This is a repository copy of *High risk regional load attacks in smart grids*.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/226634/

Version: Accepted Version

Article:

Du, M. orcid.org/0009-0009-9806-841X, Zhang, X. orcid.org/0000-0002-6063-959X and Zhao, J. orcid.org/0000-0002-8498-9666 (2025) High risk regional load attacks in smart grids. IEEE Internet of Things Journal. ISSN 2327-4662

https://doi.org/10.1109/jiot.2025.3564490

© 2025 The Authors. Except as otherwise noted, this author-accepted version of a journal article published in IEEE Internet of Things Journal is made available via the University of Sheffield Research Publications and Copyright Policy under the terms of the Creative Commons Attribution 4.0 International License (CC-BY 4.0), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/

Reuse

This article is distributed under the terms of the Creative Commons Attribution (CC BY) licence. This licence allows you to distribute, remix, tweak, and build upon the work, even commercially, as long as you credit the authors for the original work. More information and the full terms of the licence here: https://creativecommons.org/licenses/

Takedown

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk/

High Risk Regional Load Attacks in Smart Grid

Min Du, *Member, IEEE*, Xin Zhang, *Senior Member, IEEE*, Junbo Zhao, *Senior Member, IEEE*

Abstract—**This letter develops a high-risk regional load attack mechanism in a smart grid with incomplete network information. Different from previous research, the proposed attack mechanism enables an attacker to launch a regional load attack with network information limited to an attack region, while minimising the deviation in corrupted data to enhance the stealth of this attack. The attack corrupts only a limited number of loads while still overloading multiple lines within the targeted attack region, thereby causing significant impacts on smart grid operation. Case studies conducted on two modified IEEE test systems validate the effectiveness of the proposed attack mechanism and pave the foundation for the future development of practical defensive strategies.**

Index Terms—**Smart grid, deviation of corrupted data, line overloads, regional load attacks, high risk.**

I. Introduction

NOWADAYS, the smart grid is increasingly vulnerable to cyberattacks due to the widespread use of advanced devices and technologies. Cyberattacks can cause serious disruptions to the smart grid, such as the Ukrainian grid blackout, which directly affected over 220,000 customers for several hours [1]. Therefore, it is urgent to study the mechanisms and impacts of cyberattacks, as this research can provide essential insights into designing more practical defensive strategies.

As a special type of cyberattack, false data injection (FDI) attacks, such as load redistribution (LR) attacks, can inject false load data to have impacts on the smart grid [2]. More specifically, an attacker can inject false load data to manipulate the readings of load meters in the power grid, resulting in load shedding, line overloads, or even cascading failures of the power grid [3]. In [4], the authors further proved that a skilled adversary could construct a load attack vector, resulting in the power grid to the state of uneconomic operation. However, a smart attacker would prefer to overload lines rather than cause uneconomic operation of a smart grid, since overloading lines can impose more significant potential impacts on the grid. In this context, *Tan* et al. in [5] revealed that a skilled attacker can inject false load data to induce multiple line overloads while invading the minimum number of loads. However, the stealth of cyberattacks also needs to be considered. This is because traditional false load data generally deviate significantly from normal data and are easily identified as outliers by state-of-the-art detection methods.

In practice, an intelligent attacker prefers to design high-stealth false data to compromise the power grid, ensuring that the corrupted data can effectively escape detection by various anomaly detection methods. To achieve this goal, the authors in [6] ensured that the corrupted data were close to all normal data to enhance the stealth of false data, where the corrupted data was hidden among normal measurements to avoid being detected as outliers, but the computational efficiency was compromised. The authors in [7] proposed a bilevel cyberattack model based on pre- and post-dispatch to improve the stealth of false data. That is, the attack could bring the system to an uneconomic and insecure operation state after the dispatch process. Nevertheless, these works have an impractical assumption that an attacker could achieve complete network information of a smart grid. In practice, such network information is usually kept confidential within control centers, making it almost impossible for any attacker to obtain completely. Subsequently, the authors in [8] successfully designed a local LR attack with limited grid information, while ignoring its high-impact on overloading multiple lines in the power grid. The stealth of such an attack was often ignored, making the corrupted data easily identifiable as an outlier.

To address the above-mentioned issues, this letter proposes a high-risk regional load attack mechanism, in which an attacker can overload multiple lines by corrupting regional load data using only the network information of an attack region in a smart grid, while corrupting fewer loads to achieve significant attack impacts. As an additional high-risk feature, the deviation of the corrupted data is minimised to hide such false data among normal ones, thereby enhancing the stealth of the regional load attack. In addition, the total number of overloaded lines can be dynamically adjusted to control the line overloads inflicted on the grid. The revealed high-risk regional load attack mechanism is crucial to evaluating the risks in the smart grid security operation, thereby motivating further research investigation into relevant defensive strategies.

II. High Risk Regional Load Attack

A. FDI Attacks Induced Line Overload Mechanism

DC power flow model is well-suited for analysing line overloads in real-time smart grid scenarios, which can provide sufficient accuracy in steady-state analysis and avoid the infeasibility in the AC flow solution methods [9]. Based on DC state estimation, the relationship between state variable $\boldsymbol{x}$ and measurement $\boldsymbol{Z}$ can be formulated as $\boldsymbol{Z} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{e}$. Here, $\boldsymbol{H}$ indicates the Jacobian matrix, and $\boldsymbol{e}$ is the error measurement. When $\Delta\boldsymbol{Z} = \boldsymbol{H}\Delta\boldsymbol{x}$, an undetectable attack is launched. As a practical application of the FDI attack, load measurement can be corrupted by attackers in LR attacks, and the mechanism of LR attacks can be detailed as:

$$\mathbf{1}^{\mathrm{T}}\Delta\boldsymbol{D} = 0 \tag{1}$$

$$-\alpha\boldsymbol{D} \le \Delta\boldsymbol{D} \le \alpha\boldsymbol{D} \qquad 0<\alpha<1 \tag{2}$$

where constraint (1) enforces the load attack vector to sum to zero. Constraint (2) indicates the upper and lower limits of the load attack vector. Note here that the injected load vector $\Delta\boldsymbol{D}$ can mislead the incorrect dispatch decision of the system operator in a way that can induce line overloads. The injected load data which can induce overloads is detailed as follows.

We define the corrupted load data as $\boldsymbol{D}'$, i.e., $\boldsymbol{D}' = \boldsymbol{D} + \Delta\boldsymbol{D}$, where $\boldsymbol{D}$ indicates the normal load measurement. When normal load measurements are corrupted by an attacker injecting false load data $\Delta\boldsymbol{D}$, the power flow will be impacted which can be described as:

This work was supported by the U.K. Research and Innovation Future Leaders Fellowship "Digitalisation of Electrical Power and Energy Systems Operation" under Grant MR/W011360/2. (*Corresponding author: Xin Zhang.*)

M. Du and X. Zhang are with the School of Electrical and Electronic Engineering, University of Sheffield, Sheffield, S10 2TN United Kingdom (e-mail: m.du@sheffield.ac.uk; xin.zhang1@sheffield.ac.uk).

J. Zhao is with the Department of Electrical and Computer Engineering, University of Connecticut, Storrs, CT 06269 USA (email: junbo@uconn.edu).

$$\boldsymbol{F}' = \mathbf{SF} \cdot (\mathbf{KP} \cdot \boldsymbol{P} - \mathbf{KD} \cdot \boldsymbol{D}') \tag{3}$$

$$-\boldsymbol{F}^{\max} \leq \boldsymbol{F}' \leq \boldsymbol{F}^{\max} \tag{4}$$

where $\mathbf{SF}$ is the shift factor matrix. $\mathbf{KP}$ and $\mathbf{KD}$ represent bus-unit, bus-load incidence matrices, respectively. $\boldsymbol{F}'$ indicates the corrupted power flow, and $\boldsymbol{F}^{\max}$ denotes the power flow limit. $\boldsymbol{P}$ is the generation of units. Considering $\boldsymbol{D}' = \boldsymbol{D} + \Delta\boldsymbol{D}$, the true power flow can be further derived as follows:

$$\boldsymbol{F} = \mathbf{SF} \cdot (\mathbf{KP} \cdot \boldsymbol{P} - \mathbf{KD} \cdot (\boldsymbol{D}' - \Delta\boldsymbol{D})) \tag{5}$$

Then, based on constraints (3)-(5), we can derive:

$$\boldsymbol{F} = \boldsymbol{F}' + \mathbf{SF} \cdot \mathbf{KD} \cdot \Delta\boldsymbol{D} \tag{6}$$

$$-\boldsymbol{F}^{\max} + \mathbf{SF} \cdot \mathbf{KD} \cdot \Delta\boldsymbol{D} \leq \boldsymbol{F} \leq \boldsymbol{F}^{\max} + \mathbf{SF} \cdot \mathbf{KD} \cdot \Delta\boldsymbol{D} \tag{7}$$

It can be observed from constraint (7) that the designed load attack vector can induce line overloads with magnitudes of up to $|\mathbf{SF} \cdot \mathbf{KD} \cdot \Delta\boldsymbol{D}|$, which means the power flow deviation. An attacker can design false load data to induce line overloads using complete network information of a smart grid, acquiring such complete information is typically challenges in practice.

B. High-risk Regional Load Attack Model

Thus, the main challenge addressed in this letter is how to design an effective attack mechanism that achieves high-risk cyberattacks on a smart grid with only incomplete network information. In this context, we propose a high-risk regional load attack mechanism characterised by high-region concentration, high-stealth, and high-impact, as defined below:

1) ***Concept of high-regional concentration****: An attacker can design attacks to corrupt regional loads using only the network information of the attack region within a smart grid, eliminating the need for the complete network information of the entire smart grid.*

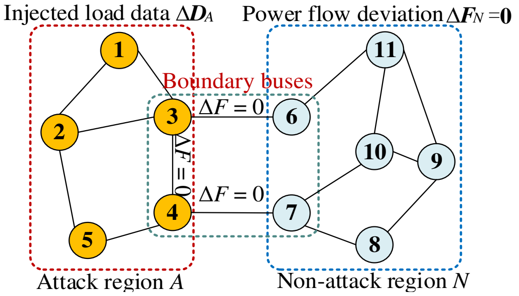

Fig. 1. Theoretical framework of regional load attacks.

As shown in Fig. 1, an entire grid is divided into two regions, namely attack region A and non-attack region N. For regional load attacks, the bus voltage angle variation is the same for all boundary buses in attack region A, ensuring that no additional power flow deviation out of attack region A. This requirement can be mathematically modeled as (8)-(12). Such a regional attack can reduce the required attack resources and network information needed by the attacker.

$$\mathbf{1}^{\mathrm{T}} \Delta\boldsymbol{D}_A = 0 \tag{8}$$

$$-\frac{\tau}{1-\tau}\boldsymbol{D}'_A \leq \Delta\boldsymbol{D}_A \leq \frac{\tau}{1+\tau}\boldsymbol{D}'_A \qquad 0 \leq \tau \leq 1 \tag{9}$$

$$\Delta\boldsymbol{F}_A = -\boldsymbol{X}_A^{-1}\mathbf{KL}_A^{\mathrm{T}}\Delta\boldsymbol{\theta}_A \tag{10}$$

$$\boldsymbol{B}_A \cdot \Delta\boldsymbol{\theta}_A = \mathbf{KD}_A \cdot \Delta\boldsymbol{D}_A \tag{11}$$

$$\Delta\theta_b = \beta \qquad \forall b \in \Omega_{BA} \tag{12}$$

where $\Delta\boldsymbol{D}_A$ and $\Delta\boldsymbol{F}_A$ indicate the injected false load data and flow data in attack region A, respectively. $\boldsymbol{D}'_A$ is the corrupted load data in attack region A. τ is the regional load attack magnitude (p.u.), and b is the bus index. $\boldsymbol{X}_A$ is the line reactance matrix in attack region A. $\Delta\boldsymbol{\theta}_A$ is the incremental bus voltage angle in attack region A. $\mathbf{KL}_A$ and $\mathbf{KD}_A$ are bus-load and bus-line incidence matrices in attack region A, respectively. $\boldsymbol{B}_A$ is the bus susceptance matrix in attack region A excluding tie lines. $\Delta\theta_b$ is the incremental bus voltage angle at bus b, and Ω_{BA} is the set of boundary buses in attack region A. β is a given value for incremental bus voltage angle. Constraints (8)-(10) represent a typical LR attack, and constraints (11)-(12) ensure that this attack only occurs in a local region of a grid. When the injected false data $[\Delta\boldsymbol{D}_A\ \Delta\boldsymbol{F}_A]^{\mathrm{T}}$ follows constraints (8)-(12), a regional load attack is successfully launched by the attacker, causing a high-regional concentration of corrupted load data that confines the power flow deviation within the attack region.

2) ***Concept of high-stealth****: Corrupted data is hidden among normal data to enhance stealth, and the spatial distribution of corrupted data is close to that of normal data.*

To achieve the above goal, corrupted data (i.e., $\boldsymbol{Z}' = \boldsymbol{Z} + \Delta\boldsymbol{Z}$) should be moved from outside regions to areas adjacent to normal data. Thus, the deviation of corrupted data should be minimised to enhance stealth. The corrupted data should satisfy the following constraint (13) under ideal conditions to launch a concealed attack that minimises the spatial distance between corrupted data and normal data.

$$\mathbf{1}^{\mathrm{T}}\|\boldsymbol{Z}' - \boldsymbol{Z}_0\|_1 \to 0 \tag{13}$$

where $\Delta\boldsymbol{Z} = [\Delta\boldsymbol{D}_A\ \Delta\boldsymbol{F}_A]^{\mathrm{T}}$. $\boldsymbol{Z}_0$ represents the centroid of the normal data, and these normal data are generated using the Monte Carlo method based on the original normal data $\boldsymbol{Z}$. Additionally, we define an edge distance that represents the largest distance between each point in the normal data and the centroid of the normal data, formulated as follows:

$$\max_{1 \leq i \leq I}\|\boldsymbol{Z}' - \boldsymbol{Z}_0\|_1 \tag{14}$$

where I is the total number of generated normal data, and t is the index of normal data. To improve the stealth of corrupted data, the spatial distance between corrupted data points must be less than the edge distance $\max_{1 \leq i \leq I}\|\boldsymbol{Z}' - \boldsymbol{Z}_0\|_1$. When this spatial distance is less than the edge distance, the corrupted data can be considered hidden among normal data, making it difficult to detect. Thus, the problem of ensuring high-stealth for corrupted data can be summarised as follows:

$$\min\ \mathbf{1}^{\mathrm{T}}\boldsymbol{S} \tag{15}$$

$$\boldsymbol{S} \geq \boldsymbol{Z}' - \boldsymbol{Z}_0 \tag{16}$$

$$\boldsymbol{S} \geq -(\boldsymbol{Z}' - \boldsymbol{Z}_0) \tag{17}$$

$$\mathbf{1}^{\mathrm{T}}\boldsymbol{S} \leq \max_{1 \leq i \leq I}\|\boldsymbol{Z}' - \boldsymbol{Z}_0\|_1 \tag{18}$$

where (15)-(17) are employed to quantify $\|\boldsymbol{Z}' - \boldsymbol{Z}_0\|_1 \to 0$ in order to enhance the stealth of corrupted data (i.e., minimising the spatial distance of corrupted data), and constraint (18) ensures this spatial distance is less than or equal to the edge distance, so that the corrupted data is hidden among normal data. In addition, $\boldsymbol{S}$ is an auxiliary variable vector.

3) ***Concept of high-impact****: Let the power flow of targeted line l exceed its power flow limit by Γ times. Meanwhile, multiple line overloads in attack region A cause an increased operation cost.*

To overload targeted line l in attack region A, its power flow is required to be no less than $\Gamma F_{A,l}^{\max}$, thus the following constraints (19)-(23) should be satisfied:

$$\boldsymbol{P}' - \left(\boldsymbol{D}' - \Delta\widehat{\boldsymbol{D}}\right) = \boldsymbol{B\theta} \tag{19}$$

$$\boldsymbol{F} = \boldsymbol{X}^{-1}\mathbf{KL}^{\mathrm{T}}\boldsymbol{\theta} \tag{20}$$

$$\left|F_{A,l}\right| \geq \lambda_l \cdot \Gamma F_{A,l}^{\max} \qquad l \in \Omega_A \tag{21}$$

$$\textstyle\sum_{l \in A}\lambda_l = k \qquad \lambda_l \in \{0,1\} \tag{22}$$

$$-F_{N,l}^{\max} \leq F_{N,l} \leq F_{N,l}^{\max} \qquad l \in \Omega_N \tag{23}$$

where $\boldsymbol{\theta}$ and $\boldsymbol{F}$ are the bus voltage angle and the power flow in an entire grid, respectively. $F_{A,l}$ and $F_{A,l}^{\max}$represent the power flow and its limit of line l within attack region A, respectively. Ω_A and Ω_N indicate the set of lines in attack region A and non-attack region N, respectively. $F_{N,l}$ and $F_{N,l}^{\max}$ represent the power flow and its limit of line l within non-attack region N, respectively. $\boldsymbol{P}'$ is the generation of units under the normal scenario. $\Delta\widehat{\boldsymbol{D}}$ is the injected false load data, with only region A being attacked, i.e., $\Delta\widehat{\boldsymbol{D}} = [\Delta\boldsymbol{D}_A \ \boldsymbol{0}_N]^{\mathrm{T}}$. $\boldsymbol{D}'$ is the load data vector, with only the load data in region A being corrupted. Constraint (19) represents the power balance in attack region A. Constraint (20) calculates the power flow. Constraint (21) requires the power flow of targeted line l (i.e., targeted line l located in attack region A) to exceed its power flow limit by Γ times, which can be linearised by the method in ref. [5]. Constraint (22) indicates that the attacker selects k lines from attack region A to overload by launching regional load attacks. Constraint (23) secures the power flow in non-attack region N. Notably, λ_l represents a binary variable that is equal to 1 if line l is attacked, and 0 otherwise.

To sum up, a high-risk regional load attack can be designed based on a single level model, and this model is summarized by the objective function in (15) with constraints (8)-(12) and (16)-(23). This single-level model can be solved directly using a commercial solver.

III. Case Studies

In this section, case studies are conducted on modified IEEE 24- and 118-bus test systems. We set the line overload threshold Γ to 1.20 p.u. Our proposed model is solved using GUROBI 10.03 in MATLAB 2019b on a PC with an Intel i7-8700 (3.2 GHz) and 16 GB RAM.

A. IEEE 24-bus Test System

We first use the modified IEEE 24-bus test system to validate the superiority of our proposed approach. This system consists of 10 thermal units, 38 lines, and 17 load buses, which is divided into attack region A and non-attack region N. If the attack region A contains p non-boundary buses and α boundary buses, and at most $p-1$ bus injection measurements are not attackable, then a feasible non-zero attacking vector exists. Based on this principle, we select the set of buses [1, 2, 3, 4, 5, 6, 7, 8, 9, 10] as attack region A, which includes 10 buses and 12 lines, and the remaining part is the non-attack region N. Specifically, boundary buses are 3, 9, and 10 in attack region A, which are set to have the same bus voltage angle variation.

1) From the high-impact perspective: Table I compares our proposed approach with methods developed in [2, 5, 6, 8]. We can observe that an attacker can launch the regional load attack using our proposed approach to increase the operation costs. Here, the attacker can optimally select multiple targeted lines to overload, and the number of overloaded lines can be flexibly adjusted to achieve controllable impacts on a smart grid. For example, when the total number of targeted overload lines is k=3, the regional load attack designed based on our method increases the operation cost to \$84,179.92 while overloading lines 3, 10, and 11. Compared to the designed attacks in [5, 6, 8], their operation costs are always lower than those achieved by our proposed approach. Although the operation cost in [2] reaches the highest value of \$97,984.92, only one line is overloaded with an overloading ratio 1.21 p.u., showing less attack impacts on the number of overloaded lines. When k=4, the power flow of the targeted line 12 exceeds its power flow limit by an overloading ratio of 1.37, causing a significant increase in the operation cost. In [5], although the targeted line 11 is overloaded by 1.49 times its power flow limit, this approach ignores the stealth of corrupted data, which can be easily identified as an outlier (as analysed in a later section). Also, comparable approaches in [6, 8] cannot cause serious line overloads with less increase in power flows. The comparison analysis verifies that our designed regional load attack can impose higher impact on the smart grid compared to other methods.

TABLE I.
Simulation Results Based on Various Load Attack Methods

Cases		Targeted lines	Overloading ratio (p.u.)	Operation cost (\$)
Our proposed approach	k=2	Line 10	1.20	80058.94
		Line 11	1.20	
	k=3	Line 3	1.20	84179.92
		Line 10	1.20	
		Line 11	1.20	
	k=4	Line 10	1.20	90437.10
		Line 11	1.20	
		Line 12	1.37	
		Line 13	1.20	
Ref.[2]		Line 17	1.21	97984.92
Ref.[5]		Line 10	1.29	81146.84
		Line 11	1.49	
Ref.[6]		Line 28	1.03	77695.18
Ref.[8]		Line 10	1.04	76342.63

† The shaded area represents the largest per-unit flow of line l. The overload rate is defined as the ratio between the power flow of the targeted line and its capacity.

2) From the high-stealth perspective: To compare the stealth of various load attack methods, Table II shows the total number of corrupted loads, the spatial distance of corrupted data, and the spatial distance ratio of corrupted data as three stealth indicators. Based on our designed regional load attacks, when k=2 to overload two lines, the total number of corrupted loads is only required to be five to successfully launch this attack, while it increases to 10 corrupted loads if k=4. However, the required total number of corrupted loads is much less than other methods in [2, 6, 8]. For example, the designed regional load attack in [2] requires 15 out of 17 loads to be manipulated in the smart grid. This verifies that our approach can significantly reduce the complexity and resources needed for executing the load attacks, while still achieving substantial disruptions with a small number of corrupted loads. Also, we can observe that, except for [6], the spatial distances of corrupted data designed in [2, 5, 8] are all greater than the edge distance calculated as 1,223.43. However, the spatial distance of our corrupted data is significantly less than the edge distance, thereby the corresponding spatial distance ratio is always less than 1.0 p.u. This indicates that the corrupted data is hidden among the normal data within the edge distance, enabling it to escape detection. In [6], although the spatial distance of corrupted data is less than the edge distance, such corrupted data is designed by invading all loads of the grid, compromising the stealth of the attack with larger number of corrupted loads. Moreover, this designed attack in [6] cannot cause serious overloads (as clarified earlier). To sum up, compared to these load attack methods in [2, 5, 6, 8], our proposed approach require fewer load data manipulation to enhance the stealth of corrupted data, which can hide among normal data to be undetectable, and still maintains its high-impact overloads.

TABLE II.
Stealth Comparison of Various Load Attack Methods Based on Different Stealth Indicators

Cases		Total corrupted loads	Spatial distance	Spatial distance ratio
Our	k=2	5	167.05	0.137
proposed	k=3	8	461.59	0.377

approach	*k*=4	10	814.11	0.665
	Ref.[2]	15	3363.75	2.749
	Ref.[5]	7	1476.24	1.207
	Ref.[6]	17	392.16	0.321
	Ref.[8]	10	1379.74	1.128

† The spatial distance ratio is the ratio of the spatial distance and the edge distance (i.e., 1223.43).

3) From the high-regional concentration perspective: To verify the effectiveness of our proposed approach in the targeted attack region, Fig. 2 shows the load deviation ratio obtained using our proposed approach, in comparison with the methods presented in [2, 5, 6, 8]. The load deviation ratio is defined as the ratio between the injected load data and normal load data at each bus. It is clear that the total load deviation ratio achieved by our proposed approach is the lowest at 2.39% when *k*=2. This means that our designed attack is more insidious and difficult to detect. Meanwhile, only five loads are corrupted, located at buses 2, 6, 7, 8, and 10 within the attack region. By focusing on a specific attack region with high-regional concentration of load manipulation, the attacker can effectively launch the attack with incomplete network information, by only knowing the regional network information within the attack region. For local LR attacks in [8], this attack designed in [8] only increases the total load deviation ratio (i.e., 21.55%) and the total number of corrupted loads (i.e., 10 loads) without significantly affecting the power flow and the operation cost, as discussed earlier. This indicates that our approach strategically focuses on a regional attack with limited network information while still inducing multiple line overloads and maintaining high-stealth performance.

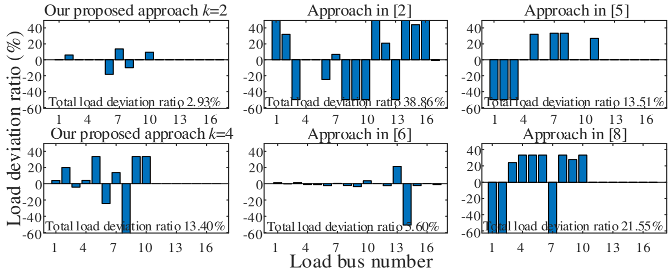

Fig. 2. Load deviation ratio obtained by various load attack approaches.

B. Larger-scale Test System

In this section, additional case studies are conducted on the modified 118-bus test system to further validate the feasibility of high-risk regional load attacks. Fig. 3 shows the topological diagram of the attack region. Note here that the number of targeted lines is set to *k*=4.

TABLE III.
COMPARATIVE RESULTS ON THE MODIFIED IEEE 118-BUS TEST SYSTEM

Cases	Targeted lines	Overloading ratio (p.u.)	Operation cost ($)	Total corrupted loads	Spatial distance
Our proposed approach (*k*=4)	Line 78	1.20	108445.03	13	482.76
	Line 103	1.20			
	Line 121	1.33			
	Line 125	1.20			
Ref.[2]	Line 129	1.32	104575.84	52	6099.49
	Line 167	1.20			
Ref.[6]	Line 104	1.20	95748.32	91	779.08

† The edge distance is 1491.04 in the modified IEEE 118-bus test system.

Compared with results in Table III, the designed attack in [2] can overload lines 129 and 167 by manipulating 52 loads, but the corrupted data deviates from normal data by almost four times of edge distance, thereby compromising the stealth of this attack. Although the corrupted data in [6] is close to the centroid of normal data within the edge distance, this designed attack can only overload line 104 by corrupting all 91 loads in the power grid. In addition, the operation cost resulting from this attack is only $95,748.32, which is lower than that of our proposed approach, showing a reduced attack impact. More specifically, our designed attack manipulates 13 loads to simultaneously overload lines 78, 103, 121, and 125, resulting in a significantly higher operation cost of $108,445.03 and a greater attack impact. Meanwhile, the spatial distance of corrupted data is only 482.76 which is significantly less than the edge distance of 1,491.04. This means that such corrupted data is sufficiently close to the centroid of normal data compared with those of [2, 6], making it harder to detect. To sum up, this comparative analysis effectively verifies the superiority of our proposed attack mechanism. In addition, Fig. 3 shows the locations of the corrupted loads and targeted lines, providing guidance for the defender to determine protection strategies that enhance system resilience.

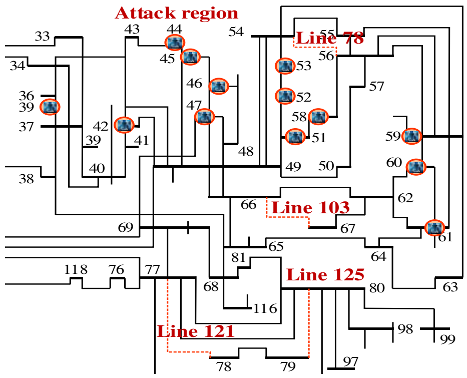

Fig. 3. Topological diagram of the attack region in the 118-bus test system.

IV. CONCLUSION

This letter develops high-risk regional load attacks using only incomplete network information limited to the attack region within a smart grid. Extensive case studies validate that such attacks are capable of overloading multiple lines within this attack region by only corrupting a limited number of loads in a stealth manner. In future work, we will further explore the design of practical detection and mitigation methods against such high-risk regional load attacks.

REFERENCES

[1] M. Cui, J. Wang, and M. Yue, "Machine Learning-Based Anomaly Detection for Load Forecasting Under Cyberattacks," *IEEE Transactions on Smart Grid,* vol. 10, no. 5, pp. 5724-5734, 2019.

[2] P. Verma and C. Chakraborty, "High Impact Local Load Redistribution Attack Without Confidential Network Information," *IEEE Transactions on Smart Grid,* vol. 15, no. 2, pp. 2383-2386, 2024.

[3] M. Zhou, J. Wu, C. Long, C. Liu, and D. Kundur, "Dynamic-Line-Rating-Based Robust Corrective Dispatch Against Load Redistribution Attacks With Unknown Objectives," *IEEE Internet of Things Journal,* vol. 9, no. 18, pp. 17756-17766, 2022.

[4] K. Singh and S. K. M, "Analyzing Financial Implications and Optimal Bus Selection Strategies for False Data Injection Attacks in Power Grids," *Electric Power Systems Research,* vol. 240, p. 111259, 2025.

[5] Y. Tan, Y. Li, Y. Cao, and M. Shahidehpour, "Cyber-Attack on Overloading Multiple Lines: A Bilevel Mixed-Integer Linear Programming Model," *IEEE Transactions on Smart Grid,* vol. 9, no. 2, pp. 1534-1536, 2018.

[6] X. Liu, Y. Song, and Z. Li, "Dummy Data Attacks in Power Systems," *IEEE Transactions on Smart Grid,* vol. 11, no. 2, pp. 1792-1795, 2020.

[7] S. Gao, J. Lei, X. Wei, Y. Liu, and T. Wang, "A Novel Bilevel False Data Injection Attack Model Based on Pre- and Post- Dispatch," *IEEE Transactions on Smart Grid,* vol. 13, no. 3, pp. 2487-2490, 2022.

[8] Y. Xiang, Z. Ding, Y. Zhang, and L. Wang, "Power System Reliability Evaluation Considering Load Redistribution Attacks," *IEEE Transactions on Smart Grid,* vol. 8, no. 2, pp. 889-901, 2017.

[9] L. Che, X. Liu, and Z. Li, "Mitigating False Data Attacks Induced Overloads Using a Corrective Dispatch Scheme," *IEEE Transactions on Smart Grid,* vol. 10, no. 3, pp. 3081-3091, 2019.