IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received July 8, 2019, accepted August 2, 2019, date of publication August 12, 2019, date of current version August 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2934646

Source-Load Coordinated Reserve Allocation Strategy Considering Cyber-Attack Risks

QI WANG[1], (Member, IEEE), MENGYA LI[1], YI TANG[1], (Senior Member, IEEE), AND MING NI[2,3,4], (Senior Member, IEEE)

[1]School of Electrical Engineering, Southeast University, Nanjing 210096, China
[2]NARI Group Corporation (State Grid Electric Power Research Institute), Nanjing 211106, China
[3]NARI Technology Company Ltd., Nanjing 211106, China
[4]State Key Laboratory of Smart Grid Protection and Control, Nanjing 211106, China

Corresponding author: Qi Wang (wangqi@seu.edu.cn)

This work was supported by the Science and Technology Project of State Grid Corporation of China (Research on Cooperative Situation Awareness and Active Defense Method of Cyber Physical Power System for Cyber Attack).

ABSTRACT With the developing cyber physical power systems and emerging threat of cyber-attacks, the traditional power services are faced with higher risks of being compromised, as vulnerabilities in cyber infrastructure can be exploited to cause physical damage. Therefore, adjustments need to be made in current control scheme design methods to mitigate the impact of potential attacks on service quality. In this paper, focusing on the service of coordinated source-load participation in primary frequency regulation, a vulnerability analysis is performed with modelling the attack intrusion process, and the risk assessment of the service is made by further modelling the attack impacts on the service's physical effects. On that basis, the traditional coordinated reserve allocation optimization model is modified and the allocation scheme is corrected according to the cyber-attack impacts. The proposed correction methods are validated through a case study, showing effectiveness in defending against the cyber-attack impacts.

INDEX TERMS Attack mitigation, cyber physical system security, coordinated control, risk assessment.

I. INTRODUCTION

In the construction of smart grids, cyber physical power systems (CPPS) and the future ubiquitous power internet of things, more entities are engaged in traditional power system services, bringing huge changes to the control methods and implementation process. Control commands are generated and given in real time, and together with a flexible mixture of hierarchical and distributed control structures, the complexity of control has been greatly improved. Moreover, with closer integration of cyber and physical space in the smart grid, the reliability of control has greater and more immediate influence on the secure operation of the power systems [1], [2]. It is important to design a reliable coordinative control method according to the nature of a service, to address the relations between control logic, communication process and physical response, and to guarantee the service can function normally.

In recent years, cyber-attacks have emerged as a new type of threatening cyber layer vulnerabilities in the current smart grid [3]. Since the 2015 Ukrainian blackout, the possibility and severity of attack induced power system failures have raised concern in the academia, and researches have been performed in the areas of cyber-attack modelling, risk assessment, prevention and mitigation. Cyber threats towards smart grid are reviewed in [4], [5], summarizing the security aims, potential attack methods and targeted use scenarios. The attack mitigation on cyber side is to take general information security measures, such as encryption [6], virtual private network, access management, authentication [7] and the currently developing techniques of trustworthy computation and blockchain [8]. Mitigation on physical side can use physical rules to recover corrupted data [9], correct false commands [10] and deploy backup resources to compensate for the attacked assets [11]. The cyber side protection measures are designed for computer systems originally, which may not meet the real-time requirement or suit the physical environment for CPPS and cannot be installed, leaving vulnerabilities. Meanwhile, exploitation of zero-day vulnerabilities can cause worse consequences in CPPS, as attacks will result in loss of power supply and affect the public directly.

The associate editor coordinating the review of this article and approving it for publication was Zhiyi Li.

The physical side protection can be implemented in addition to the cyber side measures to improve the security, but protection from both sides should be coordinated carefully, so that the vulnerabilities can be covered and the coordinated scheme balances the needs of security, reliability and efficiency.

One effective way to coordinate cyber and physical side control is using the control logic of a service to establish the cyber-physical interdependency [12], [13]. Research has proposed a service-oriented cyber physical system design method addressing the importance of service quality [14], which integrates the cyber and physical side effect according to services. Some cyber-attack modeling methods have taken into consideration the construction of the corresponding relations between certain attack types and physical impacts [15], and designed service-specified attack [16], [17] and defense methods [18], [19]. However, current researches usually only use the interdependency to interpret the cyber side erroneous data to physical impacts, whereas the uncertainty of attacks and attack vectors, which describe the attack process from intrusion points to target devices and the modification attackers make, are not fully used.

In this paper, the focus is put on the service of primary frequency regulation in power systems with coordinated participation of generating units and demand response (DR) resources. Section II establishes the cyber-attack models for cyber and physical side, and performs vulnerability analysis in the service scenarios. Section III proposes a modified coordinated frequency regulation reserve allocation model based on the vulnerability analysis and risk assessment results. A case study based on IEEE 14 bus system is presented in Section IV to validate the proposed methods, and conclusions are given in Section V.

II. FREQUENCY REGULATION PERFORMANCE CONSIDERING CYBER-ATTACK RISKS

Primary frequency regulation is a service that functions in seconds after a disturbance. Traditional method is using the inertia and automatic local control to put into effect the spinning reserves in the generating units to regulate the frequency in a short time. With the improved communication systems and demand side management techniques, interruptible loads can be used as frequency regulation reserves as well. Considering the response time limit, the main demand response services that can collaborate with spinning reserves and participate in primary frequency regulation are direct load control (DLC) and distributed demand response (DDR). The features and vulnerabilities of both are analyzed below.

A. VULNERABILITY ANALYSIS OF LOAD CONTROL SCHEMES

The control and communication design of a load control service is crucial to the determination of the possible cyber-attack threat it is facing. To identify a potential threat, the control method and communication network design of a service have to be examined.

The physical structure of the CPPS control system typically consists of several layers. The top layer is the control center, also called master station, where SCADA, human machine interface (HMI) and network management system are deployed, and all actions in the system are monitored there. It is often well-defended, with a security perimeter that stops the attacks physically and virtually. For example, personnel will have to be authorized to enter and operate, and firewalls are installed to screen the data traffic. The intermediate layer is the communication system, the main function of which is to transmit orders and data, while usually only simple computation may happen in the slave station. The slave stations are likely to have access control as a method of protection. The bottom layer is the terminals, which includes the field devices, load controllers and other terminal devices. The terminals are vastly distributed in the user side, and are not often fully protected.

For direct load control service, the control action takes the following steps to effectuate: 1) the master station generates a control order according to real-time system power shortage and predefined control strategy; 2) the order, in the form of a message, is passed from the master station to a slave station and finally distributed to the corresponding load control terminal; 3) the terminal takes action as instructed by the order. The control strategy is typically made offline through simulations, and it contains a table that provides a specific scheme for each value of power shortage. The scheme will include how much load will be shed, which load will be commandeered and the time when the shedding order should be given. To reduce the latency during the process, the messages are not always encrypted, which increases the possibility of integrity attacks. Also, the control messages travel through several nodes before reaching the terminals, making it vulnerable to availability attacks, such as denial-of-service (DoS) attacks aiming at the communication network.

For distributed demand response, the control actions are implemented locally with preset action thresholds and real-time on-site measurements. The lack of real-time control order transmission makes the service immune to data alteration or loss due to attacks aiming at communication network, but the distributed method makes it harder to examine the authenticity of the preset thresholds by crosschecking. Therefore, the attackers can launch distributed false data injection attacks (DFDIA) to the locally stored action thresholds and change the preset values, or give fake commands to the control terminals and disguise the attack as a normal update of settings. The altered action threshold setting can cause unnecessary load shedding during normal operation, or deficient load shedding during fault.

However, the services are under certain levels of protection, designed according to standards and protocols. In order to successfully carry out an attack, attackers have to find necessary vulnerabilities to exploit in order to breach the deployed defenses. The types of typical attack threats to DLC and DDR and the vulnerabilities required for each type are summarized in Table 1.

TABLE 1. Vulnerability combinations required for successful attacks with different methods and targets.

Target service	Attack method	Target location	CIA vulnerability needed
DLC	DoS attack	Master station	Availability vulnerability in communication management system
		Slave station	Availability vulnerability in server/router
		Control terminal	Availability vulnerability in field device
DDR	DFDIA	Control terminal	Confidentiality vulnerability in terminal (if terminal has encryption); integrity vulnerability in terminal
	Fake command attack	Master station	Confidentiality and integrity vulnerability in SCADA
		Communication network	Confidentiality vulnerability of communication network; Integrity vulnerability in application

The combinations are composed with the following information regarding one attack attempt: 1) the attack method, to decide the properties of the devices that need to be compromised, i.e., the confidentiality, integrity and availability (CIA) security aims; 2) the attack target, which the attack finally gains the control of and make modification to; and 3) the propagation path, which may consist of several network locations and require vulnerability exploitation along the steps. The attack targets may not be the terminal devices which carry out the physical actions directly, but the location where false actions take place. With the vulnerability combination, the attack propagation process on the cyber side can be constructed and the attack successful rate can be evaluated.

Given the vulnerability combination, the occurrence probability of a successful attack can be calculated using the occurrence probabilities of the vulnerabilities. Therefore, the occurrence probabilities of above listed attacks are given as follows.

$$P_{DoS} = 1 - \prod_{k=1}^{n_a} \left(1 - P_{a,k}\right) \tag{1}$$

$$P_{DFDIA} = P_{i,ter} \cdot P_{c,ter} \tag{2}$$

$$P_{FC} = P_{i,cen} \cdot P_{c,cen} + P_{i,app} \cdot P_{c,app} \tag{3}$$

P_{DoS} is the occurrence probability of DoS attacks, $P_{a,k}$ is the occurrence probability of availability vulnerability at k-th device, n is the total number of devices in the command transmission process. P_{DFDIA} is the occurrence probability of DFDIA, $P_{i,ter}$ and $P_{c,ter}$ are the occurrence probabilities of integrity vulnerability and confidentiality vulnerability at terminals, respectively. P_{FC} is the occurrence probability of fake command attacks, $P_{i,cen}$ and $P_{c,cen}$ are the occurrence probabilities of integrity vulnerability and confidentiality vulnerability at control center SCADA, $P_{i,app}$ and $P_{c,net}$ are the occurrence probabilities of integrity vulnerability at applications and confidentiality vulnerability at communication network.

B. SYSTEM FREQUENCY RESPONSE MODEL WITH DR PARTICIPATION

The low-order system frequency response (SFR) model [20] as shown in Fig. 1, is widely used in power system frequency analysis to evaluate the frequency dynamics of power systems after disturbances. This model involves the thermal generator units as the frequency regulation resources.

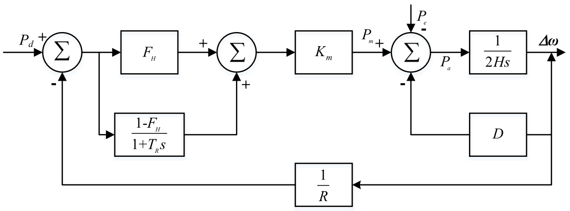


FIGURE 1. Traditional system frequency response model.

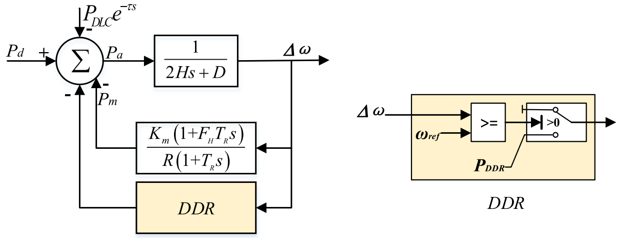
In the model, T_R is the reheat time constant, usually ranging in 6∼12s; H is system time constant, usually ranging in 3∼6s and representing system inertia. R is the governor regulation coefficient, typically ranging in 4%∼6%. P_d is the power disturbance, P_m is the mechanical power output and P_e is the electrical power output. $\Delta\omega$ is the frequency deviation. F_H is the fraction of total power generated by the steam turbine. D is the equivalent damping factor, and K_m is the mechanical power gain factor.

As DR takes part in providing capacity for frequency regulation, the basic SFR model needs to be modified to represent the influence of DR participation on frequency response after disturbances. The modification is made according to analysis of the action methods and load regulation effects of DR services.

DLC is to remove an amount of load at a certain moment after the disturbance, the effect of which can be modelled as a step signal change in power imbalance after a time delay. Meanwhile, DDR is triggered by the real-time local frequency deviation, and the loads are shed when frequency deviation is greater than the preset action threshold. Because DLC and DDR both only act to reduce the amount of load, which can be equivalent as reducing the power imbalance in the case of supply shortage, the effects of both services can be linearly added to the original model, as a change in the input P_d. Therefore, the SFR model with modification representing the effects of DLC and DDR is given in Fig 2 (a), while the dynamics of DDR service is described in detail in Fig 2 (b).

The transfer function of the SFR model with DLC and DDR participation is given as

$$\Delta\omega\left(t\right) = \Delta\omega_d\left(t\right) - \Delta\omega_{DLC}\left(t\right) - \Delta\omega_{DDR}\left(t\right), \tag{4}$$



(a) (b)

FIGURE 2. (a) Modified system frequency response model with DLC and DDR participation; (b) DDR action logic model.

where

$$\omega_n^2 = \frac{DR+K_m}{2HRT_R}, \tag{5}$$

$$\xi = \frac{2HR+(DR+K_mF_H)\,T_R}{2\,(DR+K_m)}\omega_n, \tag{6}$$

$$\omega_{\mathrm{r}} = \omega_n\sqrt{1-\xi^2}, \tag{7}$$

$$\alpha = \sqrt{\frac{1-2T_k\xi\omega_n+T_R^2\omega_n^2}{1-\xi^2}}, \tag{8}$$

$$\phi = \phi_1-\phi_2=\tan^{-1}\left(\frac{\omega_r T_R}{1-\xi\omega_n T_R}\right)-\tan_1\left(\frac{\sqrt{1-\xi^2}}{-\xi}\right), \tag{9}$$

$$\Delta\omega_d\,(t) = \left(\frac{RP_d}{DR+K_m}\right)\left[1+\alpha e^{-\xi\omega_n t}\sin\left(\omega_r t+\phi\right)\right], \tag{10}$$

$$\Delta\omega_{DLC}\,(t) = \left(\frac{RP_{DLC}}{DR+K_m}\right)\left[1+\alpha e^{-\xi\omega_n(t-\tau_{DLC})}\times\sin\left(\omega_r\left(t-\tau_{DLC}\right)+\phi\right)\right], \tag{11}$$

$$\Delta\omega_{DDR}\,(t) = \left(\frac{RP_{DLC}}{DR+K_m}\right)\left[1+\alpha e^{-\xi\omega_n(t-\tau_{DDR})}\times\sin\left(\omega_r\left(t-\tau_{DDR}\right)+\phi\right)\right]. \tag{12}$$

P_{DLC} is the load shedding amount of DLC, and τ_{DLC} is the corresponding action time when the DLC service cuts off the loads. Similarly, P_{DDR} is the load shedding amount of DDR, and τ_{DDR} is the corresponding time when the DDR load shedding actions. Considering the fact that there may be several rounds of load shedding in an actual load control scheme, the effect of each round will be linearly added to the existing equation.

III. COORDINATED RESERVE ALLOCATION SCHEME CONSIDERING CYBER-ATTACK RISKS

A. DR CAPACITY ASSESSMENT CONSIDERING THE IMPACTS OF CYBER-ATTACKS

With the frequency response model above, it can be deduced that the effect of DR participation on frequency regulation depends on the following key parameters: response power and the action time. The total response power determines the final frequency value, while the action time influences the transient dynamics. In the case of primary frequency regulation, the main focus is the final frequency recovery result. Therefore, the amount of DR power that can be utilized in the frequency regulation needs to be evaluated, in order to determine the reserve amount on generation and load sides that can satisfy frequency requirements.

Following assumptions are made when assessing the DR capacity under attacks:

1) Attackers will fully use the authority gained and maximize the impacts, i.e., the DoS attacks will stop the load controllers from switching on/off the loads, instead of just delaying the switching actions, and the DFDIA and fake commands will change the terminal threshold setting to any arbitrary value.

2) Considering the hierarchical control method of DLC, if the attacker gains access to a master station, they will attack all the load controllers deployed under the station; similarly, if a slave station is compromised, all the load controllers under the slave station will be under attack. DDoS attacks directly aimed at a control terminal will only affect the single targeted controller.

3) Considering the distributed control method of DDR, each control terminal must be compromised and attacked individually. The attacker can either use DFDIA or a fake command to change the setting of one terminal at a time.

With the assumptions to simplify the attack conditions and using the attack probability estimation from vulnerability analysis, the availability of each DR load can be determined, and the expected DR capacity of the system under cyber-attack risks can be assessed through Monte Carlo simulation.

The Monte Carlo sampling process of DLC load availability is shown in Fig. 3. Due to the hierarchical control method, the sampling also follows the order of master station – slave stations – terminals. After sampling the availability of each load, the DLC response potential is obtained through aggregating the loads into rounds with the same initialization conditions, and the parameters of a round k are expressed as a tuple $(P_{DLC,k}, \tau_{DLC,k})$, where $P_{DLC,k}$ denotes the capacity of the kth round DLC and $\tau_{DLC,k}$ denotes the initialization time.

The Monte Carlo sampling process for DDR load status is simpler due to the nature of the distributed control. The attack result of each load is directly and individually randomized according to the attack probability of DFDIA and fake command attack, and the altered threshold values are randomly chosen from potential attack schemes as well. After the sampling, the DDR response potential is obtained through aggregating the loads with same action threshold into different groups, denoted with the tuple $(P_{DDR,k}, f_{DDR,k})$, where $P_{DLC,k}$ denotes the capacity of the kth round DDR and $f_{DDR,k}$ denotes the action frequency threshold, which can be transformed into action time instant $\tau_{DDR,k}$ with time domain simulation. Additional time delay that may occur during the action process caused by dead zone or computation can be added to τ_{DDR} as well.

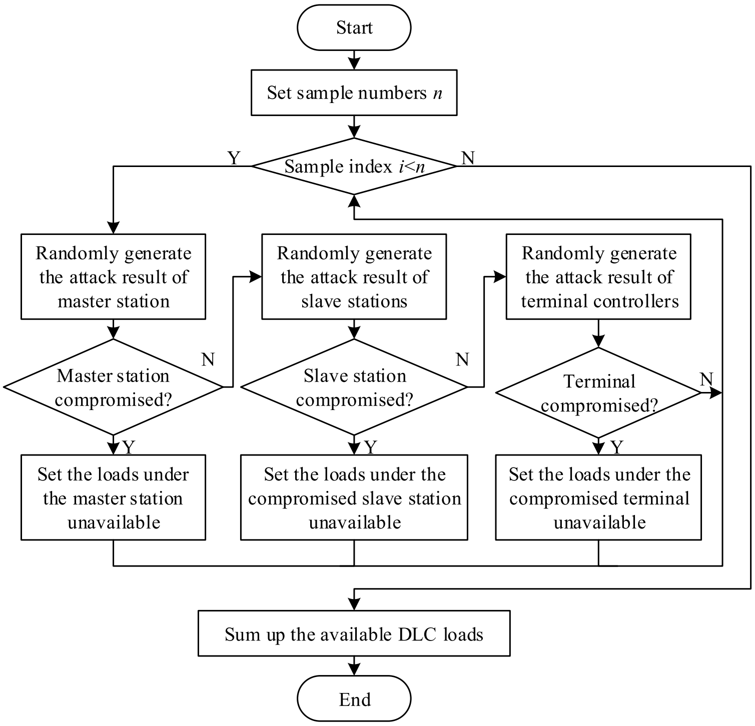

Start
Set sample numbers *n*
Sample index *i*<*n*
Y
N
Randomly generate the attack result of master station
Randomly generate the attack result of slave stations
Randomly generate the attack result of terminal controllers
Master station compromised?
Slave station compromised?
Terminal compromised?
Set the loads under the master station unavailable
Set the loads under the compromised slave station unavailable
Set the loads under the compromised terminal unavailable
Sum up the available DLC loads
End

FIGURE 3. Flowchart of DLC response capacity assessment process based on monte carlo simulation.

With the obtained DR capacity and action time, the frequency response under the risks of cyber-attacks can be estimated with the modified SFR model proposed in Section II, and the frequency regulation results can be checked for violations against operational requirements.

B. COORDINATED RESERVE ALLOCATION SCHEME WITH DR CAPACITY REASSESSMENT

The risks of cyber-attacks are ever changing with the evolvement of attack and defense methods. Therefore, it is necessary to reassess the DR capacity periodically and update the reserve allocation scheme accordingly.

The reserve allocation scheme is to minimize the cost of reserve by allocating optimal reserve amount to the generation and consumption sides, while satisfying the requirement of frequency. The optimization model is built as follows, with the objective function

$$C_{rsv} = C_{gen} + C_{DR}, \tag{13}$$

where

$$C_{gen} = \sum_{i=0}^{N_{gen}} \alpha_i \Delta P_{gen_i}, \tag{14}$$

$$\mathrm{C_{DR}} = \sum_{j=0}^{N_{DR}} \beta_j \Delta P_{DR_j}. \tag{15}$$

And the constraints are:

1) Upper and lower limits of generating unit output:

$$\Delta P_{gen_{i,min}} \leq \Delta P_{gen_i} \leq \Delta P_{gen_{i,max}}. \tag{16}$$

2) System frequency requirement:

$$\Delta f_{min} \leq \Delta f \leq \Delta f_{max}. \tag{17}$$

The frequency constraint can be transformed into power imbalance constraint as

$$\Delta \mathrm{f_{min}} \left(D + \frac{K_m}{R} \right) \leq \Delta P \leq \Delta f_{max} \left(D + \frac{K_m}{R} \right), \tag{18}$$

where $\Delta P = \Delta P_d - \Delta P_{gen} - \Delta P_{DR}$, ΔP_d is the initial power imbalance, ΔP_{gen} is the sum of reserve provided by generators on the source side, and ΔP_{DR} is the sum of demand response committed in the frequency regulation on the load side.

3) Limits of DR capacities:

$$0 \leq P_{DLC} \leq P_{DLC,total}, \tag{19}$$

$$0 \leq P_{DDR} \leq P_{DDR,total}, \tag{20}$$

$$P_{DR} = P_{DLC} + P_{DDR}, \tag{21}$$

where $P_{DLC,total}$ and $P_{DDR,total}$ are the assessment results of total DLC and DDR capacities estimated with the up-to-date attack occurrence probabilities, and P_{DLC} and P_{DDR} are the actual amount of interruptible loads that are scheduled to be shed in the power supply shortage scenario.

IV. CASE STUDY

In this section, a case study based on IEEE 14 bus system is conducted, to illustrate the performance of the proposed methods. First, the vulnerability assessment on the cyber side is performed to determine the probabilities of

TABLE 2. Load distribution in IEEE 14 bus system.

Bus #	Load active power(MW)	Load reactive power(MVar)
2	21.7	12.7
3	94.2	19
4	47.8	-3.9
5	7.6	1.6
6	11.2	7.5
9	29.5	16.6
10	9	5.8
11	3.5	1.8
12	6.1	1.6
13	13.5	5.8
14	14.9	5

TABLE 3. Interruptible loads controlled by DLC and DDR services.

Distributed Demand Response Resources			
Bus #	Initialization frequency (Hz)	Active load (MW)	Load composition (unit power × number)
2	49.8	10	2.5kW×4000
4	49.8	30	2.5kW×12000
6	49.7	6	2.5kW×2400
9	49.7	24	2.5kW×9600
Direct Load Control Resources			
Bus #	Active load (MW)	Load composition (unit power x number)	
3	16	2.5kW×4000	30kW×200
4	12	2.5kW×3600	30kW×100

successful attacks, followed by the risk assessment that gives the expectance of attack impacts on the service quality of coordinative primary frequency regulation. Finally, the original reserve allocation scheme is corrected according to the expected attack impacts, and the corrected new scheme is compared with the original one.

Table 2 gives the load located at each bus. The total system active load is 259MW and reactive load is 73.5MVar, and system base power is set as 785MW.

The controllable load resources that can participate in the scheduling for frequency regulation in the system are given in Table 3. Ideal action time of DLC is set to be 0.5s after fault. The action time of DDR is set to be 0.02s after the frequency drops below the threshold.

A. VULNERABILITY ANALYSIS AND PROBABILITY OF SUCCESSFUL ATTACKS

The raw vulnerability data are taken from China National Vulnerability Database of Information Security (CNNVD) [21], where the vulnerabilities concerning industrial control systems such as control systems in manufacturing factories, critical medical devices, emergency and alarm systems, etc. are specially selected and classified according to the hosts, providing a more specific and convincing data source. The three types of vulnerabilities that is detected at all system locations in a year (December 2017 to December 2018) are counted and summarized in Fig 4.

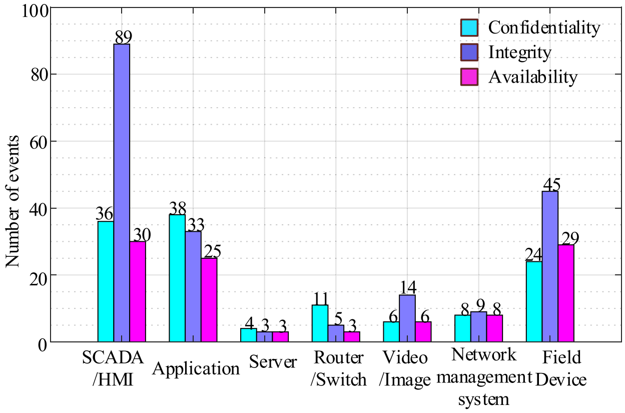


FIGURE 4. Vulnerabilities reported in a year (Dec. 2017-Dec. 2018), categorized according to the violated security aims and targets.

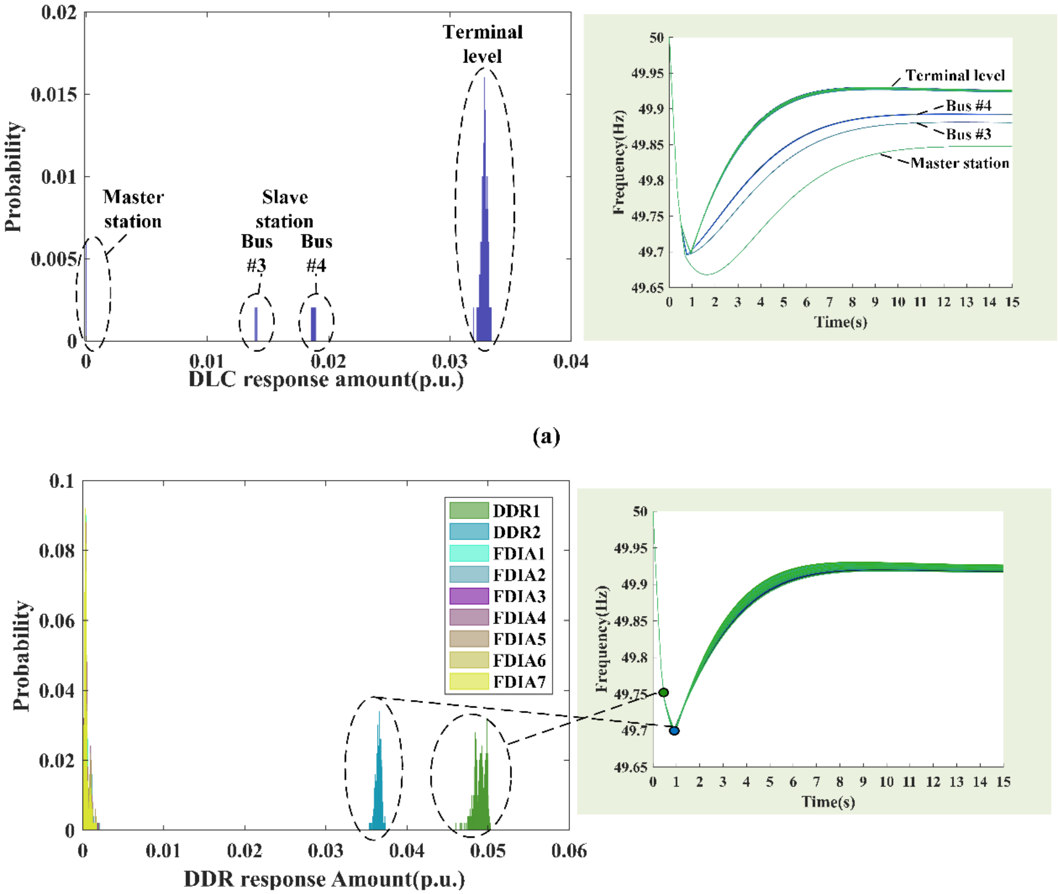
TABLE 4. Attack success probabilities of different attack methods and intrusion levels.

Target service	Attack method	Intrusion level	Success probability
DLC	DoS attack	Master station	0.0219
		Slave station	0.0082
		Terminal	0.0795
DDR	Fake command attack	Master station	0.0024
		Slave station	0.0062
	DFDIA	Terminal	0.0084

The occurrence probability of each type of vulnerabilities at each network location is hence approximated with the occurrence frequency. Assume that only on the first day when a vulnerability is discovered, it is not fixed and can be exploited by attackers. Therefore, the probability that attackers find an exploitable vulnerability is $P_v = \frac{n_v}{365}$, where n_v is the number of events of one category in a year.

The attack success probabilities are calculated with the vulnerability occurrence probabilities, and the combinations of intrusion points, attack methods and vulnerabilities needed are given in Section II A. The vulnerability assessment results are listed in Table 4.

Mind the difference of comprised locations' effects between the two types of services, which is due to the difference of control methods in the two services. When a control node in DLC is compromised, all the loads below this control level will be unavailable, as the control command cannot be passed to the loads' local controllers due to connection failure. Meanwhile, in the case of DDR service, even the control node at higher level is compromised, each terminal controller has to be individually modified with corresponding commands. That is to say, the terminal controller can stay unaffected if the compromised higher level control node does not give it a valid fake order.



(a)

(b)

FIGURE 5. Monte Carlo sampling and simulation results. (a) shows the cases with different attack results on DLC service alone and the corresponding frequency recovery process to each sample case. DDR are not influenced by attacks. (b) shows the cases with different attack results on DDR services and corresponding frequency recovery processes. Attackers change the terminal threshold settings arbitrarily, whereas DLC services are not influenced.

B. RESPONSE EFFECTS ASSESSMENT UNDER CYBER-ATTACK RISKS

The performance of DR is evaluated from two aspects: 1) the total capacity that can be put into effect in the frequency regulation time scale, which determines the final frequency values; 2) the characteristic values during transient process, which indicate the worst damage the system may endure. The DR capacity in each round, action times for DLC and action thresholds for DDR are obtained from the Monte Carlo simulation process, and transient processes are simulated with the modified SFR model. The active power deficiency is set as 0.15 p.u. with power base as 785MW.

The case study generates 500 samples of DLC and DDR attack scenarios respectively, and simulated the frequency response process for each scenario, as illustrated in Fig 5.

The available DLC resources show four peaks, which indicate the cases where the master station, either of the two slave stations or only terminals are under attack. The considerable differences in available resources result in the significant grouping features in the frequency curve figure.

Meanwhile, as there is no method to affect a wide range of DDR and one single DDR contributes to the total amount quite slightly, the DDR resources only show one peak for each round, and there is only one group of the frequency curves, since the terminal setting must be modified individually, and each terminal load power is relatively small, thus creating a continuous distribution. The two turning points in the frequency curves mark the time instants when a round of DDR load shedding actions.

It is obtained from the simulation that the expectance of available DLC capacity is 0.032 p.u., and that of DDR is 0.0490 p.u. (1st round) and 0.0365 p.u. (2nd round) respectively.

C. CORRECTED RESERVE ALLOCATION SCHEME DESIGN

The costs of generating units are based on the IEEE 14 system, which can be described with

$$C_{gen} = c_2P^2 + c_1P + c_0 \tag{22}$$

The cost parameters and initial generation amounts of the units are given in Table 5. The costs of DLC and DDR are

TABLE 5. Generating unit cost parameters.

Generating unit	Active power (MW)	Reactive power (MVar)	c_2	c_1	c_0
#1	232	-16.55	0.0430	20	0
#2	40	43.56	0.25	20	0
#3	0	25.08	0.01	40	0
#4	0	12.73	0.01	40	0
#5	0	17.62	0.01	40	0

TABLE 6. Comparison of reserve allocation scheme before and after correction considering attack risks.

Reserve source		Reserve allocation（MW）	
		Before	After
Generating unit	#1	4.9244	5.196
	#2	0.751	0.7977
	#3	18.7749	19.9429
	#4	18.7749	19.9429
	#5	18.7749	19.9429
DLC		28	25.12
DDR		70	67.1175

respectively 25.6$/MW and 9.4$/MW, calculated from data provided in [22].

With the expectance of available DR resources assessed before, the corrective reserve allocation scheme can be obtained by solving the optimization model. The schemes before and after correction are given in Table 6.

Comparison shows that after correction, the generating units are allocated with larger amount of spinning reserves, which is to compensate for the amount of DR resources that may not be able to respond if compromised by attacks.

V. CONCLUSION

With higher possibility of cyber-attacks aiming at smart grid, the traditional control methods need to be updated to guarantee the effectiveness of the services. This paper takes the service of primary frequency regulation with participation of generating units and demand response as an example, and the contributions can be concluded as below.

1) The vulnerability analysis in this paper takes into consideration the different defense strengths in the control system layers and has deduced the vulnerability combination needed for different types of attacks according to the attack vectors.

2) A quantified risk assessment method is provided to represent the influence of cyber-attack risks on the performance of a smart grid service. The risk considers both the difficulty of succeeding in an attack and the reward for attackers obtained from the success, which is closer to the real situation where the attackers choose the targets with the balance between cost and profit.

3) With the risk assessment results, the paper proposes a corrected optimization model to guide the coordinated reserve allocation between generating units and demand response loads. The correction to the traditional optimization model shows the method of interpreting cyber-attack impacts on the physical operation process and mitigating the impacts through scheme adjustment, which is applicable to other services.

REFERENCES

[1] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[2] O. Yagan, D. Qian, J. Zhang, and D. Cochran, "Optimal allocation of interconnecting links in cyber-physical systems: Interdependence, cascading failures, and robustness," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1708–1720, Sep. 2012.

[3] W. Liu, Q. Gong, H. Han, Z. Wang, and L. Wang, "Reliability modeling and evaluation of active cyber physical distribution system," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 7096–7108, Nov. 2018.

[4] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: A survey," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 1, no. 1, pp. 13–27, 2016.

[5] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, "Cyber-security in smart grid: Survey and challenges," *Comput. Elect. Eng.*, vol. 67, pp. 469–482, Apr. 2018.

[6] L. P. I. Ledwaba, G. P. Hancke, H. S. Venter, and S. J. Isaac, "Performance costs of software cryptography in securing new-generation Internet of energy endpoint devices," *IEEE Access*, vol. 6, pp. 9303–9323, 2018.

[7] H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung, "Efficient authentication and key management mechanisms for smart grid communications," *IEEE Syst. J.*, vol. 8, no. 2, pp. 629–640, Jun. 2014.

[8] T. Yang, F. Zhai, J. Liu, M. Wang, and H. Pen, "Self-organized cyber physical power system blockchain architecture and protocol," *Int. J. Distrib. Sensor Netw.*, vol. 14, no. 10, pp. 1–9, Oct. 2018.

[9] X. Liu, Z. Li, and Z. Li, "Optimal protection strategy against false data injection attacks in power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1802–1810, Jul. 2017.

[10] O. A. Osanaiye, A. S. Alfa, and G. P. Hancke, "Denial of service defence for resource availability in wireless sensor networks," *IEEE Access*, vol. 6, pp. 6975–7004, 2018.

[11] H. Mo and G. Sansavini, "Dynamic defense resource allocation for minimizing unsupplied demand in cyber-physical systems against uncertain attacks," *IEEE Trans. Rel.*, vol. 66, no. 4, pp. 1253–1265, Dec. 2017.

[12] B. Falahati, Y. Fu, and L. Wu, "Reliability assessment of smart grid considering direct cyber-power interdependencies," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1515–1524, Sep. 2012.

[13] B. Falahati and Y. Fu, "Reliability assessment of smart grids considering indirect cyber-power interdependencies," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1677–1685, Jul. 2014.

[14] M. U. Tariq, J. Florence, and M. Wolf, "Improving the safety and security of wide-area cyber–physical systems through a resource-aware, service-oriented development methodology," *Proc. IEEE*, vol. 106, no. 1, pp. 144–159, Jan. 2018.

[15] T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford, "Petri net modeling of cyber-physical attacks on smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 741–749, Dec. 2011.

[16] W.-L. Chin, C.-H. Lee, and T. Jiang, "Blind false data attacks against ac state estimation based on geometric approach in smart grid communications," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6298–6306, Nov. 2018.

[17] S. Tan, W.-Z. Song, M. Stewart, J. Yang, and L. Tong, "Online data integrity attacks against real-time electrical market in smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 313–322, Jan. 2018.

[18] H. M. Khalid and J. C.-H. Peng, "A Bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2026–2037, Jul. 2016.

[19] M. Chlela, D. Mascarella, G. Joós, and M. Kassouf, "Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4702–4711, Sep. 2018.

[20] P. M. Anderson and M. Mirheydar, "A low-order system frequency response model," *IEEE Trans. Power Syst.*, vol. 5, no. 3, pp. 720–729, Aug. 1990.

[21] (2019). *Industrial Control System Vunelarabilities*. Accessed: Jun. 2019. [Online]. Available: https://ics.cnvd.org.cn/

[22] X. Zhou, W. Li, M. Li, Q. Chen, C. Zhang, and J. Yu, "Effect of the coordinative optimization of interruptible loads in primary frequency regulation on frequency recovery," *Energies*, vol. 9, no. 3, p. 167, 2016.

QI WANG (S'13–M'17) received the bachelor's, master's, and Ph.D. degrees in electrical engineering from Southeast University, Nanjing, China, in 2010, 2012, and 2016, respectively.

He is currently a Lecturer with the School of Electrical Engineering, Southeast University. His research interests include power system stability and control, and cyber-physical power systems.

MENGYA LI received the bachelor's degree in electrical engineering from Southeast University, Nanjing, China, in 2016, the M.S. degree in electrical power systems from the University of Birmingham, in 2018, and the master's degree in electrical engineering from Southeast University, in 2019. She is currently pursuing the Ph.D. degree in computer science with The University of Manchester.

Her research interests include cybersecurity and attack defense methods in cyber-physical power systems and the Internet-of-Things environment.

YI TANG (M'07–SM'19) received the Ph.D. degree from the Harbin Institute of Technology, Harbin, China, in 2006.

He is currently a Professor with the School of Electrical Engineering, Southeast University, Nanjing, China. His research interests include smart grid, power system security, power system stability analysis, renewable energy systems, and cyber-physical systems.

MING NI (M'98–SM'05) received the bachelor's and Ph.D. degrees from Southeast University, Nanjing, China, in 1991 and 1996, respectively.

He is currently the Chief Expert of power system planning and analysis with the State Grid Electric Power Research Institute, a Researcher-Level Senior Engineer with NARI Group Corporation, and an Adjunct Professor with the School of Electrical Engineering, Southeast University. His research interests include power system planning, analysis and control, and cyber-physical systems.