A Novel Bilevel False Data Injection Attack Model Based on Pre-and Post-Dispatch

Gao, Shibin; Lei, Jieyu; Wei, Xiaoguang; Liu, Yigu; Wang, Tao

DOI
10.1109/TSG.2022.3156445

Publication date
2022

Document Version
Final published version

Published in
IEEE Transactions on Smart Grid

A Novel Bilevel False Data Injection Attack Model Based on Pre- and Post- Dispatch

Shibin Gao, Jieyu Lei, Xiaoguang Wei, Yigu Liu, and Tao Wang

***Abstract*—This letter develops a new bilevel optimization model to construct false data injection attack based on pre- and post- dispatch. In order to enhance the attack concealment, the proposed bilevel model can minimize the variation of uploaded measurements between pre- and post-attack before dispatching, after which the attack can lead the system to an uneconomic and insecure operating state after dispatching. Simulation results validate the effectiveness of the proposed bilevel model in term of operating cost and network overloads.**

***Index Terms*—Bilevel optimization model, false data injection.**

I. Nomenclature

$\boldsymbol{R}$	Vector of generation output;
$\boldsymbol{SF}$	Shifting factor matrix;
$\boldsymbol{KD}$, $\boldsymbol{KP}$	Load incidence and generation incidence matrices;
$\Delta\boldsymbol{S}$	False load measurement injection;
$\boldsymbol{R}_0$, $\boldsymbol{S}_0$, $\boldsymbol{P}_0$	Generation output, load and branch power flow in the true state;
$\Delta\boldsymbol{R}$	Generator ramp limit;
$\boldsymbol{P}'$, $\boldsymbol{P}''$	Falsified branch power flow before and after SCED;
$\boldsymbol{\delta}$	Indicator vector;
$\boldsymbol{\kappa}$, $\boldsymbol{X}^+$, $\boldsymbol{X}^-$	Artificial variable vectors;
τ	Upper bound of false load injection;
M	Sufficiently large positive constant.

II. Introduction

FALSE data injection (FDI) attacks [1], as a special type of cyber-attacks, cooperatively manipulate branch power flow measurements and bus load measurements via communication network to lead the system to an uneconomic or even insecure operation state [2], [3]. By jointly tampering with multiple measurements, an FDI attack can bypass the bad data detection [1]. Therefore, the impressive efforts have been put forward to model FDI attacks from the perspective of load redistribution to analyze the impact of FDI attacks on the system operation.

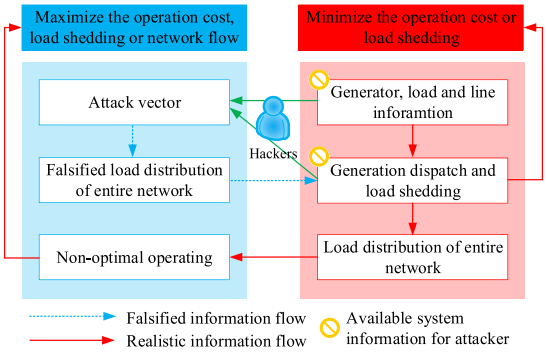

Fig. 1. Framework of existing bilevel model.

In the FDI attack model, extensive attention has been paid to bilevel optimization models to construct a representative attack vector and then investigate the system response [3]–[7]. The framework of common bilevel models is shown in Fig. 1. The objective of upper model is to maximize the disruption penalty, such as the higher generation cost, the load shedding and the network flow (e.g., the number of overloaded branches). The lower model employs the security constrained economic dispatch (SCED) to model the network response after an attack. To construct an effective FDI attack by using existing bilevel models, a basic assumption is that, except for basic network topology and operating state information, an attacker needs to obtain other full or partial network information, such as cost information, generation limits and line capacity. However, collecting such information is very difficult for an attacker, especially from the public access. This is easy to cause a misunderstanding that constructing an FDI attack may be an unrealistic idea, thus ignoring the urgency of studying FDI attacks. In addition, another aspect that needs attention is that the concealment of FDI attacks. Although FDI attacks can bypass the bad data detection as discussed above, it may still not be sufficiently concealed to avoid the operator's vigilance. It is well known that due to the existence of technical means such as load planning and forecasting, the operating states of the system is within a foreseeable range for the operator. Therefore, when the injected false data leads the operating states of the system to have a drastic change, it may still not keep operator out of sight and lead to an unsuccessful FDI attack.

Can the network information required for an attack be reduced to construct a bilevel optimization model due to the difficulty of obtaining the confidential information?

Can the variation of operating states of the system be decreased as much as possible after false data is injected to system measurements to enhance the concealment of FDI attacks?

Manuscript received June 7, 2021; revised October 13, 2021; accepted January 30, 2022. Date of publication March 3, 2022; date of current version April 22, 2022. This work was supported in part by the Fundamental Research Funds for the Central Universities under Grant 2682021CG005 and Grant 2682021CX036. Paper no. PESL-00133-2021. *(Corresponding author: Xiaoguang Wei.)*

Shibin Gao, Jieyu Lei, and Xiaoguang Wei are with the School of Electrical Engineering, Southwest Jiaotong University, Chengdu 611756, China (e-mail: gao_shi_bin@126.com; leijieyu_swjtu@126.com; wei_xiaoguang@126.com).

Yigu Liu is with the Department of Electrical Sustainable Energy, Delft University of Technology, 2628 LW Delft, The Netherlands (e-mail: liuyigu_a@126.com).

Tao Wang is with the School of Electrical Engineering and Electronic Information, Xihua University, Chengdu 610039, China (e-mail: wangatao2005@163.com).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSG.2022.3156445.

Digital Object Identifier 10.1109/TSG.2022.3156445

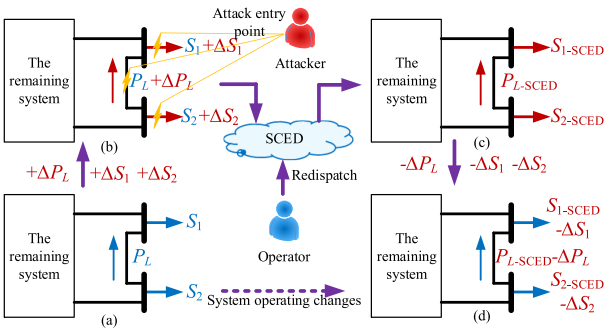

Fig. 2. Process of FDI attacks.

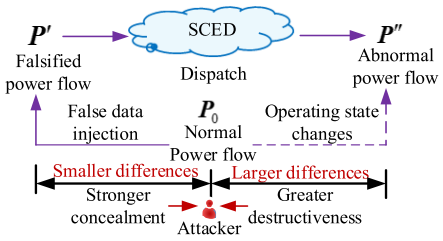

Fig. 3. Operating states before and after FDI attacks.

Answering the above two questions is very helpful for revealing the system vulnerability to analyze the impact of FDI attacks on the operating states of the system.

To solve the above issues, in this letter, we propose a novel pre- and post-dispatch-based bilevel FDI attack model that only employs the basic network information to construct a valid attack vector. The proposed bilevel model takes into account both concealment and destructiveness, which can minimize the variation between measurements of pre- and post-attack uploaded to control center before SCED. Furthermore, we compare the damage effects of the proposed pre- and post-dispatch-based FDI attack with the existing bilevel models in terms of causing uneconomic operation and branch overload.

III. Mechanism and Process of FDI Attacks

A. Mechanism of FDI Attacks

According to the basic assumptions described in reference [1], for an FDI attack, the attacker injects a non-zero attack vector $\boldsymbol{a} = [\Delta \boldsymbol{S}, \Delta \boldsymbol{P}]^T$ to the meter measurements by cooperatively manipulating power flow measurements and load injection measurements, where $\Delta \boldsymbol{S}$ and $\Delta \boldsymbol{P}$ need to satisfy

$$\Delta \boldsymbol{P} = -\boldsymbol{SF} \cdot \boldsymbol{KD} \cdot \Delta \boldsymbol{S} \tag{1}$$

In addition, to ensure that the total system load remains unchanged, the sum of false load measurements injected to all load buses is always equal to zero in (2a). Meanwhile, each measurement injected to the corresponding load-bus cannot exceed a threshold τ of the true load in (2b).

$$\mathbf{1}^T \Delta \boldsymbol{S} = 0 \tag{2a}$$

$$-\tau \boldsymbol{S}_0 \leq \Delta \boldsymbol{S} \leq \tau \boldsymbol{S}_0. \tag{2b}$$

B. Process of FDI Attacks

The process of FDI attacks can be described in Fig. 2. In the process of sampling and uploading true measurement information (Fig. 2(a)) via the cyber network to the control center, the attacker can inject an attack vector to the measurements based on (1) and (2) (Fig. 2(b)), which makes the power flow uploaded to the control center become (3).

$$\boldsymbol{P}' = \boldsymbol{SF} \cdot \boldsymbol{KP} \cdot \boldsymbol{R} - \boldsymbol{SF} \cdot \boldsymbol{KD} \cdot (\boldsymbol{S}_0 + \Delta \boldsymbol{S}) \tag{3}$$

According to the falsified power flow, the system operator will generate the error dispatch (Fig. 2(c)) after performing SCED. Therefore, the system power flow will become (4) as shown in Fig. 2(d).

$$\boldsymbol{P}'' = \boldsymbol{SF} \cdot \boldsymbol{KP} \cdot \boldsymbol{R} - \boldsymbol{SF} \cdot \boldsymbol{KD} \cdot (\boldsymbol{S}_0 - \Delta \boldsymbol{S}) \tag{4}$$

TABLE I
Comparison of Information Privilege Required for the Attacker to Construct an LR Attack

Methods	Network parameters $\boldsymbol{SF}$, $\boldsymbol{KD}$	System states $\boldsymbol{S}_0$, $\boldsymbol{P}_0$, $\boldsymbol{R}_0$	Cost information $\boldsymbol{c}$	Generation limitations $\boldsymbol{R}_{\min}$, $\boldsymbol{R}_{\max}$	Branch capacity $\boldsymbol{P}_{\max}$
[3][4]	√	√	√	√	√
Proposed method	√	√	-	-	-

After an FDI attack as shown in Fig. 3, the branch power flow of the system will be changed from the true states $\boldsymbol{P}_0$ to the abnormal states $\boldsymbol{P}''$, which leads the system to the non-economic and even insecure operating states. On the one hand, before SCED, the attacker would hope that the differences between falsified power flow $\boldsymbol{P}'$ after injecting false data and true power flow $\boldsymbol{P}_0$ can be minimal to increase the probability of an effective FDI attack, because the smaller differences can make the attack stealthier. On the other hand, after SCED, the attacker would hope that the differences between the abnormal power flow $\boldsymbol{P}''$of post-dispatch and true power flow $\boldsymbol{P}_0$ can be maximal, leading the greater destructiveness to the system. In summary, in order to pose a concealed and destructive FDI attack, $\boldsymbol{P}'$, $\boldsymbol{P}''$ and $\boldsymbol{P}_0$ should satisfy (5) in the ideal condition.

$$\left\|\boldsymbol{P}' - \boldsymbol{P}_0\right\| \to 0, \left\|\boldsymbol{P}'' - \boldsymbol{P}_0\right\| \to \infty. \tag{5}$$

The left and right formulas ensure the attack concealment and destructiveness, respectively.

IV. Proposed Bilevel FDI Attack Model

As the previous description, to ensure that constructed attack vectors can take into consideration both the concealment and destructiveness, we propose a pre-dispatch and post-dispatch-based bilevel model. Besides, compared with existing conventional bilevel models that require full network information as shown in Table I, our proposed model only needs network topology $\boldsymbol{SF}$, $\boldsymbol{KP}$ and $\boldsymbol{KD}$, and system state information $\boldsymbol{R}_0$, $\boldsymbol{P}_0$ and $\boldsymbol{S}_0$. It noted that the network topology includes the topology information and the admittance matrix.

A. Post-Dispatch-Based Upper Model

To ensure the destructiveness of attack after dispatch, we employ objective (6) to quantify $\|\boldsymbol{P}'' - \boldsymbol{P}_0\| \to \infty$. Therefore, the post-dispatch-based upper model can be constructed in (6)-(9). The goal of upper model is to maximize the differences between $\boldsymbol{P}''$ of post-dispatch and $\boldsymbol{P}_0$ so that the system can fall into the abnormal operating state.

$$\max_{\Delta \boldsymbol{S}} \ \mathbf{1}^T \left|\boldsymbol{P}'' - \boldsymbol{P}_0\right| \tag{6}$$

$$s.t.\ \ \mathbf{1}^T \Delta \boldsymbol{S} = 0 \tag{7}$$

$$-\tau \boldsymbol{S}_0 \le \Delta \boldsymbol{S} \le \tau \boldsymbol{S}_0 \tag{8}$$

$$\boldsymbol{P}'' = \boldsymbol{SF} \cdot \boldsymbol{KP} \cdot \boldsymbol{R} - \boldsymbol{SF} \cdot \boldsymbol{KD} \cdot (\boldsymbol{S}_0 - \Delta \boldsymbol{S}) \tag{9}$$

Because the objective (6) has the absolute value, the upper model is a nonlinear optimization model. To convert the model into a linear optimization model, we employ (10) instead of objective (6).

$$\max_{\Delta \boldsymbol{S}} \ \mathbf{1}^T \boldsymbol{\kappa} \tag{10a}$$

$$s.t.\ \ \left|\boldsymbol{P}'' - \boldsymbol{P}_0\right| \ge \boldsymbol{\kappa} \tag{10b}$$

The constraint (10b) can be furthermore converted into (10c) and (10d) by introducing 0-1 variable $\boldsymbol{\delta}$.

$$\boldsymbol{P}'' - \boldsymbol{P}_0 + M\boldsymbol{\delta} \ge \boldsymbol{\kappa} \tag{10c}$$

$$\boldsymbol{P}'' - \boldsymbol{P}_0 + M(\mathbf{1} - \boldsymbol{\delta}) \le -\boldsymbol{\kappa} \tag{10d}$$

The upper model of the proposed bilevel model can be summarized as

$$\text{Objective:}\ \ (10a)$$

$$s.t.\ \ \ (7)-(9),\ (10c)\ \text{and}\ (10d).$$

B. Pre-Dispatch-Based Lower Model

To ensure the concealment of attack before dispatch, we employ objective (11) to quantify $\|\boldsymbol{P}' - \boldsymbol{P}_0\| \to 0$. Therefore, the pre-dispatch-based lower model can be constructed in (11)-(14), where (13) is the limit of generator ramp. It is noted that (13) is used to limit the adjustment range of generators. The goal of lower model is to minimize the differences between $\boldsymbol{P}'$ of pre-dispatch and $\boldsymbol{P}_0$ in order to enhance the attack concealment.

$$\min_{\boldsymbol{R}} \ \mathbf{1}^T \left|\boldsymbol{P}' - \boldsymbol{P}_0\right| \tag{11}$$

$$s.t.\ \ \mathbf{1}^T \boldsymbol{S} = \mathbf{1}^T \boldsymbol{R} \tag{12}$$

$$|\boldsymbol{R} - \boldsymbol{R}_0| \le \Delta \boldsymbol{R} \tag{13}$$

$$\boldsymbol{P}' = \boldsymbol{SF} \cdot \boldsymbol{KP} \cdot \boldsymbol{R} - \boldsymbol{SF} \cdot \boldsymbol{KD} \cdot (\boldsymbol{S}_0 + \Delta \boldsymbol{S}) \tag{14}$$

Since the objective (11) has the absolute value, we can introduce two new artificial variables $\boldsymbol{X}^+$ and $\boldsymbol{X}^-$ that satisfy (15) to convert the lower model into a linear optimization model.

$$\boldsymbol{P}' - \boldsymbol{P}_0 = \boldsymbol{X}^+ - \boldsymbol{X}^- \tag{15a}$$

$$\left|\boldsymbol{P}' - \boldsymbol{P}_0\right| = \boldsymbol{X}^+ + \boldsymbol{X}^- \tag{15b}$$

$$\boldsymbol{X}^+ \ge \mathbf{0}, \boldsymbol{X}^- \ge \mathbf{0} \tag{15c}$$

Therefore, (11) and (14) can be equivalent to (16) and (17), respectively.

$$\min_{\boldsymbol{R}} \ \mathbf{1}^T \left(\boldsymbol{X}^+ + \boldsymbol{X}^-\right) \tag{16}$$

$$\boldsymbol{X}^+ - \boldsymbol{X}^- + \boldsymbol{P}_0 = \boldsymbol{SF} \cdot \boldsymbol{KP} \cdot \boldsymbol{R} - \boldsymbol{SF} \cdot \boldsymbol{KD} \cdot (\boldsymbol{S}_0 + \Delta \boldsymbol{S}) \tag{17}$$

The lower model of proposed bilevel model can be summarized as:

$$\text{Objective:}\ \ (16)$$

$$s.t.\ \ \ (12),\ (13),\ (15c)\ \text{and}\ (17).$$

Based on the discussion above, the proposed bilevel model is illustrated in Fig. 4. The goal of upper model is to maximize the variation between post-dispatch-abnormal and true network power flow from the destructiveness's perspective. The goal of lower model is to minimize the variation between pre-dispatch-falsified and true network power flow from the concealment's perspective. In addition, as the lower level can be converted to a linear programming model, it can be replaced with Karush-Kuhn-Tucker (KKT) optimality conditions.

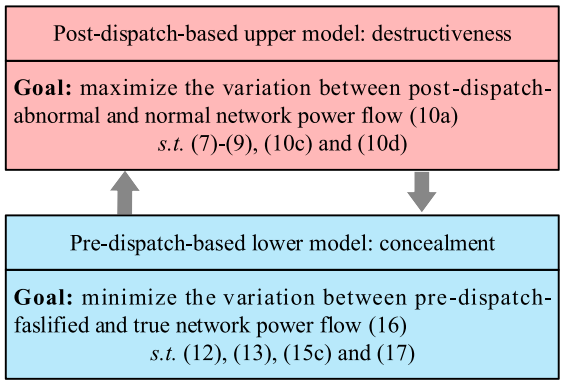

Fig. 4. Proposed bilevel FDI model.

TABLE II
OVERLOADING BRANCHES IN THE IEEE 14- AND 39- BUS SYSTEMS

Method	IEEE 14-bus system	IEEE 39-bus system
[3]	10,15	26,27
[4]	10,15	-
Proposed method	15	1,4,13,25,26,27,30

V. CASE STUDY

We employ IEEE 14-bus and IEEE 39-bus systems to verify the effectiveness of the proposed method. To analyze the advantages of the proposed method, we compare our method with the existing bilevel methods in [3], [4] where all the system information is required to model FDI attacks.

A. Destructiveness Analysis of the Proposed Method

We firstly investigate the number of overloading branches after SCED of post-attack are implemented and then erroneous dispatch is applied to the system. Table II shows the number of overloading branches in the two systems. We can see that in the 14-bus system, our method overloads one branch, while both methods in [3], [4] overload two branches. However, in the 39-bus system, our method can obviously overload more branches than other two methods. Especially, the method in [4] does not cause any branch overload. Moreover, we give the space distribution of overloaded branches caused by our method in the IEEE 39-bus system, as shown in Fig. 5. In the figure, the overloaded branches divide the system into the four regions including three islands. If the operator cannot immediately take emergency measures, the system will split and then lead to the blackout. Therefore, the proposed method can lead the system to the unsecure operating states.

Furthermore, we assume that the operator can take prompt measure to redispatch the operation states of the system by implementing SCED after the system is attacked. After redispatching, the generator outputs and operation cost of the two systems are listed in Tables III and IV, respectively. We can see that the three methods result in different generation

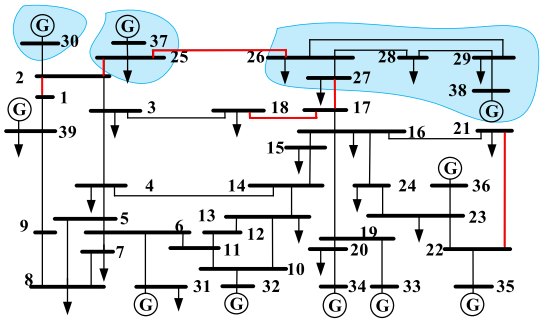

Fig. 5. Space distribution of overloading branches in the IEEE 39-bus system.

TABLE III
GENERATOR OUTPUTS IN THE IEEE 14-BUS SYSTEM(MW)

Gen.	[3]	[4]	Proposed method
1	235.359	223.907	234.008
2	4.873	22.579	18.111
3	0	12.514	0
6	18.768	0	6.88136
8	0	0	0
Total cost	$4427.291	$4536.500	$4328.700

TABLE IV
GENERATOR OUTPUTS IN THE IEEE 39-BUS SYSTEM(MW)

Gen.	[3]	[4]	Proposed method
30	900.000	900.000	849.487
31	1040.000	1040.000	1040.000
32	432.212	462.044	703.426
33	642.309	652.000	384.633
34	508.000	508.000	508.000
35	687.000	687.000	611.305
36	580.000	580.000	580.000
37	564.000	564.000	564.000
38	488.366	356.532	92.200
39	412.343	504.654	921.180
Total cost	$125650.000	$125560.000	$129745.220

outputs for the same generator node, leading to the different operation cost. In the 14-bus system, the two methods in [3], [4] result in the total operation costs of $4427.291 and $4536.500, respectively. In comparison, the proposed method results in the total operation cost of $4328.700. Although the total operation cost caused by our method is less than the ones caused by other two methods, our method still makes the system fall into the uneconomic operating. Meanwhile, in the 39-bus system, our method results in total operation cost of $129745.220, which can cause more losses to the system compared with the other two methods. Consequently, we can conclude that although the proposed method is constructed based on incomplete information, it can still lead the system to the uneconomic operating similar to the other bilevel models.

B. Concealment Analysis of the Proposed Method

To analyze the concealment of the proposed method, we investigate the changes of uploaded branch measurements of total system between pre- and post-attack before dispatching. Due to space limitations, we take the IEEE 14-bus system as an example. The variation of the power flow measurement of each branch is shown in Table V. Except for branches 11, 12, 13, 18, 19 and 20, the variations of the other branches in the proposed method are less compared with the two methods. However, it is also noted that in order to make the system fall into contingency and then trigger the SCED, the attacker must inject more false data to falsely overload some specific branches. For example, in the proposed method, to overload branch 15, the attacker must inject more false data to branch 15 compared with the other branches. Therefore, to improve the concealment of the attack, under the premise of falsely overload certain branches, the amount of false data injected into the remaining branches need to be reduced as much as possible. Similar conclusions can be concluded in the IEEE 39-bus system.

TABLE V
CHANGES OF BRANCH POWER FLOW MEASUREMENTS IN THE IEEE14-BUS SYSTEM(MW)

Branch ID	[2]	[3]	Proposed method
1	-5.46801	-6.90415	-1.8107
2	5.468012	6.904151	1.8107
3	-10.2038	-17.1194	3.939
4	6.711125	9.859686	2.1616
5	8.874671	11.20555	2.9388
6	18.72978	29.98061	-2.3309
7	8.544816	4.986005	3.0837
8	15.63674	15.50528	13.0379
9	9.125742	9.04902	7.609
10	19.0875	19.2957	11.6332
11	1.975548	2.100923	4.4225
12	3.599727	3.618141	3.8885
13	7.912226	7.976639	8.9222
14	0	0	0
15	15.63674	15.50528	13.0379
16	4.274442	4.149077	1.8275
17	5.738042	5.655219	4.0694
18	-0.22555	-0.35092	-2.6725
19	0.549728	0.568141	0.8385
20	1.711955	1.794781	3.3806

REFERENCES

[1] Y. Liu, N. Peng, and M. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Security*, vol. 14, no. 1, pp. 1–33, 2011.

[2] L. Che, X. Liu, Z. Shuai, Z. Li, and Y. Wen, "Cyber cascades screening considering the impacts of false data injection attacks," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6545–6556, Nov. 2018.

[3] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 382–390, Jun. 2011.

[4] Y. Tan, Y. Li, Y. Cao, M. Shahidehpour, and Y. Cai, "Severe cyber attack for maximizing the total loadings of large-Scale attacked branches," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6998–7000, Nov. 2018.

[5] Y. Tan, Y. Li, Y. Cao, and M. Shahidehpour, "Cyber-attack on overloading multiple lines: A bilevel mixed-integer linear programming model," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1534–1535, Mar. 2018.

[6] L. Che, X. Liu, Z. Li, and Y. Wen, "False data injection attacks induced sequential outages in power systems," *IEEE Trans. Power Syst.*, vol. 34, no. 2, pp. 1513–1523, Mar. 2019.

[7] D. Khezrimolagh, J. Khazaei, and A. Asrari, "MILP modeling of targeted false load data injection cyberattacks to overflow transmission lines in smart grids," in *Proc. North Amer. Power Symp. (NAPS)*, Wichita, KS, USA, Oct. 2019, pp. 1–7.