High-Stealth False Data Attacks on Overloading Multiple Lines in Power Systems

Min Du, *Student Member, IEEE*, Lianhong Wang, and Yicong Zhou, *Senior Member, IEEE*

***Abstract*—In this letter, we present a single mixed-integer linear programming (MILP) model for high-stealth false data attacks (FDAs) on overloading a set of lines by injecting stealthy false data. The proposed model reveals that an intelligent attacker is able to deliberately construct a valid attack vector to overload multiple transmission lines while hiding it among normal data to evade advanced anomaly detection methods. In addition, the proposed cyber-attack mode can help the attacker optimally select the targeted lines. Simulation results on multiple large-scale test systems validate the effectiveness of the proposed approach.**

***Index Terms*—Cyber-attacks, multiple lines overloaded, high-stealth, power systems.**

I. Introduction

AS THE integration of information and network technologies, modern power systems are vulnerable to cyber-attacks [1]. It is important to investigate the hackers' strategies of attacking lines, since it can help the defender to develop more practical defense strategies against cyber-attacks. In [2], a tri-level optimization model was proposed to overload a single line by launching false data injection attacks. However, the tri-level model cannot overload multiple lines. Then, the authors in [3] proposed a bi-level mixed-integer linear programming (BMILP) model that can overload multiple lines by injecting false data. Unfortunately, this model ignores the stealthiness of false data so that these false data can be detected by advanced methods, while the targeted lines are also not optimally selected. The authors in [4] revealed that an intelligent attacker can design dummy data to escape detection while ignoring the computational efficiency. In reality, the stealthiness of dummy data is not well due to the suboptimal spatial distribution of the corrupted data. Thus, this letter proposes a single MILP model to investigate the high-stealth false data attacks from the attacker's perspective. The proposed model reveals that an intelligent attacker can launch high-stealth false data attacks on overloading multiple lines that can be optimally chosen by the hacker. This high-stealth cyberattack can impose severe impact on the power system operation security. At the same time, the injected false data can be hidden among normal data to avoid the detection of anomaly detection algorithms.

II. MILP Model for High-Stealth Cyberattacks

The main obstacle to formulating a single MILP model for high-stealth false data attacks on overloading multiple lines is how to construct stealthier false data, evaluate false data stealth and optimally select these targeted lines. To address such issues, we convert them into certain constraints that need to be satisfied in the optimization problem.

Definition 1 (High-Stealth FDAs): Let the corrupted data by injecting false data not be identified as outliers by being hidden among normal measurements.

To guarantee the stealthiness of false data, the tampered data should be required to be hidden among normal ones as much as possible. In that way, if the false data is spatially close to the center point of normal data, i.e., the center data, its stealth will be the highest. Then, we describe it as a mathematical optimization problem that minimizes the distance between false data and center point of normal data.

$$\min \mathbf{1}^{\mathrm{T}}\left|\boldsymbol{x}'-\boldsymbol{x}_0\right| \tag{1}$$

where $\boldsymbol{x}_0$ denotes the center point of normal measurements; $\boldsymbol{x}'$ represents the corrupted data that can be expressed as $\boldsymbol{x}' = \boldsymbol{x}_0 + \Delta\boldsymbol{x}'$, in which $\Delta\boldsymbol{x}'$ represents the false data injected by an attacker. Note here that normal historical data are generated by the Monte Carlo (MC).

Definition 2 (Security Distance Index): Let S denote the security distance index that indicates the largest distance between the center point of normal measurements and each normal one, i.e., $S = \text{argmax}\{S_1, S_2, \ldots, S_m\}$. Let d represent the distance between the center point of normal data and the stealthy false data. The distance index for high-stealth false data is required to be satisfied

$$d \le \text{argmax}\{S_1, S_2, \ldots, S_m\} \tag{2}$$

where m represents the number of the generated normal historical data.

Definition 3 (Attackable Lines-Targeted): Given $\overline{f}_l$ as power flow limit of attacked branch l, let its loading be no less than $\Gamma\overline{f}_l$. The true line flow of targeted-line l satisfies

$$|f_l|/\overline{f}_l \ge \pi_l \cdot \Gamma \qquad \pi_l \in \{0, 1\} \qquad l \in NL \tag{3}$$

$$\sum\nolimits_{l \in NL} \pi_l = k \qquad k = 2, 3, 4 \cdots \tag{4}$$

where NL is a set of all lines; l is the index of lines; k is the number of the targeted lines; Γ is the line overloads threshold (p.u.); π_l is a binary variable that is equal 1 if line l is attacked, being 0 otherwise. Constraints (3)-(4) are overloading a set of lines that can be optimally selected by a hacker. Constraint (3) represents the overloading level of the targeted-line l is no less than $\Gamma\overline{f}_l$. Constraint (4) limits the number of tripped lines at an expected value. According to NERC Standard PRC-023-1 R1.2 [5], the line relays are set to operate above 115% of the facility's highest rating. Therefore, Γ in Eq. (3) is set to be 1.20 p.u. so that the targeted-line can be tripped by an attacker launching high-stealth FDAs. It should be pointed out that, based on the proposed algorithm for selecting high-risk lines in [6], we can fast screen out the candidate-targeted lines, which can improve the computation efficiency.

The developed cyber-attack model is to overload multiple lines by injecting high-stealth false data, which are optimally

Manuscript received 9 May 2022; revised 8 August 2022; accepted 19 September 2022. Date of publication 26 September 2022; date of current version 20 February 2023. This work was supported by the National Key Research and Development Program of China under Grant 2019YFE0105300. Paper no. PESL-00123-2022. *(Corresponding authors: Min Du; Lianhong Wang.)*

Min Du and Lianhong Wang are with the College of Electrical and Information Engineering, Hunan University, Changsha 410012, China (e-mail: dumin94@hnu.edu.cn; wanglh@hnu.edu.cn).

Yicong Zhou is with the Department of Computer and Information Science, University of Macau, Macau, China.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSG.2022.3209524.

Digital Object Identifier 10.1109/TSG.2022.3209524

selected by an attacker. The proposed model can be converted into a MILP program described as follow:

$$\min \quad \mathbf{1}^{\mathrm{T}}\boldsymbol{L} \tag{5}$$

$$\text{s.t.:} \quad \boldsymbol{L} \geq -\left(\boldsymbol{x}'-\boldsymbol{x}_0\right) \tag{6}$$

$$\boldsymbol{L} \geq \left(\boldsymbol{x}'-\boldsymbol{x}_0\right) \tag{7}$$

$$\sum_{i\in N}\mathbf{H}_i\Delta\boldsymbol{\theta}=0 \tag{8}$$

$$-\tau\left(D_i'-\mathbf{H}_i\Delta\boldsymbol{\theta}\right)\leq\mathbf{H}_i\Delta\boldsymbol{\theta}\leq\tau\left(D_i'-\mathbf{H}_i\Delta\boldsymbol{\theta}\right) \tag{9}$$

$$P_i^{inj}=\sum_{g\in G(i)}\hat{P}_g-\left(D_i'-\mathbf{H}_i\Delta\boldsymbol{\theta}\right) \tag{10}$$

$$\mathbf{H}_i\Delta\boldsymbol{\theta}=\Delta D_i' \tag{11}$$

$$f_l=\sum_{i\in N}\mathrm{PTDF}_{l,i}P_i^{inj} \tag{12}$$

$$\Delta f_l=-\sum_{i\in N}\mathbf{H}_i\Delta\boldsymbol{\theta}\cdot\mathrm{PTDF}_{l,i} \tag{13}$$

$$f_l+\mu_l\mathrm{M}\geq\pi_l\cdot\Gamma\overline{f_l} \tag{14}$$

$$-f_l+(1-\mu_l)\mathrm{M}\geq\pi_l\cdot\Gamma\overline{f_l} \tag{15}$$

$$\sum\nolimits_{l\in NL}\pi_l=k \qquad k=2,3,4\cdots \tag{16}$$

$$\mu_l\in\{0,1\};\ \pi_l\in\{0,1\};\ l\in NL;\ i\in N \tag{17}$$

where $\boldsymbol{L}$ is an additional auxiliary vector; τ represents the attack magnitude of false data, which is set at 0.5 in this paper; g/i represents the index of units/buses; N is a set of all buses; $G(i)$ is a set of all units at bus i; $\boldsymbol{x}_0$ represents the center point of normal measurements, i.e., normal load and active power measurements; $\mathbf{H}$ is a matrix between active power injection data and state variables (i.e., bus angles); $\Delta\boldsymbol{\theta}$ is angle deviation vector; D_i' is a corrupted load data at bus i. It should be pointed out that the injected false data $\mathbf{\Delta}\boldsymbol{x}'$ in *definition 1* can be express as $\mathbf{\Delta}\boldsymbol{x}'=[\ldots,\Delta D_i',\ldots,\ldots,\Delta f_l,\ldots]^{\mathrm{T}}$ (i.e., $[\ldots,\mathbf{H}_i\Delta\boldsymbol{\theta},\ldots,\ldots,-\sum_{i\in N}\mathbf{H}_i\Delta\boldsymbol{\theta}\cdot\mathrm{PTDF}_{l,i},\ldots]^{\mathrm{T}}$. Specifically, $\mathbf{H}_i\Delta\boldsymbol{\theta}$ is equal to $\Delta D_i'$, which represents the false load data injected into bus i. This implies that the attacker can change bus angles to temper load measurements. $\mathrm{PTDF}_{l,i}$ is the power transfer distribution factor for line l and bus i; Δf_l represents the injected false data into the line flow data of line l (i.e., Eq. (13)). $\hat{P}_g$ is the determined power output of generator g in base scenario. P_i^{inj} represents the actual power injection to bus i; μ_l is an auxiliary binary variable; M is a sufficiently larger positive constant. Notably, Eqs. (5)-(7) are equivalent to Eq. (1), which minimizes the distance between the false data and the center data. Constraints (8) and (9) represent that the attacking amount is summed to zero and limited with a certain range, respectively. Constraint (10) denotes the actual power injected into bus i. Constraint (11) illustrates that an attacker can manipulate bus angles to obtain variations in loads. Constraint (12) computes the true line flow f_l of line l. Constraints (14) and (15) ensure the overloading level of the attacked line l, which are equivalent to Eq. (3). Next, we intend to analyze the feasibility of the high-stealth FDAs.

III. Case Study

In this section, the proposed model is illustrated by extensive experiments. And, line overloads threshold Γ is set to 1.20 p.u. All data can be found in MATPOWER_v.6.0 [7]. M is taken as 10^4. The single MILP model is implemented in MATLAB 2014a using the CPLEX 12.4 solver on a personal computer with Intel Xeon Gold 6146 3.2GHz CPU and 128GB RAM.

TABLE I
The Simulation Results on the IEEE 118-Bus System

k	The targeted lines	Loss (MW)	$\lvert f_l\rvert/\overline{f_l}$	d_k	S
2 ($\boldsymbol{x}_1'$)	147、155	163.76	1.2	299.54	
3 ($\boldsymbol{x}_2'$)	129、147、155	253.76	1.2	437.07	954.68
4 ($\boldsymbol{x}_3'$)	128、129、147、155	271.95	1.2	691.35	

† $\boldsymbol{x}_i'$ indicates the high-stealth false data that can be obtained by solving the proposed model.

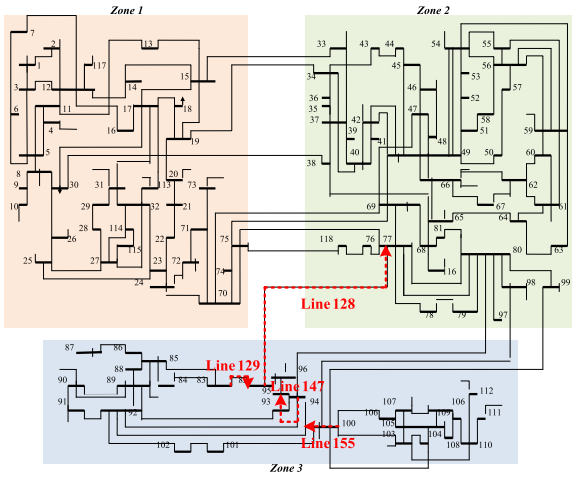


Fig. 1. Locations of lines-targeted in the IEEE 118-bus system.

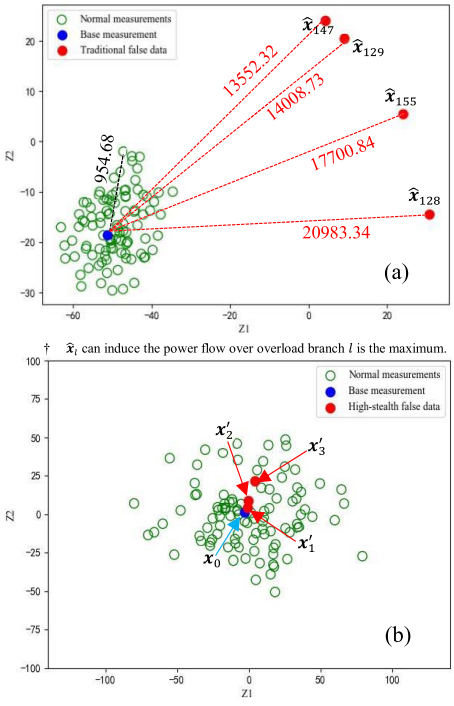
A. IEEE 118-Bus System

In this case, we first illustrate the proposed single MILP model on the IEEE 118-bus system, and the system load level is set to be 7500MW. The test data of 118-bus system can be found in motor.ece.iit.edu/ data/SCUC_118test.xls. Also, the line limit is adjusted to 80% of the respective line limit.

Table I gives the different lines-attacked that are optimally selected by an attacker, under the disruption of stealthy false data. For instance, when the number of tripped lines is required to be 2 (i.e., $k=2$ in Eq. (16)), lines 147 and 155 will be selected to be overloaded with line flows 1.2 times greater than their line flow limits. And, the load loss is 163.76MW when the attacked lines are tripped. This is, the attacker can cause severe impacts on the system security operation by injecting stealthy false data. When $k=3$, load loss reaches 253.76 MW. Load loss will reach up to 271.95 MW if k is increased to 4, lines 128, 129, 147, and 155 are simultaneously overloaded over the given Γ, which are depicted by the red dashed lines in Fig. 1 (arrows denote line flow directions). We can find that the optimal attack vector can severely overload lines at different locations. Note that the overloaded line 128 is a tie-line between zones 2 and 3, whose outage can bring serious security impacts on the system. Next, we intend to analyze the stealthiness of such false data.

To investigate the false data stealth, we employ the MC approach to generate 100 normal data (i.e., $m=100$ in *definition 2*) following the Gaussian distribution in the range of $[0.9,\ 1.1]\times\boldsymbol{x}_0$ [8]. Since the derived data are high-dimensional, we then use the T-SNE algorithm in [9] to extract their 2-dimensional features to obtain the distribution diagram. As shown in Fig. 2, these measurements are depicted by points in a 2-dimensional scatter map.

Fig. 2(a) shows the distribution of the normal data and the traditional false data. Note that the traditional false data can be obtained in [10]. It can be found from Fig. 2(a) that the 100 normal data are almost clustered together. However, each false data is far away from these normal ones due to its unique features even though it can cause the severest overloads on the



† $\widehat{\boldsymbol{x}}_l$ can induce the power flow over overload branch l is the maximum.

† (Z1: the first component, Z2: the second component)

Fig. 2. The two-dimensional scatter diagram of data.

TABLE II
DETECTIONS RESULTS BASED ON DIFFERENT DETECTION ALGORITHMS

Detection algorithms	Traditional false data [10]				High-stealth false data		
	$\widehat{\boldsymbol{x}}_{128}$	$\widehat{\boldsymbol{x}}_{129}$	$\widehat{\boldsymbol{x}}_{147}$	$\widehat{\boldsymbol{x}}_{155}$	$\boldsymbol{x}'_1$	$\boldsymbol{x}'_2$	$\boldsymbol{x}'_3$
MCD [11]	✔	✔	✔	✔	✘	✘	✘
ABOD [12]	✔	✔	✔	✔	✘	✘	✘
HBOS [13]	✔	✔	✔	✔	✘	✘	✘
LSCP [14]	✔	✔	✔	✔	✘	✘	✘

† ✔ represents the malicious data has been detected, and ✘ indicates the malicious data has not been detected.

corresponding line. In this case, the security distance indices between the center data $\boldsymbol{x}_0$ and each normal one range from 0 to 954.68. That is, if the distance between an unknown data and the center data is less than or equal to 954.68, we will view it as a normal data without injecting false data. For example, for the traditional false data $\widehat{\boldsymbol{x}}_{128}$ in Fig. 2(a), although it can cause the severest overload on line 128, the distance index for the corrupted data is 20983.34 that is much greater than 954.68. Thus, the traditional false data will be identified as an outlier without stealth.

If we make use of the developed approach to construct stealthy false data to manipulate normal ones, the corrupted data can be well hidden among normal measurements. As shown in Fig. 2(b), even though these manipulated data are spatially close to the center data, they can cause overloads on multiple lines-targeted. It can be seen from Table I, the distance index for the high-stealth false data $\boldsymbol{x}'_1$ is 299.54, which perfectly falls within the range [0, 954.68]. When k is 4, even though the distance between the center and false data is relatively large that can reach up to 691.35, it is still less than 954.68. That implies such false data cannot be recognized as an outlier. Next, we further illustrate the high stealth of such false data through advanced detection technologies.

Then, we employ several detection algorithms to identify malicious data. As shown in Table II, the traditional false data can be easily detected while the high-stealth false data cannot be recognized. In other words, this case further proves that an intelligent attacker can carefully design high-stealth false data hidden among normal ones to evade detection.

TABLE III
THE SIMULATION RESULTS ON DIFFERENT TEST SYSTEMS

Systems	k	The targeted lines	Loss /(MW)	d_k	S	Time /(min)
120-bus	2	10、192	92.25	441.28	2475.08	0.02
	3	10、86、192	229.19	762.37		0.06
	4	10、86、124、192	365.99	1083.47		0.09
300-bus	2	151、336	53.35	1633.97	4157.15	0.12
	3	78、151、336	78.05	3607.38		0.21
	4	78、151、324、336	181.69	5719.12		0.23
2383-wp	2	704、1816	822.96	380.74	5163.02	69.97
	3	704、772、1816	863.07	571.92		100.03
	4	704、772、779、1816	921.09	847.41		154.24
2736-sp	2	2141、2187	99.71	158.67	4321.52	214.21
	3	2141、2187、2207	544.37	416.55		409.38
	4	2141、2187、2269、2270	827.68	891.15		598.29
2746-wp	2	2017、2148	26.56	33.72	5796.69	301.44
	3	1670、2017、2148	184.59	190.23		366.17
	4	1234、1670、2017、2148	172.81	357.21		472.05

B. Extensive Simulations on Multiple Test Systems

In this section, we conduct extensive simulations on multiple systems for further validation. Table III gives the distance indices and the targeted lines in different cases. It can be seen from Table III that the load loss and the distance index increase as the number of targeted lines (i.e., k in Eq. (16)) increases. This is due to the fact that, the larger number of tripped lines can cause more serious impacts, and derive the difference between false data and normal ones to be more distinctive. Therefore, the corrupted data will be slightly separated from the normal ones. For $k = 2$, in the IEEE 2383-bus system, the minimized distance between the high-stealth false data and center data is 380.74, and its value is much less than 5163.02 so that it can perfectly hide among normal measurements. On the other hand, the load loss is 822.96 MW. When k is increased to 3, the distance and the load loss increase to 571.92 and 863.07 MW, respectively. Furthermore, the load loss increases up to 921.09 MW if k is increased to 4, the minimized distance reaches up to 847.41 while it still falls within the range [0, 5163.02]. This overall trend holds for the other cases in Table III. This indicates that an attacker can design stealthy false data to impose impacts on the system operational security but cannot be detected.

Next, we investigate the impacts of the different thresholds Γ on the stealthiness of false data. Three different thresholds 1.20, 1.30, and 1.50 p.u. for Γ are used to analyze the stealth of false data, and k is fixed to 2. And, the percentage of distance is employed for quantitative analysis of high-stealth false data attacks in several power systems (i.e., the ratio between d and S). It can be seen from Fig. 3 that the percentage of the distance ratio increases as the setting threshold Γ increases in respective systems. That is, the attacker needs to introduce obvious outliers into power systems, resulting in more serious line overload contingencies. However, most of the distance ratio values are less than 1, which effectively illustrates the superior performance of high-stealth false data. It is worth noting that the distance ratio values in the IEEE 118 and 300-bus systems are greater than 1 when Γ is set to 1.5 p.u. Therefore, this part of attack scenarios can be detected by advanced detection methods and should not be considered in the defensive strategies. By doing so, the defending cost will be significantly reduced.

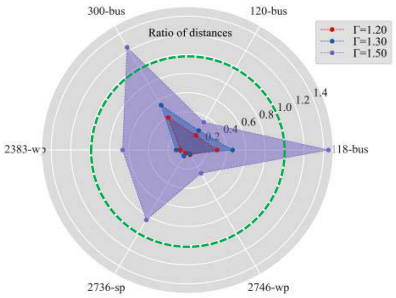


Fig. 3. The analysis of the high-stealth false data.

IV. Conclusion

This letter proposes a single MILP model for overloading multiple lines in a stealthy manner, considering the high-stealth false data injection attacks. Such false data can result in overloading multiple lines and load loss. In addition, these attacked lines can be optimally chosen by the attacker. It should be pointed out that the high-stealth false data can be well concealed among normal ones, which cannot be recognized as outliers. Simulation results on several test systems validate that the attacker can impose severe damaging effects on a system through high-stealth false data attacks. In the future, we will further investigate cascading failures induced by stealthy cyber-attacks.

Acknowledgment

The authors acknowledge and appreciate Prof. Xuan Liu for valuable discussion.

References

[1] M. Du, X. Liu, Q. Zhou, and Z. Li, "Hybrid robust tri-level defense model against multiperiod uncertain attacks," *IEEE Trans. Smart Grid*, vol. 13, no. 4, pp. 3255–3265, Jul. 2022, doi: 10.1109/TSG.2021.3139033.

[2] X. Liu and Z. Li, "Trilevel modeling of cyber attacks on transmission lines," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 720–729, Mar. 2017.

[3] Y. Tan, Y. Li, Y. Cao, and M. Shahidehpour, "Cyber-attack on overloading multiple lines: A bilevel mixed-integer linear programming model," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1534–1536, Mar. 2018.

[4] X. Liu, Y. Song, and Z. Li, "Dummy data attacks in power systems," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 1792–1795, Mar. 2020.

[5] *Transmission Relay Loadability*, NERC Standard PRC-023-1, 2006. [Online]. Available: https://www.nerc.com/files/prc-023-1.pdf

[6] L. Che, X. Liu, and Z. Li, "Fast screening of high-risk lines under false data injection attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4003–4014, Jul. 2019.

[7] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

[8] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1644–1652, Sep. 2017.

[9] L. van der Maaten and G. Hinton, "Visualizing data using T-SNE," *J. Mach. Learn. Res.*, vol. 9, no. 86, pp. 2579–2605, 2008.

[10] R. Kaviani and K. W. Hedman, "An enhanced energy management system including a real-time load-redistribution threat analysis tool and cyber-physical SCED," *IEEE Trans. Power Syst.*, vol. 37, no. 5, pp. 3346–3358, Sep. 2022, doi: 10.1109/TPWRS.2021.3135357.

[11] J. Hardin and D. Rocke, "Outlier detection in the multiple cluster setting using the minimum covariance determinant estimator," *Comput. Stat. Data Anal.*, vol. 44, pp. 625–638, Jan. 2004.

[12] H.-P. Kriegel, M. Schubert, and A. Zimek, "Angle-based outlier detection in high-dimensional data," in *Proc. 14th ACM SIGKDD Int. Conf. Knowl. Discov. Data Min.*, 2008, pp. 13–24.

[13] M. Goldstein and A. Dengel, "Histogram-based outlier score (HBOS): A fast unsupervised anomaly detection algorithm," in *Proc. 35th German Conf. Artif. Intell.*, 2012, pp. 59–63.

[14] Y. Zhao, Z. Nasrullah, M. Hryniewicki, and Z. Li, "LSCP: Locally selective combination in parallel outlier ensembles," in *Proc. SDM*, 2019, pp. 585–593.