False Data Injection Attack and Corresponding Countermeasure in Multienergy Systems

Qiwei Zhang, *Member, IEEE*, Fangxing Li, *Fellow, IEEE*, Jin Zhao, *Member, IEEE*, and Buxin She, *Graduate Student Member, IEEE*

***Abstract*—Worldwide ambitions to combat climate change have expedited the penetration of renewables and decarbonization. Multienergy systems (MES), where different energy systems are optimally coordinated, have been recognized as a key element in future low-carbon energy operations. However, MES operations involve intense exchanges of information and control signals, thereby intensify the risk of cyberattacks. Existing cybersecurity research mainly focuses on a single-energy system, with only a few pioneering cybersecurity analyses for MES focusing on uncoordinated cyberattacks. A lack of detailed discussion and analysis on the optimally coordinated cyberattack targeting MES prevents operators from accurately evaluating the potential damages of cyberattack in MES operations. Therefore, this article first proposes an optimally coordinated false data injection attack (OC-FDIA) against MES, where attacks from different energy systems are coordinated to disturb the MES operation. Then, we show that the OC-FDIA can cause synergetic effects leading to much more severe damage than single-system FDIAs and uncoordinated FDIAs. Further, an effective countermeasure is developed to mitigate the OC-FDIA based on deep learning (DL). Eventually, the proposed OC-FDIA and its countermeasures are demonstrated through integrated electricity and gas test systems.**

***Index Terms*—Multienergy system (MES), electricity-gas operation, false data injection attack (FDIA), cybersecurity deep learning, synergetic effect.**

NOMENCLATURE

Sets:

line^{gas}, *line^e*	Set of gas pipelines and electric transmission lines.
$node^{gas}$, $node^{e}$	Set of gas and electric network nodes.
$node^{GW}$, $node^{EG}$	Set of gas well and electric unit nodes.
$node^{ptg}$, $node^{gfg}$	Set of power-to-gas nodes and gas-fired-unit nodes.
$node^{c}$	Set of gas compressor nodes.
T	Set of time intervals.

Electric network:

${D_{i,t}}^{E}$	Electric load.
GSF	Generation shift factors.
$L_l^{\max}$, $L_l^{\min}$	Upper and lower limits for electricity line flow.
${P_i}^{\max}$, ${P_i}^{\min}$	Upper and lower limits for electric units.
$P_{i,t}$	Generation for electric units.
${ramp_i}^{\min}$, ${ramp_i}^{\max}$	Ramping limits for electric units.

Gas network:

c, u_0	Sound speed in gas pipeline and gas flow velocity.
${D_{i,t}}^{G}$	Gas load.
Dia, A,	pipeline diameter and cross-section area,
dx, dt	Pipeline segment length and time interval segment.
$I_{i,t}^{\mathrm{GW},\min}$, $I_{i,t}^{GW,max}$	Gas well injection boundaries.
$I_{i,t}^{GW}$	Gas well injection.
f	Friction factor for pipeline.
$m_{l,to,t}$, $m_{l,from,t}$	Gas mass flow at the sending node and receiving node.
$pr_{i,}^{min}, pr_i^{max}$	Gas nodal pressure boundary.
$pr_{i,t}$	Gas nodal pressure.

Energy conversion devices:

α_i, β_i	Gas-fired unit and power-to-gas generation conversion rate.
$I_{i,t}^{ptg}$	Power-to-gas units gas production.
$P_i^{gfg,max}$,$P_i^{gfg,min}$	Upper and lower limits for gas-fired units.
$P_i^{ptg,max}, P_i^{ptg,min}$	Upper and lower limits for power-to-gas units.
$P_{i,t}^{ptg,e}, P_{i,t}^{ptg,g}$	Power-to-gas units power generation for electricity and gas.
$P_i^{gfg,e}, D_i^{gfg}sVal$	Gas-fired unit generation and gas consumption.

Attack and countermeasure:

$M_{i,t}^{e,d}, M_{i,t}^{g,d}, M_{i,t}^{g,\rho}$	Value of LR-FDIA, GD-FDIA, and GL-FDIA.
$q_{i,t}^{e,d}, q_{i,t}^{g,d}, q_{i,t}^{g,\rho}$	Attack ability of LR-FDIA, GD-FDIA, and GL-FDIA.
$\Delta P_{i,t}^{def}, \Delta Pro_{i,t}^{def}$	Mitigation value at defending electric unit and gas well.
$\Delta P_{i,t}^{def,max}, \Delta Pro_{i,t}^{def,max}$	Boundaries of mitigation value.

Manuscript received 1 November 2022; revised 28 March 2023; accepted 7 May 2023. Date of publication 16 May 2023; date of current version 21 February 2024. This work was supported by the U.S. Department of Energy CEDS Project Watching Grid Infrastructure Stealthily Through Proxies under Award DE-OE0000899. Paper no. TPWRS-01650-2022. *(Corresponding author: Fangxing Li.)*

The authors are with the EECS Department at the University of Tennessee, Knoxville, TN 37996 USA (e-mail: qzhang41@vols.utk.edu; fli6@utk.edu; jzhao44@utk.edu; bshe@vols.utk.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TPWRS.2023.3276736.

Digital Object Identifier 10.1109/TPWRS.2023.3276736

I. Introduction

A. Background

The Paris Agreement of 2015 has driven worldwide efforts to limit greenhouse gas emissions and mitigate climate change. The U.S. has assembled task forces to reach 100% carbon pollution-free electricity by 2035 and achieve net-zero emissions by 2050 [1]. The E.U. has published the European Climate Law, making the commitment to a 55% reduction in greenhouse gas emissions legally binding [2]. Decarbonization will play a key role in the success of such efforts [3].

While there are a number of decarbonization technologies in development, one stands out as an especially promising solution: the multienergy system (MES) [4]. A MES supports the smooth transition of energy among different energy vectors, driving the future energy system towards reduced reliance on fossil fuels and embracing renewable resources. At present, the high-penetration of gas-fired generations (GfGs) and the deployment of power-to-gas (PtG) technology have already imposed strong interdependency between power and gas systems operation, planning, and control. Under MES coordination, different energy networks, such as power and gas, can fully utilize energy conversion devices to improve energy efficiency.

The MES operation breaks down the barrier in energy operations and information flow among different energy systems, but this interconnection also intensifies the risk of cyberattacks. The notorious cyberattacks on the Ukraine power system in 2015 [5] and the colonial pipeline cyberattack on the U.S. gas sector in 2021 [6] both caused significant economic losses in power and gas systems, respectively. A MES deployment would potentially escalate the impact of such cyberattacks since the coupling between different energy systems is much stronger. For example, the cyberattacks on Ukraine's power system may endanger natural gas system operations under MES framework. Single-system cybersecurity analysis is inadequate for analyzing MES cybersecurity, but cybersecurity analysis on MES is an under-investigated research area. Relevant research works are summarized and categorized in the next subsection.

B. Literature Review

The MES concept is defined in [7] as multiple energy systems that optimally interact with each other at various levels, such as the city or country level. References [8] and [9] provide comprehensive reviews on MES operations and demonstrate the impressive potential of MES in achieving decarbonization.

Existing MES research can be broadly divided into three categories: advanced modeling, efficient optimization, and coherent market structures. In the first category, various MES operation models have been proposed. Reference [10] illustrates the limitation of the steady-state gas flow model and provides a convex relaxation scheme for the MES operation model considering gas flow dynamics. References [11] and [12] propose two new linearized MES operation models reflecting gas flow dynamics. References [13] and [14] focus on integrated heat and electricity operations considering heat dynamics and system planning, respectively. In the second category, efficient optimization techniques are applied to solve a MES operation model. In [15] and [16], the MES operation model is optimized by heuristic algorithms and distributed algorithms, respectively. The last category aims to analyze the market settlement and scheme for MES. References [17] and [18] capture the market equilibrium in integrated electricity-heat and electricity-gas systems. Reference [19] proposes a locational marginal price formulation to settle the transaction in integrated electricity-heat operations. The above literature has been selected as representative of each of the MES research categories. Detailed reviews of MES research can be found in references [8] and [9].

Despite the large body of MES research, MES cybersecurity remains under-investigated. Existing cybersecurity research focuses mainly on a single-energy system, particularly on power systems. References [20] and [21] propose and investigate the impact of congestion pattern attacks and transmission line-rating attacks in power system operations, respectively. References [22], [23], and [24] provide detailed modeling, analysis, and countermeasures to power system load redistribution (LR) attacks. References [25] and [26] establish a market-level defense and analysis against power system false data injection attacks (FDIAs). Similarly, natural gas systems rely on the SCADA system, which introduces vulnerabilities from cyberattacks. Reference [27] proposes an undetectable FDIA on gas system measurement data. Reference [28] provides online-learning detection against FDIAs in natural gas and power systems.

However, the single-energy system cybersecurity research described above is inadequate for MES cybersecurity due to the strong coupling among different energy systems in a MES. A few pioneering cybersecurity studies have shifted the focus to MES. Reference [29] proposes the first FDIA on gas systems targeting gas load and gas density in MES operations. Reference [30] proposes a robust MES dispatch model to ensure the stable integrated operation of the power and heat system under cyberattacks. Reference [31] analyzes the propagation/ripple effect of cyberattack under the MES framework considering power and heat systems. Reference [32] proposes a class of FDIAs targeting natural gas demand and analyzes their impact on power systems under MES operations. Reference [33] proposes learning-based detection against cyberattacks targeting energy conversion devices in integrated power and gas system operations. Reference [34] proposes a trilevel defense strategy against transmission lines and gas pipeline attacks in integrated power and gas system operations. Reference [35] focuses on disconnecting gas-fired power plants by manipulating MES measurements. Reference [36] coordinates the energy and transportation system to prevent FDIAs in MES operations. The existing MES cybersecurity analysis has been mainly focused on analyzing the effect of FDIA in a single-energy system on the overall MES operation and a resilient coupling between different energy systems. Due to a lack of comprehensive cybersecurity analysis on the synergetic effect among FDIAs in different energy systems, the MES operators may significantly underestimate the potential damage caused by cyberattacks.

C. Motivations and Contributions

This article proposes an optimally coordinated FDIA (OC-FDIA) strategy and corresponding mitigation scheme for future

MES operator to analyze synergetic effect among FDIAs in different energy systems. The detailed contributions are presented as follows:

- Existing MES cybersecurity research has mainly focused on analyzing the propagation effect of cyberattacks in a MES, such as how attacks on one energy system impact another energy system. To the best of our knowledge, this article is the first attempt to analyze the synergetic effect of cyberattacks on MES operations. Coordinated FDIAs in different energy systems could cause more damage (i.e., synergetic effect) than the simple sum of the damage caused by FDIAs in different energy systems individually. The analysis on the OC-FDIAs provides MES operators a better understanding on the impact of FDIAs in MES operations.
- This article provides a countermeasure for MES operators to mitigate the synergetic effect in coordinated FDIAs in different energy systems. Based on the deep learning (DL) technique, the mitigation decision can be determined efficiently and effectively. Further, this article analyzes and mitigates the OC-FDIA for MES operations considering the characteristics of gas flow dynamics, which provide a more accurate cybersecurity analysis for MES operations.

D. Paper Organization

The rest of this article is organized as follows. Section II presents a MES operation model considering gas flow dynamics. The detailed mathematical model of the proposed OC-FDIA is described in Section III, followed by a comparison with traditional FDIAs. Section IV develops a mitigation scheme against the proposed OC-FDIA. Section V provides simulation studies demonstrating the proposed OC-FDIA and countermeasures. Finally, Section VI summarizes the conclusion and discusses potential directions for future studies.

II. MES Operation Model Considering Gas Dynamics

The large share of GfGs and the increasing deployment of PtG technology has made the coordination between power systems and natural gas systems one of the most promising ways to improve energy efficiency. Therefore, the MES in this article consists of a power system and a gas system with flexible energy transition units (i.e., GfGs and PtG technology). The detailed MES operation models are described in the following subsections.

A. Gas Network Model Considering Gas Flow Dynamics

Electricity is delivered instantaneously in an electricity grid, but gas flow could take hours to travel from source to demand in a gas network requiring spatio-temporal representations [10]. Under the isothermal conditions, (1) and (2) describe the gas flow dynamics through a set of partial differential equations.

$$\frac{\partial}{\partial t}p(x,t) + \frac{4c^2}{\pi D^2}\frac{\partial}{\partial x}m(x,t) = 0 \tag{1}$$

$$\frac{\partial}{\partial x}p(x,t) + \frac{4}{\pi D^2}\frac{\partial}{\partial t}m(x,t) + \frac{\partial}{\partial x}p(x,t)u^2(x,t) = -\frac{8fc^2}{\pi^2 Dia^5}\frac{m^2(x,t)}{p(x,t)} \tag{2}$$

Then, a finite difference method is applied to approximate the solution to (1) and (2) as in (3) and (4) based on [11] and [39]. The finite difference method demonstrates a good balance between model complexity and solution efficiency. Every pipeline in the gas system is segmented by Δx, and each time interval is segmented by Δt based on pipeline physical characteristics. The criteria of Δx and Δt selection can be found in [10].

$$\begin{aligned}&pr_{i+1,t+1} + pr_{i,t+1} - pr_{i+1,t} - pr_{i,t}\\ &+\frac{c^2 dt}{dxA}(m_{l,to,t+1} - m_{l,from,t+1} + m_{l,to,t+1} - m_{l,from,t}) = 0,\\ &\forall i \in node^{gas}, \forall t \in T\end{aligned} \tag{3}$$

$$\begin{aligned}&\frac{1}{A}(m_{l,to,t+1} + m_{l,from,t+1} + m_{l,to,t+1} + m_{l,from,t})\\ &+\frac{dt}{dx}(pr_{i+1,t+1} - pr_{i,t+1} + pr_{i+1,t} - pr_{i,t})\\ &+\frac{fu_0 dt}{4DA}(m_{l,from,t+1} + m_{l,to,t+1} + m_{l,from,t} + m_{l,to,t}) = 0_i,\\ &\forall i \in node^{gas}, \forall l \in line^{gas}, \forall t \in T\end{aligned} \tag{4}$$

$$m_{i,from,t}, m_{i,to,t} \geq 0_i, \forall i \in Line^{gas}, \forall t \in T \tag{5}$$

For each pipeline segment, (3)–(5) are modeled to represent the gas flow dynamics.

In addition to gas flow equations, gas system state variables are restricted within a certain range due to physical characteristics and security considerations. The upper and lower limits for the gas well supply and gas node pressure are shown in (6) and (7). The gas compressor is modeled in (8) [10], where the nodal pressure can be increased up to Γ times at the compressor node.

$$I_{i,t}^{GW,Min} \leq I_{i,t}^{GW} \leq I_{i,t}^{GW,Max}, \forall i \in node^{GW}, \forall t \in T \tag{6}$$

$$pr_i^{\min} \leq pr_{i,t} \leq pr_i^{\max}, \forall i \in node^{gas}, \forall t \in T \tag{7}$$

$$pr_i^{\min} \leq pr_{i,t} \leq \Gamma pr_i^{\max}, \forall i \in node^{c}, \forall t \in T \tag{8}$$

The gas system nodal mass flow balance is formulated in (9).

$$\begin{aligned}&I_{i,t}^{GW} + I_{i,t}^{p2g} - D_{i,t}^{gas} - D_{i,t}^{g2g} + \sum_L m_{l,to,t} - \sum_L m_{l,from,t} = 0,\\ &\forall i \in node^{gas}, \forall t \in T\end{aligned} \tag{9}$$

B. Power Network Model

A common power system economic dispatch model is shown in (10)-(14) [37]. The DC optimal power flow (OPF) is considered to formulate the power system network constraints, instead of AC optimal power flow, for simplicity. Constraint (10) ensures the overall power balance. Constraints (11)–(14) set the boundary for generator outputs, power flow, and generator ramping, respectively. The presented power system model with DC power flow is common in many MES studies, such as in [29] and [34].

$$\sum_i P_{i,t} - \sum_i D^{E}_{i,t} = 0, \forall i \in node^{e}, \forall t \in T \tag{10}$$

$$P_i^{\min} \leq P_{i,t} \leq P_i^{\max}, \forall i \in node^{EG}, \forall t \in T \tag{11}$$

$$\sum_{i=1}^{N_b} GSF_{l-i}(P_{i,t} - D^{E}_{i,t}) \leq L_l^{\max} \forall l \in line^{e}, \forall t \in T \tag{12}$$

$$\sum_{i=1}^{N_b} GSF_{l-i}(P_{i,t} - D^{E}_{i,t}) \geq L_l^{\min} \forall l \in line^{e}, \forall t \in T \tag{13}$$

$$ramp_i^{\min} \leq P_{i,t} - P_{i,t-1} \leq ramp_i^{\max}, \forall i \in node^{EG}, \forall t \in T \tag{14}$$

C. Energy Conversion Devices

Bi-directional energy conversion devices couple the power system and gas system to enhance energy efficiency. The GfG unit consumes gas to generate electricity, which is described by (15). The conversion coefficient α_i represents the energy conversion relationship and device efficiency. The generation limits of GfG units are restricted by (16) [11].

$$D^{gfg}_{i,t} = \alpha_i P^{gfg}_{i,t}, \forall i \in node^{gfg}, \forall t \in T \tag{15}$$

$$P_i^{gfg,\min} \leq P^{gfg}_{i,t} \leq P_i^{gfg,\max}, \forall i \in node^{gfg}, \forall t \in T \tag{16}$$

The PtG unit consumes electricity to produce natural gas. For example, surplus renewable energy could be converted to hydrogen gas through polymer electrolyte membrane electrolysis technology. The relationship between the produced gas and consumed power can be represented by (17). The subscripts k and i indicate that the PtG unit converts energy from bus i in the power system to node k in the natural gas system. The generation limits of PtG units are restricted by (18) [11].

$$I^{ptg}_{k,t} = \beta_i P^{ptg,g}_{i,t}, \forall i \in p2g \tag{17}$$

$$P_i^{ptg,\min} \leq \frac{1}{\beta_i} I^{ptg}_{i,t} + P^{ptg,e}_{i,t} \leq P_i^{ptg,\max}, \forall i \in node^{ptg} \tag{18}$$

D. Overall MES Operation Model

The overall objective of the MES operation model is to minimize the supply cost, as shown in (19). The power system operation cost consists of conventional unit costs, and PtG unit costs for electricity generation. The gas system operation cost consists of gas well costs and PtG unit costs for gas generations.

$$\min \sum_t \begin{bmatrix} \underbrace{\sum_i C_{i,t}(P^{TU}_{i,t}) + \sum_i C_{i,t}(P^{ptg}_{i,t})}_{PowerSystem} \\ \underbrace{+\sum_i C_i(I^{ptg}_{i,t}) + \sum_i C_i(I^{GW}_{i,t})}_{GasSystem} \end{bmatrix} \tag{19}$$

Subject to

$$\text{Gas system constraint } (3) - (9)$$

$$\text{Power system constraint } (10) - (14)$$

$$\text{Conversion devices constraint } (15) - (18)$$

The operation constraints in power systems, gas systems, and conversion devices are described above. MES operators solve the above optimal dispatch model to determine optimal power system and gas system dispatches.

In summary, this section describes the operation model of a MES consisting of a power system and a natural gas system. The proposed attack strategy against MES operation is presented and analyzed in the next section.

III. Optimally Coordinated FDIAs Against MES Operations

The proposed OC-FDIA is a bilevel optimization model, where the attacker is modeled at the upper-level, and the overall MES operation model is placed at the lower-level. The attacker selects the most effective attack paths in MES operations targeting different energy systems.

A. Upper-Level Attacker Model

Various cyberattack paths in power systems have been proposed and demonstrated in the literature, such as LR attacks in [22]. A few cyberattack paths in gas systems have also been investigated, such as gas load attacks (GL-FDIAs) and gas density attacks (GD-FDIA) [29]. By proposing the OC-FDIA, where individual system FDIAs are coordinately launched, this article aims to provide an analysis on the synergetic effect of FDIAs in different energy systems. In other words, the attacker's knowledge, assumption, goals, and entry points of these individual FDIAs remain unchanged, but the attacker has comprehensive information on these individual attacks for coordination. The OC-FDIA provides new attack decisions leading to synergetic effects, which cause more severe disruptions in the overall MES operation compared with the sum of the loss caused by individual FDIAs. The OC-FDIA model considers the most common types of FDIAs in power and gas systems: LR attacks [22], GL-FDIAs [29], and GD-FDIAs [29]. Other types of attacks can be easily added based on the interests of future researchers.

The LR attack is modeled through (20), (21) based on [22]. Constraint (20) limits the attack magnitude ensuring that it is a stealthy attack. Constraint (21) ensures that the total load is unchanged.

$$-q^{e,d}_{i,t} D^{E}_{i} \leq M^{e,d}_{i,t} \leq q^{e,d}_{i,t} D^{E}_{i,t}, \forall i \in node^{e}, \forall t \in T \tag{20}$$

$$\sum_i M^{e,d}_i = 0, \forall i \in node^{e}, \forall t \in T \tag{21}$$

Similar to the LR attack, the GL-FDIA and GD-FDIA are modeled in (22)–(24) based on [29]. Different from the attack presented in [29], which considers a steady-state gas flow model, this article includes gas flow dynamics. Therefore, the gas density impacts the value of the gas pressure as in (24), instead of the Weymouth coefficient. In this article, we consider the attacker's objective to damage the operation cost (19), but any other objectives can be integrated similarly.

$$-q^{g,d}_{i,t} D^{G}_{i,t} \leq M^{g,d}_{i,t} \leq q^{g,d}_{i,t} D^{G}_{i,t},\ \forall i \in node^{gas}, \forall t \in T \tag{22}$$

$$0 \le M^{g,\rho}_{i,t} \le \sigma^{g,\rho}_{i,t} \rho^{g,\rho}_{i,t}, \forall i \in node^{gas}, \forall t \in T \tag{23}$$

$$pr_{i,t} = pr_{i,t} + c^2 M^{g,\rho}_{i,t}, \forall i \in node^{gas}, \forall t \in T \tag{24}$$

B. Lower-Level MES Operation

Considering the LR attack, GL-FDIA, and GD-FDIA, normal MES operation model is disturbed. The power balance constraint remains the same because attack constraint (21) restricts the sum of LR to 0. The power flow constraints (12), (13) become constraints (25), (26). Although the total generation remains the same, an effective LR attack changes the marginal pattern of economic dispatches.

$$\sum_{i=1}^{N_b} GSF_{l-i}(P_{i,t} - D^E_{i,t} + M^{e,d}_{i,t}) \le L^{\max}_l, \forall l \in L, \forall t \in T \tag{25}$$

$$\sum_{i=1}^{N_b} GSF_{l-i}(P_{i,t} - D^E_{i,t} + M^{e,d}_{i,t}) \ge L^{\min}_l, \forall l \in L, \forall t \in T \tag{26}$$

The gas flow (3) and (4) are reformulated to (27) and (28) under the GD-FDIA.

$$\begin{aligned}
&pr_{i+1,t+1} + pr_{i,t+1} - pr_{i+1,t} - pr_{i,t}\\
&+ c^2(M^{g,\rho}_{i+1,t+1} + M^{g,\rho}_{i,t+1} - M^{g,\rho}_{i+1,t} - M^{g,\rho}_{i,t})\\
&+ \frac{c^2 dt}{dxA}(m_{l,to,t+1} - m_{l,from,t+1} + m_{l,to,t+1} - m_{l,from,t}) = 0\\
&, \forall i \in node^{gas}, \forall t \in T
\end{aligned} \tag{27}$$

$$\begin{aligned}
&\frac{1}{A}(m_{l,to,t+1} + m_{l,from,t+1} + m_{l,to,t+1} + m_{l,from,t}) +\\
&\frac{dt}{dx}\,[pr_{i+1,t+1} - pr_{i,t+1} + pr_{i+1,t} - pr_{i,t}\\
&+ c^2(M^{g,\rho}_{i+1,t+1} - M^{g,\rho}_{i,t+1} + M^{g,\rho}_{i+1,t} - M^{g,\rho}_{i,t})]\\
&\frac{fu_0 dt}{4DA}(m_{l,from,t+1} + m_{l,to,t+1} + m_{l,from,t} + m_{l,to,t}) = 0,\\
&\forall i \in node^{gas}, \forall l \in line^{gas}, \forall t \in T
\end{aligned} \tag{28}$$

The gas nodal pressure boundary constraint is reformulated to (29).

$${pr_i}^{\min}{}_i \le pr_i + c^2 M^{g,\rho}_{i,t} \le {pr_i}^{\max}{}_i, \forall i \in node^{gas} \tag{29}$$

The gas nodal balance (9) is reformulated to (30) under the GL-FDIA.

$$\begin{aligned}
&I^{GW}_{i,t} + I^{ptg}_{i,t} - D^{gas}_{i,t} - D^{g2g}_{i,t} - M^{g,d}_{i,t} + \sum_L m_{l,to,t}\\
&- \sum_L m_{l,from,t} = 0_i,\\
&\forall i \in node^{gas}, \forall t \in T
\end{aligned} \tag{30}$$

The overall OC-FDIA model is shown in (31), and it is a bi-level optimization model, whose solution algorithms have been widely discussed in literature, such as [26]. By considering multiple types of FDIAs in different energy systems, the optimization model provides an optimal FDIA combination targeting MES operations.

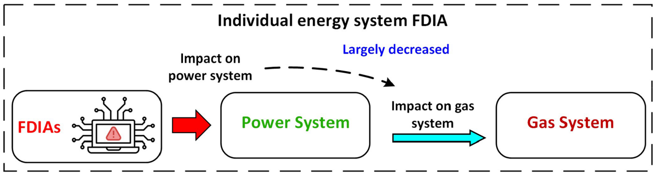


Fig. 1. Individual energy system FDIAs.

$$\begin{aligned}
&\max(19)\\
&\textbf{Subject to}\\
&\text{Attack constraint } (20)-(24)\\
&\underbrace{M^{E,d}_{i,t}, M^{G,d}_{i,t}, M^{G,\rho}_{i,t}}_{\text{Attack decision}}\\
&\in \arg\left\{\begin{array}{l}\text{Lower - level problem:}\\ (5),(6),(10),(11),(14),(25)-(30)\end{array}\right\}
\end{aligned} \tag{31}$$

C. Comparisons Between Single-System FDIAs, Uncoordinated FDIAs, and the OC-FDIAs

The above subsection proposes an OC-FDIA strategy to analyze the synergetic effect caused by FDIAs in different energy systems. This subsection will discuss the difference between single-system FDIAs, uncoordinated FDIAs, and the OC-FDIA from the perspective of concept and modeling. The case study in Section V will numerically describe the severity of the synergetic effect by OC-FDIA.

1) Traditional Single-System FDIAs: This category of FDIA has a minimal impact on other energy systems in general. For example, if a LR attack happens to a power system, the disturbance could be entirely covered by conventional units, and the gas system operation would not be impacted. Even if the attack disturbed the GfG units, causing a change $\Delta d^G{}_{i,t}$ in gas consumption, the MES operation model tries to cover the $\Delta d^G{}_{i,t}$ at minimal cost, decreasing the impact, as shown in Fig. 1. Further, the cybersecurity analysis for single-system FDIAs generally models the impact within its energy system, even if the FDIA affects the operation of other energy systems.

2) Uncoordinated FDIA in MES Operations: This category of FDIA disturbs multiple energy systems, but the impact may not be significant. For example, if a LR attack Δd^E is launched to increase the operation cost, which changes the generations and gas consumption of a GfG unit. An FDIA Δd^G on gas systems may lower the gas supply price for the GfG unit (e.g., switch from PtG to gas well). Then, the effectiveness of Δd^E decreases, although the Δd^G also damages MES operation. Without coordination, FDIAs on different systems may neutralize each other's attack objective, as shown in Fig. 2. The cybersecurity analysis model for uncoordinated FDIAs in MES operations has

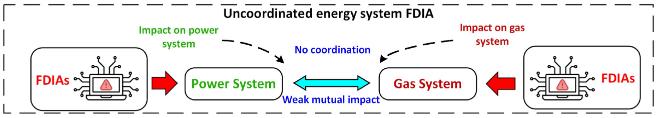


Fig. 2. Uncoordinated FDIAs.

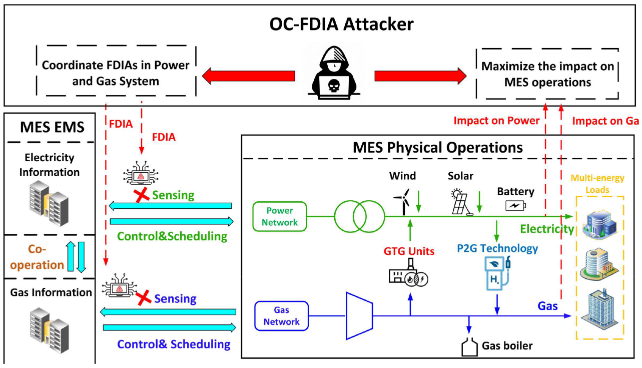


Fig. 3. Structure of OC-FDIA.

limited ability to investigate the synergetic effect of FDIAs and underestimates the impact of cyberattacks in MES operations.

3) The OC-FDIA: Fig. 3 illustrates the structure of the OC-FDIA, where the FDIA on power systems is strategically coordinated with an FDIA on gas systems to cause more damage. Considering the same scenario when a Δd^E increases the generations and gas consumption of a GfG unit, the FDIA Δd^G may try to switch the gas supply of a GfG unit from the gas well to PtG, increasing the operation cost. It is worth noting that the mathematical formulation for any individual attack may appear to be similar to the proposed OC-FDIA and traditional uncoordinated FDIAs. However, there is a significant difference that the proposed OC-FDIA combines different attack models to coordinate with each other, while traditional uncoordinated FDIAs design attack strategy separately and uncoordinatedly.

In summary, the cybersecurity analysis for conventional single-system FDIAs and uncoordinated FDIAs present limited implications on the synergetic effect in MES operations. However, the proposed OC-FDIA will simulate the coordination among different FDIAs providing an accurate analysis on synergetic effect in MES operations.

IV. Countermeasure to the Proposed OC-FDIA

This section develops a countermeasure to mitigate the proposed OC-FDIA.

A. Countermeasure Model Formulation

The countermeasure adjusts the dispatch to mitigate the OC-FDIA by perturbing the boundary of the operation model. Without the mitigation action, the attacker freely applies the OC-FDIA model to achieve maximum damage to the system. With the mitigation action, the OC-FDIA deviates from the optimal solution, which decreases the damage. The mitigation strategy represents a robust MES dispatch result, where the OC-FDIAs are unable to cause the expected damage. Defending units are selected to perform the mitigation actions, and perturbation variables are restricted, as shown in (32), (33). The $\Delta P_i{}^{def}$ and $\Delta Pro_i{}^{def}$ are the boundaries of perturbations on defending units. The MES dispatch is also perturbed by the mitigation actions, as shown in (34) and (35).

$$\Delta P_i^{def,\max} \le \Delta P_i^{def} \le 0, \forall i \in node^{E,def} \tag{32}$$

$$\Delta Pro_i^{def,\max} \le \Delta Pro_i^{def} \le 0, \forall i \in node^{G,def} \tag{33}$$

$$P_i^{\min} \le P_{i,t} \le P_i^{\max} + \Delta P_i^{def}, \forall i \in node^{e,def}, \forall t \in T \tag{34}$$

$$I_{i,t}^{GW,Min} \le I_{i,t}^{GW} \le I_{i,t}^{GW,Max} + \Delta Pro_i^{def}, \quad \forall i \in node^{g,def}, \forall t \in T \tag{35}$$

The overall mitigation model is a two-stage optimization model, as shown in (36) and (37). The mitigation action is determined at the first stage to minimize the no-attack loss, and the mitigation effectiveness is realized at the second stage. The following three factors are considered in the model to ensure a practical implementation of the proposed countermeasure.

- First, mitigations result in robust operations decreasing the impact of cyberattacks, but they inevitably deviate normal MES operations from the optimal dispatch. This means that when there is no attack, mitigations induce loss to normal MES operations. In an ideal situation, mitigation strategies are only applied when an attack happens, which means the “no-attack loss” is 0. However, defenders/operators generally cannot accurately foresee when an attack will happen. Experienced operators are more likely to estimate the possibility of being attacked instead of sensing the exact time of attack directly. Therefore, the proposed countermeasure is modeled to maximize the mitigation ability (36) and minimize the no-attack loss (37). A list of mitigation actions is provided to operators to choose based on their preference.
- Second, the defender hardly knows the capability of the attackers until the operation has already been damaged, and attackers hardly know the mitigation actions before they launch attacks. Defenders anticipate potential OC-FDIAs under different attack abilities (e.g., variable q), without knowing the exact value. Attackers anticipate the MES operation without knowing the mitigation action. Therefore, the mitigation strategy is a two-stage model instead of a Stackelberg model. The first stage determines the mitigation action (36). The second stage (37) realizes the effectiveness of the mitigation action against the OC-FDIA.
- Third, mitigation is achieved by perturbing the boundary of defending units to disturb the solution of the OC-FDIA. The perturbation of defending units is always negative to ensure feasibility, and defending units are selected from base units, which are generally dispatched at maximum. Operators should select defending units as little as possible to decrease the no-attack loss.

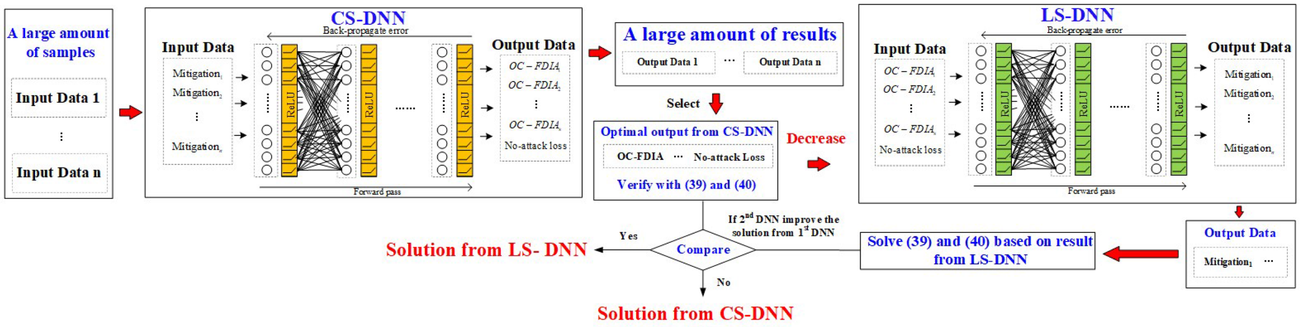


Fig. 4. Overall process of the applied DNNs.

***First stage**: determination of mitigations*

$$\Delta P_i^{def}, \Delta Pro_i^{def} \underset{\text{Decrease}}{\overset{\min}{\Rightarrow}} \underbrace{\begin{bmatrix} \text{MES operation model(19)} \\ (3)-(5),(7)-(10),(12)-(18),(34),(35) \end{bmatrix}}_{\textbf{No}-\textbf{attack Loss}}$$

$$\textit{Subject to}$$

$$\text{Perturbation constraint}\,(32)\,,(33) \tag{36}$$

***Second stage:** realization of mitigation abilities*

$$\Delta P_i^{def}, \Delta Pro_i^{def} \underset{\text{Mitigate}}{\overset{\min}{\Rightarrow}} \underbrace{\text{E}\begin{bmatrix} \text{OC}-FDIA\text{model}(31) \\ (34),(35) \underset{\text{replace}}{\Rightarrow} (6),(11) \end{bmatrix}}_{\textbf{Mitigation Effectiveness}} \tag{37}$$

B. Solution Methodology

The proposed countermeasure (36) and (37) is a two-stage model with a bilevel optimization integrated at the second stage requiring expensive computations. We apply the deep learning (DL) technique to facilitate the optimization process because the bilevel models at the second stage impede model-based algorithms from returning a timely solution. General descriptions of the deep neural network (DNN) model, including the active function and affine transformation function can be found in [40].

Two DNNs are trained and applied to quickly approximate the optimal solution of (36) and (37). The overall process is shown in Fig. 4. First, a comprehensive search DNN (CS-DNN), is trained to replace the mapping from the first-stage mitigation action to the second-stage mitigation effectiveness. The training data consists of a group of mitigation samples generated uniformly according to constraints (32) and (33), a group of mitigation effectiveness under different attackers, and a group of no-attack loss by solving (36) and (37) based on generated mitigation samples. The DNN mapping is almost instantaneous. Therefore, the well-trained CS-DNN is used to give a comprehensive search over a large number of randomly generated mitigation samples. Among a large amount of output, the optimal solution can be identified as the best value of the sum of (36) and (37). Further, a list of suboptimal solutions is also available as the minimal no-attack loss (36) and maximum mitigation effectiveness (37).

Second, a local search DNN (LS-DNN) reverses the input-output relationship of the CS-DNN, which means that the LS-DNN is trained with the value of mitigation effectiveness and no-attack loss as input and with mitigation actions as output. As such, the well-trained LS-DNN will output mitigation actions that correspond to the given mitigation effectiveness and no-attack loss. It is worth noting that the input data for the well-trained LS-DNN needs to be close to the training set to ensure mapping accuracy. Therefore, for each optimal solution from the CS-DNN, a small perturbation is applied to increase the value of mitigation effectiveness and decrease no-attack loss value. The increased mitigation effectiveness and decreased no-attack loss are applied as input to the LS-DNN, which returns a corresponding new mitigation action. If the mitigation action returned from the LS-DNN provides a better no-attack loss and mitigation, then the solution from the LS-DNN is used. Otherwise, the solution from the CS-DNN is used.

In summary, the CS-DNN provides a comprehensive random search over the solution space since the DNN mapping is extremely fast and the number of defending units is small. The LS-DNN aims to progress around the solution returned from the CS-DNN. Through the two DNN approximations, operators are provided with a speedy tool to determine mitigation actions. The mitigation effectiveness is shown in section V.B, and the training of the DNNs are described in the Appendix.

V. Case Study

In this section, numerical studies are performed to demonstrate the proposed OC-FDIA and its countermeasure. The simulation is performed on a widely used MES case consisting of an IEEE 39-bus New England test system [30] and a 14-bus gas system [38]. The simulation is also performed on an integrated IEEE 118-bus test system [41] with two 14-bus gas systems [38] for demonstrations on large test systems. Detailed parameters can be found in [30], [38], and [41]. Simulation runs were performed in MATLAB 2017 on a laptop with an Intel i7-8650U processor and 16 GB RAM.

A. Analyses of OC-FDIA in MES Operations

1) Significant Loss Caused By the Proposed OC-FDIA: In this study, the damage caused by the OC-FDIA is compared with conventional single-system FDIAs and uncoordinated FDIA

TABLE I
LOSS CAUSED BY OC-FDIAS, SINGLE-SYSTEM FDIAS, AND UNCOORDINATED FDIAS

	OC-FDIA	FDIA on Power	FDIA on Gas	Uncoordinated FDIA
5%	$3,911.2	$2,700.0	$1,106.6	$3,806.6
10%	$9,615.9	$7,331.2	$2,208.4	$8,323.0
15%	$14,199.9	$10,040.5	$2,532.5	$12,839.4
20%	$22,054.2	$12,394.0	$4,848.9	$17,356.8
25%	$37,200.4	$17,793.9	7,539.8	$25,921.0

strategies. The attacker is assumed to be able to launch attacks on all of the electricity and gas buses under the attack budget constraint. The single-system FDIA is considered an optimal FDIA in the power system alone and an optimal FDIA in the gas system alone with the same attack penetration level as the OC-FDIA. Although single-system FDIAs inject false data into one energy system, they generally cause propagation/ripple effects, which means that the other system is impacted through energy coupling in the MES. The uncoordinated FDIA strategies are considered to be the combination of single-system FDIAs. The penetration abilities of the LR attack, GL-FDIA, and GD-FDIA gradually increase with a maximum value of 26%. The operation cost loss caused by the OC-FDIA, single-system FDIA, and uncoordinated FDIAs are compared in Table I.

Overall, the OC-FDIA is expected to cause 83.1%, 374.7%, and 33.1% more loss than the two single-system FDIAs and uncoordinated FDIA. The OC-FDIA leads to more severe damage than other FDIAs in Table I. It is worth noting the difference between the loss caused by the OC-FDIA and other attacks sharply increases with the attack ability. When the attack ability is low, the difference between the loss caused by the OC-FDIA and other attacks is less significant. For example, when the attack ability is 5%, the loss caused by OC-FDIA is only 2.7% more than the loss caused by the uncoordinated FDIA, but the loss difference increases to 43.5% when the attack ability is increased to 25%. In short, the OC-FDIA can cause much more severe damages than conventional FDIAs, and the impact of the OC-FDIA sharply increases when the attacker is more competent because higher attack abilities offer more room for FDIAs in different energy systems to coordinate.

Further, the loss caused by uncoordinated FDIAs is generally not equal to the sum of the loss caused by two single-system FDIAs, although the considered uncoordinated FDIA is a combination of the two single-system FDIAs. When the attack ability is as low as 5%, loss caused by uncoordinated FDIA equals the sum of the loss caused by two single-system FDIAs (i.e., the value of column 5 equals the sum of the value of column 3 and column 4). The reason is that the FDIAs may not lead to propagation/ripple effects when attack ability is low, which means that the FDIA on one system does not impact the operation of another system.

When the attack ability is higher, the propagation/ripple effects emerge. The loss caused by an uncoordinated FDIA could be less than the sum of the loss caused by two single-system FDIAs (i.e., the value of column 5 is less than the sum of the values of column 3 and column 4), such as the third row in Table I. The reason is that the propagation/ripple effects could cancel the impact of each other without coordination between FDIAs. However, the OC-FDIA coordinates FDIAs by utilizing the propagation/ripple effects to maximize the damage to MES operations. The above observations show that the propagation/ripple effects are vital for the proposed OC-FDIA to cause more damage than other FDIAs.

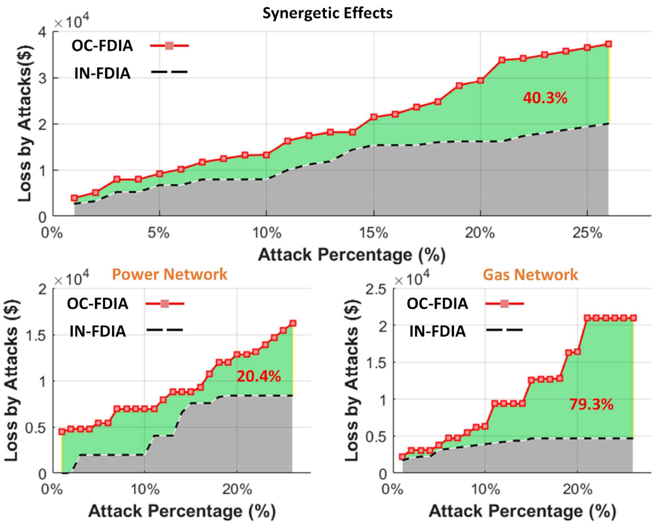


Fig. 5. Synergetic effect of the proposed OC-FDIA.

2) Propagation Effect of the Proposed OC-FDIA: The propagation/ripple effects from the OC-FDIA are analyzed next. The OC-FDIA consists of two FDIAs targeting power and gas networks, which are defined as IN-FDIA representing the FDIA in power and gas network, respectively. The two IN-FDIAs are different from previous single-system FDIAs, and they are the FDIAs that the OC-FDIA injects into different energy systems. Fig. 5 compares the propagation/ripple effects of the proposed OC-FDIA, where the two IN-FDIAs are injected together, with the propagation/ripple effects when the two IN-FDIAs are injected separately. Although the false data value of the OC-FDIA is the same as the two IN-FDIAs, the coordination by the OC-FDIA causes more damage.

The green area in the upper subplot of Fig. 5 represents the extra loss caused by the OC-FDIA over the loss of the sum of two IN-FDIAs. The extra loss increases with the increasing attack ability percentage. The green area represents the extra 40.3% loss by the OC-FDIA.

Next, we examine the propagation effect from power system to gas system and from gas system to power system individually.

B. Countermeasure to the Proposed OC-FDIA

1) Effectiveness of the Mitigation Against OC-FDIA: Two low-cost units are selected as defending units for perturbations: a power unit at electricity node 31 and a gas well at gas node 4. Based on operators' experience, the attack with penetration ability from 2% to 26% occurs with the same probability, and they can launch attacks at electricity nodes 7, 23, and 29 and gas

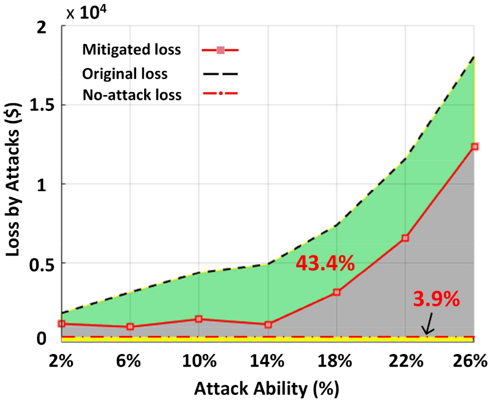


Fig. 6. Mitigation effectiveness and no-attack loss.

TABLE II
MITIGATION ACTION LIST

	1	2	3	4
No-attack Loss (Yellow Area in Fig. 6)	1.3%	3.9%	8.6%	12.3%
Mitigation Effectiveness (Green Area in Fig. 6)	37.1%	43.4%	46.8%	48.6%
Defensing unit 1	1.2%	7.6%	9.3%	13.3%
Defensing unit 2	3.4%	5.6%	6.7%	8.9%

nodes 11 and 14. The applied DNNs find the optimal mitigation to perturb the boundary of the two defending units by 7.6% and 5.5%, respectively. The training and accuracy for the applied DNNs can be found in the Appendix section. The result of mitigation effectiveness and no-attack loss are shown in Fig. 6.

Under the mitigation action, the effectiveness of the OC-FDIA is decreased by 43.4%, as shown in the green area, which largely discourages attackers from launching such attacks. The loss under mitigation is similar when penetration is less than 14%, which means that mitigation can always achieve a desirable value, but when penetration is higher than 14%, the mitigated loss increases along with the loss of the OC-FDIA. It is worth noting that mitigation actions induce loss to normal operations when there is no attack, as shown in the yellow area of Fig. 6, but the no-attack loss is considerably smaller: only 3.9% of normal operations. Therefore, mitigation provides an operation solution to largely mitigate the OC-FDIA attack without sacrificing large losses on normal operations.

Further, operators may have different preferences on the bearable no-attack loss and the desired mitigation. A list of mitigation actions can be generated by applying the DNNs rapidly. Four different mitigations are provided in Table II. Mitigation 2 In Table II is showcased in Fig. 6 while the other three mitigations are not graphed due to space limit. If the operator can bear a higher no-attack loss, mitigation effectiveness can be higher. However, mitigation effectiveness may increase in a much slower pace than attack effectiveness. For example, when the no-attack loss increases almost ten times (i.e., from 1.3% to 12.3%), mitigation effectiveness only increases 30% (i.e., from 37.1% to 48.6%). Operators can apply different mitigation actions from the list based on their preferences.

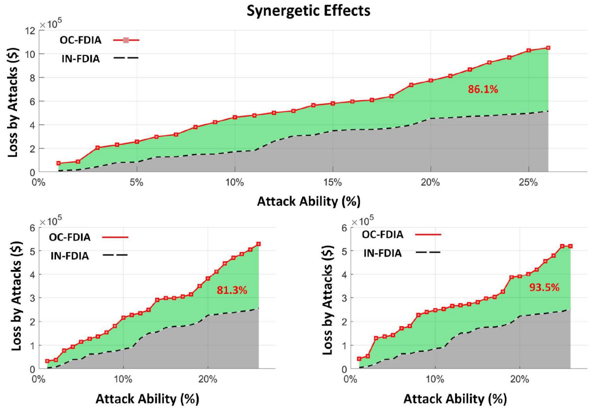


Fig. 7. Synergetic effect of the proposed OC-FDIA of large test systems.

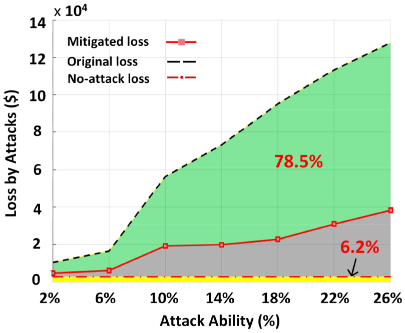


Fig. 8. Mitigation effectiveness and no-attack loss of large test systems.

C. Demonstration on Large Test Systems

Similar to the above 39-bus New England test case, the OC-FDIA targeting this large test system contains two coordinated FDIAs targeting power and gas networks, respectively.

The results of the OC-FDIA are shown in Fig. 7. With an increase in attack ability, the loss incurred by attacks increases correspondingly. A 24% increase in attack ability led to an extra 1335.6% loss. It can be seen from the green area that the OC-FDIA causes much higher losses to the system due to the synergetic effect, which can lead to up to 86.1% extra losses. Further, the synergetic effect increases with attack ability. The reason is that a higher attack ability gives attackers more flexibility to coordinate, and when the attack ability is low, there is less room for coordination. Compared with the previous small test case, the magnitude of losses caused by the OC-FDIA has largely increased, as well as the synergetic effect. The lower two plots in Fig. 7 compare the impact of OC-FDIA with the impact of two IN-FDIAs on electric and gas system, respectively. It is observed that the operators may significantly underestimate the potential impact of cyberattacks without analyzing the potential coordination and synergetic effect between different FDIAs.

The mitigation effectiveness is shown in Fig. 8. The defending scheme finds that the optimal mitigation decision is to perturb the boundary of the three defending units by 8.2%, 3.5%, and 10.3%, respectively. The effectiveness of the OC-FDIA decreases by 78.5%, as shown in the green area, which will essentially discourage attackers from launching such attacks. The no-attack loss amount is 6.2%, as shown in the yellow area. The mitigation effectiveness for this large system is stronger than the small system, although the no-attack loss increased from 3.9% to 6.2%. If the decision-maker considers the no-attack loss too high, the no-attack loss can be tuned down by reducing the upper limit in (32)-(35) at the cost of reducing mitigation effectiveness.

It is worth noting that this large case study does not draw different or new conclusions but only with an increase in the magnitude of loss caused by cyberattacks to show the severity of OC-FDIA and the effectiveness of the mitigation scheme.

VI. Conclusion

In conclusion, this article is the first work to provide a detailed investigation and countermeasure on the potential damage caused by coordinated cyberattacks targeting MES operations. An OC-FDIA model is proposed, where FDIAs on different energy systems are coordinated to cause greater damage. Then, a countermeasure to the proposed OC-FDIA is developed to mitigate the damage based on DNNs. A list of mitigation actions has been provided for operators, which compromises between mitigation effectiveness and no-attack loss. The severity of the proposed OC-FDIA and the effectiveness of the developed countermeasure are demonstrated and discussed analytically and numerically.

Future works may focus on analyzing the sensitivity of the proposed OC-FDIA in MES operations.

VII. Disclaimer

This article was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Appendix

The training and accuracy of applied DNNs are shown in this Appendix. Two thousand mitigation samples were generated uniformly between zero and the upper limit in (32) and (33). The feasibility region for both defending units is sliced into 10 pieces, which gives 100 combinations. For each combination, 20 samples are generated, which results in 2000 mitigation samples. Models (36) and (37) are solved for each mitigation sample to obtain the corresponding value of mitigation effectiveness and no-attack loss, which forms the training dataset. The training accuracy and MES loss of the two DNNs are shown in Fig. 9. The accuracy rates of CS-DNN and LS-DNN in the test dataset (i.e., 500 test samples) are 99.4% and 98.6%, respectively.

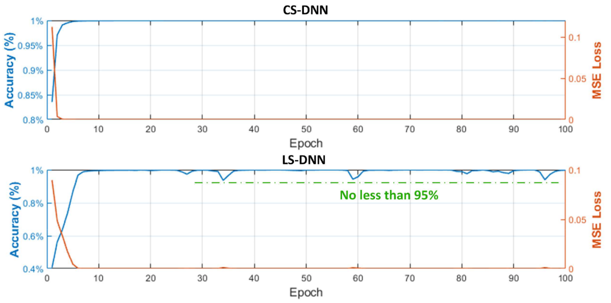


Fig. 9. Accuracies of the CS-DNN and LS-DNN.

References

[1] U.S. White House National Climate Task Force, Jan. 2021. [Online]. Available: https://www.whitehouse.gov/climate/

[2] E.U. European Climate Law, Jul. 2021. [Online]. Available: https://ec.europa.eu/clima/eu-action/European-green-deal/European-climate-law_en

[3] C. Wu, X.-P. Zhang, and M. J. H. Sterling, "Economic analysis of power grid interconnections among Europe, North-East Asia, and North America with 100% renewable energy generation," *IEEE Open Access J. Power Energy*, vol. 8, pp. 268–280, 2021.

[4] W. Huang, N. Zhang, Y. Cheng, J. Yang, Y. Wang, and C. Kang, "Multi-energy networks analytics: Standardized modeling, optimization, and low carbon analysis," *Proc. IEEE*, vol. 108, no. 9, pp. 1411–1436, Sep. 2020.

[5] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[6] J. Voas, N. Kshetri, and J. F. DeFranco, "Scarcity and global insecurity: The semiconductor shortage," *IT Professional*, vol. 23, no. 5, pp. 78–82, Sep./Oct. 2021.

[7] P. Mancarella, "MES (multi-energy systems): An overview of concepts and evaluation models," *Energy*, vol. 65, pp. 1–17, 2014.

[8] M. J. O'Malley et al., "Multicarrier energy systems: Shaping our energy future," *Proc. IEEE*, vol. 108, no. 9, pp. 1437–1456, Sep. 2020.

[9] E. A. Martínez Ceseña, E. Loukarakis, N. Good, and P. Mancarella, "Integrated electricity– heat–gas systems: Techno–economic modeling, optimization, and application to multienergy districts," *Proc. IEEE*, vol. 108, no. 9, pp. 1392–1410, Sep. 2020.

[10] R. Bayani and S. D. Manshadi, "Natural gas short-term operation problem with dynamics: A rank minimization approach," *IEEE Trans. Smart Grid*, vol. 13, no. 4, pp. 2761–2773, Jul. 2022.

[11] J. Fang, Q. Zeng, X. Ai, Z. Chen, and J. Wen, "Dynamic optimal energy flow in the integrated natural gas and electrical power systems," *IEEE Trans. Sustain. Energy*, vol. 9, no. 1, pp. 188–198, Jan. 2018.

[12] W. Liu, P. Li, W. Yang, and C. Y. Chung, "Optimal energy flow for integrated energy systems considering gas transients," *IEEE Trans. Power Syst.*, vol. 34, no. 6, pp. 5076–5079, Nov. 2019.

[13] S. Yao et al., "Dynamic optimal energy flow in the heat and electricity integrated energy system," *IEEE Trans. Sustain. Energy*, vol. 12, no. 1, pp. 179–190, Jan. 2021.

[14] X. Zhang, G. Strbac, N. Shah, F. Teng, and D. Pudjianto, "Whole-system assessment of the benefits of Integrated electricity and heat system," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 1132–1145, Jan. 2019.

[15] A. Shabanpour-Haghighi and A. R. Seifi, "Energy flow optimization in multicarrier systems," *IEEE Trans. Ind. Inform.*, vol. 11, no. 5, pp. 1067–1077, Oct. 2015.

[16] D. Xu, Q. Wu, B. Zhou, C. Li, L. Bai, and S. Huang, "Distributed multi-energy operation of coupled electricity, heating, and natural gas networks," *IEEE Trans. Sustain. Energy*, vol. 11, no. 4, pp. 2457–2469, Oct. 2020.

[17] S. Chen, A. J. Conejo, R. Sioshansi, and Z. Wei, "Equilibria in electricity and natural gas markets with strategic offers and bids," *IEEE Trans. Power Syst.*, vol. 35, no. 3, pp. 1956–1966, May 2020.

[18] C. Wang, W. Wei, J. Wang, F. Liu, and S. Mei, "Strategic offering and equilibrium in coupled gas and electricity markets," *IEEE Trans. Power Syst.*, vol. 33, no. 1, pp. 290–306, Jan. 2018.

[19] Y. Cao, W. Wei, L. Wu, S. Mei, M. Shahidehpour, and Z. Li, "Decentralized operation of interdependent power distribution network and district heating network: A market-driven approach," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5374–5385, Sep. 2019.

[20] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 659–666, Dec. 2011.

[21] H. Ye, Y. Ge, X. Liu, and Z. Li, "Transmission line rating attack in two-settlement electricity markets," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1346–1355, May 2016.

[22] 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.

[23] Y. Xiang, Z. Ding, Y. Zhang, and L. Wang, "Power system reliability evaluation considering load redistribution attacks," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 889–901, Mar. 2017.

[24] R. Kaviani and K. W. Hedman, "A detection mechanism against load-redistribution attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 704–714, Jan. 2021.

[25] Q. Zhang, F. Li, H. Cui, R. Bo, and L. Ren, "Market-level defense against FDIA and a new LMP-disguising attack strategy in real-time market operations," *IEEE Trans. Power Syst.*, vol. 36, no. 2, pp. 1419–1431, Mar. 2021.

[26] Q. Zhang and F. Li, "Cyber-vulnerability analysis for real-time power market operation," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3527–3537, Jul. 2021.

[27] Z. Wang and R. S. Blum, "Elimination of undetectable attacks on natural gas networks," *IEEE Signal Process. Lett.*, vol. 28, pp. 1002–1005, 2021.

[28] G. Li et al., "Detecting cyberattacks in industrial control systems using online learning algorithms," *Neurocomputing*, vol. 364, pp. 338–348, 2019.

[29] P. Zhao, C. Gu, and D. Huo, "Coordinated risk mitigation strategy for integrated energy systems under cyber-attacks," *IEEE Trans. Power Syst.*, vol. 35, no. 5, pp. 4014–4025, Sep. 2020.

[30] B. Huang, Y. Li, F. Zhan, Q. Sun, and H. Zhang, "A distributed robust economic dispatch strategy for integrated energy system considering cyber-attacks," *IEEE Trans. Ind. Inform.*, vol. 18, no. 2, pp. 880–890, Feb. 2022.

[31] S. Ding, W. Gu, S. Lu, R. Yu, and L. Sheng, "Cyber-attack against heating system in integrated energy systems: Model and propagation mechanism," *Appl. Energy*, vol. 311, Apr. 2022, Art. no. 118650.

[32] B. Zhao et al., "A coordinated scheme of electricity-gas systems and impacts of a gas system FDI attacks on electricity system," *Int. J. Electr. Power Energy Syst.*, vol. 131, Oct. 2021, Art. no. 107060.

[33] A. M. Sawas, H. Khani, and H. E. Z. Farag, "On the resiliency of power and gas integration resources against cyber attacks," *IEEE Trans. Ind. Inform.*, vol. 17, no. 5, pp. 3099–3110, May 2021.

[34] C. Wang et al., "Robust defense strategy for gas–electric systems against malicious attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 2953–2965, Jul. 2017.

[35] M. Zadsar, A. Abazari, A. Ameli, J. Yan, and M. Ghafouri, "Prevention and detection of coordinated false data injection attacks on integrated power and gas systems," *IEEE Trans. Power Syst.*, early access, Oct. 20, 2022, doi: 10.1109/TPWRS.2022.3216118.

[36] P. Zhao et al., "Coordinated cyber security enhancement for grid-transportation systems with social engagement," *IEEE Trans. Emerg. Topics Comput. Intell.*, early access, Oct. 13, 2022, doi: 10.1109/TETCI.2022.3209306.

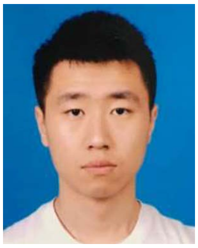
[37] Q. Zhang, F. Li, W. Feng, X. Wang, L. Bai, and R. Bo, "Building marginal pattern library with unbiased training dataset for enhancing model-free load-ED mapping," *IEEE Open Access J. Power Energy*, vol. 9, pp. 88–98, 2022.

[38] L. Bai et al., "Interval optimization based operating strategy for gas-electricity integrated energy systems considering demand response and wind uncertainty," *Appl. Energy*, vol. 167, pp. 270–279, Apr. 2016.

[39] H. Shuai, X. M. Ai, J. K. Fang, T. Ding, Z. Chen, and J. Y. Wen, "Real-time optimization of the integrated gas and power systems using hybrid approximate dynamic programming," *Int. J. Elect. Power Energy Syst.*, vol. 118, 2020, Art. no. 105776.

[40] J. Zhao, F. Li, X. Chen, and Q. Wu, "Deep learning based model-free robust load restoration to enhance bulk system resilience with wind power penetration," *IEEE Trans. Power Syst.*, vol. 37, no. 3, pp. 1969–1978, May 2022.

[41] Q. Zhang, F. Li, L. Bai, H. Wang, J. Zhao, and H. Shuai, "Coupling analysis for multienergy systems by self and cross critical load level," *IEEE Open Access J. Power Energy*, early access, Mar. 06, 2023, doi: 10.1109/OAJPE.2023.3253783.



Qiwei Zhang (Member, IEEE) received the M.S. and Ph.D. degrees in electrical engineering from the University of Tennessee, Knoxville, TN, USA, in 2018 and 2022, respectively. He is currently a Postdoctoral Researcher with the Department of Environmental Health and Eng., Johns Hopkins University, Baltimore, MD, USA. He was a Research Scientist with the University of Tennessee. His research interests include renewable integration risk assessment, power system cybersecurity, and electricity market.

Fangxing Li (Fellow, IEEE) is also known as Fran Li. He received the B.S.E.E. and M.S.E.E. degrees from Southeast University, Nanjing, China, in 1994 and 1997, respectively, and the Ph.D. degree from Virginia Tech, Blacksburg, VA, USA, in 2001. He is currently the James W. McConnell Professor of electrical engineering and the Campus Director of CURENT with the University of Tennessee, Knoxville, TN, USA. His research interests include resilience, artificial intelligence in power, demand response, distributed generation and microgrid, and electricity markets. From 2020 to 2021, he was the Chair of IEEE PES Power System Operation, Planning and Economics (PSOPE) Committee. He has been the Chair of *IEEE WG on Machine Learning for Power Systems* since 2019 and the Editor-In-Chief of IEEE Open Access Journal of Power and Energy *(OAJPE)* since 2020. Dr. Li was the recipient of numerous awards and honors, including *R&D 100* Award in 2020, IEEE PES Technical Committee Prize Paper award in 2019, five best or prize paper awards at international journals, and six best papers/posters at international conferences.

Jin Zhao (Member, IEEE) received the Ph.D. degrees in electrical engineering from Shandong University, Jinan, China, in 2020. She is currently an Alexander von Humboldt Researcher hosted by TU Dortmund University, Dortmund, Germany. She was a Research Scientist with The University of Tennessee, Knoxville, TN, USA. Her research interests include power system resilience, transmission & distribution system restoration, renewable energy integration, resilient microgrid, and machine-learning. She is the Chair of IEEE PES task force on Advanced Intelligence Techniques for Resilient Power System Restoration. She was an outstanding Reviewer of IEEE Transactions on Power Systems and IEEE OAJPE. She is an Associate Editor for the *Protection and Control of Modern Power*.

Buxin She (Graduate Student Member, IEEE) received the B.S.E.E. and M.S.E.E. degrees from Tianjin University, Tianjin, China, in 2017 and 2019, respectively. He is currently working toward the Ph.D. degree with the Department of Electrical Engineering and Computer Science, The University of Tennessee, Knoxville, TN, USA. His research interests include microgrid operation and control, machine learning in power systems, distribution system operation and plan, and power grid resilience.