Analysis of Joint Cyber-Attacks Strategy in Micro-Grid System

Cheng-Wu Shao
Dept of Industrial Engineering, Tsinghua University
Beijing, China
scw18@mails.tsinghua.edu.cn

Yan-Fu Li
Dept of Industrial Engineering, Tsinghua University
Beijing, China
liyanfu@tsinghua.edu.cn

***Abstract*—The information transmission process in the communication network of micro-grid might be attacked by the malicious attacker, misleading the decision of its control center and then increase cost. Different from the previous researches, which focus on the effect of single cyber-attack on micro-grid, this work explores the effect of joint cyber-attacks on micro-grid. Based on our previous work, we can evaluate the performance of the micro-grid under cyber-attack. In this paper, we will first quantify the impacts of denial of service attack(DOS) and false data injection attack(FDI) to the micro-grid, and study different severities of DOS and FDI to micro-grid. Then we will explore the effect of joint cyber-attacks on the micro-grid system, and analysis of co-effect of joint cyber-attacks. At last, we can give attack strategies to attackers as well as defensive strategies to defenders.**

Keywords- Joint cyber-attacks, DOS, FDI, Co-effect

I. INTRODUCTION

Distributed renewable energy is widely used in power grid, taking economy and cleanliness to the power grid as well as unreliability. Micro-grid has emerged to enhance stability and reduce cost by means of dispatching optimal power flow in micro-grid. To achieve this goal, information exchange is needed between its control center and physical components[1]. The Open communication network is more popular for micro-grid operators because of high installation cost of a new closed network, whose openness leaves opportunity for malicious cyber attackers[2-4].

In previous researches, most researchers focus on the system frequency and network status of micro-grid, ignoring the voltage variation and main grid connecting dependency. For example, system frequency declining model by Jahan and Habiba[5], DDoS attacks simulation on NeSSi2 platform by Asri and Pranggono[6], and study of frequency variation on isolated or clustered micro-grids by Farraj et al[7]. However, severe frequency drop hardly happens in a micro-grid system connecting with the main grid, and attacking generator is difficult for attackers because it is the most heavily defended place in the system. Therefore, the influences of most cyber-attacks are beyond the reach of severe frequency problems. Thus, a new evaluation method for identifying the effect of cyber-attack on micro-grid is needed.

In our former research presented in the 65th Annual Reliability & Maintainability Symposium, we have investigated the performance variations of micro-grid system under four types of cyber-attacks, which are denial of service attack, RF jamming attack, replay attack, and false data injection attack. This work put forwards a quantitative evaluation method for performance analysis of micro-grid under cyber-attack, which is helpful for attack and defense strategy making for the grid operator. Similar to former work, little of them have involved with multiple cyber-attacks, although coordinated attacks become a trend nowadays. So, the studies on multiple cyber-attacks on micro-grid simultaneous and asynchronous are urgent.

The rest of this paper organizes as follows: Section II describes the micro-grid system model and cyber-attacks model; Section III analyses the impact of different situations of joint cyber-attacks to micro-grid; Section IV concludes this work.

II. MODEL OF MICRO-GRID AND CYBER-ATTACKS

A. Simulator structure

We inherited the simulator, a radial topology micro-grid connected with the main grid, used in the previous study. This micro-grid has four areas ($a_i, i = 1,\dots,4$), each area may consist of loads (sl_{ik}), storage (st_i) or renewable generator (solar photovoltaics pv_i) and connects to a main transmission line l through a shunt compensator(qb_i)and a transformer. Feeders impedance in an area is negligible, but the main transmission line impedance cannot be ignored. A typical structure of micro-grid is shown in Figure 1.

B. Physical component characteristics

For storage st_i, US_i is the capacity, PSm_i is the rated power, $LS_{i,\mathrm{n}}$ is real-time energy stored at the beginning of $t = n$ period, $PS_{i,n}$ is real-time power output at the beginning of $t = n$ period, μ is transformation efficiency, Δt is time duration of one period. Restrictions are the Eqs. (1) to (3).

978-1-7281-0860-5/19/$31.00 ©2019 IEEE

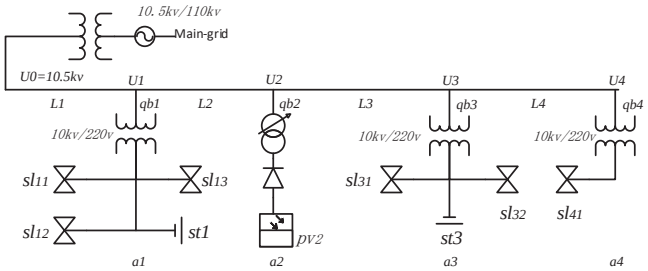

Figure 1. Structure of micro-grid

$$\left|PS_{i,n}\right| \le PSm_i \tag{1}$$

$$LS_{i,n+1} = \mu \cdot PS_{i,n} \cdot \Delta t + LS_{i,n} \tag{2}$$

$$0 \le LS_{i,n+1} \le US_i \tag{3}$$

For transmission line l, U_i is the voltage of area a_i, I_i is current of area a_i, the length between each area is L_i $(i = 1,2,3,4)$, the unit impedance of the main transmission line is z, i represents the serial number of different areas. Their relationship is shown as Eq. (4). U_0 is voltage at the start point of l.

$$U_{(i-1)} = U_i + z \cdot L_i \cdot \sum_{j=i}^{4} I_j \tag{4}$$

For load $sl_{ik}(sl_{ik} \in a_i)$ under the rated voltage $(U_s = 220V)$ at $t = n$ period, $ELP_{ik,n}$ is the expected active power and $ELQ_{ik,n}$ is the expected reactive power. For load $sl_{ik}(sl_{ik} \in a_i)$ under actual voltage (U_i) at $t = n$ period, $ALP_{ik,n}$ is the real-time active power and $ALQ_{ik,n}$is the real-time reactive power. For simplicity, we suppose that loads are linear loads, and their relationships are shown in Eq. (5).

$$\frac{ALP_{ik,n}}{ELP_{ik,n}} = \frac{ALQ_{ik,n}}{ELQ_{ik,n}} = \left(\frac{U_i}{U_s}\right)^2 \tag{5}$$

For power of each load sl_{ik} and solar photovoltaics pv_i, we amuse them follow the standard daily curve (O_n^l and O_n^{pv} represent usage rate of load and solar photovoltaics, shown in Figure 2). Then, once we give their maximum power(LPm_{ik}, LQm_{ik} are maximum active and reactive power of sl_{ik}, PVm_i is the maximum power of pv_i), we can obtain their power in each period $t = n$ from Eqs. (6) to (8).

$$ELP_{ik,n} = O_n^l \cdot LPm_{ik} \tag{6}$$

$$ELQ_{ik,n} = O_n^l \cdot LQm_{ik} \tag{7}$$

$$PV_{i,n} = O_n^{pv} \cdot PVm_i \tag{8}$$

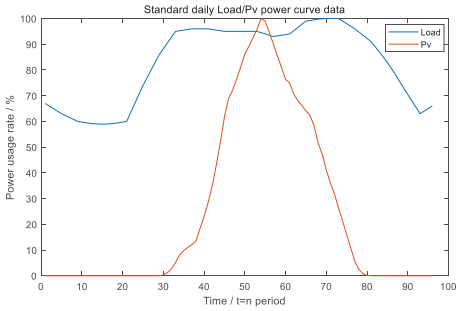

Figure 2. Power usage rate of load and pv during N=96 periods

C. Optimal power flow

In our system, micro-grid connects with the control center through the communication network. The system runs for $\Delta t = 15$ minutes each period, and the procedure of the system is shown in Figure 3. The system runs for total $N = 96$ periods.

Step 1: At the beginning of one period, smart meters collect the status of each component such as voltage, current, and power.

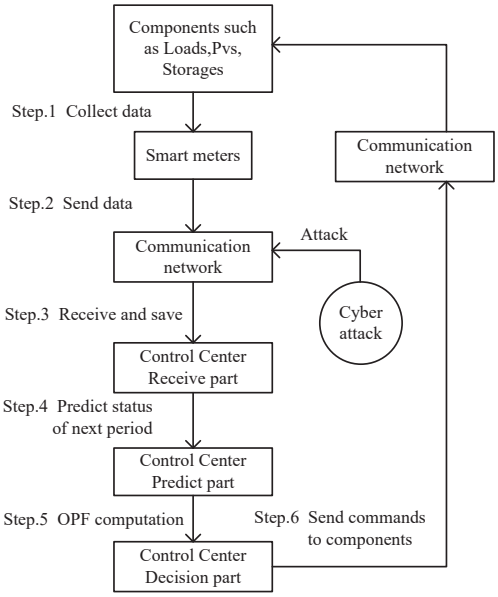

Figure 3. System running procedure and cyber-attack point

Step 2: Smart meters send these data to the control center.

Step 3: The control center can receive the data from smart meters under successful transmission, and may fail to receive when it suffers from cyber-attack. When receive failure happens, the missing data will be replaced by the data stored in the last period, as shown in Eq. (9).

$$\begin{cases} Re(X_n) = X_n & successful \\ Re(X_n) = Re(X_{n-1}) & failure \end{cases} \tag{9}$$

where X_n represents $status\ of\ component$ at the $t = n$ period, $Re(X_n)$ represents the received and saved data of X_n by the control center.

Step 4: Based on the received data of each component, numerical and trend weighted average prediction method (shown in Eq. (10)) is used to predict the status of each component in the next period.

$$\overline{X_{n+1}} = Predict(X) = \sum_{t=n-w+1}^{n} Y_t Re(X_t) + \sum_{t=n-w+1}^{n-1} Z_t \Delta Re(X_t) \tag{10}$$

where $\overline{X_{n+1}}$ is predicted data, $w = 4$, $\Delta Re(X_t) = Re(X_{t+1}) - Re(X_t)$, Y_t is the weight of number and Z_t is the weight of trend.

Step 5: After the control center predicts active power($PLP_{ik,t}$) and reactive power($PLQ_{ik,t}$) of loads sl_{ik} and predicted power($PPV_{2,t}$) of renewable generator pv_2 in the next period$(t = n + 1)$. Then it computes the optimal power flow (OPF) with the aim of minimizing the total cost C_{total}^{n+1} at $t =$

$n+1$ period. Total cost contains three parts (shown in Eq. (11)): transmission loss (C_{line}^{n+1}), loads energy loss caused by redundant power or energy not supplied (C_{load}^{n+1}) and energy loss of charging or discharging in storages C_{st}^{n+1}.

$$C_{total}^{n+1} = C_{line}^{n+1} + C_{load}^{n+1} + C_{st}^{n+1} \tag{11}$$

Transmission loss is the power loss on transmission line due to its impedance, and this part of electricity is converted to heat energy (shown in Eq. (12)).

$$C_{line}^{n+1} = \Delta t \cdot Pr \cdot \sum_{i=1}^{4}[(\sum_{k=i}^{4} I_k) \cdot (U_k - U_{k-1})] \tag{12}$$

where Δt is the time of one period, and Pr is unit energy price in micro-grid.

Loads energy loss occurs when energy supply and demand are unbalanced. Usually, the control center's unreasonable energy dispatching lead to either redundant power or energy not supplied. Besides, loads energy loss is related to the importance of the loads (shown in Eq. (13)).

$$C_{load}^{n+1} = KR \cdot Pr \cdot \sum\left(ALP_{ik,n+1} - ELP_{ik,n+1}\right) \cdot \Delta t \cdot (U_i > U_s) + KI \cdot Pr \cdot \sum\left(ELP_{ik,n+1} - ALP_{ik,n+1}\right) \cdot \Delta t \cdot (U_i < U_s) \tag{13}$$

where KI is the punishment coefficient of energy not supplied, and KR is the punishment coefficient of redundant power.

Energy loss of charging or discharging in storages (shown in Eq. (14)) exists because the charge-discharge efficiency is below 100%.

$$C_{st}^{n+1} = PS_{i,n+1} \cdot (1-\mu) \cdot Pr \cdot \Delta t \tag{14}$$

The optimal power flow of micro-grid is shown in Eq. (15) to (21). Eq. (15) is our objective function, and Eqs. (16) to (21) are restricted conditions. Eqs. (16) is approximate voltage calculation formula, Eqs. (17) is active power equation of each area. Eqs. (18) is reactive power equation of each area. Eqs. (19) to (20) are restricted conditions of storages. Eqs. (21) is the number of areas and loads in each area.

$$\min C_{total}^{t} = C_{line}^{t} + C_{load}^{t} + C_{st}^{t} \tag{15}$$

$$\widetilde{U}_{j-1} = \widetilde{U}_j + \sum_{j=i}^{4} \frac{P_j r L_i + Q_j x L_i}{\widetilde{U}_j} \tag{16}$$

$$P_{i,t} = \sum_{k=1}^{k_i}\left(PLP_{ik,t}\right) \cdot \left(\frac{\widetilde{U}_3}{U_s}\right)^2 + \mu \cdot PS_{i,t} - PPV_{i,t} \tag{17}$$

$$jQ_{i,t} = \sum_{k=1}^{k_i}\left(jPLQ_{ik,t}\right) \cdot \left(\frac{\widetilde{U}_1}{U_s}\right)^2 + jQb_{i,t} \tag{18}$$

$$\left|PS_{i,t}\right| \le PSm_i \tag{19}$$

$$0 \le PS_{i,n} \cdot \Delta t + LS_{i,n} \le US_{i,n} \tag{20}$$

$$(j = 1,2,3,4, i = 1,2,3,4, k_i = 3,0,2,1) \tag{21}$$

Step 6: At last, optimum power of storages($[PS_{3,t}, PS_{3,t}]$) and reactive power compensation ($[jQb_{1,t},\ jQb_{3t}, jQb_{4,t}]$) in the next period($t = n+1$) will be scheduled and the control center will send the control command to storages and shunt compensators, to set their power outputs to the optimal values.

D. Model of cyber-attacks

For simplicity, the communication network is supposed to perfect without cyber-attack, which means $Re(X_n) = X_n$. However, the cyber-attack will interfere with the transmission process of the data or even modify the data, triggering chain reactions in micro-grid optimal power flow procedure. For example, the control center fails to receive data properly in step 3, then the prediction process will be more inaccurate in step 4, leading to optimal power flow deviates from optimal in step 5, resulting in performance degradation of the system.

According to the targets of cyber-attacks, they can be divided into three types, i.e, confidentiality attack, integrity attack and availability attack[8]. In our former work, we have studied four types of single cyber-attack, including denial of service attack (DOS), RF jamming attack, replay attack, and false data injection attack (FDI). Due to the receiving process in step 3, we think RF jamming attack and replay attack can be regarded as a special case of DOS. DOS is a representative of availability attack, which can prevent the control center from receiving data at some probability, and we called this probability as severity[6, 8, 9]. FDI is a representative of integrity attack, which can modify the data sent from smart meters in different severities[7, 10, 11]. Their expressions and descriptions are shown in TABLE I.

TABLE I. CYBER-ATTACKS EXPRESSIONS AND DESCRIPTIONS

Type	Expression	Description
DOS	$Pn = P(Re(X_n) = 0) > 0$	Causing transmission delay and packet dropout.
FDI	$Re(X_n) = X_n + \Delta x_n = mX_n$	Modifying The data sent from smart meters.

where $P(Re(X_n) = 0)$ represents the probability of receiving failure, which can describe the severity of DOS. Besides, m in $Re(X_n) = mX_n$ can describe the severity of FDI. We denote $[T_1,\ T_2]$ as attack time, where T_1 is start period and T_2 is end period.

In this paper, we study two cyber-attacks implemented in micro-grid and find their co-effect. joint cyber-attacks can be implemented in micro-grid, whether same or different areas, and simultaneously or asynchronous. For example, when attacker implement DOS in area a_1, time $[T_1,\ T_2] = [30,50]$, severity $Pn = 0.9$; FDI in area a_1, time $[T_1,\ T_2] = [10,30]$, severity $m = 0.85$, the received data from area a_1 is shown in Figure 4.

III. SIMULATION OF MULTIPLE CYBER-ATTACKS ON MICRO-GRIE

We simulate our micro-grid system model for $N = 96$ consecutive periods (24 hours) as electricity production and consumption is similar between days. We can use the circuit equations to get the real status of micro-grid. Then we use total cost $TC = \sum_{n=1}^{N} C_{total}^{n}$ to evaluate the performance of micro-grid during N periods. We use TC_s to represent total cost in standard situation, and TC_a under cyber-attacks. In standard situation, $\sum_{n=1}^{96} C_{total}^{n} = 957.99$. Thus, $TC_a - TC_s$ can reflect the effect of cyber-attacks.

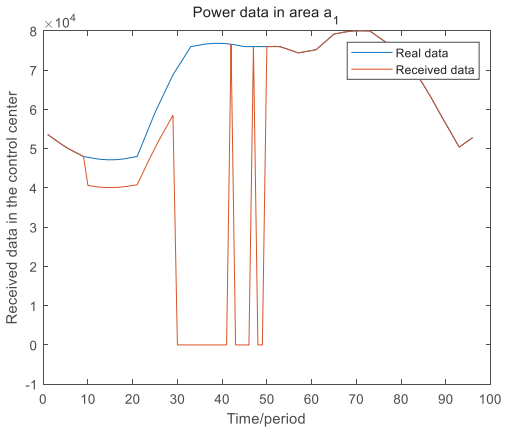

Figure 4. Cyber-attack influence on transmission

A. *Single attack*

For simplicity, we amuse that the control center lacks the ability to defend DOS and FDI of relatively low severity($m \geq 0.8$) because the treatment of the control center to DOS is constant(as Eq. (9)) and FDI of relatively high severity can be detected by the control center. The malicious attacker can implement cyber-attack(DOS or FDI) in different areas and different time steps. Attack area can be area $a_i(a_1, a_2, a_3, a_4)$. Attack time step can be $[T_1, T_2] = \{[10,30], [20,40], [30,50], [40,60], [50,70], [60,80]\}$.

For DOS attack of severity $Pn = 0.9$, we implement this attack in different areas and different time steps. We calculate $TC_a - TC_s$ of each situation and show the result in TABLE II. We can find that, in area a_1, a_3, and a_4, the effect of DOS attack implemented in time steps $[10,30]$, $[20,40]$, and $[60,80]$ is more significant than other time steps. However, in area a_2, we can find that it is totally different. Because in area a_1, a_3, and a_4, from Figure 2 we can know that power of these components changes more in time steps $[10,30]$, $[20,40]$, and $[60,80]$. Similarly, in area a_2, power of pv_2 change a lot in time step $[10,30]$, $[20,40]$, and $[60,80]$. We can conclude that the more significant change happens in a time step, the more significant effect of DOS attack implemented in this time step.

TABLE II. EFFECT OF DOS ATTACK TO MICRO-GRID

Time / Area	[10,30]	[20,40]	[30,50]	[40,60]	[50,70]	[60,80]
a_1	3.33	-0.34	-0.95	0.08	0.22	0.03
a_2	0	1.27	16.85	11.16	4.09	0.37
a_3	7.5	8.04	-0.85	1.97	0.49	1.98
a_4	2.49	2.71	0.82	-0.02	-1.1	0.61

For FDI attack of severity $m = 0.9$, we implement this attack in different areas and different time steps. We calculate $TC_a - TC_s$ of each situation and show the result in TABLE III. We can find that the effect of FDI attack implemented in time steps $[40,60]$ and $[50,70]$ are relatively greater than other time steps. From Figure 2, we can find that the power of components in these time steps is relatively higher than other time steps, the same modification ratio causes more numerical variation. So, we can conclude that the more power of the components in a time step, the more significant effect of FDI attack implement in this time step.

TABLE III. EFFECT OF FDI ATTACK TO MICRO-GRID

Time / Area	[10,30]	[20,40]	[30,50]	[40,60]	[50,70]	[60,80]
a_1	-0.52	0.38	-0.69	-2.71	-2.5	-0.81
a_2	-1.12	-1.12	-0.24	4.02	3.61	1.24
a_3	1.56	3.1	4.55	5	4.16	3.95
a_4	-3.25	-1.59	-3.92	-4.47	6.53	0

B. *Different severities of attacks*

Pn is the severity of DOS, and m is the severity of FDI. In this paper, we investigate $Pn = [0.6, 0.7, 0.8, 0.9, 1]$ and $m = [0.8, 0.85, 0.9, 0.95]$.

The higher the Pn, the more serious the DOS attack is. We implement DOS attack of different severities in area a_2, because malicious attacker prefers to implement cyber-attack in the area causing more effect. We use $TC_a - TC_s$ to describe its effect, and their results are shown in Figure 5. We can find the effect of DOS attack has a positive relationship with its severity Pn.

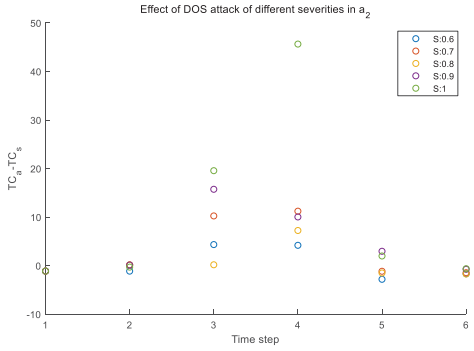

Figure 5. Effect of DOS attack on area 2
where the abscissas 1 to 6 represent time steps [10,30], [20,40], …, [60,80] in turn, follow figures are same.

The lower the m, the more serious the FDI attack is. We implement FDI attack of different severities in area a_3, where malicious attacker prefers to implement cyber-attack in this area to increase more total cost. We use $TC_a - TC_s$ to describe its effect, and their results are shown in Figure 6. We can find the effect of FDI attack has a positive relationship with its severity m.

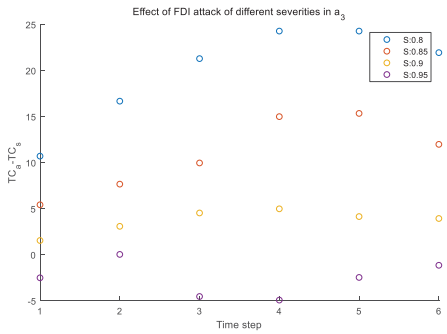

Figure 6. Effect of FDI attack on area 3

C. *Joint cyber-attacks in the same area*

We simulate the cyber-attacks in area a_3, including DOS attack of severity $Pn = 0.9$ and FDI attack of severity $m = 0.9$. Because we can find that the effect of these two cyber-attacks in area a_3 is relatively higher among areas. Besides, the effect of the DOS attack of severity $Pn = 0.9$ and the FDI attack of severity $m = 0.9$ are similar, which reduces the difficulty of analyzing combined effects of joint cyber-attacks.

Considering the computational complexities of computing effect of joint cyber-attacks, we only consider two joint cyber-attacks implemented in different time steps. We use $TC_j = TC_a - TC_s(V1)$ to represent the effect of joint cyber-attacks on micro-grid. We also simulate the effect of each cyber-attack in joint cyber-attacks pairs separately and use TC_1 and TC_2 to denote it correspondingly. Thus, we can use $TC_j - TC_1 - TC_2(V4)$ to evaluate the interaction between two cyber-attacks in this pair. $TC_j - TC_1(V2)$ is useful for us to identify whether cyber-attack 2 promotes or weakens cyber-attack 1. $TC_j - TC_2(V3)$ is similar.

For two DOS attacks implemented in different time steps, we can get results in TABLE IV. We can find that the extensive of the attack time can significantly increase the DOS attack effect. Comparing with single time step DOS attack, joint DOS attacks implemented in two steps have a greater impact on the micro-grid. We also find that the effect is huge especially when components' power has obvious change.

TABLE IV. EFFECT OF JOINT DOS ATTACKS TO MICRO-GRID IN AREA a_3

Steps / Value	[10,30] [20,40]	[10,30] [30,50]	[10,30] [40,60]	[10,30] [50,70]	[10,30] [60,80]	[20,40] [30,50]	[20,40] [40,60]
V1	13.77	7.28	12.04	3.52	10.86	27.01	19.87
V2	7.39	0.9	5.66	-2.86	4.48	20.09	12.95
V3	6.85	9.25	11.19	4.15	10.01	28.99	19.02
V4	0.47	2.88	4.82	-2.23	3.63	22.07	12.1
[20,40] [50,70]	[20,40] [60,80]	[30,50] [40,60]	[30,50] [50,70]	[30,50] [60,80]	[40,60] [50,70]	[40,60] [60,80]	[50,70] [60,80]
7.94	11.37	-2.24	0.01	0.38	-0.09	-0.08	-1.05
1.02	4.45	-0.26	1.99	2.35	-0.94	-0.93	-0.42
8.57	10.52	-3.09	0.64	-0.48	0.54	-0.94	-1.9
1.65	3.6	-1.11	2.62	1.5	-0.31	-1.78	-1.27

For two FDI attacks implemented in different time steps, we can get results in TABLE V. We can find that the extension of the FDI attack time cannot increase the effect significantly and even decrease the effect. Effect results of steps pairs prove our point of view such as $([10,30],[20,40])$ and $([10,30],[30,50])$. Besides, the effect of the FDI attack is relative higher implemented in the time steps pairs when the components' power is relatively high than other time steps pairs. For example, the effect of time steps pair $([30,50],[50,70])$ is the most significant among the simulation results.

TABLE V. EFFECT OF JOINT FDI ATTACKS TO MICRO-GRID IN AREA a_3

Steps / Value	[10,30] [20,40]	[10,30] [30,50]	[10,30] [40,60]	[10,30] [50,70]	[10,30] [60,80]	[20,40] [30,50]	[20,40] [40,60]
V1	5.54	0.29	3.28	3.1	6.87	8.67	1.65
V2	3.99	-1.27	1.73	1.55	5.31	5.57	-1.45
V3	2.44	-4.27	-1.72	-1.06	2.92	4.12	-3.35
V4	0.89	-5.82	-3.27	-2.61	1.37	1.02	-6.46
[20,40] [50,70]	[20,40] [60,80]	[30,50] [40,60]	[30,50] [50,70]	[30,50] [60,80]	[40,60] [50,70]	[40,60] [60,80]	[50,70] [60,80]
7.94	3.65	7.41	12.84	4.26	7.95	12.72	7.48
1.02	0.55	4.31	8.29	-0.29	3.4	7.71	2.48
8.57	-0.5	3.47	7.84	0.1	4.01	8.56	3.53
1.65	-3.6	0.37	3.29	-4.45	-0.54	3.56	-1.47

For DOS attack and FDI attack implemented in different time steps, we find that the DOS attack plays a more important role in the joint cyber-attacks. Figure 7 shows the relationship between the effect of a single DOS attack and the effect of joint DOS and FDI attacks implemented in time steps pair. We find that when the effect of a single DOS attack is higher, the effect of joint DOS and FDI attacks will be higher.

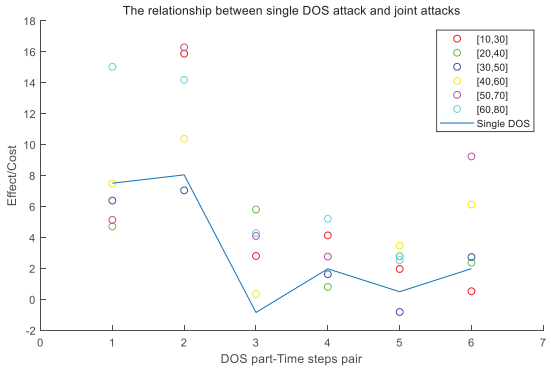

Figure 7. Joint DOS and FDI attacks in time steps pair in area a_3

D. *Joint cyber-attacks in different areas*

We simulate the DOS attack of severity $Pn = 0.9$ and the FDI attack of severity $m = 0.9$ in area a_2 and a_3 respectively. For a rational attacker, he will implement DOS attack in area a_2 and FDI attack in area a_3, because the effect of these single attack is relatively high. Besides, the effect of the DOS attack of severity $Pn = 0.9$ and the FDI attack of severity $m = 0.9$ are similar, which reduces the difficulty of analyzing the combined effects of joint cyber-attacks. The DOS attack and FDI attack can be implemented in different time steps or the same time step.

We find that the effect of joint DOS attack and FDI attack implemented in different areas is greater than the same area in the most time steps pair. Figure 8 confirms our point of view.

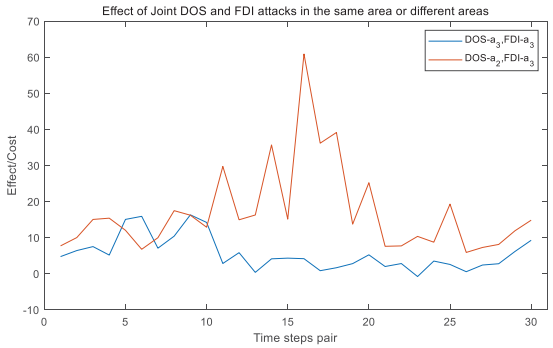

Figure 8. Effect of Joint DOS and FDI attacks in the same area or different areas, where the abscissas represent time different time steps combinations.

We also find that the DOS attack plays a more important role in the joint cyber-attacks, which is similar to the simulation result in Section III.C. Their relationship ship was shown in Figure 9.

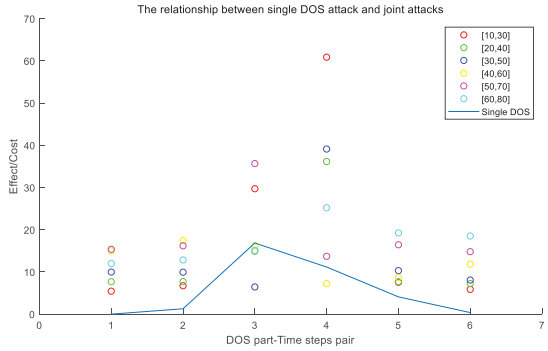

Figure 9. The relationship between single DOS attack and joint attack

IV. CONCLUSION

We have simulated our micro-grid model under single cyber-attack and joint cyber-attacks in Section IV. Based on our simulation results and analysis, we can give some suggestions for malicious attacker and defender.

As a malicious attacker, he aims for maximizing the total cost of micro-grid. A malicious attacker can implement different cyber-attack strategies based on his resource and ability.

If a malicious attacker is only capable of the DOS attack, he needs to choose the time step during which the components' power in his target area change significantly, and time step $[30,50]$ of area a_2 in this micro-grid model is the best choice for him to attack. Extending DOS attack time is useful for the malicious attacker such as choose different time steps. Besides, the malicious attacker can increase the severity of DOS attack to increase the cost of micro-grid, especially when the severity $Pn = 1$.

If a malicious attacker is only capable of the FDI attack, he needs to choose the time step when the components' power is relatively high, and time step $[50,70]$ of area a_4 in this micro-grid model is the best choice for him to attack. Increasing the severity of FDI attack is helpful for the malicious attacker to increase the cost of micro-grid. However, Extending FDI attack time is not recommended for the malicious attacker because the extension of the FDI attack time cannot increase the effect significantly and even decrease the effect.

If a malicious attacker is capable of joint DOS attack and FDI attack, he'd better implement the joint cyber-attack in different areas rather than the same area. Besides, the DOS attack plays a more important role in the joint cyber-attacks, thus the malicious attacker should choose a time step and an area where the effect of DOS attack is relatively high. In our simulation, DOS attack implemented in area a_2 in time step $[40,60]$ and FDI attack implemented in area a_2 in time step $[10,30]$ is the best strategy for the malicious attacker.

For a defender, he should allocate defense resources to defend the malicious attacker. We amuse the malicious attacker is rational, so the defender should allocate more defense resources to the time step and the area where the cyber-attack causes more effect on micro-grid. For the DOS attack, the defender should allocate more DOS defense resources to the time step in an area during which the components' power changes significantly. For FDI attack, the defender should allocate more FDI defense resources to the time step in an area when the components' power is relatively high.

Besides, there are three situations that the defender should pay more attention to. First one is that the malicious attacker increases the severity of FDI attack, and the defender should establish an efficient detection mechanism to discover the FDI attack accurately and timely. Secondly, the defender should be alert when the DOS attack continues for a relatively long time. Under such circumstance, the defender should resolve the transmission malfunction timely to avoid the huge cost. Third, joint DOS attack and FDI attack implemented in different areas may have a huge effect on micro-grid. Thus, the defender can resolve the malfunction caused DOS attack first and then FDI attack because the DOS attack plays a more important role in the joint cyber-attacks.

For future research, we can extend our efforts to the design of attack and defense strategies from a game theory perspective.

V. REFERENCE

[1] S. Morozumi and Ieee, "Micro-grid demonstration projects in Japan," (in English), *2007 Power Conversion Conference - Nagoya, Vols 1-3,* Proceedings Paper pp. 606-613, 2007.

[2] V. C. Gungor *et al.*, "Smart Grid Technologies: Communication Technologies and Standards," (in English), *Ieee Transactions on Industrial Informatics,* Article vol. 7, no. 4, pp. 529-539, Nov 2011.

[3] A. Timbus, M. Larsson, and C. Yuen, "Active Management of Distributed Energy Resources Using Standardized Communications and Modern Information Technologies," (in English), *Ieee Transactions on Industrial Electronics,* Article vol. 56, no. 10, pp. 4029-4037, Oct 2009.

[4] G. Z. Han, B. Y. Xu, K. J. Fan, and G. X. Lv, "An open communication architecture for distribution automation based on IEC 61850," (in English), *International Journal of Electrical Power & Energy Systems,* Article vol. 54, pp. 315-324, Jan 2014.

[5] P. Srikantha and D. Kundur, "A DER Attack-Mitigation Differential Game for Smart Grid Security Analysis," (in English), *Ieee Transactions on Smart Grid,* Article vol. 7, no. 3, pp. 1476-1485, May 2016.

[6] S. Asri and B. Pranggono, "Impact of Distributed Denial-of-Service Attack on Advanced Metering Infrastructure," (in English), *Wireless Personal Communications,* Article vol. 83, no. 3, pp. 2211-2223, Aug 2015.

[7] A. Farraj, E. Hammad, and D. Kundur, "On the Impact of Cyber Attacks on Data Integrity in Storage-Based Transient Stability Control," (in English), *Ieee Transactions on Industrial Informatics,* Article vol. 13, no. 6, pp. 3322-3333, Dec 2017.

[8] Y. L. Mo *et al.*, "Cyber-Physical Security of a Smart Grid Infrastructure," (in English), *Proceedings of the Ieee,* Article vol. 100, no. 1, pp. 195-209, Jan 2012.

[9] Z. El Mrabet, N. Kaabouch, and H. El Ghazi, "Cyber-security in smart grid: Survey and challenges," (in English), *Computers & Electrical Engineering,* Article vol. 67, pp. 469-482, Apr 2018.

[10] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart Grid Data Integrity Attacks," (in English), *Ieee Transactions on Smart Grid,* Article vol. 4, no. 3, pp. 1244-1253, Sep 2013.

[11] O. Kosut, L. Y. Jia, R. J. Thomas, and L. Tong, "Malicious Data Attacks on the Smart Grid," (in English), *Ieee Transactions on Smart Grid,* Article vol. 2, no. 4, pp. 645-658, Dec 2011.