energies

MDPI

Article

Asymmetric Information in Military Microgrid Confrontations—Evaluation Metric and Influence Analysis

Peng Jiang [1,2], Shengjun Huang [1,3,*] and Tao Zhang [1,3]

1 College of Systems Engineering, National University of Defense Technology, Changsha 410073, China; jiangpeng_nudt@aliyun.com (P.J.); zhangtao@nudt.edu.cn (T.Z.)
2 China Academy of Launch Vehicle Technology, China Aerospace Science and Technology Corporation, Beijing 100076, China
3 Hunan Key Laboratory of Multi-Energy System Intelligent Interconnection Technology (HKL-MESI^{2}T), National University of Defense Technology, Changsha 410073, China
* Correspondence: huangshengjun@nudt.edu.cn; Tel.: +86-152-0080-9007

Received: 16 March 2020; Accepted: 8 April 2020; Published: 15 April 2020

Abstract: Due to the wide integration of information technology in equipment and weapons, a stable and reliable power supply has become one of the pivotal factors in modern warfare to achieve victory. As a critical infrastructure to provide continuous energy supply during long-duration electrical outage, military microgrid always suffers fierce attacks from the enemy. In order to improve the defense effect, a lot of investigation has been made into resource allocation, Distributed Generator (DG) distribution, network reconfiguration, and so forth. Nevertheless, the information gap between defender and attacker has not been considered in the literature. Therefore, this paper is intended to highlight this information mismatch to appeal for community attention and evaluate its capability to improve defensive performance. Firstly, a novel assessment metric is proposed to identify the level of asymmetric information. Then, an Attacker-Defender (AD) model is developed to describe the zero-sum game between two opposite agents, which is subsequently tackled with dual theory and big-*M* method. Finally, three cases ranging from 6-bus to 57-bus are utilized for numerical experiments to analyze the influence of asymmetric information on military microgrid confrontation. Results on various levels of attack strength validated the effectiveness and significance of asymmetric information in eliminating the attack damage and improving the defensive performance.

Keywords: asymmetric information; microgrid confrontation; attacker-defender model; mixed integer linear programming

1. Introduction

The military force of a country is founded primarily for protecting national territory and global interests from aggression and loss, but its task has gone far beyond that in recent years, including emergency rescue, humanitarian aid, public order maintenance, and so forth. Therefore, the intensity and scope of military operations keep increasing, resulting in the consumption of all sorts of fossil fuel skyrocketed to great heights [1]. It has been reported that the United States Department of Defense (DOD) is the largest single energy consumer in the country [2]. In order to deliver petroleum products to forward operation and stationary bases, soldiers need to risk their lives in midway due to unexpected explosions caused by the enemy. Furthermore, a considerable amount of fuel will be exhausted during the transportation trip. On the other hand, consisting of various energy sources and storage units that may work in a coordinated manner to support loads, a microgrid provides a lot of prominent benefits, for example, island ability, reliability, security, and utilization of Renewable Energy Sources (RES),

and so forth. Of which the most crucial is providing continuous energy supply during long-duration electrical outage, which is of great significance in real warfare since the domestic electric grid is always the first to be hit as critical infrastructures. Therefore, driven by the motivation to improve security and efficiency, a lot of demonstration projects are implemented by DOD [3], including the Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS) Joint Capability Technology Demonstration (JCTD) [4], Fort Sill Microgrid Demonstration [5], and Environmental Security and Technology Certification Program (ESTCP) [3]. Due to profound advantages of microgrid and the vast leading effects of US DOD, microgrid has been constructed in a lot of countries for military utilization in the last five years [1,6,7].

Generally, microgrid is immune to unforeseen cascading failures in central grid due to its island capability. Nevertheless, it is still vulnerable when faced with targeted attacks, for example, cyber and physical (CP) actions to cut the real-time balance between energy generation and consumption. Compared with domestic grid, microgrid has a smaller capacity and inertia, thus it is more sensitive to power imbalance. Therefore, microgrid security concern has been proposed and investigated in the community of academic, industry, and military.

In Reference [8], the CP attack was categorized into three types: physical attack, cyberattack, and human attack. The operation through or against people who are related to power system is termed as 'human attack', including bribery, threat, and social engineering, and so forth. Cyberattack launches action to disrupt the availability, integrity, and confidentiality of Supervisory Control and Data Acquisition (SCADA) system, of which the most popular ones are: denial of service/distributed denial of service (DoS/DDoS) attack [9], false data injection attack [10], load redistribution attack [11], traffic analysis, and cracking password, and so forth. Physical attack affects the system via invaliding component and equipment, such as tripping line [12], isolating bus, disconnecting generator, and damaging transformer, and so forth. For more details, the interested reader is referred to References [13,14]. In addition to CP attack, natural disasters, such as hurricane and flood, are popular factors to induce power outage [15]. A comprehensive review of the impacts of natural disasters on power system is generated in Reference [16].

Although cyberattack gained the most attention in the literature, physical attack is the most popular method in military microgrid confrontation between defenders and attackers due to the following two reasons: (1) The communication network of military microgrid is physically isolated with the Internet, thus cyberattack is very hard or almost impossible to implement; (2) Human attack is also very difficult since the spy is trained to gain more valuable information. Consequently, tripping a line with a bomb turns to be a direct and the most effective method, which is then regarded as the type of attack for consideration in this paper.

Concentrated on a fixed type of attack, there is a zero-sum game between two opposite agents: defender and attacker. A tri-level optimization model is proposed to identify the optimal allocation strategy of defending resources in Reference [17], where coordinated attacks including physical short-circuiting of transmission lines and intruding of communication network are considered. In Reference [18], malicious attack is alleviated via optimal Distributed Generator (DG) islanding and network topology reconfiguration, where a Defender-Attacker-Defender (DAD) model is developed and addressed by the Column and Constraint Generation (CCG) method [19]. Following on from the combination of DAD and CCG, the single wave of attack is extended to multi-period by Reference [20], where defensive transmission lines and DGs are respectively planned and allocated to mitigate the multi-period attack damage. In Reference [21], the role of Battery Energy Storage Systems (BESSs) in enhancing microgrid robustness in overcoming attacks is investigated, where four participants are included in a framework involving interactions between a robustness-oriented economic dispatch model and a bilevel Attacker-Defender (AD) model. In Reference [22], the problem of allocating fortification resources in power grid for the purpose of maximizing its immunity against malicious attack is investigated, resulting in a two-stage optimization model with the capability of generalizing several other network fortification problems and the corresponding exact solution algorithm.

Although sophisticated problems, models, and algorithms are reported in the above literature, there is an implicit assumption that the attacker is informed with full information of the target system, for example, the topology, generator capacity, load amount, branch distribution, and other component parameters, and so forth, which is impossible in most cases of real confrontation. Actually, there is an information gap between attacker and defender in military microgrid confrontation since deception strategies are ubiquitous in the battlefield. In order to highlight this information mismatch to appeal for community attention and evaluate its capability to improve defensive performance, the information possessed by defender and attacker is defined as symmetric and asymmetric information in this paper, and the impact of asymmetric information in military microgrid confrontation is comprehensively investigated.

Since asymmetric information in military microgrid confrontation has not been numerically investigated before, an assessment metric should be defined, which consists the first contribution of this paper. The asymmetric and symmetric information are abstracted as binary vectors, then the distance between them is naturally determined as assessment metric. However, after testing on a 6-bus demo system, various traditional vector distance definitions, for example, Minkowski distance, Hamming distance, and Jaccard distance, and so forth, are not suitable for the case in this paper since they cannot identify full characteristic of information mismatch. Therefore, a novel definition of binary vector distance combining coverage rate and deviation rate is proposed in this paper as the assessment metric of asymmetric information.

In order to analyze the influence of asymmetric information in military microgrid confrontation, the game between defender and attacker is formulated as an AD model. Based on dual theory and big-M method, the bilinear $max - min$ AD model is evolved into a single level Mixed Integer Linear Programming (MILP) problem and tackled with commercial solver Cplex. Set the symmetric information of 6-bus, 24-bus, and 57-bus systems as benchmark, the influence of asymmetric information is quantitatively analyzed based on a lot of numerical experiments, which is the second contribution of this paper. Based on simulation results on various levels of attack strength and asymmetric information across all three systems, the effectiveness and significance of asymmetric information in eliminating attack damage and improving defensive performance have been validated.

The rest of this paper is organized as follows. Section 2 reveals the information involved in military microgrid confrontation and proposes assessment metric on the basis of comparison and analyses. Based on the AD model of microgrid confrontation, solution methodology to analyze the influence of asymmetric information is provided in Section 3. Three cases including 6-bus, 24-bus, and 57-bus systems are employed for numerical experiment in Section 4, with results are presented and discussed. Section 5 concludes this paper.

2. Assessment Metric of Asymmetric Information

Microgrid confrontation is ubiquitous ranging from industry to military, where terrorists and enemies are typical attackers taking cyber and physical actions respectively. Based on years of training and practicing, attackers might be sophisticated and professional, but the attack decision and action cannot be made without comprehensive recognition of the target system. Therefore, the microgrid information/data is of great significance for attackers. In order to illustrate what information is involved in the microgrid confrontation, a military conflict scenario is introduced. However, due to the extensive utilization of defensive and deception strategies, there is an information gap between defender and attacker, which is very important in real confrontation and should not be omitted. Thus, how to quantitatively analyze the asymmetric information is investigated in this section.

2.1. Information Involved in the Microgrid Confrontation

In the era of information, IT equipments are playing fundamental roles in modern warfare. Generally, IT devices are powered by electricity, thus microgrid is widely built to provide reliable, continuous, and stable electricity. On the other hand, in order to grasp the initiative in a war, disabling

all types of IT equipment is the most common and efficient strategy. Therefore, microgrid always suffers various types of attacks from the enemy. Correspondingly, defense operations will be taken by the defender.

In the confrontation of microgrid, a lot of information will be utilized by both sides to make rational decisions, including network topology, nodal feature, branch attribute, generator/load characteristic, and so forth. In order to facilitate the description, a 6-bus system retrieved in Reference [23] is employed as an example, whose topology is shown in Figure 1.

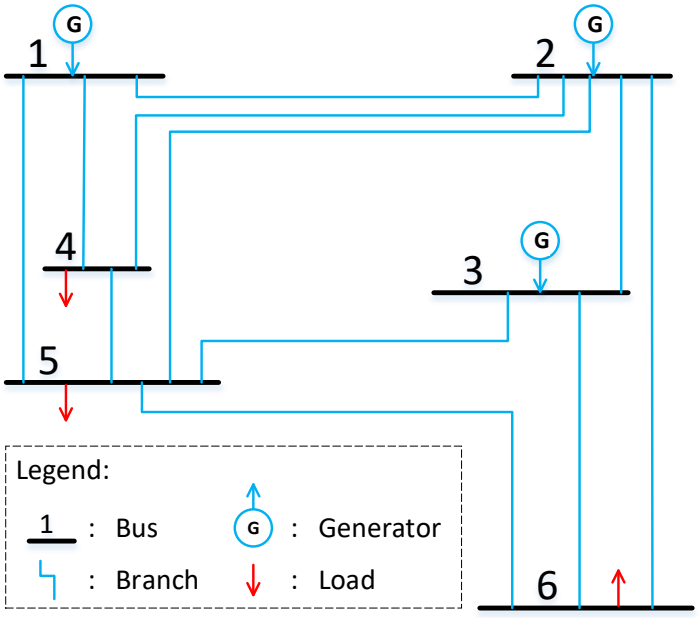

Figure 1. Single line diagram of 6-bus sample system.

As shown in Figure 1, the system includes 6 buses, 11 branches, 3 generators, and 3 loads. In the smart grid era, distributed generators and battery storage systems will be placed as well to improve the robustness, for example, minimizing the unserved load. Although the sum number of components is revealed in Figure 1, a lot of physical quantity is still unknown, such as generator capacity, load level, branch power flow limit, and so forth. In reality, the accurate information of system topology is very hard to be squeezed by enemies, not to mention other detailed physical data. Therefore, the scope of this paper on asymmetric information analysis is restricted in topology level based on the following assumptions.

- **Assumption 1**: The number of buses is recognized by enemies, that is, the number of nodes is exposed and fixed during the microgrid confrontation.
- **Assumption 2**: The detailed physical quantity of each equipment is inaccessible by enemies, thus from the perspective of an attacker, each branch/generator/load is indifferent and the average data will be utilized.

Generally, the node is very difficult to conceal, thus **Assumption 1** is proposed to provide a basic framework for this research. The accurate information of each component can only be achieved by physical measurement or document retrieval, but both methods are impractical for enemy to implement, thus **Assumption 2** states that the detailed physical quantity is inaccessible. Although the exact data cannot be gained, estimation is much easier, therefore the average data is employed by enemy according to **Assumption 2**. It should be noted that both assumptions are proposed to facilitate the description and demonstration, and the methodology of asymmetric information analysis can still be established without these assumptions.

2.2. Assessment Metric

In terms of microgrid data, the defender has full access permission, thus the topology information obtained by him/her is accurate and utilized as the reference for asymmetry analysis. On the other hand, the attacker is trying to collect microgrid information via satellite observation, Unmanned Aerial Vehicle (UAV) detection, and espionage, and so forth. Since the successful implementation of each method depends on political, technical, meteorological, and geographical conditions, the accuracy of acquired data cannot be guaranteed. Figure 2 illustrates the asymmetric information on system topology between attackers and defenders. For each sub-figure, defender is regarded as the benchmark with respect to the total number (sum) and position (binary numbers: 1 represents there is a generator/load/branch, and 0 otherwise). It can be observed that attacker 1 has accurate information on the sum, but the distribution exists a minor deviation. Attacker 2 and 3 has a bigger and smaller estimation of system scales respectively, resulting in the inaccurate assessment of component number and location.

Bus	1	2	3	4	5	6	Sum
Defender	1	1	1	0	0	0	3
Attacker 1	1	1	0	0	0	1	3
Attacker 2	1	0	1	0	1	1	4
Attacker 3	1	0	0	1	0	0	2

(a)

Bus	1	2	3	4	5	6	Sum
Defender	0	0	0	1	1	1	3
Attacker 1	0	1	0	0	1	1	3
Attacker 2	1	0	1	0	1	1	4
Attacker 3	0	0	1	1	0	0	2

(b)

Order	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Sum
Branch	1 - 2	1 - 3	1 - 4	1 - 5	1 - 6	2 - 3	2 - 4	2 - 5	2 - 6	3 - 4	3 - 5	3 - 6	4 - 5	4 - 6	5 - 6	
Defender	1	0	1	1	0	1	1	1	1	0	1	1	1	0	1	11
Attacker 1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	0	11
Attacker 2	1	1	1	0	1	1	1	0	1	1	1	1	0	1	1	12
Attacker 3	1	0	1	1	0	1	0	1	1	1	0	1	1	0	0	9

(c)

Figure 2. Illustration of asymmetric information on system topology between attackers and defenders: (**a**) The installation of generators; (**b**) The distribution of loads; (**c**) The existence of branches.

Based on Figure 2, it is obvious that the system topology information can be generated as binary row vectors, for example, $\boldsymbol{x} = [1\ 1\ 1\ 0\ 0\ 0]$ and $\boldsymbol{y} = [1\ 1\ 0\ 0\ 0\ 1]$ for defender and attacker 1 in Figure 2a. Therefore, the asymmetric information between attacker and defender can be represented by the distance between vectors $\boldsymbol{x}$ and $\boldsymbol{y}$.

Traditionally, vector differences can be measured by a lot of methods, of which the most popular one is Minkowski distance:

$$D_{Minkowski} = \sqrt[p]{\sum_{j=1}^{n} |x_j - y_j|^p}, \tag{1}$$

where n is the total number of elements in vector $\boldsymbol{x}$; p takes the value of $1, 2, 3, \ldots, \infty$ to identify various types of definition.

If $p = 1$, the Minkowski distance evolves into city block distance:

$$D_{Cityblock} = \sum_{j=1}^{n} |x_j - y_j|. \tag{2}$$

If $p = 2$, the Minkowski distance emerges into Euclidean distance:

$$D_{Euclidean} = \sqrt{(\boldsymbol{x} - \boldsymbol{y})(\boldsymbol{x} - \boldsymbol{y})^T}. \tag{3}$$

If $p = \infty$, the Minkowski distance results into Chebychev distance:

$$D_{Chebychev} = max\left\{\left|x_j - y_j\right|_{j=1}^{n}\right\}. \tag{4}$$

In addition, other types of vector distance definitions are popular in the literature, such as Cosine distance (5), Hamming distance (6), and Jaccard distance (7).

$$D_{Cosine} = 1 - \frac{\boldsymbol{x}\boldsymbol{y}^T}{\sqrt{\left(\boldsymbol{x}\boldsymbol{x}^T\right)\left(\boldsymbol{y}\boldsymbol{y}^T\right)}}, \tag{5}$$

$$D_{Hamming} = \frac{\#\left\{\left(x_j \neq y_j\right)_{j=1}^{n}\right\}}{n}, \tag{6}$$

$$D_{Jaccard} = \frac{\#\left\{\left(x_j \neq y_j\right)_{j=1}^{n} \bigcap \left[\left(x_j \neq 0\right)_{j=1}^{n} \bigcup \left(y_j \neq 0\right)_{j=1}^{n}\right]\right\}}{\#\left\{\left(x_j \neq 0\right)_{j=1}^{n} \bigcup \left(y_j \neq 0\right)_{j=1}^{n}\right\}}, \tag{7}$$

where #{ } is an operator counting the number of elements in the set enclosed by braces.

All the above distance definitions are employed to identify the asymmetric information between attacker and defender in the 6-bus system, and results are summarized in Table 1.

Table 1. Vector distances measured by various methods.

Distance	Generator Information			Load Information			Branch Information		
	Atker. 1	**Atker. 2**	**Atker. 3**	**Atker. 1**	**Atker. 2**	**Atker. 3**	**Atker. 1**	**Atker. 2**	**Atker. 3**
$D_{Cityblock}$	2.00	3.00	3.00	2.00	3.00	3.00	6.00	7.00	4.00
$D_{Euclidean}$	1.41	1.73	1.73	1.41	1.73	1.73	2.45	2.65	2.00
$D_{Chebychev}$	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
D_{Cosine}	0.33	0.42	0.59	0.33	0.42	0.59	0.27	0.30	0.20
$D_{Hamming}$	0.33	0.50	0.50	0.33	0.50	0.50	0.40	0.47	0.27
$D_{Jaccard}$	0.50	0.60	0.75	0.50	0.60	0.75	0.43	0.47	0.33

It can be seen from Table 1 that $D_{Chebychev}$ is constant for all cases, thus nothing can be generated in terms of the sufficiency of information between different attackers. For generator and load information, $D_{Cityblock}$, $D_{Euclidean}$, and $D_{Hamming}$ cannot distinguish the difference between attacker 2 and 3. To sum up, D_{Cosine} and $D_{Jaccard}$ gain better performance in this dataset. However, they are far away to be nominated as a candidate to evaluate binary vector distances in this research since the obtained single value might be resulted by two completely opposite scenarios. For example, if

$$\begin{aligned} \boldsymbol{x} &= [1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0], \\ \boldsymbol{y}_1 &= [1\,1\,\mathbf{0}\,\mathbf{0}\,1\,1\,\mathbf{0}\,\mathbf{0}\,1\,1\,0\,0\,0\,0\,0], \\ \boldsymbol{y}_2 &= [1\,1\,1\,1\,1\,1\,1\,1\,1\,\mathbf{0}\,\mathbf{1}\,\mathbf{1}\,\mathbf{1}\,\mathbf{1}\,\mathbf{1}], \end{aligned}$$

there has $D_{Jaccard}(\boldsymbol{y}_1) = 0.4$ and $D_{Jaccard}(\boldsymbol{y}_2) = 0.4$; however, $\boldsymbol{y}_1$ and $\boldsymbol{y}_2$ are totally different since the former attacker missed 4 real branches while the latter included 5 fake circuits.

To address the above concerns, a novel definition of vector distance (8) is proposed in this paper.

$$\begin{aligned} D_{Hybrid} &= f\left(\frac{\#\left\{\left(x_j = 1\right)_{j=1}^{n} \bigcap \left(y_j = 1\right)_{j=1}^{n}\right\}}{\#\left\{\left(x_j = 1\right)_{j=1}^{n}\right\}}\right) \times 100 + \frac{\#\left\{\left(x_j = 0\right)_{j=1}^{n} \bigcap \left(y_j = 1\right)_{j=1}^{n}\right\}}{\#\left\{\left(y_j = 1\right)_{j=1}^{n}\right\} + \epsilon} \\ &= 100 \cdot f(A) + B,, \end{aligned} \tag{8}$$

where $f(A)$ is a function rounding A to 2 digits to the right of the decimal point, that is, $f(A) = round(A, 2)$ in Matlab; ϵ is an arbitrary small positive number. Examples of $f(\ )$ and ϵ can be given as $f(0.9735) = 0.97$ and $\epsilon = 0.001$. In order to give a full explanation of Equation (8), the following questions are proposed and answered:

- What is A? The numerator of A is $\#\left\{(x_j = 1)_{j=1}^{n} \bigcap (y_j = 1)_{j=1}^{n}\right\}$, showing the number of real components confirmed by attacker. The denominator is the total number of elements in vector $\boldsymbol{x}$. Therefore, A is defined as coverage rate from the viewpoint of defender, representing how much real information has been identified.
- What is B? The numerator of B is $\#\left\{(x_j = 0)_{j=1}^{n} \bigcap (y_j = 1)_{j=1}^{n}\right\}$, representing the number of fake components (it is not exist in reality but incorrectly confirmed by attacker). The denominator is the total number of elements in vector $\boldsymbol{y}$. Therefore, B is defined as deviation rate in respect to attacker, indicating how much fake information has been introduced.
- Why is the function $f(\ )$ employed? According to the mathematical formulation, the range of A is valued in $[0, 1]$. In terms of precision concerns, 2 digits after decimal point is acceptable. The reason to utilize function $f(\ )$ is cutting tail to avoid duplicates in the following addition operation $100 \cdot f(A) + B$.
- Why is the term $\times 100$ utilized? Combined with $f(\ )$, the reason to include $\times 100$ is eliminating duplicate numbers. Due to the rounding operation, values $f(A)$ are fixed into 101 discrete numbers $\{0.00,\ 0.01,\ 0.02,\ \cdots,\ 0.98,\ 0.99,\ 1.00\}$. By multiplying 100, the term $100 \cdot f(A)$ turns into an integer in $[0,\ 100]$, while B is decimal, thus adding these two terms will deduce a unique number and the addition operation is reversible, which means given a number within the domain of $D_{Hybrid} \in [0.00,\ 101.00)$, the values of A and B can be exactly derived. For example, if $D_{Hybrid} = 97.4323$, there have $A = 0.97$ and $B = 0.4323$.
- Why is the term $+\epsilon$ introduced? ϵ is included to restrict the range of B is $[0, 1)$, that is, eliminating the number $B = 1$. If B can arrive at 1, the duplication might arise in some special cases. For instance, $D_{Hybrid} = 98.00$ can be interpreted as $[A,\ B] = [0.97,\ 1.00]$ or $[A,\ B] = [0.98,\ 0.00]$, resulting completely opposite conclusion for B. Therefore, by adding ϵ, $B = 1.00$ is evolved into $\frac{1}{1+\epsilon} < 1.00$, the value $D_{Hybrid} = 98.00$ can only be interpreted as $[A,\ B] = [0.98,\ 0.00]$.

According to the vector distance definition (8), the value of D_{Hybrid} can be decoded into integer and decimal parts, representing coverage and deviation rate respectively. From the attacker's point of view, one prefers a higher coverage rate and lower deviation rate, thus $D_{Hybrid} = 100.00$ is optimal, meaning accurate microgrid information is acquired. Based on coverage and deviation rates, the quality of D_{Hybrid} can be quickly identified. In order to facilitate quality identification, a fitness function is proposed in (9), and the corresponding variation tendency along with D_{Hybrid} changing is given in Figure 3.

$$V_{Fitness} = A - B. \tag{9}$$

In Figure 3, there is a red baseline $V_{Fitness} = 0$, indicating the coverage rate is equal to deviation rate, thus it can be regarded as an acceptance line. If $A < B$, the quality of information is poor and the attack action may conduct on fake components; if $A > B$, the attacker may implement a threatening attack based on the obtained information.

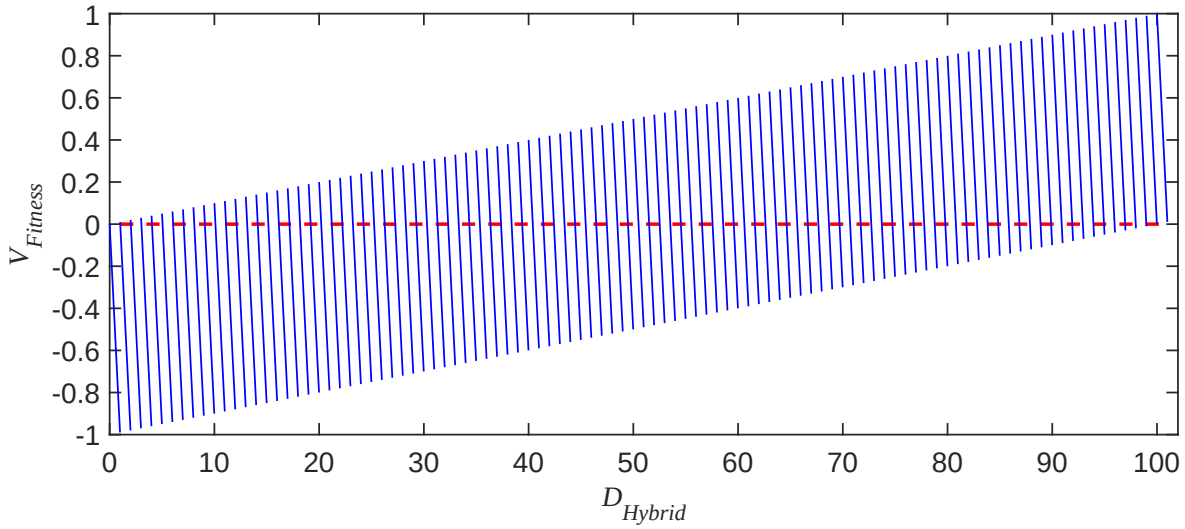

Figure 3. Fitness value evaluation of vector distance D_{Hybrid}.

3. Influence Analysis of Asymmetric Information on Microgrid Confrontation

It is known in Section 2 that the asymmetric information between attacker and defender can be measured by binary vector distance D_{Hybrid}. Nevertheless, the impact of D_{Hybrid} on microgrid confrontation is still waiting to be discovered. To fill this gap, a mathematical model of microgrid confrontation is developed in this section, where the attack strength is sensitive to the accuracy of acquired information. Therefore, by comparing the attack effectiveness derived from symmetric and asymmetric information, impacts can be identified and analyzed.

3.1. Confrontation with Symmetric Information

In a microgrid confrontation, the attacker is always trying to maximize the unserved power via various types of assault, and the defender utilizes Optimal Power Flow (OPF) tools to minimize the power imbalance. Different kinds of attacks can result in the invalidation of generator, load, and branch, and so forth. In this paper, the attack action to destroy circuits is investigated as a representative. On the other hand, OPF strategies to redispatch generator and branch power flow is employed by defenders. Therefore, the mathematical model of microgrid confrontation in accordance with References [24–29] is formulated as follows:

$$\max_{z_l} \quad \Delta \tag{10}$$

$$subject\ to:$$

$$z_l = \{0,1\}; \forall l \in L \tag{11}$$

$$\sum_{l \in L} z_l \leq N \tag{12}$$

$$\Delta = \min_{p_i, f_l, S_b^+, S_b^-, \theta_{fr(l)}, \theta_{to(l)}} \left\{ \sum_{b \in B} \left(S_b^+ + S_b^- \right) \right. \tag{13}$$

$$subject\ to:$$

$$\sum_{i \in I | bu(i)=b} p_i + \sum_{l \in L | to(l)=b} f_l - \sum_{l \in L | fr(l)=b} f_l - S_b^+ + S_b^- = D_b : (\beta_b); \forall b \in B \tag{14}$$

$$f_l = (1 - z_l)\gamma_l(\theta_{fr(l)} - \theta_{to(l)}) : (\pi_l); \forall l \in L \tag{15}$$

$$-F_l \leq f_l \leq F_l : (\sigma_l, \phi_l); \forall l \in L \tag{16}$$

$$0 \leq p_i \leq P_i : (\mu_i); \forall i \in I \tag{17}$$

$$S_b^+ \geq 0, S_b^- \geq 0; \forall b \in B \Big\}. \tag{18}$$

where the definition of utilized indexes, sets, parameters, and decision variables are summarized in Table 2.

Table 2. Definition of indexes, sets, parameters, and decision variables.

Symbol	Definition
Δ	System power imbalance.
z_l	Binary variable, if circuit l is attacked $z_l = 1$; otherwise $z_l = 0$.
L	Set of branch indexes.
N	Maximum number of branches can be attacked.
p_i	Power output of generator i.
f_l	Power flow of line l.
S_b^+	Power surplus at bus b.
S_b^-	Power deficit at bus b.
$fr(l)$	Origin bus of line l.
$to(l)$	Destination bus of line l.
θ_b	Phase angle at bus b.
B	Set of bus indexes.
I	Set of generator indexes.
$bu(i)$	The bus that generator i is connected with.
D_b	Demand at bus b.
γ_l	Suspectance of line l.
F_l	Power flow capacity of line l.
P_i	Capacity of generator i.
$\beta, \pi, \sigma, \phi, \mu$	Dual variables corresponding to each constraints.

The objective function (10) to be maximized is the system power imbalance after attack. Constraint (11) restricts the decision variable to be binary. Due to limited resources and budget, constraint (12) states that the maximum number of actions can be implemented is N. Equation (13) defines the system power imbalance as the sum of nodal unserved power, which is the objective function of the OPF minimization subproblem as well. The nodal power balance equation is formulated as constraint (14) according to Kirchhoff's Current Law (KCL). Equation (15) defines the DC power flow for each branch. Constraints (16), (17), and (18) give the lower and upper limit for branch power flow, generator output power, and nodal power surplus/deficit, respectively.

The optimization problem (10)–(18) is a two-level AD model: the upper-level (10)–(13) represents the attacker's decision to maximize the system power imbalance; the lower-level (13)–(18) corresponds to the defender's OPF reaction strategy. It should be noted that the lower-level problem is parameterized by the upper-level decision variables z_l.

Although both objective function and constraint of optimization problem (10)–(18) are linear, the optimization problem (10)–(18) cannot be tackled by the majority of off-the-shelf solvers, for example, Cplex, Matlab, and Lingo, and so forth, due to its mixed-integer bilinear *max-min* property. Therefore, the dual theory is utilized in this paper to reformulate the lower-level minimize problem into a maximize one, facilitating the transformation from *max-min* to *max-max*. Since two two-level maximize problem can be easily merged into a single-level one, resulting in a MILP problem, which is suitable for commercial and open-source solvers. In addition to dual theory, the Karush–Kuhn–Tucker (KKT) condition can also be employed to perform the transformation as well.

According to dual theory, the single-level maximize equivalent problem is given as:

$$\Delta = \max_{z_l, \beta_b, \pi_l, \sigma_l, \phi_l, \mu_i} \left\{ \sum_{b \in B} D_b \beta_b - \sum_{l \in L} F_l \sigma_l - \sum_{l \in L} F_l \phi_l - \sum_{i \in I} P_i \mu_i \right\} \tag{19}$$

$$subject\ to:$$

$$z_l = \{0, 1\}; \forall l \in L \tag{20}$$

$$\sum_{l\in L} z_l \le N \tag{21}$$

$$\beta_{bu(i)} - \mu_i \le 0; \forall i \in I \tag{22}$$

$$\beta_{to(l)} - \beta_{fr(l)} + \pi_l + \sigma_l - \phi_l = 0; \forall l \in L \tag{23}$$

$$-1 \le \beta_b \le 1; \forall b \in B \tag{24}$$

$$\sum_{l\in L|to(l)=b} (1-z_l)\,\gamma_l \pi_l - \sum_{l\in L|fr(l)=b} (1-z_l)\,\gamma_l \pi_l = 0; \forall b \in B \tag{25}$$

$$\sigma_l, \phi_l \ge 0; \forall l \in L \tag{26}$$

$$\mu_i \ge 0; \forall i \in I, \tag{27}$$

where constraints (20)–(21) are identical with upper-level constraints (11)–(12), whereas (22)–(25) are dual constraints corresponding to primal variables p_i, f_l, $\{S_b^+,\ S_b^-\}$, and θ, respectively.

Although the optimization problem (19)–(27) is single-level, it is nonlinear due to the production term $z_l \pi_l$ in constraint (25) between binary and continuous variables. For the sake of generating MILP, linearizion process should be implemented, that is, substituting (25) with the following constraints:

$$\sum_{l\in L|to(l)=b} (\gamma_l \pi_l - \gamma_l \tau_l) - \sum_{l\in L|fr(l)=b} (\gamma_l \pi_l - \gamma_l \tau_l) = 0; \forall b \in B \tag{28}$$

$$-M(1-z_l) \le \tau_l - \pi_l \le M(1-z_l); \forall l \in L \tag{29}$$

$$-Mz_l \le \tau_l \le Mz_l; \forall l \in L, \tag{30}$$

where τ_l is introduced to replace $z_l \pi_l$; M is a big positive number; constraints (29)–(30) are included to guarantee the equivalence between τ_l and $z_l \pi_l$, that is, achieving $\tau_l = z_l \pi_l$.

Finally, the mixed-integer bilinear *max-min* problem (10)–(18) is converted into a standard MILP as:

$$Objective: \quad Eq.(19) \tag{31}$$

$$Constraints: \quad Eq.(20)-(24),\ Equation\ (26)-(27),\ Equation\ (28)-(30). \tag{32}$$

3.2. Confrontation with Asymmetric Information

Take branch data into consideration, the asymmetric information means the attacker obtained dataset L' is different from the reality, that is, $L' \neq L$. In order to evaluate the impact of asymmetric information, the following two steps should be implemented:

- Step 1: Calculate the MILP (31)–(32) with the input of L' rather than L, then collect the optimal attack plan z';
- Step 2: Substitute the obtained z' into (25), and calculate the MILP (19)–(27) after the elimination of constraints (20) and (21), then remark the final objective value as Δ'.

In Step 1, the attacker generates an attack plan z' due to asymmetric information L'. In step 2, the attack plan z' is validated with original network, where dataset L is utilized, to evaluate how much power imbalance can be caused to the real system. Therefore, the subtraction between Δ and Δ' provides an ideal indicator to illustrate the impact of asymmetric information. Generally, $\Delta - \Delta'$ is greater than 0, showing that less power imbalance is induced due to the mismatch between L' and L. Therefore, the magnitude of $\Delta - \Delta'$ has a positive correlation with the impact of asymmetric information.

4. Numerical Experiments

In order to identify the impacts of asymmetric information on microgrid confrontation, 3 systems retrieved from Matpower [23] are employed for numerical experiments in this section—`case6ww`,

`case24_ieee_rts`, and `case57`. The simulation program is coded with Matlab 2019b, where Cplex 12.10.0 is called via YALMIP [30] for the solution of MILP. The execution hardware is a 64-bit Windows PC with 16.0 GB RAM and 2 Intel Core i7-7700HQ CPU running at 2.80 GHz.

4.1. Experiment Settings

As shown in Section 3.2, the asymmetric information L' is utilized as input for impact analysis. However, in reality, it is almost impossible to achieve the explicit details of L'. Actually, the difficulty is identical to the attacker who wants to obtain L. Fortunately, the quality of asymmetric information D_{Hybrid} is much easier to be gained, thus it is supposed to be available in the following experiments.

Therefore, in this experiment, the asymmetric information L' is generated based on D_{Hybrid}. It can be seen from (8) that a variety of L' may result into a single D_{Hybrid} value, thus giving a D_{Hybrid} can generate several L'. In order to address this concern, the random sampling strategy is utilized as follows:

- Step 1: Generate the pool of real and fake branches L_{real} and L_{fake}. Obviously, real branch pool is the original circuit, that is, $L_{real} = L$, whose cardinality is n_L. On the other hand, any fake branch can be built between two nodes where there is no real branch, thus $L_{fake} = L_{full} - L_{real}$, where L_{full} is the full set of branch linking any two bus in a system, whose cardinality is $C_n^2 = \frac{n(n-1)}{2}$.
- Step 2: Get the coverage and deviation rates A and B based on the value of D_{Hybrid} and its definition Equation (8).
- Step 3: Compute the number real and fake circuits n_{real} and n_{fake} in the asymmetric information L'. Based on Steps 1 and 2, there has

$$\frac{n_{real}}{n_L} = A, \qquad \frac{n_{fake}}{n_{real} + n_{fake}} = B. \tag{33}$$

  Thus the following result can be obtained

$$n_{real} = An_L, \qquad n_{fake} = \frac{AB}{1-B} n_L. \tag{34}$$

  It should be noted that n_{real} and n_{fake} might not be integers, thus a $round()$ process should be implemented, that is, let $n_{real} = round(n_{real})$ and $n_{fake} = round(n_{fake})$.
- Step 4: Randomly select a number of n_{real} and n_{fake} branches from L_{real} and L_{fake}, then L' can be obtained by combining these two resulted subsets.

It should be pointed out that random numbers are introduced in Step 4, thus a single D_{Hybrid} value may result in a lot of L'. In order to eliminate the influence of randomness, the above steps are implemented 50 times for each D_{Hybrid}, resulting in 50 sets of L'. Taking these L' as input for asymmetric information analysis illustrated in Section 3.2, the minimum, average, maximum value of $\Delta - \Delta'$ will be reported.

Although the original and terminal nodes of each branch in L_{fake} have been fixed in Step 1, other parameters are not identified, for example, susceptance γ_l and power flow capacity F_l. Since each fake line is not included in the original dataset, γ_{ij} and F_{ij} for all $ij \in L_{fake}$ are generated according to the following equations:

$$\gamma_{ij} = average\left(\gamma_l\right), \ where \ \left\{l \in L | fr(l) = i \cup to(l) = i \cup fr(l) = j \cup to(l) = j\right\}, \tag{35}$$

$$F_{ij} = average\left(F_l\right), \ where \ \left\{l \in L | fr(l) = i \cup to(l) = i \cup fr(l) = j \cup to(l) = j\right\}. \tag{36}$$

Take the fake branch 1–6 shown in Figure 1 as an example, there has

$$\gamma_{16} = \frac{\gamma_{12} + \gamma_{14} + \gamma_{15} + \gamma_{26} + \gamma_{36} + \gamma_{56}}{6}. \tag{37}$$

All the datasets utilized in this paper are fetched from Reference [23], but the power flow capacity F_l for `case57` is vacant, that is, $F_l = 0$ for all branches. In this experiment, we randomly generate F_l for these missing values according to the following equation:

$$F_l = 70 + round(10a_l), \tag{38}$$

where $a_l \in [0, 1]$ is a random number subject to standard uniform distribution. Combined with (38), the domain of F_l is $[70,\ 80]$, which is suitable for this system according to the explanation revealed in Reference [31]. For quick reference and reproductivity purposes, `case57` data reported in the appendix of Reference [31] is utilized in this experiment.

If the impact of asymmetric information on microgrid confrontation is analyzed in single fixed circumstance, the conclusion might be biased. Thus a variety of scenarios are generated for simulation, including different levels of asymmetric information D_{Hybrid} and attack strength R_a. In this experiment, D_{Hybrid} is sampled on 6 values: 100.0, 90.1, 80.2, 70.3, 60.4, and 50.5, with the $V_{Fitness}$ corresponds to 1.0, 0.8, 0.6, 0.4, 0.2, and 0.0, respectively; R_a takes 5 values: 10%, 20%, 30%, 40%, and 50%. For each R_a, the result of N in (21) is obtained as $N = R_a n_L$, that is, the attack strength is capable to destroy a rate of R_a branches compared with the total number of real circuits.

Based on the above settings, 30 sets of simulation results will be generated for each target system, and each set is obtained based on a statistic of 50 random simulations.

4.2. The 6-bus System

As shown in Figure 1, the 6-bus system consists of 6 buses, 11 branches, 3 generators, and 3 loads, thus $n = 6$ and $n_L = 11$. In terms of different values of D_{Hybrid}, the numbers of n_{real} and n_{fake} can be calculated according to (34). Table 3 summarizes the result. Based on $C_n^2 = \frac{n(n-1)}{2}$, L_{full} contains 15 circuits, therefore the cardinality of L_{fake} is 4, which means n_{fake} should be less than or equal to 4. However, n_{fake} is 6 when D_{Hybrid} takes 50.5, indicating that $D_{Hybrid} = 50.5$ is not suitable for this system. Therefore, another set of D_{Hybrid} ranging from 100.0 to 70.25 is employed for `case6ww`, and the corresponding n_{real} and n_{fake} are reported in Table 3 as well. In Table 3, 'Sum' is equal to the cardinality of asymmetric information L'.

Table 3. Two settings of D_{Hybrid} for `case6ww`.

Setting 1					**Setting 2**				
D_{Hybrid}	$V_{Fitness}$	n_{real}	n_{fake}	**Sum**	D_{Hybrid}	$V_{Fitness}$	n_{real}	n_{fake}	**Sum**
100.0	1.0	11	0	11	100.0	1.0	11	0	11
90.10	0.8	10	1	11	95.05	0.9	10	1	11
80.20	0.6	9	2	11	90.10	0.8	10	1	11
70.30	0.4	8	3	11	85.15	0.7	9	2	11
60.40	0.2	7	4	11	80.20	0.6	9	2	11
50.50	0.0	6	6	12	75.25	0.5	8	3	11

Based on the above Setting 2 and different values of R_a, numerical experiments are implemented on `case6ww` and the result is collected in Table 4. $D_{Hybrid} = 100.0$ means the information obtained by attacker is symmetric, thus there is no variation for 50 random simulations, that is, the minimum, average, and maximum are always identical. Due to its symmetric information feature, its result on different attack strength is utilized as a denominator to calculate the damage percentage. It can be seen from Table 4 that the majority of damage percentage value is less than 100%, which means the resulted system power imbalance is smaller than symmetric information, that is, the effect of attack is weakened by the introduction of asymmetric information.

Table 4. Numerical simulation results of `case6ww`.

$(D_{Hybrid}, V_{Fitness})$		Attack Strength = (R_a, N); Power Imbalance = (Δ, Damage Percentage)									
		(10%, 1)		(20%, 2)		(30%, 3)		(40%, 4)		(50%, 6)	
		Δ	**Per.**	**Δ**	**Per.**	**Δ**	**Per.**	**Δ**	**Per.**	**Δ**	**Per.**
(100.0, 1.0)	Min.	0.00	\	50.00	100.0%	70.00	100.0%	95.00	100.0%	180.00	100.0%
	Avg.	0.00	\	50.00	100.0%	70.00	100.0%	95.00	100.0%	180.00	100.0%
	Max.	0.00	\	50.00	100.0%	70.00	100.0%	95.00	100.0%	180.00	100.0%
(95.05, 0.9)	Min.	0.00	\	0.00	0.0%	0.00	0.0%	35.00	36.8%	100.00	55.6%
	Avg.	0.00	\	19.02	38.0%	44.56	63.7%	79.97	84.2%	135.73	75.4%
	Max.	0.00	\	50.00	100.0%	70.00	100.0%	95.00	100.0%	180.00	100.0%
(90.10, 0.8)	Min.	0.00	\	0.00	0.0%	0.00	0.0%	35.00	36.8%	116.54	64.7%
	Avg.	0.00	\	29.84	59.7%	44.63	63.8%	77.70	81.8%	144.46	80.3%
	Max.	0.00	\	50.00	100.0%	70.00	100.0%	95.00	100.0%	180.00	100.0%
(85.15, 0.7)	Min.	0.00	\	0.00	0.0%	0.00	0.0%	10.00	10.5%	40.00	22.2%
	Avg.	0.00	\	12.98	26.0%	23.92	34.2%	48.08	50.6%	109.36	60.8%
	Max.	0.00	\	50.00	100.0%	70.00	100.0%	95.00	100.0%	180.00	100.0%
(80.20, 0.6)	Min.	0.00	\	0.00	0.0%	0.00	0.0%	5.71	6.0%	50.00	27.8%
	Avg.	0.00	\	9.96	19.9%	21.89	31.3%	52.52	55.3%	109.13	60.6%
	Max.	0.00	\	50.00	100.0%	70.00	100.0%	95.00	100.0%	180.00	100.0%
(75.25, 0.5)	Min.	0.00	\	0.00	0.0%	0.00	0.0%	0.00	0.0%	3.33	1.9%
	Avg.	0.00	\	1.77	3.5%	14.45	20.6%	34.52	36.3%	70.56	39.2%
	Max.	0.00	\	50.00	100.0%	58.57	83.7%	84.53	89.0%	120.00	66.7%

Although Table 4 concludes all experiment results, it is very difficult to draw significant conclusions due to its messy layout. In order to facilitate the observation, Figure 4 is given to rephrase the data reported in Table 4, where the box chart is introduced for presentation, with the lower bar, middle mark, and upper bar corresponding to the minimum, average, and maximum values, respectively. If the middle mark is closer to the lower/upper bar, the average suffers more effect from the minimum/maximum value. At first sight, it is obvious that the power imbalance is higher with the stronger attack strength. For each R_a, $D_{Hybrid} = 100.0$ should be observed first since it represents the symmetric information, and the result provides a basis for the analysis of asymmetric information. Take $R_a = 10\%$ as an example, the system power imbalance is 0 for all $D_{Hybrid} = 100.0$, indicating that the system can withstand a broken of 10% branches. If the damage caused by an attacker with accurate information is 0, then 0 power imbalance can be induced with asymmetric information, which is identical to Figure 4. If R_a goes higher to 20%, 50MW load cannot be served when $D_{Hybrid} = 100.0$. It should be pointed out that, the minimum of Δ can reach 0 for all five $D_{Hybrid} \neq 100.0$ cases, which means the attack has no effect on system loads at some scenarios out of 50 samples. On the other hand, a 50 MW power imbalance can also be caused by these attacks, showing the effect of asymmetric information may not be helpful. However, the average of Δ is reducing with the decreasing of D_{Hybrid}, thus benefits from the introduction of asymmetric information have been validated. Similar findings can be generated for R_a equals 30%, 40%, and 50%. One interesting observation is that, if $D_{Hybrid} = 75.25$, the minimum damage can be as small as 0, and the maximum is always smaller than the case of $D_{Hybrid} = 100.0$. Therefore, it can be concluded that asymmetric information with a level of $D_{Hybrid} = 75.25$ or lesser will always result in weaker damage than symmetric information.

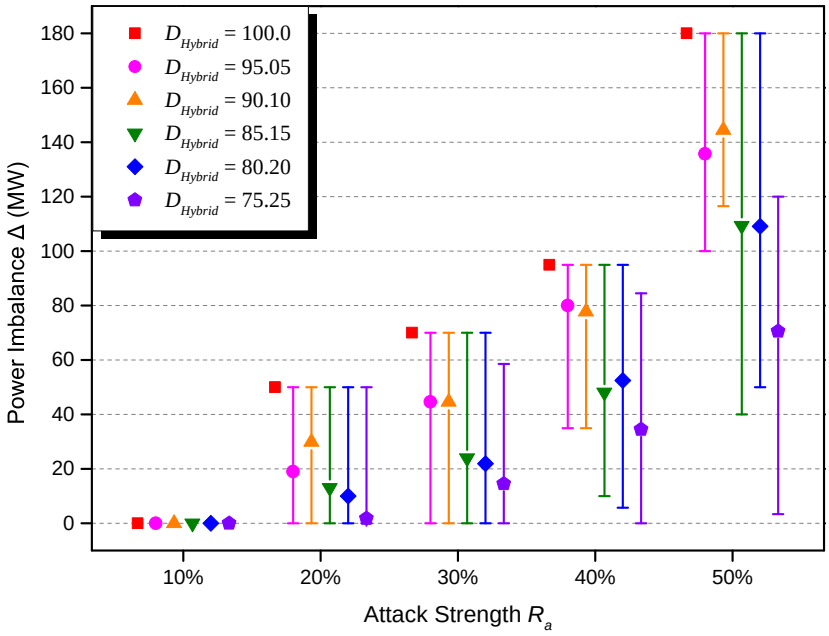

Figure 4. The impact of asymmetric information on system power imbalance under different attack strength levels for `case6ww`.

In addition to Figure 4, Table 4 can be interpreted from another dimension as shown in Figure 5. It can be seen that the difference between $R_a = 10\%$ and $R_a = 50\%$ is getting smaller from $D_{Hybrid} = 100.0$ to $D_{Hybrid} = 75.25$, indicating that the destruction effect gained form the increase of attack strength is diminished by asymmetric information. Therefore, if deception strategies are utilized by defender to increase the level of asymmetric information, the microgrid system can withstand stronger attack strength in confrontations.

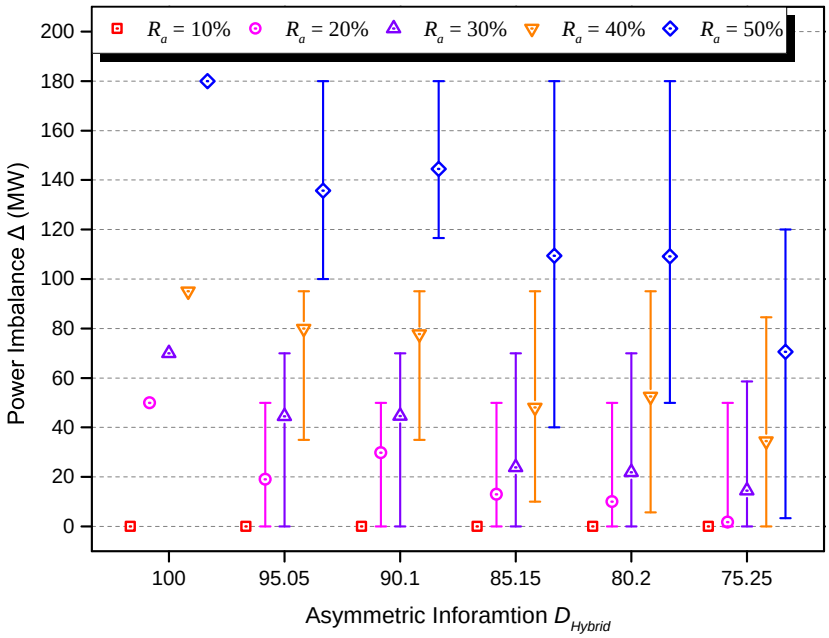

Figure 5. The impact of attack strength on system power imbalance under different asymmetric information levels for `case6ww`.

4.3. The 24-bus System

The original data of `case24-ieee-rts` are downloaded from Reference [23], where several generators are connected into one node and there exist two or more circuits between two buses. In this experiment, these supplement generators and circuits are evolved into a single one with their capability accumulated, thus 24 buses, 34 branches, 10 generators, and 17 loads, are included in this system. Based on the default experiment settings given in Section 4.1, results are generated and reported in Table 5.

Table 5. Numerical simulation results of `case24-ieee-rts`.

$(D_{Hybrid}, V_{Fitness})$		Attack Strength = (R_a, N); Power Imbalance = (Δ, Damage Percentage)									
		(10%, 3)		(20%, 7)		(30%, 10)		(40%, 14)		(50%, 17)	
		Δ	**Per.**	**Δ**	**Per.**	**Δ**	**Per.**	**Δ**	**Per.**	**Δ**	**Per.**
(100.0, 1.0)	Min.	387.0	100.0%	1373.0	100.0%	1468.0	100.0%	1607.0	100.0%	1607.0	100.0%
	Avg.	387.0	100.0%	1373.0	100.0%	1468.0	100.0%	1607.0	100.0%	1607.0	100.0%
	Max.	387.0	100.0%	1373.0	100.0%	1468.0	100.0%	1607.0	100.0%	1607.0	100.0%
(90.1, 0.8)	Min.	0.0	0.0%	106.0	7.7%	110.0	7.5%	445.0	27.7%	456.0	28.4%
	Avg.	114.4	29.6%	832.1	60.6%	1033.9	70.4%	1144.4	71.2%	1248.2	77.7%
	Max.	387.0	100.0%	1373.0	100.0%	1468.0	100.0%	1607.0	100.0%	1607.0	100.0%
(80.2, 0.6)	Min.	0.0	0.0%	0.0	0.0%	0.0	0.0%	0.0	0.0%	299.9	18.7%
	Avg.	59.3	15.3%	305.1	22.2%	534.8	36.4%	666.1	41.4%	923.4	57.5%
	Max.	309.0	79.8%	973.0	70.9%	1052.0	71.7%	1428.0	88.9%	1607.0	100.0%
(70.3, 0.4)	Min.	0.0	0.0%	0.0	0.0%	0.0	0.0%	0.0	0.0%	0.0	0.0%
	Avg.	32.3	8.3%	156.5	11.4%	229.4	15.6%	456.8	28.4%	593.3	36.9%
	Max.	309.0	79.8%	698.0	50.8%	698.0	47.5%	1428.0	88.9%	1253.0	78.0%
(60.4, 0.2)	Min.	0.0	0.0%	0.0	0.0%	0.0	0.0%	0.0	0.0%	0.0	0.0%
	Avg.	10.4	2.7%	55.1	4.0%	113.5	7.7%	226.4	14.1%	431.2	26.8%
	Max.	309.0	79.8%	473.0	34.5%	873.0	59.5%	977.0	60.8%	1373.0	85.4%
(50.5, 0.0)	Min.	0.0	0.0%	0.0	0.0%	0.0	0.0%	0.0	0.0%	0.0	0.0%
	Avg.	3.3	0.9%	39.5	2.9%	80.6	5.5%	97.8	6.1%	184.0	11.5%
	Max.	165.0	42.6%	309.0	22.5%	564.0	38.4%	698.0	43.4%	623.0	38.8%

Generally, Table 5 shows a similar feature with Table 4. In order to further investigate the difference, damage percentage is employed for comparison as the level of system power imbalance is quite different. Therefore, Table 6 is obtained from the subtraction of Table 4 by Table 5. It can be seen that the majority of percentage difference value is greater or equal than 0%, indicating that better performance on the defense (less damage percentage) has been achieved by `case24-ieee-rts`.

Figure 6 illustrates the increase of power imbalance Δ across different level of attack strength R_a. If $D_{Hybrid} = 100.0$, there is a flat tail on the trend line, that is, $\Delta_{\{R_a=40\%\}} = \Delta_{\{R_a=50\%\}}$, meaning the attack limit has been reached. Therefore, it can be concluded that the system can be destroyed with $R_a = 40\%$ of attack strength under symmetric information. On the other hand, the attack limit is much larger than 40% for asymmetric information, which is validated by Figure 7, where additional experiments are carried out on $R_a = \{60\%,\ 70\%,\ 80\%,\ 90\%,\ 100\%\}$. It is shown in Figure 7 that, if symmetric information is obtained by attacker, the power imbalance can be reached under $R_a = 10\%$ is 387 MW, which cannot be arrived without $R_a = 50\%$ and 90% under asymmetric information circumstance $D_{Hybrid} = 70.30$ and 50.50, respectively. In addition, if asymmetric information $D_{Hybrid} = \{90.1,\ 80.2,\ 70.3,\ 60.4,\ 50.5\}$ is involved, the system cannot be destroyed even it suffers an attack strength of $R_a = 100\%$.

Table 6. Difference on the damage percentage between `case6ww` and `case24-ieee-rts`.

$(D_{Hybrid}, V_{Fitness})$		R_a = 10%	R_a = 20%	R_a = 30%	R_a = 40%	R_a = 50%
(100.0, 1.0)	Min.	\	0.00%	0.00%	0.00%	0.00%
	Avg.	\	0.00%	0.00%	0.00%	0.00%
	Max.	\	0.00%	0.00%	0.00%	0.00%
(90.1, 0.8)	Min.	\	−7.72%	−7.49%	9.15%	27.18%
	Avg.	\	−22.57%	−6.76%	12.97%	−2.27%
	Max.	\	0.00%	0.00%	0.00%	0.00%
(80.2, 0.6)	Min.	\	0.00%	0.00%	36.84%	46.08%
	Avg.	\	37.46%	27.32%	40.34%	22.80%
	Max.	\	29.13%	28.34%	11.14%	0.00%
(70.3, 0.4)	Min.	\	0.00%	0.00%	10.53%	22.22%
	Avg.	\	14.56%	18.54%	22.18%	23.84%
	Max.	\	49.16%	52.45%	11.14%	22.03%
(60.4, 0.2)	Min.	\	0.00%	0.00%	6.02%	27.78%
	Avg.	\	15.91%	23.53%	41.19%	33.79%
	Max.	\	65.55%	40.53%	39.20%	14.56%
(50.5, 0.0)	Min.	\	0.00%	0.00%	0.00%	1.85%
	Avg.	\	0.67%	15.15%	30.26%	27.75%
	Max.	\	77.49%	45.25%	45.55%	27.90%

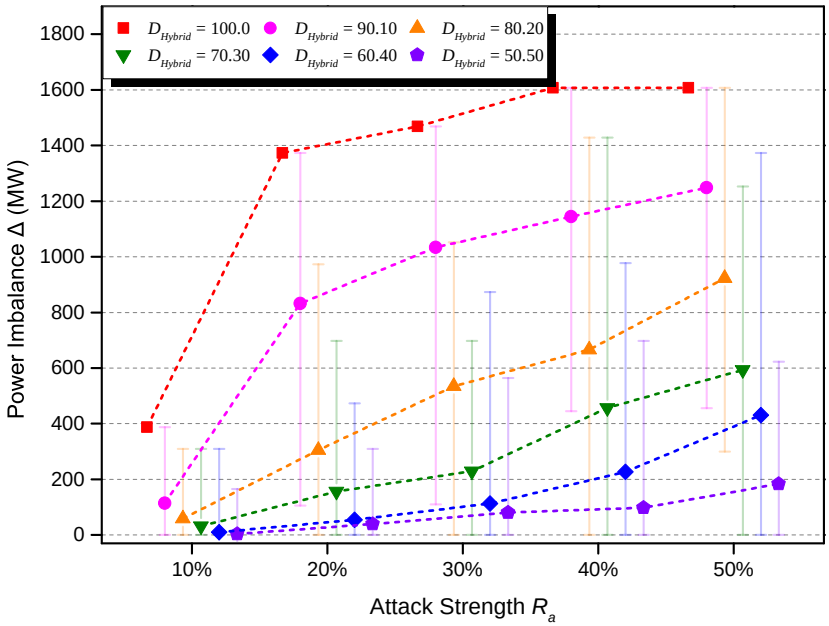

Figure 6. The impact of asymmetric information on system power imbalance under different attack strength levels for `case24-ieee-rts`.

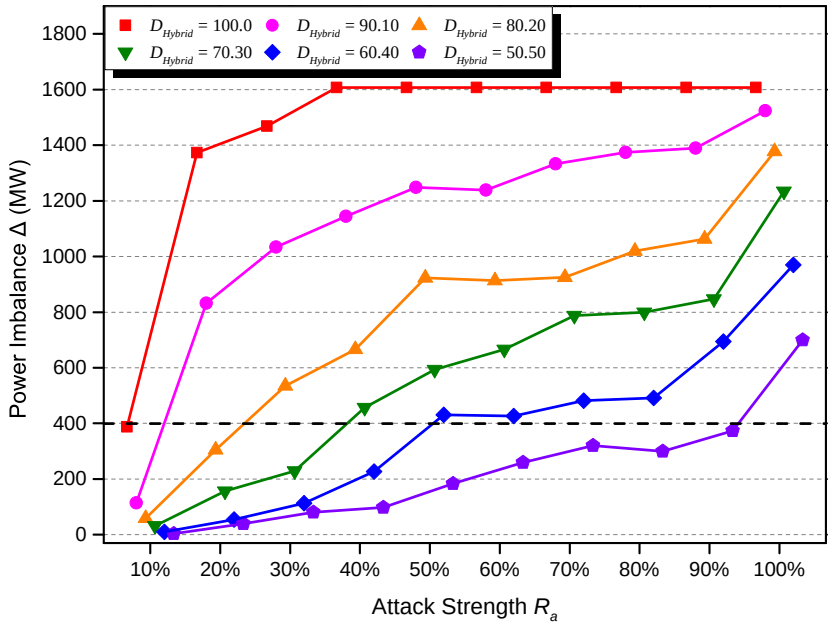

Figure 7. Influence of asymmetric information on system power imbalance for `case24-ieee-rts`.

4.4. The 57-bus System

This grid consists of 57 buses, 78 branches, 7 generators, and 42 loads. Table 7 summarizes the simulation results. In each column, the power balance is decreasing as D_{Hybrid} decreases, validating the fact that system damage is partially eliminated by asymmetric information. Similar to the former two cases, Figure 8 is presented to give an intuitive vision. It can be seen that the attack limit is reached when $R_a = 20\%$, which is much earlier than `case24-ieee-rts`, resulting in a long flat tail. In order to adjust the tail into similar figure with `case6ww` and `case24-ieee-rts`, the following two attempts are taken:

- If the branch capacity is increased, the system might not be such easy to be destroyed. Thus, the first strategy is increasing the predefined range of F_l from $[70,\ 80]$ to $[100,\ 110]$ by adding 30 MW to (38). However, only minor variations are obtained in comparison with Table 7 and Figure 8.
- The second strategy is reducing the attack strength from $R_a = \{10\%,\ 20\%,\ 30\%,\ 40\%,\ 50\%\}$ to $R_a = \{00\%,\ 5\%,\ 10\%,\ 15\%,\ 20\%\}$ based on the assumption that the system attack limit cannot be easily revised. Result is illustrated in Figure 9, expressing a similar pattern with the former two cases.

Table 7. Numerical simulation results of `case57`.

$(D_{Hybrid}, V_{Fitness})$		Attack Strength = (R_a, N); Power Imbalance = (Δ, Damage Percentage)									
		(10%, 8)		(20%, 16)		(30%, 23)		(40%, 31)		(50%, 39)	
		Δ	Per.	Δ	Per.	Δ	Per.	Δ	Per.	Δ	Per.
(100.0, 1.0)	Min.	403.8	100.0%	449.8	100.0%	449.8	100.0%	449.8	100.0%	449.8	100.0%
	Avg.	403.8	100.0%	449.8	100.0%	449.8	100.0%	449.8	100.0%	449.8	100.0%
	Max.	403.8	100.0%	449.8	100.0%	449.8	100.0%	449.8	100.0%	449.8	100.0%
(90.1, 0.8)	Min.	140.4	34.8%	226.8	50.4%	230.8	51.3%	259.8	57.8%	255.8	56.9%
	Avg.	302.1	74.8%	362.1	80.5%	379.3	84.3%	398.5	88.6%	375.6	83.5%
	Max.	403.8	100.0%	449.8	100.0%	449.8	100.0%	449.8	100.0%	449.8	100.0%
(80.2, 0.6)	Min.	117.5	29.1%	159.6	35.5%	214.8	47.8%	177.1	39.4%	219.7	48.8%
	Avg.	250.9	62.1%	303.3	67.4%	318.2	70.7%	340.2	75.6%	331.1	73.6%
	Max.	403.8	100.0%	424.8	94.4%	449.8	100.0%	449.8	100.0%	449.8	100.0%
(70.3, 0.4)	Min.	55.0	13.6%	154.8	34.4%	136.0	30.2%	166.9	37.1%	105.6	23.5%
	Avg.	183.0	45.3%	257.7	57.3%	275.7	61.3%	268.4	59.7%	274.8	61.1%
	Max.	303.6	75.2%	416.8	92.7%	417.0	92.7%	416.8	92.7%	416.8	92.7%
(60.4, 0.2)	Min.	42.2	10.5%	79.0	17.6%	109.8	24.4%	120.3	26.7%	60.5	13.5%
	Avg.	153.5	38.0%	206.6	45.9%	238.7	53.1%	244.4	54.3%	227.4	50.6%
	Max.	314.8	78.0%	403.8	89.8%	403.8	89.8%	365.8	81.3%	345.8	76.9%
(50.5, 0.0)	Min.	6.7	1.7%	38.6	8.6%	41.1	9.1%	56.8	12.6%	72.7	16.2%
	Avg.	96.6	23.9%	155.6	34.6%	186.9	41.6%	187.9	41.8%	188.3	41.9%
	Max.	229.8	56.9%	293.8	65.3%	329.0	73.1%	403.8	89.8%	360.8	80.2%

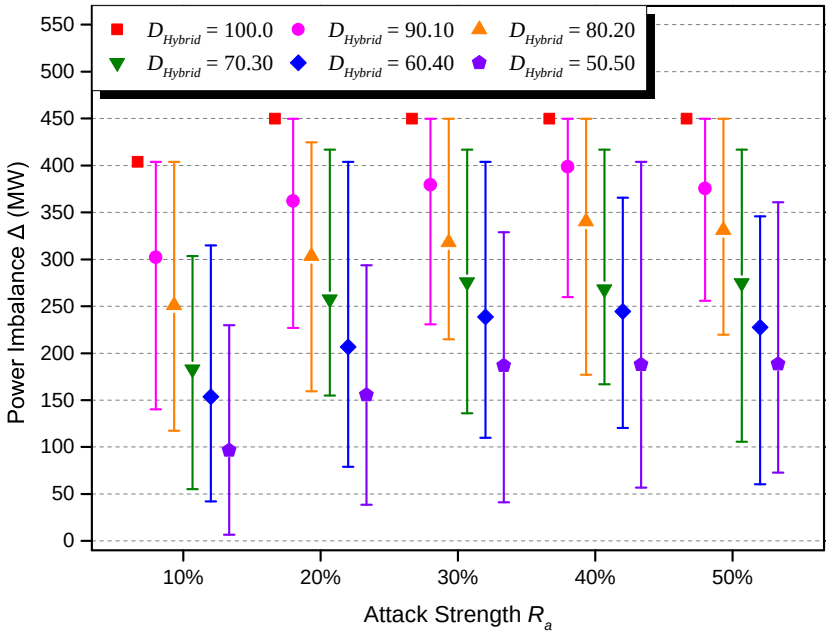

Figure 8. The impact of asymmetric information on system power imbalance under different attack strength levels for `case57`.

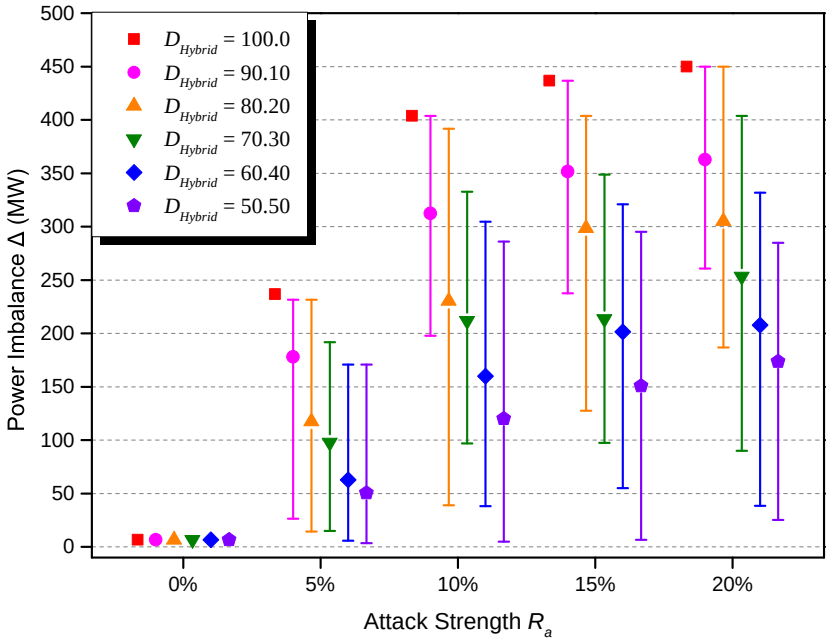

Figure 9. The impact of asymmetric information on system power imbalance under different attack strength levels for `case57`.

4.5. Discussion

Observing Figures 6, 8 and 9, it can be seen that in each column with a fixed R_a value, the system power imbalance is monotonically decreasing from $D_{Hybrid} = 100.0$ to $D_{Hybrid} = 50.50$. Since the $V_{Fitness}$ value corresponding to $D_{Hybrid} = \{100.0,\ 90.1,\ 80.2,\ 70.3,\ 60.4,\ 50.5\}$ is $\{1.0,\ 0.8,\ 0.6,\ 0.4,\ 0.2,\ 0.0\}$, showing an monotonic decrease trend as well, it can be carefully deduced that under any given R_a, the system suffers less damage if $V_{Fitness}$ is smaller. However, Figure 4 is an exception with violations at $R_a = 20\%$, $R_a = 40\%$, and $R_a = 50\%$. Take $D_{Hybrid} = 95.05$ and $D_{Hybrid} = 90.10$ at $R_a = 20\%$ as an example, there has $\Delta_{\{D_{Hybrid}=95.05\}} < \Delta_{\{D_{Hybrid}=90.10\}}$ in Figure 4. Compared with $D_{Hybrid} = 95.05$, the attacker with $D_{Hybrid} = 90.10$ asymmetric information has smaller coverage rate A and larger deviation rate B, thus the caused power imbalance should be less based on common sense and logical analysis. The reason for the irrational results in Figure 4 is statistical bias due to limited sample number. In order to validate the explanation, additional experiments with 200 samples are implemented. Finally, the violation is eliminated. Therefore, it can be concluded that the definitions of D_{Hybrid} and $V_{Fitness}$ are generally reasonable for wide utilization on judgment, comparison, and decision-making, and so forth.

5. Conclusions

The asymmetric information in military microgrid confrontation is proposed and investigated in this paper. In order to facilitate the description, symmetric and asymmetric information is distinguished. Since the existing method is not suitable to evaluate the level of information mismatch, a novel asymmetric information assessment metric is proposed, where coverage and deviation rates are included. On the other hand, the military microgrid confrontation is formulated as an AD model, which is addressed via dual theory and big-M method. The resulted MILP is then solved by the on-the-shelf solver Cplex. With the consideration of various levels of attack strength, numerical experiments are implemented on three systems retrieved from Matpower ranging from 6-bus to 57-bus. Results indicate that asymmetric information is beneficial to alleviate attack damage and improve defensive performance. Although only branch-tripping is considered in this paper, we intend to claim that the definition of assessment metric and influence analysis methodology can be easily extended to other types of attacks where there is an information gap between defender and attacker.

Author Contributions: Investigation, P.J.; Methodology, P.J.; Supervision, T.Z.; Validation, S.H.; Writing—original draft, S.H.; Writing—review & editing, T.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Distinguished Natural Science Foundation of Hunan Province (No. 2017JJ1001) and the National Natural Science Foundation of China (Nos. 71901210, 61973310). This work was also supported by the China Postdoctoral Science Foundation (No. 2017M623381).

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

References

1. Kashem, S.B.A.; De Souza, S.; Iqbal, A.; Ahmed, J. Microgrid in military applications. In Proceedings of the IEEE 12th International Conference on Compatibility, Power Electronics and Power Engineering (CPE-POWERENG), Doha, Qatar, 10–12 April 2018; pp. 1–5.
2. Strakos, J.K.; Quintanilla, J.A.; Huscroft, J.R. Department of Defense energy policy and research: A framework to support strategy. *Energy Policy* **2016**, *92*, 83–91. [CrossRef]
3. Van Broekhoven, S.; Judson, N.; Galvin, J.; Marqusee, J. Leading the Charge: Microgrids for Domestic Military Installations. *IEEE Power Energy Mag.* **2013**, *11*, 40–45. [CrossRef]
4. Stamp, J. The SPIDERS project—Smart Power Infrastructure Demonstration for Energy Reliability and Security at US military facilities. In Proceedings of the IEEE PES Innovative Smart Grid Technologies (ISGT), Washington, DC, USA, 16–20 January 2012; p. 1.
5. Johnson, M.D.; Ducey, R.A. Overview of U.S. Army microgrid efforts at fixed installations. In Proceedings of the IEEE Power & Energy Society General Meeting, Detroit, MI, USA, 24–29 July 2011; pp. 1–2.
6. Podlesak, T.; Vitale, J.; Wilson, B.; Bohn, F.; Gonzalez, M.; Bosse, R.; Siegfried, S.; Lynch, J.; Barnhill, W. Auto-Tuning for Military Microgrids. In Proceedings of the IEEE Energy Conversion Congress and Exposition (ECCE), Baltimore, MD, USA, 29 September–3 October 2019; pp. 6270–6277.
7. Masrur, M.A.; Skowronska, A.G.; Hancock, J.; Kolhoff, S.W.; McGrew, D.Z.; Vandiver, J.C.; Gatherer, J. Military-Based Vehicle-to-Grid and Vehicle-to-Vehicle Microgrid—System Architecture and Implementation. *IEEE Trans. Transp. Electrif.* **2018**, *4*, 157–171. [CrossRef]
8. Xiang, Y.; Wang, L.; Liu, N. Coordinated attacks on electric power systems in a cyber-physical environment. *Electr. Power Syst. Res.* **2017**, *149*, 156–168. [CrossRef]
9. Ali, S.; Li, Y. Learning Multilevel Auto-Encoders for DDoS Attack Detection in Smart Grid Network. *IEEE Access* **2019**, *7*, 108647–108659. [CrossRef]
10. Liu, X.; Li, Z. False data attack models, impact analyses and defense strategies in the electricity grid. *Electr. J.* **2017**, *30*, 35–42. [CrossRef]
11. Xiang, Y.; Wang, L. A game-theoretic study of load redistribution attack and defense in power systems. *Electr. Power Syst. Res.* **2017**, *151*, 12–25. [CrossRef]
12. Zhu, Y.; Yan, J.; Tang, Y.; Sun, Y.L.; He, H. Joint Substation-Transmission Line Vulnerability Assessment Against the Smart Grid. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1010–1024. [CrossRef]
13. He, H.; Yan, J. Cyber-physical attacks and defences in the smart grid: A survey. *IET Cyber-Phys. Syst. Theor. Appl.* **2016**, *1*, 13–27. [CrossRef]
14. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2020**, *169*, 107094. [CrossRef]
15. Lu, X.; Wang, J.; Guo, L. Using microgrids to enhance energy security and resilience. *Electr. J.* **2016**, *29*, 8–15. [CrossRef]
16. Wang, Y.; Chen, C.; Wang, J.; Baldick, R. Research on Resilience of Power Systems Under Natural Disasters—A Review. *IEEE Trans. Power Syst.* **2016**, *31*, 1604–1613. [CrossRef]
17. Lai, K.; Illindala, M.; Subramaniam, K. A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyber-physical environment. *Appl. Energy* **2019**, *235*, 204–218. [CrossRef]
18. Lin, Y.; Bie, Z. Tri-level optimal hardening plan for a resilient distribution system considering reconfiguration and DG islanding. *Appl. Energy* **2018**, *210*, 1266–1279. [CrossRef]
19. Zeng, B.; Zhao, L. Solving two-stage robust optimization problems using a column-and-constraint generation method. *Oper. Res. Lett.* **2013**, *41*, 457–461. [CrossRef]

20. Lei, H.; Huang, S.; Liu, Y.; Zhang, T. Robust Optimization for Microgrid Defense Resource Planning and Allocation Against Multi-Period Attacks. *IEEE Trans. Smart Grid* **2019**, *10*, 5841–5850. [CrossRef]
21. Lai, K.; Wang, Y.; Shi, D.; Illindala, M.S.; Jin, Y.; Wang, Z. Sizing battery storage for islanded microgrid systems to enhance robustness against attacks on energy sources. *J. Mod. Power Syst. Clean Energy* **2019**, *7*, 1177–1188. [CrossRef]
22. Costa, A.; Georgiadis, D.; Ng, T.S.; Sim, M. An optimization model for power grid fortification to maximize attack immunity. *Int. J. Electr. Power Energy Syst.* **2018**, *99*, 594–602. [CrossRef]
23. Zimmerman, R.D.; Murillo-Sanchez, C.E.; Thomas, R.J. MATPOWER: Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education. *IEEE Trans. Power Syst.* **2011**, *26*, 12–19. [CrossRef]
24. Haghighat, H.; Zeng, B. Bilevel Mixed Integer Transmission Expansion Planning. *IEEE Trans. Power Syst.* **2018**, *33*, 7309–7312. [CrossRef]
25. Xiang, Y.; Wang, L. An Improved Defender–Attacker–Defender Model for Transmission Line Defense Considering Offensive Resource Uncertainties. *IEEE Trans. Smart Grid* **2019**, *10*, 2534–2546. [CrossRef]
26. Davarikia, H.; Barati, M.; Al-Assad, M.; Chan, Y. A novel approach in strategic planning of power networks against physical attacks. *Elect. Power Syst. Res.* **2020**, *180*, 106140. [CrossRef]
27. Wang, Z.; Perera, A. Robust optimization of power grid with distributed generation and improved reliability. *Energy Procedia* **2019**, *159*, 400–405. [CrossRef]
28. Zeraati, M.; Aref, Z.; Latify, M.A. Vulnerability Analysis of Power Systems Under Physical Deliberate Attacks Considering Geographic-Cyber Interdependence of the Power System and Communication Network. *IEEE Syst. J.* **2018**, *12*, 3181–3190. [CrossRef]
29. Davarikia, H.; Barati, M. A tri-level programming model for attack-resilient control of power grids. *J. Mod. Power Syst. Clean Energy* **2018**, *6*, 918–929. [CrossRef]
30. Löfberg, J. YALMIP: A Toolbox for Modeling and Optimization in MATLAB. In Proceedings of the 2004 IEEE International Conference on Robotics and Automation (IEEE Cat. No.04CH37508), New Orleans, LA, USA, 2–4 September 2004; pp. 284–289.
31. Jiang, P.; Huang, S.; Zhang, T. Optimal Deception Strategies in Power System Fortification against Deliberate Attacks. *Energies* **2019**, *12*, 342. [CrossRef]