Iran J Sci Technol Trans Electr Eng (2018) 42:63–74
https://doi.org/10.1007/s40998-018-0049-5

RESEARCH PAPER

Improving Adaptive Protection to Reduce Sensitivity to Uncertainties Which Affect Protection Coordination of Microgrids

S. A. Hosseini[1] · H. Askarian Abyaneh[2] · S. H. H. Sadeghi[2] · R. Eslami[2]

Received: 6 September 2016 / Accepted: 5 January 2018 / Published online: 5 February 2018

Abstract
Uncertainties in microgrid topology, protection system, and communication links involve accidental variables that affect the protection coordination of a microgrid. To resolve this issue, a method is proposed that uses a decision tree after each fault to ensure a robust protection coordination. The decision tree creates an optimal composition of strategies, such that for each unsuccessful strategy, the best possible strategy is substituted according to a number of uncertainty indices. The indices considered in this work include successfulness probability of strategies in clearing faults and the amount of loads outages caused by implementing these strategies. The probability of successfulness of strategies is considered to correct operation of circuit breakers and communication links involved in each strategy. The proposed method enables adaptive protection to decide according to microgrid topology and the probability of correct operation of protection system and communication links. In addition, it avoids saving too many offline decisions. The performance of the proposed method is tested on a sample microgrid in DIgSILENT Power Factory software, where the results of various case studies will be reported.

Keywords Microgrid · Uncertainty · Decision tree · Protection coordination

1 Introduction

In some cases, the behavior of protection system takes effect from accidental behavior of different variables. Facing such problems highlights the requirement in the application of methods which reduce sensibility of answers to uncertainty of accidental variables. Therefore, every plan for microgrid protection coordination is not adequately validated without considering uncertainties that affect the robustness of a protection system (Hosseini et al. 2016a).

Accidental variables that affect microgrid protection coordination plans include uncertainty in microgrid topology, protection system, and communication links (Hosseini et al. 2016a). The source of uncertainty in microgrid topology is its dynamic nature. Connecting or disconnecting of distributed generations (DGs) and capability of microgrid operation in both normal and islanded modes are the main reasons for microgrid dynamic behavior (Hosseini et al. 2015). The uncertainty in protection system often occurs during its operation in the event of a fault, thus causing undesirable outages and reducing the reliability of the system (Kai and Singh 2011). On the other hand, the secure operation of a microgrid protection systems can be affected by the speed, latency, and reliability of the respective communication links often used within the microgrid (Eissa et al. 2010).

However, according to Hosseini et al. (2016a), none of the previous studies considered uncertainties of protection system and communication links in protection coordination process, Sortomme et al. (2010) propose adaptive

✉ S. A. Hosseini
hosseini.amir@gut.ac.ir

H. Askarian Abyaneh
askarian@aut.ac.ir

S. H. H. Sadeghi
sadeghi@aut.ac.ir

R. Eslami
reza.eslami@aut.ac.ir

[1] Department of Electrical Engineering, Golpayegan University of Technology, Isfahän, Iran

[2] Department of Electrical Engineering, Amirkabir University of Technology, Tehran, Iran

protection coordination as a powerful method in responding to microgrid structural uncertainties. Adaptive protection is an online activity that modifies the preferred protective response to a change in system conditions or requirements (Mahat et al. 2011). Accordingly, Mahat et al. (2011) and Hosseini et al. (2016b) utilize offline adaptive protection schemes that store all possible settings associated with microgrid structural uncertainties. The performance of offline schemes has been challenged for two reasons (Conti and Nicotra 2009; Conti 2009). First, such schemes require large memory resources for storing all possible uncertainties in a microgird. Second, they are unable to cover all dynamic changes of a typical microgrid. To avoid these shortcomings, El-Khattam and Sidhu (2009) and Najy et al. (2013) suggested calculation of protection coordination after each change in network. Evidently, this is not a viable approach in a practical network with large number of structural uncertainties, resulting in excessive computation times.

With the advent of high speed and reliable communication links, microgrid adaptive protection schemes have been able to operate online with high selectivity (Su et al. 2006). Accordingly, the studies done in Liu et al. (2000), Fenghui et al. (2012) and Lim et al. (2007) utilize shared between various protection systems to achieve the best decision. Using offline reactions during fault events and ignoring the uncertainties in protection system and communication links are found to be the most important defects of these studies (Ustun et al. 2011).

In this paper, we propose a decision tree scheme that efficiently responds to uncertainties in microgrid protection coordination. The affecting factors include uncertainties in protection system, communication links, and microgrid topology. Considering that, in the event of a fault in a network, the circuit breakers (CBs) are stressed more than any other equipment (Jazaeri et al. 2015), we model the uncertainty in protection system with the uncertainty of the respective CBs. The proposed scheme provides an optimal combination of strategies in a way that for each failed case, the best possible strategy is offered according to the uncertainty indices. In this scheme, it is not necessary to store a high amount of offline decisions. In addition, the probability of correct operation of CB modules and communication links is not considered to be constant; it can vary according to the fault current flowing through CB modules and the latency of communication links, respectively.

This paper is structured as follows. In Sect. 2, the problem of microgrid protection coordination in the absence of uncertainty in protection system is analyzed. In Sect. 3, the new method for creating protection coordination in microgrid considering the uncertainties is presented. In Sect. 4, the performance of the proposed method is tested on a sample microgrid, where the results of various case studies will be reported.

2 Problem Statement

Adaptive protection is a powerful means for treating uncertainties that affect the robustness of microgrid protection (Basak et al. 2012). This issue is correct if the uncertainties affecting microgrid protection were identified and necessary plans for facing them were provided since without considering these uncertainties, adaptive protection would not be able to provide required reliability to protect microgrid (Hosseini et al. 2016a). This issue is explained using sample network, as shown in Fig. 1, which is used in Dewadasa et al. (2011).

Referring to Fig. 1, it is assumed that a local offline adaptive protection system [such as the one described in Mahat et al. (2011)] is used. Suppose that all DG resources are connected to the network and a fault occurs at the location of F1. It follows that for a desired protection coordination scheme, both the protection systems at 5 and 6 should successfully operate to clear the fault. In the case, where the protection system at five fails to clear the fault, it is expected that the protection system at 3 will clear the fault as a backup system. If the failure rate of CB3 was high, the backup system could fail to operate during the preset clearance interval of protection system at 5. This scenario could be repeated involving further backup systems, causing eventual irreversible cascading outages.

Considering that the uncertainties in a protection system are found to prevent undesirable outages and increase system reliability (Jazaeri et al. 2015), unfortunately, the conventional offline (local) protection coordination schemes are unable to treat the uncertainties that affect their performance with little success in dealing with uncertainties in the network topology (Conti and Nicotra 2009; Conti 2009). Alternatively, a global protection scheme can utilize the probability of correct operation of various components (i.e., circuit breakers, communication links, etc.) as a priori data for a proper decision making before cascading outages (Hosseini et al. 2016a). As well as the correct operations of protection components, the microgrid topology is also subject to unpredictable variations.

3 Proposed Method

According to Fig. 2, to implement proposed method of this paper, a central server which is connected to CB modules via communication links is used. CB modules are placed at two ends of all lines and are responsible for performing

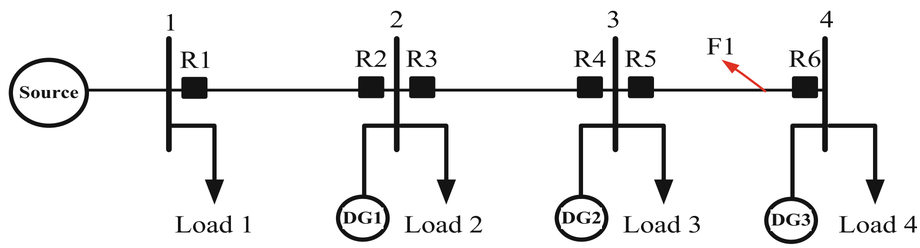

Fig. 1 Sample network with local adaptive protection coordination

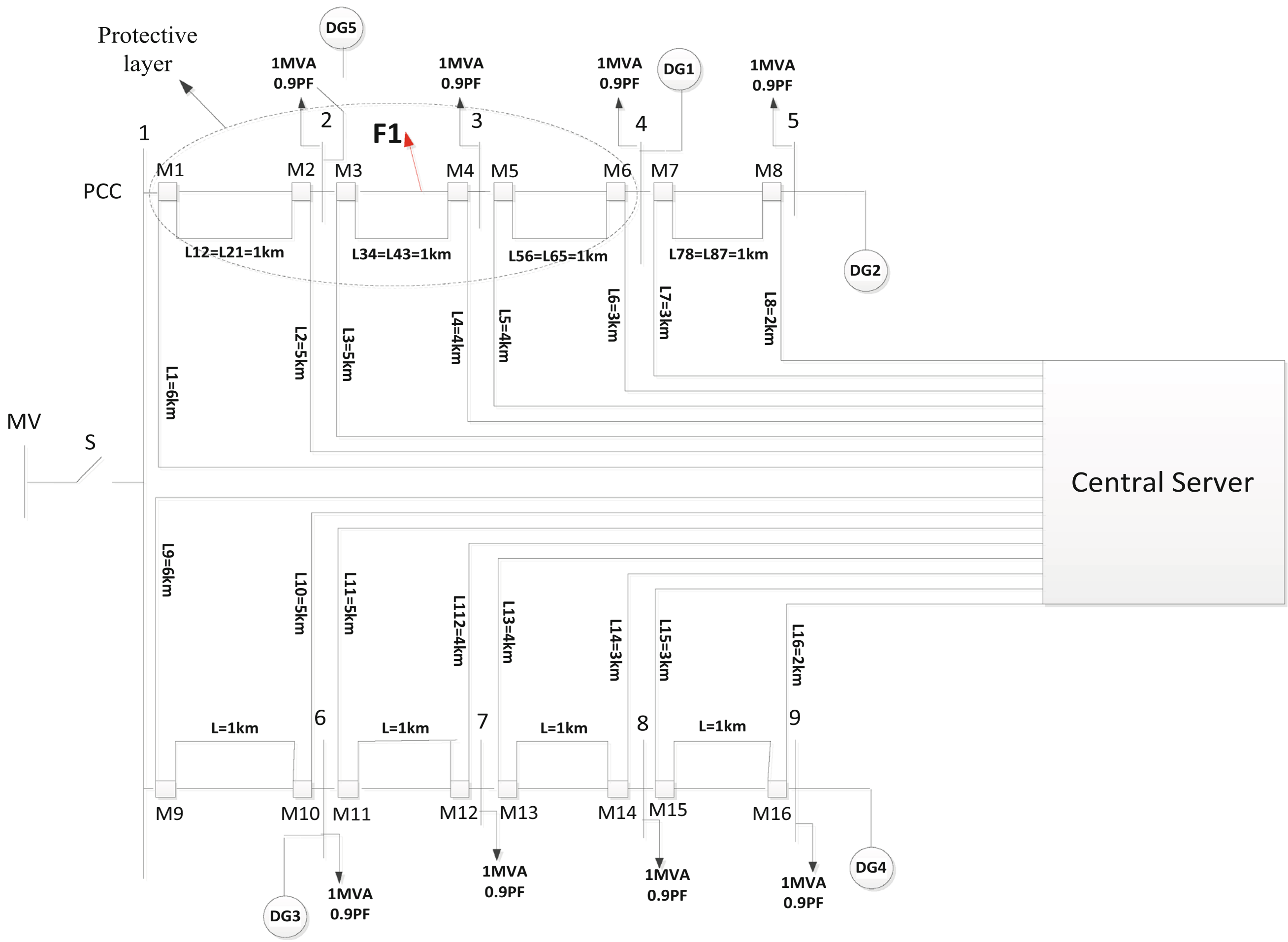

Fig. 2 Creating the proposed protection coordination using central server

commands received from central server. To identify the best strategy of clearing faults, just after detecting a fault, central server creates a protective layer around the fault. Protective layer is comprised of CB modules in which the faults have occurred in their connecting line and modules of their neighboring lines. For example, as presented in Fig. 2, for a fault in F1, the protective layer includes M_1–M_6 modules. After creating the protective layer, central server selects the sequence of implementing strategies which is able to clear the fault according to microgrid topology and probability of correct operation of CB modules and communication links in a way that the predicted protective purposes are formed in the best way.

Creating optimal sequence of implementing strategies results in decision tree. Decision tree is an efficient and strong tool for classification and decision making for high-dimensional data spaces (Kar and Ranjan Samantaray 2015). Decision tree is based on the previous data of system and can be used for classifying new data (Kar 2017). It also can estimate the behavior of the system by using and analyzing a learning set. Decision tree has been suggested in Kar and Ranjan Samantaray (2015), Kar (2017), Mishra et al. (2016) and Kar et al. (2015) to detect faults in microgrids. However, in this paper, it is used for providing protection coordination in microgrids.

Similar to Fig. 3, the proposed decision tree is made of branches and decision points (DP). DPs are the best strategies which are able to provide the best protection coordination according to microgrid exploitation situations and healthiness of protection system. Each branch is made by a factor which causes the best strategy to fail in clearing fault, and transfers the tree to a new DP.

To reduce calculations required for forming decision tree, as it is clear from Fig. 3, decision tree is suggested to be made layer by layer. In each layer, two levels of DPs are identified which consist of DP1 and DP2s. Each DP2 strategy is created for one of the factors for failure of DP1 strategy.

With identifying strategies of each layer, these strategies are implemented for clearing fault by the central server. If the fault remains, as illustrated in Fig. 3, the next layer would be created from the point, where strategies of the previous layer have failed to succeed. The process of identifying each layer of decision tree includes, producing strategy, identifying candidate strategies, assessing strategies, filtering, and calculating index.

3.1 Producing Strategy

Each strategy identifies CB modules which should operate with central server command for fault clearing and communication links which the central server uses to issue the command. Total number of strategies, which are able to clear fault, is proportional to the number of CB modules in protective layer and the number of communicating links between central server and each CB module and is calculated by Eq. (1) for radial networks:

$$N_{\mathrm{S}} = (N_{\mathrm{L}} \times N_{\mathrm{R}} \times N_{\mathrm{Link}}^2) - (N_{\mathrm{Link}} - 1), \tag{1}$$

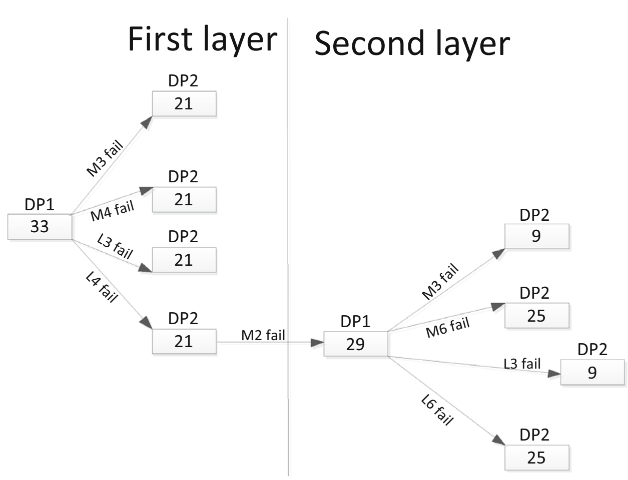

Fig. 3 Decision tree for F1 fault in network of Fig. 2 when DG5 is OFF

where N_{S} is the number of strategies of each protective layer, N_{Link} is the number of communication links that the central server can use to access each CB module, and N_{L} and N_{R} are the number of CB modules on right hand and left hand of fault, respectively.

Since in smart grids, communication links are used as mesh topology (Nguyen and Flueck 2011), in this paper, this combination is assumed for communication links. Accordingly, in Fig. 2, central server has access to each CB module via two links ($N_{\mathrm{Link}} = 2$). For instance, central server can command M_4 module via links L_4 and L_{34}. This combination increases reliability of communications of the proposed plan (Hajian-Hoseinabadi 2013). Therefore, in Fig. 2, the number of strategies which are able to clear the fault are 35 ($N_{\mathrm{S}} = (3 \times 3 \times 2^2) - (2 - 1) = 35$). Table 1 presents all possible strategies in protective layer to clear fault F1.

3.2 Identifying Candidate Strategies

The next step of forming each layer of decision tree is identifying strategies which can be a candidate to be placed in DPs of that layer. This is done according to different situations of failure of the previous strategies and layers. For example, Table 2 illustrates the candidate strategies for DP2 of the first layer in which strategy number 1 is candidate strategy for DP1 of this layer. As it is clear from this table, for all four reasons of failure of strategy number 1, appropriate DP2 strategies are the candidate.

3.3 Assessing Candidate Strategies

To ensure that the candidate strategy can clear the fault successfully, it is required that all its components, including CB modules and communication links, carry out their duty successfully. To understand the probability of correct operation of each strategy ($P_{\mathrm{Success}}(t_{\mathrm{D}}, I_{\mathrm{F}})$) against fault, Eq. (2) is presented. According to this equation, $P^s_{\mathrm{Success}}(t_{\mathrm{D}}, I_{\mathrm{F}})$ is composed of probability of simultaneous correct operation of CB modules ($P^s_{\mathrm{Success}_{M_s}}(t_{\mathrm{D}}, I_{\mathrm{F}})$) and communication links ($P^s_{\mathrm{Success}_{L_s}}(t_{\mathrm{D}})$) involved in sth strategy. In this equation, the unit of all currents is ampere and the unit of times is second:

$$\begin{aligned} P^s_{\mathrm{Success}}(t_{\mathrm{D}}, I_{\mathrm{F}}) &= P^s_{\mathrm{Success}_{M_s}}(t_{\mathrm{D}}, I_{\mathrm{F}}) \times P^s_{\mathrm{Success}_{L_s}}(t_{\mathrm{D}}) \\ &= \prod_{M=1}^{M_s} P^s_M(t_{\mathrm{D}}, I^M_{\mathrm{F}}) \cdot \prod_{L=1}^{L_s} P^s_L(t_{\mathrm{D}_L}), \end{aligned} \tag{2}$$

where $P^s_M(t_{\mathrm{D}}, I^M_{\mathrm{F}})$ and $P^s_L(t_{\mathrm{D}_L})$ are probability of correct operation of the Mth CB module and the Lth communication link, respectively. t_{D_L} and I^M_{F} are latency of the Lth communication link and fault current flowing through the Mth CB module, respectively. In addition, M_s and L_s are all

Table 1 Possible strategies in protective layer for clearing F1 fault in Fig. 2

Number	Strategy components	Number	Strategy components	Number	Strategy components
1	M_1–M_4–L_1–L_4	13	M_2–M_4–L_2–L_4	25	M_3–M_5–L_3–L_5
2	M_1–M_4–L_1–L_{34}	14	M_2–M_4–L_2–L_{34}	26	M_3–M_5–L_3–L_{65}
3	M_1–M_4–L_{21}–L_4	15	M_2–M_4–L_{12}–L_4	27	M_3–M_5–L_{43}–L_5
4	M_1–M_4–L_{21}–L_{34}	16	M_2–M_4–L_{12}–L_{34}	28	M_3–M_5–L_{43}–L_{65}
5	M_1–M_5–L_1–L_5	17	M_2–M_5–L_2–L_5	29	M_3–M_6–L_3–L_6
6	M_1–M_5–L_1–L_{65}	18	M_2–M_5–L_2–L_{65}	30	M_3–M_6–L_3–L_{56}
7	M_1–M_5–L_{21}–L_5	19	M_2–M_5–L_{12}–L_5	31	M_3–M_6–L_{43}–L_6
8	M_1–M_5–L_{21}–L_{65}	20	M_2–M_5–L_{12}–L_{65}	32	M_3–M_6–L_{43}–L_{56}
9	M_1–M_6–L_1–L_6	21	M_2–M_6–L_2–L_6	33	M_3–M_4–L_3–L_4
10	M_1–M_6–L_1–L_{56}	22	M_2–M_6–L_2–L_{56}	34	M_3–M_4–L_3–L_{34}
11	M_1–M_6–L_{21}–L_6	23	M_2–M_6–L_{12}–L_6	35	M_3–M_4–L_{43}–L_4
12	M_1–M_6–L_{21}–L_{56}	24	M_2–M_6–L_{12}–L_{56}		

Table 2 Sample of identifying candidate strategies for each layer

Candidate DP1 strategy	Defective component	Candidate DP2 strategies
1	M_1	13–35
	M_4	5–12, 17–32
	L_1	3, 4, 7, 8, 11–14, 17, 18, 21, 22, 25–35
	L_4	2, 4–12, 14, 16, 17–26, 29, 30, 34

CB modules and communication links involved in sth strategy, respectively.

3.3.1 Probability of Correct Operation of CB Modules in Each Strategy

The probability of correct operation of CB module is a function of fault current passing through it and its duration (Jazaeri et al. 2015; Binh Dam and Meliopoulos 2006). Accordingly, in this paper, probability of correct operation of CB modules is obtained from Eq. (3) (Jazaeri et al. 2015). In this equation, the unit of all currents is ampere and the unit of t_s is second:

$$P_M(t_\mathrm{D}, I_\mathrm{F}) = \begin{cases} 1; & \text{if } I_\mathrm{F}^M(t) \le I_\mathrm{R}^M \\ 1 - (I_\mathrm{F}^M - I_\mathrm{R}^M) \cdot t_s; & \text{if } I_\mathrm{U}^M > I_\mathrm{F}^M(t) > I_\mathrm{R}^M \\ 0; & \text{if } I_\mathrm{F}^M(t) \ge I_\mathrm{U}^M \end{cases}, \tag{3}$$

where t_s and I_R^M are time of implementing the sth strategy and rated current of the Mth CB module, respectively. According to Eq. (3), if fault current of the Mth module was less than I_R^M, this module would certainly carry out the commands from central server correctly. In addition, if fault current flowing through this module was higher than I_U^M (the upper failure threshold of CB module), this module would certainly fail to operate. In addition, if the fault current was between I_R^M and I_U^M, the probability of correct operation of this module would be $0 < P_M(t_\mathrm{D}, I_\mathrm{F}) < 1$ (Jazaeri et al. 2015).

3.3.2 Probability of Correct Operation of Communication Links in Each Strategy

The type of dependency on communication links, which is chosen in this paper, is indirect interdependencies, which is presented in Falahati and Yong (2014). Based on Falahati and Yong (2014), although a problem in a communication link causes a strategy to fail, the presented protection coordination plan can change performance and substitute another strategy by moving on appropriate branch.

The term “probability of correct operation of communication links” means that commands issued by central server reach each CB module in appropriate time. According to Nguyen and Flueck (2011), the probability of correct operation of communication links depends on their latency and their latency depends on link type and its length (Xiaoyang et al. 2013).

It should be noticed that in the presented plan, CB modules of each strategy operate simultaneously during fault. Therefore, in each strategy, some links may have more latency than the standard defined latency ($t_{\mathrm{D-Standard}}$) which is obtained using Eq. (4) (Xiaoyang et al. 2013):

$$t_{\mathrm{D-Standard}} = \tau \left(\frac{\mathrm{ms}}{\mathrm{km}}\right) \times d\ (\mathrm{km}), \tag{4}$$

where d is the length of communication link and τ is the propagation delay which depends on the type of communication link.

Excessive latency is the time that the command of central server reaches the CB which is located the farthest distance to the server. Accordingly, in Eq. (2), the probability of correct operation of communication links in the sth strategy is the probability of data transfer in a time which is less than maximum standard latency in communication links of that strategy ($t^{s}_{\mathrm{D\_Max}}$). Therefore, using probability density function proposed in Nguyen and Flueck (2011), Eq. (5) is written to calculate probability of correct operation of communication links in the sth strategy:

$$P^{s}_{\mathrm{Success}_{L_s}}(t_{\mathrm{D}}) = P^{s}_{\mathrm{Success}_{L_s}}(t^{s}_{\mathrm{D}} \le t^{s}_{\mathrm{D\_Max}}) = \prod_{L=1}^{L_s}\left(\sum_{i=p_L}^{P^{s}_{\mathrm{m}}} P(i)\right), \tag{5}$$

where P_L is the point associated with probability of correct operation of the Lth link and P^{s}_{m} is the point number associated with probability of correct operation of communication link with maximum latency in the sth strategy in table of distribution probability of communication links.

According to Eq. (3), in addition to the current magnitude, the time of applying the strategy (t_s) also affects probability of success of CB modules. The time of applying the sth strategy is the time that the process of applying strategies in decision tree reaches the point, where the sth strategy is identified as the best strategy for clearing the fault. Therefore, to calculate applying time of the sth strategy, the time of passing through other strategies should also be mentioned. According to Eq. (5), time of passing through each strategy equals the maximum latency of communication links of that strategy. Accordingly, in Eq. (6), the time of applying the sth strategy is equal to summation of maximum latency of communication links of the previous strategies plus the maximum latency of active communication links of the sth strategy:

$$t_s = t^{s}_{\mathrm{D\_Max}} + \sum_{j=1}^{s-1} t^{j}_{\mathrm{D\_Max}}. \tag{6}$$

3.4 Filtering

In this paper, two factors are considered to create decision tree. The first factor is that the fault clears with the least possible outages ($\mathrm{Min}(L_{\mathrm{Loss}})$) and the second is that the priority of strategies in DPs is that faults clear with highest probability of correct operation of protection system ($\mathrm{Max}(P_{\mathrm{Success}})$). Accordingly, for each layer, strategies have a chance to be selected in DP layers which have the highest probability of correct operation or have the least outages. Although for two strategies which have a similar outages rate or probability of correct operation, the strategy which has the highest probability of correct operation or the least outages rate remains in the output of the filter, respectively. In addition, if all parameters of two or more strategies were similar, one of them is selected.

3.5 Calculating Indices and Identifying Sequence of Strategies in Under Study Layer

In filter output, for each failure of candidate DP1, several DP2 s might be candidate. To decide the best strategy among DP2 remaining strategies, Eq. (7) is written. In Eq. (7), I_{S} is strategy index, L_{Total} is total load of microgrid, $L^{\mathrm{DP1}}_{\mathrm{Loss}}$ and $L^{\mathrm{DP2}}_{\mathrm{Loss}}$ are the amount of outages from DP1 and DP2 strategies, α and β are weighting coefficients of importance of outages by DP1 and DP2 strategies, and δ and λ are weighting coefficients of each considered index for forming decision tree, respectively. Since the lower the value of I_{S} index the better, weighting coefficient of α is considered higher than β to ensure that least possible outages occur by DP1.

Equation (7) has two sentences. The first sentence illustrates the load outage which is caused by DP1–DP2 candidate strategies which is normalized with the total load of the microgrid. The second sentence in Eq. (7) represents the probability of correct operation of candidate DP1–DP2 strategies. In this sentence, it is assumed that either the fault is cleared by DP1 strategy or if the DP1 strategy failed to clear the fault, the substitute strategy of DP2 clears the fault. Since the probability of correct operation of DP1–DP2 is desired to be more, this sentence is assumed to be reverse in Eq. (7), and besides, the first sentence of this equation, which shows the least possible outage caused by DP1–DP2 strategies, forms I_{S} index:

$$\begin{aligned} I_{\mathrm{S}} = {} & \delta\left(\frac{\alpha \cdot L^{\mathrm{DP1}}_{\mathrm{Loss}} + \beta \times L^{\mathrm{DP2}}_{\mathrm{Loss}}}{L_{\mathrm{Total}}}\right). \\ & + \lambda\left(\frac{1}{\left(\prod_{M=1}^{M_{\mathrm{DP1}}} P^{\mathrm{DP1}}_{M}(t_{\mathrm{DP1}}) \cdot \prod_{L=1}^{L_{\mathrm{DP1}}} P^{\mathrm{DP1}}_{L}(t^{\mathrm{DP1}}_{\mathrm{D\_Max}}) + \left(1 - \prod_{M=1}^{M_{\mathrm{DP1}}} P^{\mathrm{DP1}}_{M}(t_{\mathrm{DP1}}) \cdot \prod_{L=1}^{L_{\mathrm{DP1}}} P^{\mathrm{DP1}}_{L}(t^{\mathrm{DP1}}_{\mathrm{D\_Max}})\right)\right).\left(\prod_{M=1}^{M_{\mathrm{DP2}}} P^{\mathrm{DP2}}_{M}(t_{\mathrm{DP2}}) \cdot \prod_{L=1}^{L_{\mathrm{DP2}}} P^{\mathrm{DP2}}_{L}(t^{\mathrm{DP2}}_{\mathrm{D\_Max}})\right))}\right). \end{aligned} \tag{7}$$

After identifying DP2 strategy substituted for each failure of DP1 strategy, the most optimal DP1–DP2s strategies should be located in the layer of decision tree. For this purpose, Eq. (8) is used:

$$I_{\mathrm{P}}^{k} = \frac{1}{n_{\mathrm{f}}^{k}} \sum_{i=1}^{n} I_{\mathrm{S}i}^{k}, \tag{8}$$

where I_{P}^{k} is path index for the kth DP1 along with all its optimal DP2s. The value of $I_{\mathrm{S}i}^{k}$ for each DP1–DP2 composition is calculated using Eq. (7). In addition, n_{f}^{k} is the number of failures factors of the kth candidate strategy for DP1. According to Eq. (8), a composition of DP1 and its associated DP2s, which have the least value of I_{P}^{k} index is decided as the optimal composition in the decision tree.

Based on the aforementioned description, to create decision tree, the following steps should be carried out.

Step 1: Creating the protective layer.
Step 2: Identifying candidate strategies of DP1 in the protective layer.
Step 3: Analyzing candidate strategies using Eq. (2) and calculating amount of outages of each strategy.
Step 4: Filtering DP1 candidate strategies.
Step 5: Identifying DP2 strategies for DP1s of Step 4.
Step 6: Analyzing candidate strategies of Step 5 using Eq. (2) and filtering them.
Step 7: Identifying optimal DP2 strategy for each failure factor of DP1 candidate strategies, using Eq. (7).
Step 8: Identifying the most optimal DP1–DP2s composition as the superior strategies in the considered layer.
Step 9: Applying the identified DP1–DP2s of the layer for clearing the fault by central server.
Step 10: If the fault was not cleared, go to Step 2 and create the new layer from the point where previous layer is failed.

4 Simulation Results

To test efficiency of the proposed method of this paper, it is implemented on the sample microgrid, as shown in Fig. 2, which is also used in Najy et al. (2013). This system is fed from a primary distribution substation at bus 1. Five 2 MVA DGs are installed at buses 2, 4, 5, 6, and 9. The loads shown in Fig. 2 are the rated loads. Similar to Jazaeri et al. (2015), I_{R}^{M} and I_{U}^{M} of all CB modules are assumed to be 1.25 and 10 kA, respectively. Power loss of transmission lines is neglected and it is assumed that DG resources are able to supply loads in islanded mode.

Comparing to other cables, fiber optic cables have less latency and higher bandwidth (Nguyen and Flueck 2011). Therefore, these links are used for communication between central server and each CB module in this paper. Xiaoyang et al. (2013) have estimated standard latency of these links to be 0.005 $\left(\frac{\mathrm{ms}}{\mathrm{km}}\right)$; thus, this value is assumed for latency of communication links in the presented paper. Accordingly, the standard latency of communication links is presented in Table 3 according to the distance of CB module and central server. Latency of communication links between CB modules is proportionate with the line length.

According to the probability density function presented in Nguyen and Flueck (2011), the probability of correct operation of communication links in the presented study is assumed to be similar to values, as shown in Table 4.

To assess efficiency of the presented method, response of this method to a fault in F1 point of the network, as shown in Fig. 2, which is working in islanded mode in two states of with and without DG5, is investigated.

4.1 Assessing the Proposed Method when DG5 is OFF

As presented before, after fault in F1, protective layer is formed instantly and M_1–M_6 CB modules are selected as modules which have to clear the fault. Fault current which flows through each module of protective layer are presented in Table 5. As illustrated in Table 5, fault current of all CB modules is between I_{R}^{M} and I_{U}^{M}. Therefore, according to Eq. (3), probability of correct operation of CB modules of protective layer is between 0 and 1.

In the first layer of decision tree, all 35 introduced strategies in Table 1 can be candidate for clearing the fault in DP1 level. To identify strategies which have a chance to be located in DP1, operational situation of these 35 strategies is calculated in Table 6. According to Table 6, although in strategies 33–35, CB modules at two ends of the faulted line operate (modules of M_3 and M_4), there are also some outages. This issue is due to the fact that the sample microgrid is operating in islanded mode and with operation of M_3 and M_4 modules, DG3 and DG4 would not be able to supply the load of bus number 2, and this load must be disconnected.

After applying the filter, as illustrated in Table 6 (in italic), strategies 21 and 33 remain as candidate for DP1 of the first layer, since they have the highest successfulness probability and the lowest amount of outage, respectively. Therefore, situations of DP2 substituted strategies are analyzed only for these DP1 candidate strategies. Table 7 shows the situation of DP2 candidate strategies when they are substituted by strategy DP1 = 33. The time of implementing DP2 strategies is identified using Eq. (6). For

Table 3 Latency of communication links between central server and CB modules of Fig. 2

Module number	Latency (ms)	Module number	Latency (ms)	Module number	Latency (ms)
1	0.03	7	0.015	13	0.02
2	0.025	8	0.01	14	0.015
3	0.025	9	0.03	15	0.015
4	0.02	10	0.025	16	0.01
5	0.02	11	0.025		
6	0.015	12	0.02		

Table 4 Probability density function of the latency of the communication links

Point	Latency (ms)	Probability	Point	Latency (ms)	Probability
1	0.005	0.05	5	0.025	0.2
2	0.01	0.1	6	0.03	0.1
3	0.015	0.2	7	0.035	0.05
4	0.02	0.3			

Table 5 Short-circuit current of protective layers' modules when DG5 is OFF

Module number	Short-circuit current (kA)	Module number	Short-circuit current (kA)	Module number	Short-circuit current (kA)
1	3.96	3	3.96	5	4.42
2	3.96	4	4.42	6	4.42

Table 6 Situation of candidate strategies for DP1 in the first layer when DG5 is OFF

Strategy number	t_s (ms)	$P^s_{\text{Success}}(t_{\text{D}}, I_{\text{F}})$	L^s_{Loss} (MW)	Strategy number	t_s (ms)	$P^s_{\text{Success}}(t_{\text{D}}, I_{\text{F}})$	L^s_{Loss} (MW)
1	0.03	0.049	1	19	0.035	0.026	2
2	0.03	0.008	1	20	0.035	0.026	2
3	0.03	0.049	1	*21*	*0.025*	*0.12*	*2*
4	0.03	0.008	1	22	0.025	0.034	2
5	0.03	0.049	2	23	0.035	0.034	2
6	0.03	0.049	2	24	0.035	0.014	2
7	0.03	0.049	2	25	0.025	0.085	2
8	0.03	0.024	2	26	0.025	0.085	2
9	0.03	0.066	2	27	0.025	0.085	2
10	0.03	0.024	2	28	0.025	0.085	2
11	0.03	0.066	2	29	0.025	0.12	2
12	0.03	0.024	2	30	0.025	0.034	2
13	0.025	0.085	1	31	0.025	0.12	2
14	0.03	0.024	1	32	0.025	0.034	2
15	0.035	0.026	1	*33*	*0.025*	*0.085*	*1*
16	0.035	0.006	1	34	0.03	0.024	1
17	0.025	0.085	2	35	0.025	0.085	1
18	0.025	0.085	2				

instance, in Table 7, for strategy number 3, operation time equals $t_{33} + t_3 = 0.055$ (ms). It is clear from Table 7 that the probability of correct operation of strategies is reduced over the time.

Table 8 illustrates the amount of path index for each candidate DP1 and its superior DP2s. As it is clear, the lowest path index belongs to strategy DP1 = 33 and its complex of DP2 strategies. Therefore, according to Fig. 3,

Table 7 Situation of DP2 candidate strategies in the first layer for DP1 = 33

Strategy number	$P^{s}_{\mathrm{Success}}(t_{\mathrm{D}}, I_{\mathrm{F}})$	Strategy number	$P^{s}_{\mathrm{Success}}(t_{\mathrm{D}}, I_{\mathrm{F}})$	Strategy number	$P^{s}_{\mathrm{Success}}(t_{\mathrm{D}}, I_{\mathrm{F}})$
1	0.042	13	0.072	25	0.072
2	0.007	14	0.021	26	0.072
3	0.042	15	0.022	27	0.072
4	0.007	16	0.005	28	0.072
5	0.042	17	0.072	29	0.101
6	0.042	18	0.072	30	0.029
7	0.042	19	0.022	31	0.101
8	0.021	20	0.022	32	0.029
9	0.056	21	0.098	33	0.072
10	0.021	22	0.029	34	0.021
11	0.056	23	0.028	35	0.072
12	0.021	24	0.011		

Table 8 Amount of path index for the first layer when DG5 is OFF

Candidate strategy for DP1	Defective component	Superior candidate strategy for DP2	I_{P}	Candidate strategy for DP1	Defective component	Candidate strategy for DP2	I_{P}
21	M_2	29	8.4	33	M_3	21	8.1
	M_6	13			M_4	21	
	L_2	29			L_3	21	
	L_6	13			L_4	21	

Table 9 Amount of optimal DPs of the second layer when DG5 is OFF

Defective component of DP1 of layer 1	Defective component of DP2 of layer 1	Candidate DP1 strategies of layer 2	Filter output	Defective component	Candidate DP2 strategies of layer 2	Filter output	Superior strategy for DP2	I_{P}
L_4	M_2	2, 4–12, 25, 26, 29, 30, 34	29	M_3	2, 4–12	2, 9	9	11.7
				M_6	2, 4–8, 25, 26, 34	25, 34	25	
				L_3	5–12	9	9	
				L_6	2, 4, 5, 7, 10, 12, 25, 30, 34	25, 34	25	
			34	M_3	2, 4–12	2, 9	9	19.2
				M_4	5–12, 25, 26, 29, 30	25	25	
				L_3	5–12	9	9	
				L_{34}	5–12, 25, 26, 29, 30	25	25	

strategy 33 and its substitute strategies are located in DPs of the first layer. It should be mentioned that, since outages should be minimized by the first strategy, weighting coefficients of α and β are assumed to be 2 and 1, respectively, and to balance the sentences of Eq. (7), weighting coefficients of δ and λ are assumed to be 5 and 1, respectively.

As it is clear, the proposed method does not follow traditional rules of protection coordination, since it considers uncertainties which affect protection coordination. For example, according to the traditional rules of protection coordination, in case of M_3 module defects, it is expected that strategy 1 clear the fault as the backup

Table 10 Calculations of decision tree when DG5 = ON

The first layer calculations

Candidate strategy for DP1	Defective component	Superior candidate strategy for DP2	I_P	Candidate strategy for DP1	Defective component	Candidate strategy for DP2	I_P
21	M_2	33	8.26	33	M_3	21	7.13
	M_6	33			M_4	29	
	L_2	33			L_3	21	
	L_6	33			L_4	29	
29	M_3	21	7.38				
	M_6	33					
	L_3	35					
	L_6	33					

The second layer calculations

Defective component of DP1 of layer 1	Defective component of DP2 of layer 1	Candidate DP1 strategies of layer 2	Filter output	Defective component	Candidate DP2 strategies of layer 2	Filter output	Superior strategy for DP2	I_P
L_4	M_3	2,4-12,14,16-24	14	M_2	2, 4–12	2, 9	9	17.5
				M_4	5–12, 17–24	21	21	
				L_2	2, 5, 6, 9, 10, 16, 19, 20, 23, 24	2, 9	9	
				L_{34}	5–12, 17–24	21	21	
			21	M_2	2, 4–12	2, 9	9	11.6
				M_6	2, 4–8, 14, 16–20	14, 17	17	
				L_2	2, 5, 6, 9, 10, 16, 19, 20, 23, 24	2, 9	9	
				L_6	2, 4, 5, 7, 10, 12, 14, 16, 17, 19, 22, 24	14, 17	17	

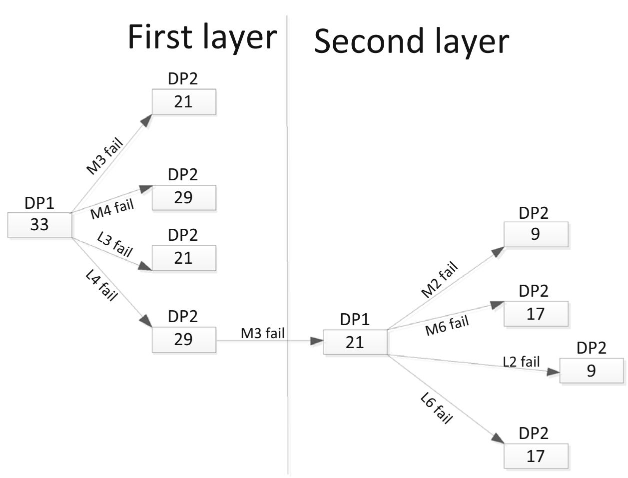

Fig. 4 Decision tree for F1 fault in network of Fig. 2 when DG5 is ON

strategy, but Fig. 3 shows that strategy 21, which also has a higher amount of outages, is substituted by strategy 33.

To explain the method of creating the next layers, it is assumed that strategy 33, due to a defect in L_4 link, and strategy 21, due to a defect in M_2 CB module, failed to clear the fault. In this case, central server has to create the second layer to test new strategies for clearing the fault. As it is clear from Fig. 3, creating the second layer starts from the point, where the first layer failed to clear the fault.

According to Fig. 3, in the second layer of decision tree, strategy 29 is selected for DP1 strategy and strategies 9 and 25 are selected as DP2 strategies of this layer and for each failure factor of strategy 29. Calculation results, associated with selection of optimal DPs of the second layer, are presented in Table 9. As it is clear, strategy 29 and its associated DP2s have the least values of I_P index. Comparing Tables 8 and 9 shows that the optimal I_P index in Table 9 is increased comparing to Table 8. This issue is due to reduction of probability of correct operation of strategies with the time.

4.2 Assessing the Proposed Method When DG5 is ON

To assess the presented method during changes of topology in microgrid, protection coordination in Fig. 2 is analyzed for a fault in F1 point when DG5 is ON.

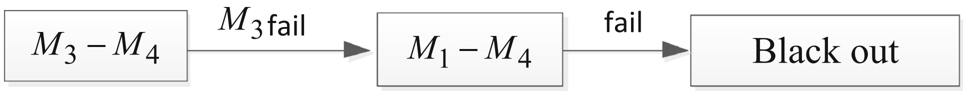

Fig. 5 Reaction of the proposed protection system in Ustun et al. (2012) during F1 fault and when DG5 is disconnected

Protective layer and candidate strategies for located in DPs of decision tree are shown in Table 1. Short-circuit analysis shows that in existence of DG5, fault current of M_3 module is increased to 6.75 (kA), while fault current of other modules is almost equal to values, as shown in Table 5. In addition, because DG5 is ON, there is no outage during operation of M_3 and M_4 modules (strategies 33–35). On the other hand, it is assumed that if the fault was not cleared by M_3 module, DG5 is disconnected due to central server command, to prevent the supply fault current. Therefore, amount of outages in other strategies are shown in Table 6.

Calculations of different DPs of decision tree are presented in Table 10. According to this table, decision tree for DG5 = ON is presented in Fig. 4. Comparing Figs. 3 and 4, it is obvious that the presented method was able to create the best possible coordination considering uncertainties.

Since one of the main problems of the previous studies was using offline reaction, the proposed method of this paper solved this problem appropriately, so that using online decisions, besides preventing saving too much information of settings for each microgrid operation topology, all possible situations that protection system may encounter are covered.

To test the presented method, it is compared with Ustun et al. (2012). In Ustun et al. (2012), the traditional protection coordination which is achieved with central server is used for clearing fault. Figure 5 represents the behavior of the protection system for F1 fault in Fig. 2 and when DG5 is disconnected. Comparing Figs. 3 and 5 shows that both methods use M_3–M_4 local modules as the first strategy. According to Fig. 3, if M_3 module failed, the strategy with M_2–M_6 modules would operate as the substitute strategy. The probability of correct operation of this strategy is 0.189 and amount of outage is 2 (MW). While the traditional method of study (Ustun et al. 2012) uses M_1–M_4 modules as the substitute strategy. The probability of correct operation of this strategy is 0.042. If M_1–M_4 failed to clear the fault, the probability of correct operation of substitute strategy decreases drastically, and according to Fig. 5, black out occurs in the system.

On this basis, using the proposed method, it is clear that the best strategy is decided according to the probability of successfulness of protection system and the network topology. Accordingly, the reliability of this method is higher than traditional methods. Furthermore, the proposed method enhances the shortcomings of similar studies such as Hosseini et al. (2016b) and El-Khattam and Sidhu (2009) which store lots of offline settings for protection coordination in different topologies.

5 Conclusion

To make the protection system able to respond to uncertainties which affect protection coordination of microgrid, using decision tree is proposed in this paper. Using decision tree, central server is able to be applied for clearing fault according to microgrid topology and the probability of correct operation of communication links and protection system, and implementing the best strategy for clearing fault, in a way that both the least outages occur and the fault is cleared with the highest probability of correct operation of protection system. Selecting optimal strategy for clearing fault does not necessarily lead to the closest protection systems to clear the fault and this issue represents the difference of the proposed approach to the traditional protective plans. As the simulation results illustrated, this method can be considered as an effective method for solving problems of microgrid protection coordination. In addition, because of using decision tree in online mode, it is not necessary to store a considerable amount of offline settings.

References

Basak P et al (2012) A literature review on integration of distributed energy resources in the perspective of control, protection and stability of microgrid. Renew Sustain Energy Rev 16:5545–5556

Binh Dam Q, Meliopoulos APS (2006) Failure probability methodology for overdutied circuit breakers. In: 38th North American power symposium. pp 667–672

Conti S (2009) Analysis of distribution network protection issues in presence of dispersed generation. Electr Power Syst Res 79:49–56

Conti S, Nicotra S (2009) Procedures for fault location and isolation to solve protection selectivity problems in MV distribution networks with dispersed generation. Electr Power Syst Res 79:57–64

Dewadasa M et al (2011) Fault isolation in distributed generation connected distribution networks. IET Gener Transm Distrib 5:1053–1061

Eissa MM et al (2010) A novel back up wide area protection technique for power transmission grids using phasor measurement unit. IEEE Trans Power Deliv 25:270–278

El-Khattam W, Sidhu TS (2009) Resolving the impact of distributed renewable generation on directional overcurrent relay coordination: a case study. IET Renew Power Gener 3:415–425

Falahati B, Yong F (2014) Reliability assessment of smart grids considering indirect cyber-power interdependencies. IEEE Trans Smart Grid 5:1677–1685

Fenghui R et al (2012) Conceptual design of a multi-agent system for interconnected power systems restoration. IEEE Trans Power Syst 27:732–740

Hajian-Hoseinabadi H (2013) Availability comparison of various power substation automation architectures. IEEE Trans Power Deliv 28:566–574

Hosseini SA et al (2015) Presenting a new method for identifying fault location in microgrids, using harmonic impedance. Iran J Sci Technol Trans Electr Eng 39:167–182

Hosseini SA et al (2016a) An overview of microgrid protection methods and the factors involved. Renew Sustain Energy Rev 64:174–186

Hosseini SA et al (2016b) Merging the retrieval of the protection coordination of distribution networks equipped with DGs in the process of their siting and sizing. J Renew Sustain Energy 8:035502

Jazaeri M et al (2015) Evaluation of the impacts of relay coordination on power system reliability. Int Trans Electr Energy Syst 25:3408–3421

Kai J, Singh C (2011) New models and concepts for power system reliability evaluation including protection system failures. IEEE Trans Power Syst 26:1845–1855

Kar S (2017) A comprehensive protection scheme for micro-grid using fuzzy rule base approach. Energy Syst 8:449–464. https://doi.org/10.1007/s12667-016-0204-x

Kar S, Ranjan Samantaray S (2015) A fuzzy rule base approach for intelligent protection of microgrids. Electr Power Compon Syst 43:2082–2093

Kar S et al (2015) Data-mining model based intelligent differential microgrid protection scheme. IEEE Syst J PP:1–9

Lim IH et al (2007) Multi-agent system-based protection coordination of distribution feeders. In: International conference on intelligent systems applications to power systems. pp 1–6

Liu CC et al (2000) The strategic power infrastructure defense (SPID) system. A conceptual design. IEEE Control Syst 20:40–52

Mahat P et al (2011) A simple adaptive overcurrent protection of distribution systems with distributed generation. IEEE Trans Smart Grid 2:428–437

Mishra DP et al (2016) A combined wavelet and data-mining based intelligent protection scheme for microgrid. IEEE Tran Smart Grid 7:2295–2304

Najy WKA et al (2013) Optimal protection coordination for microgrids with grid-connected and islanded capability. IEEE Trans Ind Electron 60:1668–1677

Nguyen CP, Flueck AJ (2011) Modeling of communication latency in smart grid. In: IEEE power and energy society general meeting. pp 1–7

Sortomme E et al (2010) Microgrid protection using communication-assisted digital relays. IEEE Trans Power Deliv 25:2789–2796

Su S et al (2006) Agent-based self-healing protection system. IEEE Trans Power Deliv 21:610–618

Ustun TS et al (2011) Recent developments in microgrids and example cases around the world—a review. Renew Sustain Energy Rev 15:4030–4041

Ustun TS et al (2012) Modeling of a centralized microgrid protection system and distributed energy resources according to IEC 61850-7-420. IEEE Trans Power Syst 27:1560–1567

Xiaoyang T et al (2013) The study of a regional decentralized peer-to-peer negotiation-based wide-area backup protection multi-agent system. IEEE Trans Smart Grid 4:1197–1206