False Relay Operation Attacks in Power Systems with High Renewables

Mohamadsaleh Jafari, Md Hassan Shahriar, Mohammad Ashiqur Rahman, and Sumit Paudyal
Department of Electrical and Computer Engineering, Florida International University, USA
Emails: mjafari@fiu.edu, mshah068@fiu.edu, marahman@fiu.edu, spaudyal@fiu.edu

***Abstract*—Load-generation balance and system inertia are essential for maintaining frequency in power systems. Power grids are equipped with Rate-of-Change-of-Frequency ($ROCOF$) and Load Shedding (LS) relays in order to keep load-generation balance. With the increasing penetration of renewables, the inertia of the power grids is declining, which results in a faster drop in system frequency in case of load-generation imbalance. In this context, we analyze the feasibility of launching False Data Injection (FDI) in order to create False Relay Operations (FRO), which we refer to as FRO attack, in the power systems with high renewables. We model the frequency dynamics of the power systems and corresponding FDI attacks, including the impact of parameters, such as synchronous generators' inertia, and governors' time constant and droop, on the success of FRO attacks. We formalize the FRO attack as a Constraint Satisfaction Problem (CSP) and solve using Satisfiability Modulo Theories (SMT). Our case studies show that power grids with renewables are more susceptible to FRO attacks and the inertia of synchronous generators plays a critical role in reducing the success of FRO attacks in the power grids.**

***Index Terms*—False data injection, false relay operation, load shedding relay, ROCOF relay, frequency response.**

I. Nomenclature

Δf	Change in frequency.
ΔP	Total power imbalance.
ΔP^{gov}	Change in power due to governor's action.
ΔP^{a}	Change in generator's setpoint due to FDI attack.
ΔP^{sh}	Shed load due to Load Shedding (LS) relay.
ΔP^{tg}	Change of power generation due to $ROCOF$.
Δt	Simulation time step.
f	Frequency.
$\overline{f}$	Frequency threshold for load shedding.
$\dot{f}$	Rate-of-Change-of-Frequency ($ROCOF$).
$\overline{\dot{f}}$	Threshold value of $ROCOF$.
H	Inertia constant of multi-machine System.
M	Number of cycles in $\dot{f}$ calculation.
n	Discrete time step.
P^{e}	Electrical power output of generators.
P^{m}	Mechanical power input to generators.
P^{sh}	Load shed by LS relays at each time step.
P^{tg}	Power of tripped generators by $ROCOF$ relays.
R	Droop of the governors.
T	Time constant of governors.
t	Time.

II. Introduction

A large part of power generation in bulk power systems is supplied by synchronous generators. However, these days, Distributed Energy Resources (DERs) are becoming an integral part of the power systems [1]. As the power grid evolves with increasing penetrations of inverter-based DERs such as solar photovoltaics (PV) and wind turbines, the inertia of the grid tends to decline [2], [3].

Wind turbines and solar panels are equipped with several sensor measurements such as wind velocity, wind direction, and solar irradiance. These measurements are connected to the control center using wireless/wired technologies to facilitate analyzing and adjusting the power output of generators to maintain the grid frequency. Protective devices, such as Rate-of-Change-of-Frequency ($ROCOF$) and Load Shedding (LS) relays are equipped in the power system to maintain load-generation balance when frequency changes [4], [5]. In the case of load-generation imbalance, the system frequency deviates from the nominal value, and if the frequency/$ROCOF$ goes beyond an acceptable range, these relays trip their corresponding generators/loads to keep the frequency within the range. An attacker can exploit this relay functionality by performing False Data Injection (FDI) attacks. The attacker may inject necessary false data into various DER sensor measurements causing a False Relay Operation (FRO) (i.e., false operation of an LS/$ROCOF$ relay) in the grid. For example, the attacker can inject false data into the air density and wind velocity measurements of a wind turbine to mislead the control center to perceive a power abundance in the network. Then, the operator of the control center adjusts the power output of synchronous generators. However, as the actual generation is less than the load, the frequency drops. If this attack continues, some generators may trip by $ROCOF$ relay operation or some loads may get disconnected by LS relays. We name such exploitations as FRO attacks.

Various FDI attacks in power grids have been widely studied in the literature. The authors in [6], [7] presented an FDI attack on contingency analysis of the power system, where the target was created to mislead the operational cost only. Chlela et al. [8] addressed the impacts of FDI cyber-attacks on critical microgrid control functions as well as the loss of load resulting from under-frequency load shedding. Zhang et al. [9] discussed security issues of a dynamic microgrid partition process and investigated three different scenarios of

FDI attacks against it. In [10], the authors analyzed FDI attacks with incomplete information, where the attacker has limited information about the network topology. The possible FDI vulnerabilities on an integrated Volt-VAr control is studied in [11]. Teixeira et al. [12] studied the impact of FDI attacks on the measurement data and reference signals received by the voltage droop controllers in microgrids. Liu et al., [13] focus on the continuous injection of time-varying false data and load redistribution in the system. A pre-overload vulnerability graph approach is proposed in [14] to systematically assess, evaluate, and quantify the system vulnerability under a load redistribution FDI attack. Some researchers studied the defense against the above-mentioned attacks. For example, a reachability analysis-based mechanism is presented in [15] to detect FDI attacks. Saad et al. [16] presented an IoT-based cyber-physical system at mitigating FDI attacks.

However, to the best of our knowledge, the current literature does not address the possibility of launching FDI attacks leading to FRO. In this context, this paper aims at studying the feasibility of FRO attacks in power systems. We represent the overall problem in a generic, formal manner by recognizing it as a Constraint Satisfaction Problem (CSP). We apply Satisfiability Modulo Theories (SMT), a powerful constraint satisfaction tool [17], to solve this CSP.

The rest of the paper is organized as follows. In section III, we model the frequency behavior of the power system considering the change of the generator setpoints due to FDI, the generator's governor reaction, *LS*, and *ROCOF* relay operations. In section IV, we show case studies by considering different combinations of power system parameters and analyze their impacts on the success of FDI in launching FRO attacks. We conclude the paper in section V.

III. Formal Models

In this section, we present the formal models of the power system frequency dynamics and the synthesis of potential FRO attack vectors. An attack vector identifies a set of sensor measurements and necessary FDIs that can lead to a FRO attack. We also model the power grid relay operations and how the attack can percolate into this system leading to false activation of the relays. We specifically focus on *ROCOF* and *LS* relays.

A. Power System Frequency Dynamics

The system frequency response in a power grid can be determined using swing equation, and load/generation changes. For multi-machine power systems, the swing equations can be equivalently represented in terms of center of inertia (COI) as,

$$\frac{d\,f(t)}{dt} = \frac{1}{2H}\,(P^m - P^e). \tag{1}$$

The above form of swing equation can be linearized for a multi-machine power system as follows [18],

$$\frac{d\,\Delta f(t)}{dt} = \frac{1}{2H}\,\Delta P(t). \tag{2}$$

B. FDI Attacks on Grid Frequency Control

In this study, the FDI attack on measurements from DERs (e.g., wind velocity, solar irradiance) will be perceived as generation change at the control center level. We assume that the attacker cannot directly change the generators' setpoints. Therefore, the attacker tries to launch FDI attacks on the DER measurements. These compromised measurements are sent to the control center to mislead the operator of the abundance or shortage of power in the network. Then, the operator sends new setpoints to the synchronous generators to address the issue, while unknowingly participating in the attacker's goal. We assume that the frequency regulation takes place mainly due to the primary frequency response and secondary frequency control actions.

We model the power imbalance as [18],

$$\Delta P_n = \Delta P_n^{gov} - \Delta P_n^{a} + \Delta P_n^{sh} - \Delta P_n^{g}. \tag{3}$$

Governor operation ($\Delta P_n^{gov} \neq 0$), as shown in Fig. 1, changes the generators input power during any load-generation imbalances. The discretized dynamic response of the governor is modeled using the following [18],

$$\Delta P_{n+1}^{gov} = \Delta P_n^{gov} + \frac{\Delta t}{T}\Big(- \frac{\Delta f_n}{R} - \Delta P_n^{gov}\Big), \tag{4}$$

We model the frequency resulting from the actions of governors, *ROCOF*, and *LS* relays using the following,

$$\begin{aligned}\Delta f_{n+1} = \frac{\Delta t}{4H}\Big[&\Delta P_n^{gov}(2 - \frac{\Delta t}{T}) - 2\Delta P_n^{a} \\ &- \Delta f_n(\frac{\Delta t}{RT} - \frac{4H}{\Delta t}) - \Delta P_{n+1}^{tg} - \Delta P_{n+1}^{sh}\Big],\end{aligned} \tag{5}$$

$$f_n = 1 + \Delta f_n, \tag{6}$$

If f_n is less than $\overline{f}$, the total amount of shed load at time $n+1$ is computed as,

$$\Delta P_{n+1}^{sh} = \Delta P_n^{sh} + P^{sh}, \qquad \forall f_n \leq \overline{f} \tag{7}$$

To model the activation of *ROCOF* relays, we compute $\dot{f}$ as follows [19],

$$\dot{f} = \frac{1}{M}\sum_{n-M+1}^{n}\frac{\Delta f_n}{\Delta t}, \tag{8}$$

If $\dot{f}$ is greater than $\overline{\dot{f}}$, the *ROCOF* relay operates and disconnects the generator from the grid. This generator disconnection is modeled by,

$$\Delta P_{n+1}^{tg} = \Delta P_n^{tg} + P^{tg}, \qquad \forall \dot{f} \geq \overline{\dot{f}} \tag{9}$$

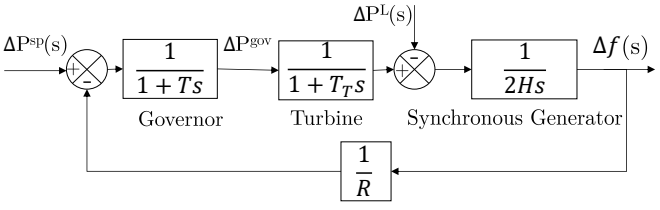

Fig. 1. Model of generators' Equivalent Governor.

IV. Case Studies

In order to study the proposed method, we consider a 5-bus power system as shown in Fig. 2 with three generators, three wind farms, two solar parks, and four bulk loads. The total amount of the load is 4.5 p.u., 3.0 p.u. of which is supplied by the generators (1.0 p.u. each), and 1.50 p.u. is supplied by the wind and solar generations. We consider a nominal frequency of 60 Hz. All the loads are equipped with *LS* relays with $\overline{f}$ = 59.5 Hz. Generators are equipped with *ROCOF* relays with $\overline{\dot{f}}$= 0.5, 0.6, and 1.2 Hz/s at buses 4, 5, and 1, respectively. The reason for considering different $\overline{\dot{f}}$ values for the relays is that not all of the generators in case of any *ROCOF*-type attack get disconnected simultaneously from the grid [20]. The acceptable maximum $\overline{\dot{f}}$ is usually ranged between 0.5 and 1.2 Hz/s [21]. The value of M typically varies between 2 and 40 cycles [22]. In our study, we set M to 6 cycles. Also, we assume that the FDI attack takes place only at a single time step (not a recurring attack attempt). We encode the formalization presented in the previous section and solve it using Z3, which is an efficient SMT solver [17]. During the execution of the FDI attack, the solution to the model returns either a successful or unsuccessful status. If the result is successful, it denotes that the SMT solver identified an attack vector that satisfies all the given constraints. On the other hand, unsuccessful status implies that there is no solution to the given problem (with the given attack constraints). In this work, an attack vector represents an assignment variable value for which the framework identifies a satisfiable solution. We run our experiments on an Intel Core i7 processor with 16 GB memory. In order to evaluate the impact of power system parameters on the feasibility of FDI on FRO, we consider different combinations of H, R, and T for the example power grid and run the proposed framework. We also consider the Threshold of Injection (ToI) and Attackable DERs (AD) parameters in our studies. ToI is the maximum percentage of the change that the attacker can make in measurements as false data and AD is the percentage of attackable DERs (including wind turbines and solar panels). By attackable, we mean that the measurements in DERs are not secured and the attacker can access them. Table I shows different values of the example power grid parameters used to evaluate the performance of the proposed framework in different case studies. To generate a generic relationship among the parameters, we created 10,000 different combinations of these values and observed the successful attacks at launching FRO. Among these combinations, we pick two to show the frequency and *ROCOF* behaviors of the power system. Then, we show a bigger picture of these parameters impact on attack success.

TABLE I
Power system parameters used for the case studies.

Parameter	Case Study		
	$C1$	$C2$	$C3$
$R(pu)$	0.2	0.2	0.2, 0.4, 0.6, 0.8, 1.0
$T(s)$	0.2	0.2	0.2, 0.4, 0.6, 0.8, 1.0
$AD\%$	20.0	20.0	20.0, 40.0, 60.0, 80.0, 100.0
$H(s)$	2.0	6.0	2.0, 4.0, 6.0, 8.0, 10
$ToI\%$	2.0	6.0	2.0, 4.0, 6.0, 8.0, 10

- Case 1 ($C1$): Injecting false data into DERs' measurements, the attacker launches an attack of ΔP_1^a = 0.322 p.u. in the system. This attack convinces the operator to reduce the generators' setpoints to address this power abundance. Therefore, $\dot{f}$ sharply changes and reaches 0.510 Hz/s in 12 cycles which is greater than the $\overline{\dot{f}}$ of the generator at bus 4. Therefore, *ROCOF* relay at bus 4 operates falsely and disconnects its corresponding generator from the grid (P^{tg} = 1.0 p.u.). The frequency and $\dot{f}$ changes are shown in Table II for n = 0,...,12.
- Case 2 ($C2$): As can be seen from Table I, parameters R, T, and AD remains the same as $C1$ while H increases. In order to launch a successful attack, the attacker needs to be able to inject at least 6.0% of false data into the measurements i. e., ToI = 6.0% which results in ΔP_1^a = 1.015 p.u. This attack makes $\dot{f}$ reach 0.513 Hz/s in 12 cycles, which is greater than the $\overline{\dot{f}}$ of the generator at bus 4. Hence, the *ROCOF* relay at bus 4 operates falsely and its generator gets disconnected from the grid (P^{tg} = 1.0 p.u.). The behavior of frequency and *ROCOF* are shown in Table II.
- Case 3 ($C3$): In this case, we show the number of successful FRO attacks from the 10,000 generated combinations and

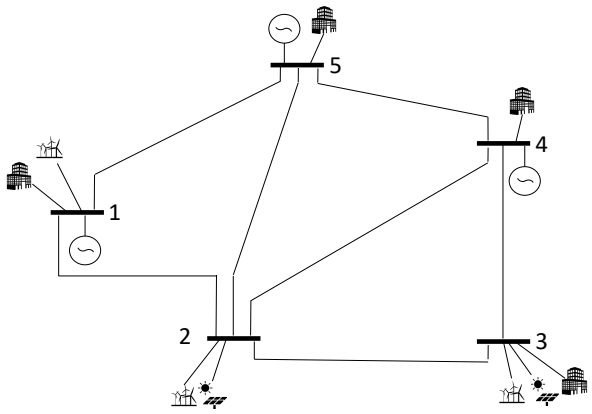

Fig. 2. A 5-Bus Test Network for case studies.

TABLE II
Frequency and ROCOF behavior of the example power system for case studies $C1$ and $C2$.

n	$\dot{f}(Hz/s)$		$f(Hz)$	
	$C1$	$C2$	$C1$	$C2$
0	-	-	60.000	60.000
1	-	-	59.991	59.991
2	-	-	59.983	59.983
3	-	-	59.976	59.974
4	-	-	59.968	59.966
5	-	-	59.960	59.957
6	0.480	0.490	59.952	59.951
7	0.470	0.500	59.944	59.941
8	0.460	0.500	59.937	59.933
9	0.460	0.500	59.930	59.924
10	0.460	0.500	59.922	59.916
11	0.450	0.490	59.915	59.908
12	**0.510**	**0.530**	59.901	59.898

discuss the impact of the power system parameters on FRO attack success.

Fig. 3 shows the impact of H on FRO success. As can be seen, there is almost a negative correlation between H and the number of successful FRO. In other words, When H increases, the number of successful FRO decreases. This is due to the fact that with a higher value of H, the frequency of the system becomes more stable and has less fluctuation. Therefore, the possibility of a larger $\dot{f}$ occurrence below $\overline{f}$ becomes less.

Fig. 4 also shows that there is a negative correlation between R and the number of successful FRO attacks. This is because, with increasing values of the droop, the power grid's generators show a slower reaction to the frequency changes in the power grid. This slow reaction goes against the attacker's goal, which tries to cause a sharp $\dot{f}$ or a frequency drop below $\overline{f}$. From Fig. 5, it can be observed that an increase in T leads to more successful FRO attacks. This positive correlation is due to the fact that larger T makes the governor's response slower to any frequency abnormalities that actually gives more chances to the frequency fluctuations. This creates more possibilities for the attacker to achieve his goal.

In Fig. 6, it is shown that the relationship between ToI and the number of successful FRO attacks is almost a proportional relationship. This is in accordance with the fact that if the attacker is able to change each of the measurements with a greater absolute value, the possibility of convincing the control center of sending a greater change to the generator setpoints is higher. The greater the changes in the setpoints, the greater the fluctuations in the frequency, and the greater the possibility of having successful FRO attacks. Fig. 7 the result of Fig. 6. It shows that if the attacker has access to a larger number of DER measurements, i. e., greater AD, more successful FRO attacks are possible to happen in the grid.

Comparing Fig. 3, Fig. 4, and Fig. 5, it can be seen that the slop of number of successful FRO attacks vs. H is greater than the ones of R and T. This shows the importance of considering the inertia of the power system while increasing the penetration of DERs in the grid. Inertia can have significant effects on a power grid's vulnerability against FDI attacks. With increasing the penetration of low-inertia DERs such as wind turbines and solar panels into power systems, the frequency of the grid becomes less stable to any type of disturbances or attacks. This makes the power grids more potent to FRO attacks.

From Table III, it can be observed that inertia has an impact on the FRO attack type (i. e., $ROCOF$ or LS attack), as well. When H is less than 4 (in the example power system), we have both $ROCOF$ and LS attacks in the power grid while with an increase in H, we observe only $ROCOF$ attacks. This is because of the fact that for low H, the power grid shows a faster reaction to any load-generation imbalances. If these

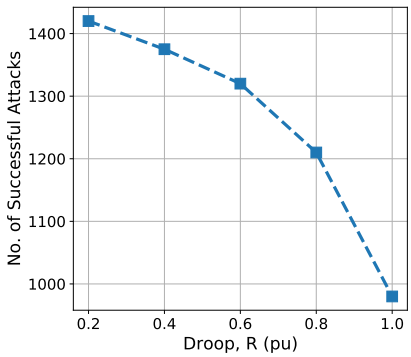

Fig. 4. Number of successful FRO attacks vs. governor's droop (R).

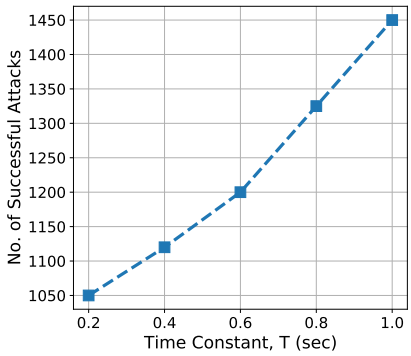

Fig. 5. Number of successful FRO attacks vs. governor's time constant (T).

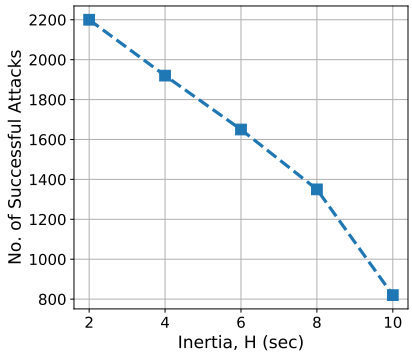

Fig. 3. Number of successful FRO attacks vs. inertia (H).

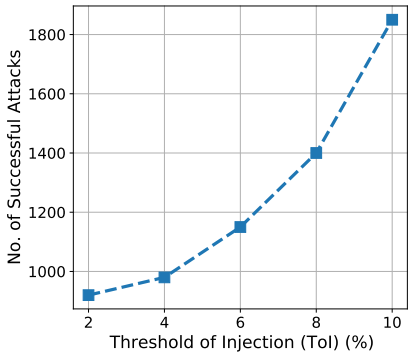

Fig. 6. Number of successful FRO attacks vs. threshold of injection (ToI).

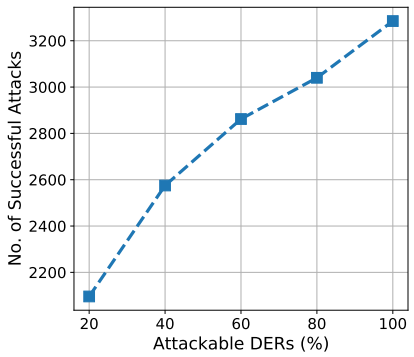

Fig. 7. The number of successful FRO attacks vs. attackable DERs (*AD*).

imbalances are big enough the frequency might drop in less than 6 cycles (the number of cycles considered in this paper for calculation of $\dot{f}$). This possibility of fast operation of *LS* relays is eliminated with an increment of H. Moreover, according to Fig. 4 and Fig. 5, it can be noticed that an increase in T or decrease in R reduces the number of successful FRO attacks.

TABLE III
IMPACT OF INERTIA (H) ON THE ATTACK TYPE.

H (s)	*ROCOF* Attack	*LS* Attack
< 4	✓	✓
≥ 4	✓	×

V. CONCLUSION

In this work, we study the feasibility of FDI attacks on power systems that falsely trigger protective relays (i.e., rate-of-change-of-frequency and load shedding relays). The proposed formal model considers the impact of different power system's parameters, including generators' inertia, equivalent governors' droop and time constant, the threshold of false data injection, and the number of attackable DERs and synthesizes successful FRO attacks, if exists. Our results show that, among various parameters, inertia has the most impact on reducing the success of the FRO attacks as higher inertia can reduce the possibility of launching a successful FRO attack in the power system. Moreover, it is demonstrated that an increase in droop or decrease in the time constant of governors can lower the possibility of launching a FRO attack in the power system.

REFERENCES

[1] M. Jafari, T. O. Olowu, A. I. Sarwat, and M. A. Rahman, "Study of smart grid protection challenges with high photovoltaic penetration," in *Proc. North American Power Symposium (NAPS)*, 2019, pp. 1–6.

[2] U. Tamrakar, D. Shrestha, M. Maharjan, B. P. Bhattarai, T. M. Hansen, and R. Tonkoski, "Virtual inertia: Current trends and future directions," *Applied Sciences*, vol. 7, no. 7, p. 654, 2017.

[3] P. Denholm, T. Mai, R. W. Kenyon, B. Kroposki, and M. O'Malley, "Inertia and the power grid: A guide without the spin," Technical Report: NREL/TP-6A20-73856, National Renewable Energy Laboratory, May 2020.

[4] M. Grebla, J. R. A. K. Yellajosula, and H. K. Høidalen, "Adaptive frequency estimation method for ROCOF islanding detection relay," *IEEE Transactions on Power Delivery*, vol. 35, no. 4, pp. 1867–1875, 2020.

[5] Y. Tofis, S. Timotheou, and E. Kyriakides, "Minimal load shedding using the swing equation," *IEEE Transactions on Power Systems*, vol. 32, no. 3, pp. 2466–2467, 2017.

[6] M. Ashiqur Rahman, M. Hasan Shahriar, M. Jafari, and R. Masum, "Novel Attacks against Contingency Analysis in Power Grids," *arXiv e-prints*, p. arXiv:1911.00928, Nov. 2019.

[7] J.-W. Kang, I.-Y. Joo, and D.-H. Choi, "False data injection attacks on contingency analysis: Attack strategies and impact assessment," *IEEE Access*, vol. 6, pp. 8841–8851, 2018.

[8] M. Chlela, G. Joos, M. Kassouf, and Y. Brissette, "Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks," in *Proc. IEEE Power and Energy Society General Meeting (PESGM)*, July 2016, pp. 1–5.

[9] X. Zhang, X. Yang, J. Lin, and W. Yu, "On false data injection attacks against the dynamic microgrid partition in the smart grid," in *Proc. IEEE International Conference on Communications (ICC)*, 2015, pp. 7222–7227.

[10] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *Proc. IEEE Global Communications Conference (GLOBECOM)*, Dec 2012, pp. 3153–3158.

[11] A. Teixeira, G. Dán, H. Sandberg, R. Berthier, R. B. Bobba, and A. Valdes, "Security of smart distribution grids: Data integrity attacks on integrated volt/var control and countermeasures," in *Proc. American Control Conference*, June 2014, pp. 4372–4378.

[12] A. Teixeira, K. Paridari, H. Sandberg, and K. H. Johansson, "Voltage control for interconnected microgrids under adversarial actions," in *Proc. IEEE 20th Conference on Emerging Technologies Factory Automation (ETFA)*, Sep. 2015, pp. 1–8.

[13] Y. Liu, S. Gao, J. Shi, X. Wei, and Z. Han, "Sequential-mining-based vulnerable branches identification for the transmission network under continuous load redistribution attacks," *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5151–5160, 2020.

[14] Y. Liu, S. Gao, J. Shi, X. Wei, Z. Han, and T. Huang, "Pre-overload-graph-based vulnerable correlation identification under load redistribution attacks," *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5216–5226, 2020.

[15] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical DC microgrids," *IEEE Transactions on industrial informatics*, vol. 13, no. 5, pp. 2693–2703, 2017.

[16] A. Saad, S. Faddel, T. Youssef, and O. A. Mohammed, "On the implementation of IoT-based digital twin for networked microgrids resiliency against cyber attacks," *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5138–5150, 2020.

[17] L. De Moura and N. Bjørner, "Satisfiability modulo theories: An appetizer," in *Brazilian Symposium on Formal Methods*. Springer, 2009, pp. 23–36.

[18] T. Amraee, M. G. Darebaghi, A. Soroudi, and A. Keane, "Probabilistic under frequency load shedding considering rocof relays of distributed generators," *IEEE Transactions on Power Systems*, vol. 33, no. 4, pp. 3587–3598, 2018.

[19] M. R. Alam, M. T. A. Begum, and K. M. Muttaqi, "Assessing the performance of ROCOF relay for anti-islanding protection of distributed generation under subcritical region of power imbalance," *IEEE Transactions on Industry Applications*, vol. 55, no. 5, pp. 5395–5405, 2019.

[20] J. C. M. Vieira, W. Freitas, W. Xu, and A. Morelato, "Performance of frequency relays for distributed generation protection," *IEEE Transactions on Power Delivery*, vol. 21, no. 3, pp. 1120–1127, July 2006.

[21] "IEEE standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces," *IEEE Std 1547-2018*, pp. 1–138, April 2018.

[22] C. F. Ten and P. A. Crossley, "Evaluation of Rocof relay performances on networks with distributed generation," in *Proc. IET 9th International Conference on Developments in Power System Protection*, 2008, pp. 523–528.