, 20, 30, 100, 20] ms is adopted. For bit error, data of [−log (β)] are used where β is the bit error ratio of [10^{-8}, 10^{-8},

$$V(C_i) = \sum_{C_i \in Path_P(S_n^{mn})} \left(P_0^{\text{C}_i} + P_1^{\text{C}_i}\right) \times C\left(S_n^{mn}\right) + \sum_{C_i \in Path_\text{S}(S_n^{mn})} P_2^{\text{C}_i} \times C\left(S_n^{mn}\right) + \sum_{C_i \in Path_\text{P}(S_n^{mn}) \text{ or } Path_\text{S}(S_n^{mn})} P_3^{\text{C}_i} \times C\left(S_n^{mn}\right)$$

$$\begin{cases} P_a^{\text{C}_i} = P_a\left(S_n^{mn}\right) \times \left[1 - P_{\text{P}\_\text{S}_n^{mn}}\left(t < T_{\text{S}_n^{mn}}\right)\right] \times \dfrac{\mu(C_i)}{\sum\limits_{C_j \in Path_\text{P}(S_n^{mn})} \mu\left(C_j\right)}, \quad a = 0,\ 1 & \cdots \text{i} \\ P_2^{\text{C}_i} = \sum\limits_{k=1}^{K} \left\{ P_{2\_k}\left(S_n^{mn}\right) \times \left[1 - P_{\text{S}\_k\_\text{S}_n^{mn}}\left(\left(t + t_{\text{switch}}\right) < T_{\text{S}_n^{mn}}\right)\right] \times \dfrac{\mu(C_i)}{\sum\limits_{C_j \in Path_{\text{S}\_k}(S_n^{mn})} \mu\left(C_j\right)} \right\} & \cdots \text{ii} \\ P_3^{\text{C}_i} = P\_C_i \times \left[1 - \sum\limits_{C_j \in Path_{\text{parallel}\_\text{C}_i}(\text{S}_n^{mn})} \left(1 - P\_C_j\right)\right] & \cdots \text{iii} \end{cases} \tag{11}$$

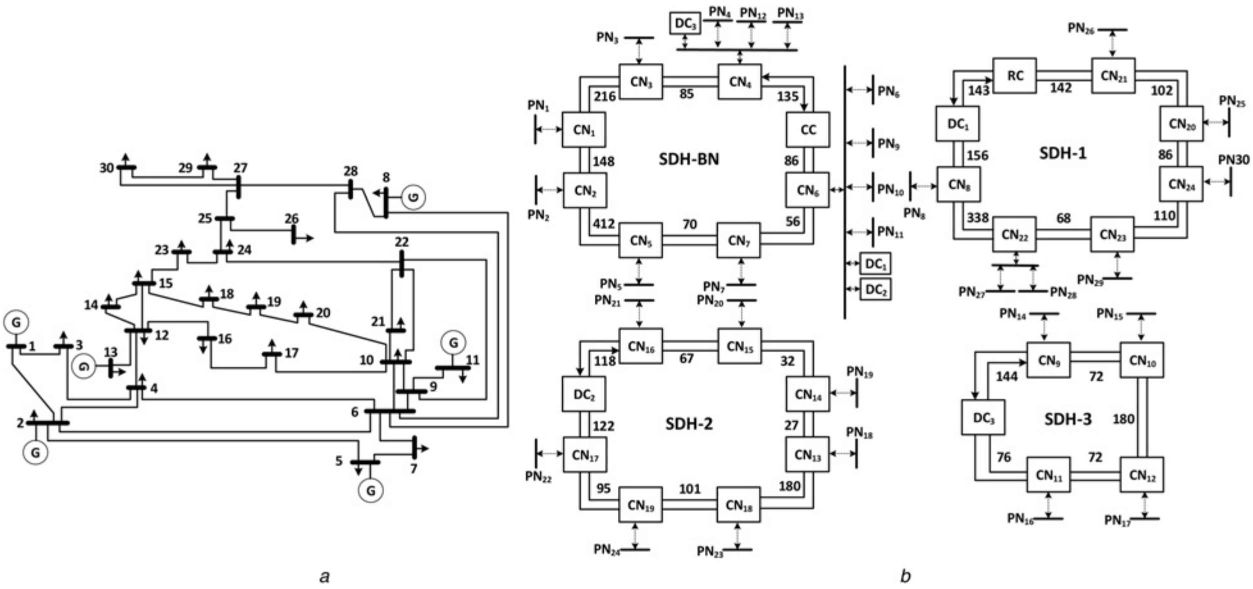

Fig. 6 *Case study*

a IEEE 30-bus test system

b Corresponding communication network of the IEEE 30-bus test system (CC – control centre, RC – regional centre and DC – data concentrator)

10^{-8}, 10^{-8}, 10^{-6}, 10^{-6}]. For the sampling time and protection channel, judgment of human experts is adopted.

ALR represents the adequate level of reliability for each kind of service. First, set values 1–6 to each requirement, where larger value represents more importance. The six kinds of services (S_1–S_6) match with ALR values of 6, 3, 2, 2, 1 and 1, respectively. Construct a pairwise comparison matrix $\boldsymbol{L_2}$ to compare each requirement, which represents relative importance between every two requirements. Using $\boldsymbol{L_2}$, the eigenvectors corresponding to the maximum eigenvalues are [0.1601, 0.2184, 0.2624, 0.3591]; therefore, $\boldsymbol{ALR}$ = [0.3591, 0.2624, 0.2184, 0.2184, 0.1601, 0.1601]

$$\boldsymbol{L_1} = \begin{bmatrix} 0.5 & 0.9 & 0.9 & 0.7 \\ & 0.5 & 0.7 & 0.3 \\ & & 0.5 & 0.3 \\ & & & 0.5 \end{bmatrix} \boldsymbol{L_2} = \begin{bmatrix} 0.5 & 0.33 & 0.25 & 0.14 \\ & 0.5 & 0.4 & 0.25 \\ & & 0.5 & 0.33 \\ & & & 0.5 \end{bmatrix}$$

$$\boldsymbol{F} = \begin{bmatrix} 0.2911 & 0.1743 & 0.1599 & 0.2773 \\ 0.1395 & 0.1743 & 0.1599 & 0.1811 \\ 0.1668 & 0.1743 & 0.1059 & 0.1202 \\ 0.1494 & 0.1743 & 0.2103 & 0.1811 \\ 0.0864 & 0.1514 & 0.1217 & 0.1202 \\ 0.1668 & 0.1514 & 0.2423 & 0.1202 \end{bmatrix}$$

The result in Table 4 shows the resulting important degree of six different services.

Table 2 Interruption and latency data for communication components

Network unit	Interruption data			Time delay data	
	FIT[a] rate	MTTR[b], h	Interruption probability[c]	Mean time, ms	Standard deviation, ms
node	8000	4	3.2×10^{-5}	0.4	0.04
OFL[d]	300	24	7.2×10^{-6}	5×10^{-3}	4.17×10^{-4}

[a] One *FIT* is equivalent to the failure rate of one failure per 10^9 hours

[b] *MTTR* = mean time to repair (hours)

[c] Interruption probability = (*MTTR*×*FIT*)/10^9

[d] OFL: optical fibre line (/km)

Wide-area relay protection services (S_1) have the highest importance degree, followed by predictive under frequency load shedding services (S_2) and closed-loop transient stability control services (S_4). Table 4 also summarises resulting vulnerability values calculated based on (1)–(10) and their rankings as shown in parentheses.

Table 3 Importance indices of each PN

CN	PN	$P_{\text{LOL}}^{\text{PN}_i}$	L_{N_i}	I_{PN}	CN	PN	$P_{\text{LOL}}^{\text{PN}_i}$	L_{N_i}	I_{PN}
1	1	0	1.8	1	13	18	3.2	1.8	0.0277
2	2	21.7	1	1	14	19	9.5	1.9	0.0471
3	3	2.4	1.4	0.1483	15	20	2.2	1.8	0.0205
4	4, 12, 13	18.8	1.1	0.7624	16	21	17.5	2.0	0.0618
5	5	94.2	2.0	0.3324	17	22	0	1.8	0
6	6, 9, 10, 11	5.8	1	1	18	23	3.2	1.8	0.0277
7	7	22.8	1.9	0.1035	19	24	8.7	1.9	0.0435
8	8	30	1.9	0.1325	20	25	3.5	1.8	0.0297
9	14	6.2	1.8	0.0470	21	26	3.5	1.8	0.0297
10	15	8.2	1.8	0.0588	22	27, 28	13	1.9	0.0624
11	16	3.5	1.8	0.0297	23	29	2.4	1.8	0.0220
12	17	9	1.9	0.0448	24	30	10.6	1.9	0.0520

Table 4 Vulnerability assessment results and ranking of services

Service	I_{S_n}	Mean P_{I}^{a}	Mean P_{T}^{b}	Mean P_{R}^{c}	Mean V^{d}
S_1	0.3610 1	1.07×10^{-5} 6	1.14×10^{-3} 1	0.9988 6	2.12×10^{-4} 1
S_2	0.1722 2	5.97×10^{-5} 3	5.80×10^{-24} 5	0.9999 1	1.41×10^{-6} 4
S_3	0.1315 4	1.89×10^{-5} 5	4.28×10^{-8} 3	0.9999 1	1.44×10^{-6} 3
S_4	0.1538 3	6.97×10^{-5} 2	4.49×10^{-24} 4	0.9999 1	1.26×10^{-6} 5
S_5	0.0742 6	8.13×10^{-5} 1	0 6	0.9999 1	4.30×10^{-7} 6
S_6	0.1073 5	4.59×10^{-5} 4	1.61×10^{-4} 2	0.9998 5	4.32×10^{-6} 2
S^{e}	0.2143	4.16×10^{-5}	4.31×10^{-4}	0.9995	7.84×10^{-5}

[a] P_{I} is interruption probability calculated using (6)

[b] P_{T} is outage probability caused by latency calculated using (7)

[c] P_{R} is reliability value calculated as $1-P_{\text{I}}-P_{\text{T}}$

[d] V is vulnerability value calculated using (1)

[e] Values in the last row are the average values of their respective columns

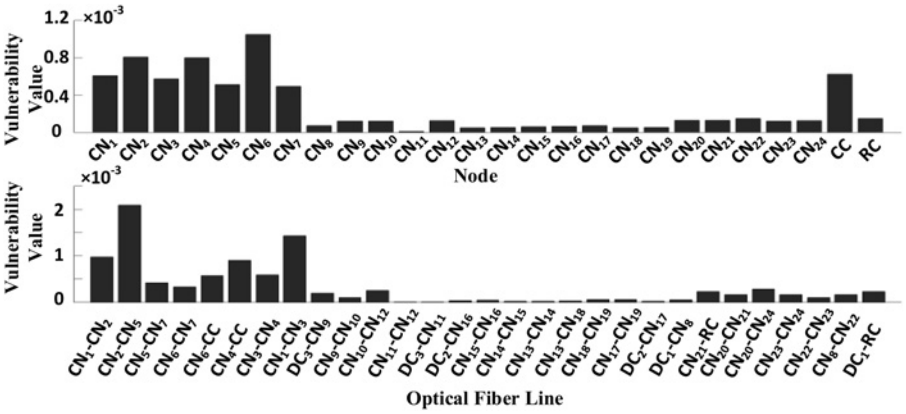

Fig. 7 *Vulnerability values of components in communication networks for IEEE 30-bus system*

Interruption probability (P_{I}) of a service is related to the transmission path and interruption probability of components in this path. For being mainly transmitted between two neighbouring nodes, relay protection services (S_1) have the lowest mean interruption probability. While the outage probability (P_{T}) caused by latency of a service is related to the threshold latency value and the distribution function of latency in relevant transmission paths. Owing to the lowest threshold value, relay protection services (S_1) have relatively high P_{T}. On the other hand, wide-area voltage stability monitoring services (S_5) have the lowest P_{T}. All services have a reliability value (P_{R}) above 99.5%, which means, in a normal condition, these communication services are highly reliable.

7.3 Vulnerability assessment result of communication networks in a normal condition

The vulnerability values of components in communication networks are evaluated using (11). Fig. 7 illustrates the resulting vulnerability values for nodes (top) and those for each optical fibre line connecting any two nodes (bottom). With the most communication connections and as the key component to CC, node CN_6 has the highest vulnerability value, followed by CN_2 and CN_4.

Table 5 summarises the average vulnerability values of all components in each of the four ring networks. The backbone ring network (SDH-BN) has the highest average vulnerability value, followed by the subnet network (SDH-1), whereas the other two subnets have much lower values. This is mainly because of relative longer optical fibre lines in SDH-BN and SDH-1 and more communication services being transmitted to the CC and the LC.

7.4 Impact of communication faults on vulnerability values

To study the impact of communication interruption on vulnerability values, this study considers two interruption scenarios: (i) an interruption occurs in the communication optical fibre line data concentrator (DC_3)–CN_9 in the SDH-3 ring and (ii) an interruption occurs in the communication optical fibre line CN_6–CC in the SDH-BN ring. The variation in service reliability is shown in Table 6.

Table 5 Average vulnerability of components in four ring network

	SDH-BN	SDH-1	SDH-2	SDH-3
mean $V_{\mathrm{CN}}^{\mathrm{a}}$	6.85×10^{-4}	1.25×10^{-4}	5.68×10^{-5}	9.44×10^{-5}
mean $V_{\mathrm{OFL}}^{\mathrm{b}}$	9.17×10^{-4}	1.75×10^{-4}	3.40×10^{-5}	1.11×10^{-4}
mean $V_{\mathrm{C}}^{\mathrm{c}}$	8.01×10^{-4}	1.52×10^{-4}	4.66×10^{-5}	1.03×10^{-4}

[a] V_{CN} is vulnerability value of communication node calculated using (11)
[b] V_{OFL} is vulnerability value of optical fibre line calculated using (11)
[c] V_{C} is vulnerability value of all components

Vulnerability of services in scenario 1 slightly increases, but the whole system still stays in an acceptable safety range as all available services have reliability values >0.95. While in scenario 2, for optical fibre line CN_6–CC being the key path to the system CC, its interruption causes more serious consequences. As shown in Table 6, seven services out of all available services have reliability value <0.95, and five services have reliability value <0.1, implying that they have an extremely high chance of failure. These include, for example, wide-area relay protection services between CN_4–CN_6 and CN_{12}–CN_6, and PMU-based state estimation services between nodes CN_{18}–CC.

The vulnerability of each component of the communication network in scenarios 1 and 2 is illustrated in Figs. 8*a* and *b*, respectively, where the dotted red lines represent the proportion of vulnerability value variation.

In scenario 1, the interruption of line DC_3–CN_9 results in the services being switched to its standby paths. The vulnerability values of components in the same SHRN increase significantly (e.g. CN_{11}, optical fibre line CN_{11}–CN_{12} and DC_3–CN_{11}). While because of the reselection of some service paths, the vulnerability value of other components decline slightly (e.g. vulnerability value of the CN_9 declines from 1.21×10^{-4} shown in Fig. 7 to 1.05×10^{-4} shown in Fig. 8*a*).

In scenario 2, the interruption of line CN_6–CC causes vulnerability values of a number of components to increase significantly, and the consequence is obviously more serious than scenario 1. CN_4, CN_6 and CC have become the most vulnerable CNs, whereas optical lines CN_4–CC, DC_3–CN_9 and CN_{10}–CN_{12} have become the most vulnerable optical fibre lines.

7.5 Dynamic variation of vulnerability

With smart grid development, communication channels may need to be shared with many other smart grid applications. In some situations with the channel utilisation close to 100% of its capacity during certain peak periods or selected devices in a CN becoming out of service, the latency may increase due to the queuing delay caused by high data transfer [30, 31]. For this analysis, it is assumed that the latency of CN_6 increases 0.2 ms per second.

The dynamic variation of vulnerability values during the first six seconds is shown in Fig. 9. With increasing time, the vulnerability values of several wide-area relay protection services [e.g. S_1 (2–6)

Table 6 Vulnerability variation with communication interruptions

Scenario	Number of services with $P_{\mathrm{R}} < 0.95$	Number of services with $P_{\mathrm{R}} < 0.1$	Mean V	Mean increase in V
1	0	0	8.98×10^{-5}	1.14×10^{-5}
2	7	5	6.21×10^{-3}	6.13×10^{-3}

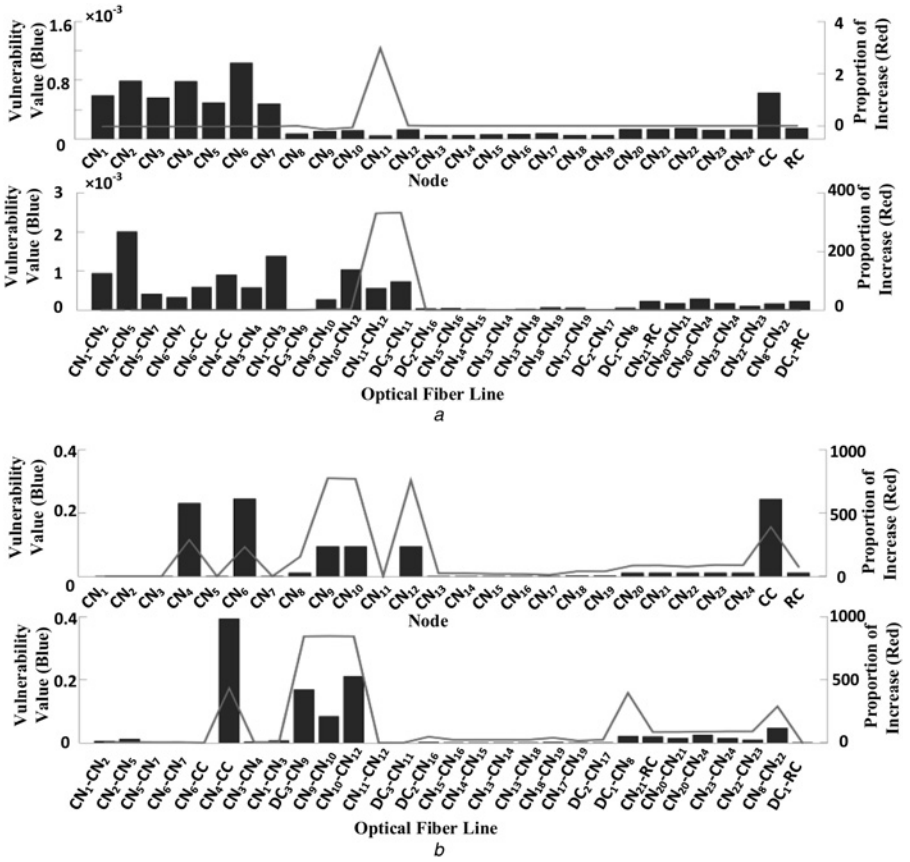

Fig. 8 *Vulnerability of each component of the communication network in scenarios 1 and 2*

a Vulnerability of communication components with interruption in optical fibre line DC_3–CN_9
b Vulnerability of communication components and lines with interruption in optical fibre line CN6–CC

in Fig. 9*a*, which is a relay protection service transmitted through CN_2–CN_6) rise sharply while the reliability of corresponding paths is dropping as shown in Fig. 9*b*. As shown in Figs. 9*c* and *d*, the vulnerability value of node CN_6 substantially increases over time, while that of other nodes and optic fibre lines increase gradually.

Fig. 10 illustrates vulnerability values of optical fibre lines when latency of the CN CN_6 increases at the rate of 0.2 ms per second (i.e. the total latency is 10 ms in 50 s).

It is interesting to note that in some time period (e.g. time = 5–7 s, 13–15 s, 18–22 s), the vulnerability values of optical fibre lines increase. This is because the vulnerability values of communication

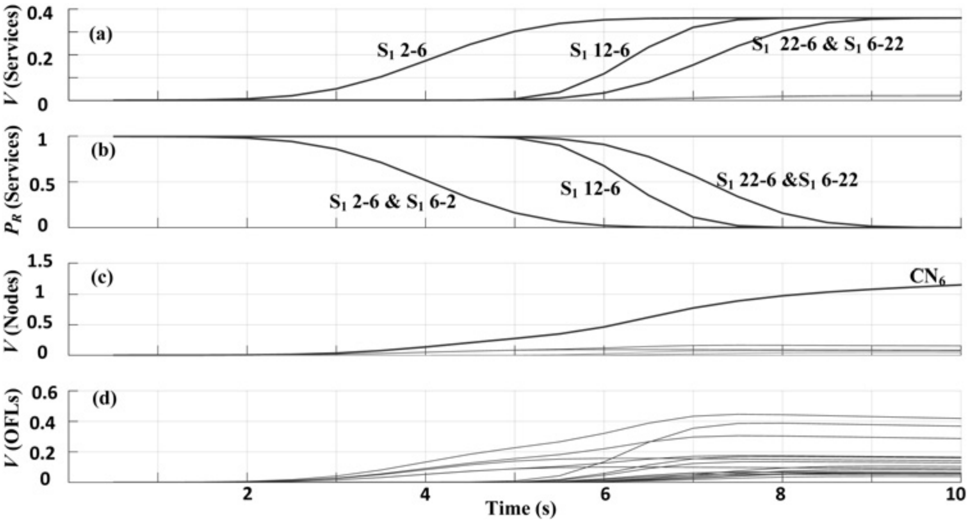

Fig. 9 *Dynamic variation of vulnerability values during the first 6 s*

a Dynamic variation of service vulnerability with latency of CN CN6 increasing at the rate of 0.2 ms/s (i.e. the total latency is 2 ms in 10 s). This is calculated using the method discussed in Section 6
b Dynamic variation of service reliability
c Dynamic variation of vulnerability value of CNs
d Dynamic variation of vulnerability value of optical fibre lines

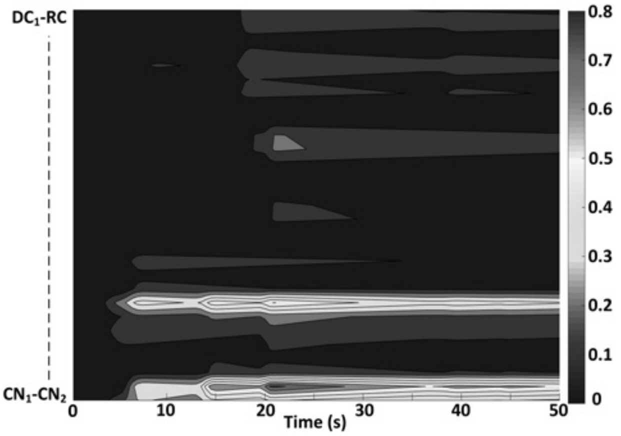

Fig. 10 *Variation of vulnerability of optical fibre lines when latency of the CN CN6 increases at 0.2 ms/s for 50 s. This is calculated using (11). The sequence of optical fibre lines is same as that in Fig. 7*

services transmitted through the associated path(s) increase. However, during some other period (e.g. time = 15–18 s, 22–37 s), these vulnerability values slightly decline due to a larger increase in the total latency of service paths [$\sum \mu(C_j)$] as compared the increase in vulnerability values of communication services.

7.6 Application of vulnerability assessment

Vulnerability assessment of communication services and communication network can be used to provide auxiliary information for the planning of an integrated power-communication system. Changes in vulnerability values as a result of communication failures can be used to determine the most vulnerable component(s) in different scenarios. The real-time variation of vulnerability values can be used to support power system monitoring and operation, and provide warning signals in real time.

8 Conclusion

It is crucial to study adverse effects of communication system failures on power system operation. This paper introduces a framework for vulnerability assessment of communication systems for electric power grids. The proposed approach takes into account the probability and consequence of communication services failures caused by interruption faults and abnormal latency occurred in different communication network components. Assessment results provide key information for identification of the most vulnerable components of the integrated communication in electric power systems, which can be used for power system planning and operation. The proposed vulnerability assessment method takes into account intrinsic characteristics of communication networks such as interruption and latency. Other factors such as cyberattacks and sabotages can be included in future work.

9 Acknowledgments

This work was supported by China Scholarship Council (file no 20140690151), State Grid Corporation of China project: Key Technologies for Power System Security and Stability Defense Considering the Risk of Communication and Information Systems and National Natural Science Foundation of China (Grant No. 51577030).

10 References

1 Kuzlu, M., Pipattanasomporn, M., Rahman, S.: 'Communication network requirements for major smart grid applications in HAN, NAN and WAN', *Comput. Netw.*, 2014, **67**, pp. 74–88

2 Eissa, M.M., Fayek, W.M., Hadhoud, M.M.A., *et al.*: 'Frequency/voltage wide-area measurements over transmission control protocol/internet protocol communication network for generator trip identification concerning missed data', *IET Gener. Transm. Distrib.*, 2014, **8**, (2), pp. 290–300

3 Sodhi, R., Sharieff, M.I.: 'Phasor measurement unit placement framework for enhanced wide-area situational awareness', *IET Gener. Transm. Distrib.*, 2015, **9**, (2), pp. 172–182

4 Terzija, V., Valverde, G., Deyu, C., *et al.*: 'Wide-area monitoring, protection, and control of future electric power networks', *Proc. IEEE*, 2011, **99**, (1), pp. 80–93

5 Shen, X., Shu, Z., Liu, Y., *et al.*: 'Statistics and analysis on operation situation of protective relayings of state grid corporation of china in 2009', *Power Syst. Technol.*, 2011, **35**, (2), pp. 189–193

6 'Investigation report into the loss of supply incident affecting parts of the west midlands at 10:10 on the morning of Friday, 5 September 2003'. Available at http://www.g4jnt.com/hams_hall_investigation_report.pdf, accessed 11 February 2015

7 Andersson, G., Donalek, P., Farmer, R., *et al.*: 'Causes of the 2003 major grid blackouts in North America and Europe and recommended means to improve system dynamic performance', *IEEE Trans. Power Syst.*, 2005, **20**, (4), pp. 1922–1928

8 Wang, Y., Li, W., Lu, J.: 'Reliability analysis of wide-area measurement system', *IEEE Trans. Power Deliv.*, 2010, **25**, (3), pp. 1483–1491

9 Dai, Z., Wang, Z., Jiao, Y.: 'Reliability evaluation of the communication network in wide-area protection', *IEEE Trans. Power Deliv.*, 2011, **26**, (4), pp. 2523–2530

10 Song, Z., Vittal, V.: 'Design of wide-area power system damping controllers resilient to communication failures', *IEEE Trans. Power Syst.*, 2013, **28**, (4), pp. 4292–4300

11 Panteli, M., Kirschen, D.S.: 'Assessing the effect of failures in the information and communication infrastructure on power system reliability'. IEEE PES Power System Conf. and Exposition, Phoenix, USA, March 2011, pp. 1–7

12 Aminifar, F., Fotuhi-Firuzabad, M., Shahidehpour, M., *et al.*: 'Impact of WAMS malfunction on power system reliability assessment', *IEEE Trans. Smart Grid*, 2012, **3**, (3), pp. 1302–1309

13 Niyato, D., Dong, Q., Wang, P., *et al.*: 'Optimizations of power consumption and supply in the smart grid: analysis of the impact of data communication reliability', *IEEE Trans. Smart Grid*, 2013, **4**, (1), pp. 21–35

14 Ray, S., Venayagamoorthy, G.K.: 'Real-time implementation of a measurement-based adaptive wide-area control system considering communication delays', *IET Gener. Transm. Distrib.*, 2008, **2**, (1), pp. 62–70

15 Buldyrev, S.V., Parshani, R., Paul, G., *et al.*: 'Catastrophic cascade of failures in interdependent networks', *Nature*, 2010, **464**, pp. 1025–1028

16 Ten, C., Liu, C., Manimaran, G.: 'Vulnerability assessment of cybersecurity for SCADA systems', *IEEE Trans. Power Syst.*, 2008, **23**, (4), pp. 1836–1846

17 Falahati, B., Yong, F., Lei, W.: 'Reliability assessment of smart grid considering direct cyber-power interdependencies', *IEEE Trans. Smart Grid*, 2012, **3**, (3), pp. 1515–1524

18 International Telecommunication Union: 'Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks'. Available at https://www.itu.int/rec/T-REC-G.783–200603-I/en

19 Johansson, J., Hassel, H., Zio, E.: 'Reliability and vulnerability analyses of critical infrastructures: comparing two approaches in the context of power systems', *Reliab. Eng. Syst. Saf.*, 2013, **120**, pp. 27–38

20 Li, W.: 'Risk assessment of power systems: models, methods, and applications' (John Wiley & Sons, 2014)

21 Zhu, K., Nordström, L.: 'Design of wide-area damping systems based on the capabilities of the supporting information communication technology infrastructure', *IET Gener. Transm. Distrib.*, 2014, **8**, (4), pp. 640–650

22 Yang, B., Wei, L., Zhan, Z., *et al.*: 'Analysis on characteristics of communication delay in wide area measurement system based on probability distribution', *Autom. Electr. Power Syst.*, 2015, **39**, (12), pp. 38–43

23 Wang, Q., Pipattanasomporn, M., Kuzlu, M., *et al.*: 'Impact assessment of communication service in wide-area power system'. Proc. IEEE PES General Meeting, Denver, USA, July 2015, pp. 1–6

24 Saaty, T.L.: 'Part one: the analytic hierarchy process', in 'The analytic hierarchy process' (McGraw-Hill, New York, USA, 1980, 1st ed.)

25 Lin, P.-C., Gu, J.-C., Yang, M.-T.: 'Intelligent maintenance model for condition assessment of circuit breakers using fuzzy set theory and evidential reasoning', *IET Gener. Transm. Distrib.*, 2014, **8**, (7), pp. 1244–1253

26 Mikhailov, L., Tsvetinov, P.: 'Evaluation of services using a fuzzy analytic hierarchy process', *Appl. Soft Comput.*, 2004, **5**, (1), pp. 23–33

27 'Integrated bulk power system risk assessment concepts' (North American Electric Reliability Corporation, Atlanta, GA, USA)

28 Xu, Z., Liao, H.: 'Intuitionistic fuzzy analytic hierarchy process', *IEEE Trans. Fuzzy Syst.*, 2014, **22**, (4), pp. 749–761

29 Antonopoulos, A., O'Reilly, J.J., Lane, P.: 'A framework for the availability assessment of SDH transport networks'. Proc. Second IEEE Symp. Computers and Communications, Alexandria, USA, July 1997, pp. 666–670

30 Chenine, M., Karam, E., Nordstrom, L.: 'Modeling and simulation of wide area monitoring and control systems in IP-based networks'. Proc. IEEE PES General Meeting, Calgary, Canada, July 2009, pp. 1–8

31 Bian, D., Kuzlu, M., Pipattanasomporn, M., *et al.*: 'Real-time co-simulation platform using OPAL-RT and OPNET for analyzing smart grid Performance'. Proc. IEEE PES General Meeting, Denver, USA, July 2015, pp. 1–6