Topology Reduction for Determining Worst-Case Attacks in Radially Operated Distribution Networks

Sho Cremers[*†], Marten van Dijk[*‡], Han La Poutré[*†]
[*]*Centrum Wiskunde & Informatica (CWI)*, Amsterdam, The Netherlands
[†]*Delft University of Technology*, Delft, The Netherlands
[‡]*Vrije Universiteit Amsterdam*, Amsterdam, The Netherlands
{sho.cremers, marten.van.dijk, han.la.poutre}@cwi.nl

***Abstract*—With the increasing digitalization of the power system, cyber attacks that threaten physical disruption, such as power outages, are increasing. Hence, understanding system resilience and the operator responses is crucial for anticipating and mitigating threats that may cause outages through power line disconnections. A common approach to assessing grid resilience is to consider the worst-case attack, in which the attack is assumed to maximize the potential damage while the operators react to minimize such loss. This assessment, however, can have a vast number of possible actions by the attacker as the size of the power network and the severity of the attack increase, making it computationally expensive. We propose a topology reduction technique on radially operated distribution networks, which reduces the set of lines to be considered in the worst-case attack. The reduced network can determine such an attack more efficiently compared to the original network. Case studies on 33- and 119-bus systems showed that the introduced method reduced the network sizes by 25% and 38%, respectively, and its effectiveness on the worst-case attack computation increased as larger attacks with more line disconnections were considered.**

***Index Terms*—Cyber attack, Distribution network, Grid resilience, Worst-case attack, Topology reduction**

I. Introduction

While digitalization has become essential in today's power system, it has also become more vulnerable to cyber threats. Cyber attacks on the power system can have significant consequences for society. For example, the attack on the Ukrainian network in 2015 left about 225,000 consumers without power for several hours [1], showing a glimpse of the capabilities of such attacks. As a result, assessing the network's resilience to these threats has become an important area of study.

To study the physical impact of cyber attacks on the power grid, the attacks are often represented by topology attacks [2]. Here, the network is represented by a graph with electrical buses as nodes and power lines as edges. An attack is shown as the removal of graph components, particularly line disconnections represented by edge removal from the active network topology. Medium-voltage (MV) distribution networks are commonly operated radially [3]. While this has advantages, such as easier fault protection and control [4], [5], a single line disconnection can separate a group of buses from the network and potentially cause load loss due to demand-supply imbalances within each of the isolated components, i.e., cause power outages to consumers. To mitigate formations of such isolated parts, they contain normally open points (NOPs): distribution lines not used in normal operation but available to reconnect separated components after faults elsewhere. Therefore, graph representation is especially useful to study the resilience of MV distribution networks, as both the attacker's and defender's actions can be depicted as topological changes.

Various studies on the resilience of the distribution network have considered line disconnections that maximize the loss to study the worst-case event. Identifying these events can provide an upper bound on the potential loss or damage the network may experience. Such knowledge can not only inform response actions to mitigate loss but is also highly valuable for making optimal long-term planning and investment decisions. In [6], they modeled a three-level optimization for optimal placement of soft open points for increased resilience against cyber attacks. In their model, a worst-case attack that maximizes its loss was considered in the second level, whereas the third level was modeled as the system operator minimizing loss by network reconfiguration. The authors in [3] also applied a three-layer model for optimal line hardening investment strategy against a malicious attacker or a natural disaster, with the second optimization layer modeling the worst k-line disconnection. Another three-level model proposed in [7] also considered the worst-case $N-k$ contingency in the middle layer. In [8], a generalized game-theoretical model was proposed for topology attacks and the defender's response actions in distribution networks. The study considered opposing objectives for the actors, where the attacker was modeled to maximize load loss against a defender that minimizes loss. It also showed that a simplified single-round game can give insights into actions and losses of a multi-round game.

While system resilience against multiple line disconnections is commonly studied for natural disasters and physical attacks, cyber attacks differ because the locations and timing of disconnections may not be geographically constrained. Cyber attacks can be executed at multiple locations nearly simultaneously once the attacker gains remote access. Thus, the attacker's action space (i.e., the potential disconnected lines) can be considerably larger, requiring greater computation time to

This work was supported by the RESCUE Project funded by the Dutch Research Council under Grant NWO ESI.2019.006.

979-8-3315-2503-3/25/$31.00 ©2025 IEEE

determine the worst-case attack. Note that possible combinations of disconnected lines grow exponentially with the attack size (i.e., the number of line disconnections allowed). Hence, reducing actors' action spaces can become helpful or even necessary to compute the impact of worst-case attacks.

In this study, we propose a topology reduction method that groups neighboring nodes with certain characteristics into clusters. We mathematically prove that any edge inside such a group (which connects nodes within the cluster) can be ignored under certain conditions from the attacker's action space when considering the worst-case attack. Hence, the group of nodes can be treated as a single node, which we call a *supernode*. Case studies on 33- and 119-bus systems present the results of the topology reduction, and the efficiency of computing the worst-case attack is compared between the original and reduced topologies. The results show that reduced topology exhibits slower growth in required computation as the maximum number of allowed line disconnections increases, amplifying the benefit of topology reduction for computing losses under larger attack scenarios.

The remaining sections are organized as follows. Section II describes the network representation and the optimization problem. In Section III, the topology reduction method is proposed. Section IV presents the case studies and simulation results. Finally, Section V concludes the study.

II. Distribution Network and Game Model

A. MV Distribution Network Representation

The topology of a network is represented as an undirected graph $G = (V, E)$ with the set of nodes V for buses and the set of edges E for distribution lines. Every node has a power demand, and at least one node is connected to the power grid that can supply the total load of the network at any time. Additionally, some nodes may also have generation from distributed generators (DGs). While most lines are active during normal operation, a subset of lines in E called the NOPs are inactive [9]. During normal operation, the network is connected and is operated radially, i.e., no cycles can be formed with active lines. Once lines are disconnected unintentionally, the system operator can either close NOPs to reconnect separated components or leave the network separated and operate them independently using the local generation. In either case, the network is expected to operate radially. Furthermore, power flow constraints are applied to guarantee safe operation.

Fig. 1 is a graph of an example network. Active lines are shown in solid lines, and NOPs are shown in dotted lines. Node 1 (red) is connected to the grid, and nodes 6 and 13 (blue) are connected to the DGs.

B. Game Model and Optimization

In this study, we apply the sequential game model [8], where the attacker disconnects lines through breaker-jammer attacks [6], and the defender can connect available NOPs as its response. While this framework allows us to model several rounds of actions, we restrict ourselves to a single-round game due to the limited space. However, the topology reduction method can also be applied in multi-round settings.

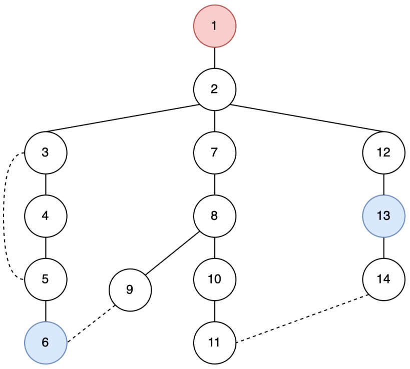


Fig. 1: Graph representation of a distribution network.

Let us denote the attacker's action as set A, which represents the disconnected lines, and is constrained by the following:

$$A \subseteq E^a, \text{ and} \tag{1}$$

$$1 \leq |A| \leq r^a. \tag{2}$$

Here, $E^a \subseteq E$ represents the attacker's action space, i.e., lines that are accessible by the attacker to disconnect, and r^a is the maximum number of lines the attacker can disconnect.

Similarly, the defender's action is denoted as set D, NOPs that are closed as its response, and is subject to the following:

$$D \subseteq E^d, \text{ and} \tag{3}$$

$$|D| \leq r^d. \tag{4}$$

Again, $E^d \subset E$ represents the defender's action space, which is the set of all NOPs. The parameter r^d is the maximum number of NOPs that can be connected. Given both players' actions, the active topology $G' = (V, E')$ is updated. By the abuse of notation, let us denote $E(A, D)$ as the set of active edges at the end of the game as a function of A and D,

$$E' = E(A, D) = \Big[(E \setminus E^d) \cup (D \cap E^d)\Big] \setminus \Big[A \cap E^a\Big]. \tag{5}$$

In (5), the attacked lines are removed if they are present in E^a. Moreover, NOPs closed by the defender are added to the active lines. Note that the set of initially active lines is $(E \setminus E^d)$, as the network during normal operation has all non-NOP lines connected. Recall that the network has to be operated radially, and hence, the initial active topology is acyclic, i.e., it is a tree. Radiality must also be satisfied after the players' actions. The attacker's action only consists of edge removal, and hence, its action will not generate any cycle. In contrast, the defender may generate cycles if not constrained, and thus, another important constraint for the defender is given by

$$G' = (V, E') = (V, E(A, D)) \text{ is a forest (i.e., acyclic).} \tag{6}$$

The impact of the above actions is determined by the active power load loss caused by topology changes, a key metric to study the quality of the actions and the resilience of the network. Let $\mathbb{P}(G')$ be the set of constraints from the Linearized

DistFlow model [3], along with the associated variables and parameters, given the active radial network $G' = (V, E')$. The operator performs redispatch to minimize the loss after the players' actions. Hence, load loss of G' is computed through optimal power flow as

$$l(G') = \min_{\mathbb{P}(G')} \sum_{x \in V} P_{shed,x}, \tag{7}$$

where $P_{shed,x}$ is the load loss at bus x from the DistFlow constraints. The solution minimizes the sum of active power load loss across the network. Clearly, the defender may want to minimize the load loss such that fewer consumers are disrupted, whereas the attacker may want to maximize such loss, signifying a greater impact on society. Thus, the overall optimization problem can be defined as the *maximin loss* of the single-round game [8], defined as follows.

Definition II.1. The maximin loss of a single-round game is the largest final loss achievable by the attacker when the defender minimizes the final loss, denoted as

$$\max_{A} \min_{D} l\Big((V, E(A, D))\Big), \tag{8}$$
$$\text{s.t. } (1) - (4), (6).$$

The maximin loss represents the worst-case attack given the attacker's resource constraints, when the operators act to reduce the loss. This provides insights into the resilience of the topology against involuntary line disconnections.

III. Topology Reduction

Determining the maximin loss can rapidly become computationally expensive as the network size grows, since it requires loss evaluations for all combinations of both players' actions. One method of reducing computation is to narrow the search space of player actions by removing suboptimal lines. Here, we introduce a method to remove such lines from the attacker's action space E^a by creating clusters of connected nodes (and their lines) in the network topology called *supernodes*. We show that any line within such clusters can be discarded from E^a to determine the maximin loss. First, let us define a value function $v : V \to \mathbb{R}$ for a node in the graph $G = (V, E)$. The value function is defined as the net load at the node. Hence, the value of node $x \in V$ is defined as

$$v(x) = P_{L,x} - P_{G,x}^{max}, \tag{9}$$

where $P_{L,x}$ and $P_{G,x}^{max}$ are parameters of the network at a given time and represent the active power load and the maximum active power generation at node x, respectively. A positive $v(x)$ value indicates that node x requires power to be supplied from other nodes, whereas a negative $v(x)$ value indicates that node x has enough generation to supply loads of other nodes.

A. Supernode

Definition III.1. A *supernode* ϕ in a full topology graph $G = (V, E)$ is a simple path in G,

$$w_1 - w_2 - \ldots - w_m$$

such that, 1) each node participates in at most two edges (i.e., only w_1 and w_m may have another edge not in the path), 2) all nodes have non-negative values $v(w_t)$, and 3) the adjacent edges (i.e., edges of w_1 and w_m not in the path) are in E^a.

Fig. 2a shows an example of a supernode. Nodes 2, 3, and 4 all participate in two lines and have non-negative $v(\cdot)$ values. Nodes 1 and 5 cannot be part of the super node, as it has three edges, and there is excess generation, respectively.

For the theoretical mathematical analysis below, the line capacity and voltage constraints are omitted when computing the load loss. While load loss after topological changes may occur for several reasons, a major influence on the loss is the formation of separated components (or islands) due to line disconnections. Load loss occurs when these islands have limited generation capacity, such that it cannot cover the loads. While these constraints are important for the safe operation of the system, note that in practice, MV networks were typically designed conservatively to accommodate peak load conditions [10], particularly since many buses (and the downstream buses they supply) depend on single lines for power delivery during radial operation. By omitting the line capacity and voltage constraints, load loss is then computed as the sum of the positive net load of each separated component in the graph, in which the property of this simplified loss calculation is used for the analysis of the supernode below. Therefore, the attacker's objective can be treated as creating such islands that have maximum net load. Furthermore, when ignoring line capacities, the optimal defense is to close all NOPs that reconnect separated components in the graph, while satisfying radiality. Hence, the attacker's maximum loss from generating such islands on a full topology with all NOPs connected is equivalent to the loss achievable against an optimal defender. Thus, we consider supernodes that can be formed on the full topology rather than only the active topology.

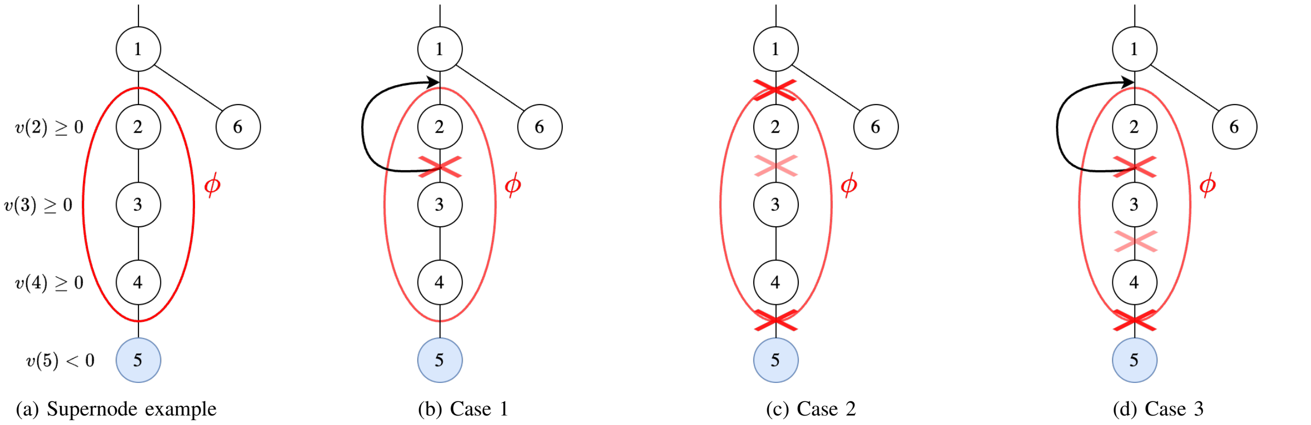
Let us denote all the nodes in a supernode ϕ as V^ϕ, and all lines in ϕ as E^ϕ. With the above assumptions, we have the theorem below.

Theorem III.1. *Assume the load loss is computed according to* (7)*, with the line capacity and voltage constraints omitted. If there exists a supernode ϕ (Definition III.1) in full topology G, then an attack strategy that maximizes the loss can be formed while excluding lines in $(E^\phi \cap E^a)$ from the attack.*

Below, we prove the theorem. This can also be shown by deriving mathematical formulas in a sequence, which we will not state here for reasons of limited space.

Proof. Consider an attack $A \subset E^a$ that contains a line $e \in E^\phi$ from a supernode ϕ. Here, we present three possible scenarios of A, and for each case, we show that substituting e with another line in E^a can generate at least the same loss.

In the first scenario, e is the only line in A from ϕ, and at least one of the adjacent edges of ϕ is not in A, as shown in Fig. 2b. The removal of e divides the nodes in V^ϕ into two components. Assume the net load of one of the components is greater than or equal to the other, i.e., given the two sets of



(a) Supernode example (b) Case 1 (c) Case 2 (d) Case 3

Fig. 2: Example of a supernode and three scenarios of when a line inside the supernode is disconnected by the attacker.

nodes V_1 and V_2 of the components created by disconnecting e, they have the following characteristic:

$$\sum_{x \in V_1} v(x) \geq \sum_{y \in V_2} v(y). \tag{10}$$

Then, by disconnecting an adjacent edge of ϕ instead of e, all nodes in V^{ϕ} can be pushed further to the component with a larger net load (V_1). Recall that load loss is generated when a component has a positive net load, and adding the load of the whole supernode to one component can guarantee as much loss as can be caused by disconnecting a line inside a supernode.

In the second scenario, e is the only line in $(A \cap E^{\phi})$, but all adjacent lines of ϕ are disconnected, as shown in Fig. 2c. As no node in ϕ has positive net generation, disconnecting e does not impact the loss. Hence, disconnecting any other available line in E^a instead of e can guarantee the same or larger loss (as a line disconnection always generates non-negative loss).

In the final case, multiple lines are disconnected from E^{ϕ}, as shown in Fig. 2d. In such a scenario, we can first push all disconnecting lines in E^{ϕ} to the adjacent lines of ϕ using the same reasoning as in the first scenario. If all existing adjacent lines are disconnected, the remaining lines do not impact the loss, as in the second scenario. Thus, these lines can be replaced with any lines outside E^{ϕ}.

Since there is an alternative action for $e \in (E^{\phi} \cap E^a)$ that achieves at least the same loss, A that maximizes loss can be formed without edges in the supernode ϕ. □

While we have shown the above results for a single-round game, the same results can be obtained for a multi-round game with several sequences of attack and defense. Once the non-extendable supernodes (that cannot be further extended with neighboring nodes to create a larger supernode) are determined, we can replace the supernodes with single nodes in the graph G and remove all edges inside supernodes to determine A that maximizes the loss. Such supernodes can be identified by a depth-first search algorithm that runs in linear time in the number of nodes and edges. Besides the efficiency, it is also noteworthy that the formed supernodes only change when there is a modification to the full topology, such as changes in buses, lines, and generator locations, or to E^a. Since the full topology does not change frequently, supernode detection has to be performed only once every time a different attacker with different capabilities is considered, making the introduced method a low implementation burden.

IV. Case Studies

In this study, we considered the 33- and the 119-bus systems. The experimental code was written in Python (3.10.13). DistFlow constraints (including line capacity and voltage constraints) and their optimization problem were modeled using CVXPY [11] (1.7.1) and GLPK-MI solver for determining the load loss. The network's radiality was verified with a depth-first search algorithm from NetworkX [12] (3.2.1).

A. 33-Bus System

Network Description: The system from [3] with five controllable DGs was used. The total active load of the network was 3.715 MW, and each DG had a 0.6 MW capacity. The defender's E^d consisted of all available NOPs, and the attacker's E^a included all normally operating lines, except for the line that connects the network to the power grid.

Topology Reduction: The network topology and the generated supernodes are shown in Fig. 3. Node 1 (red) is connected to the power grid, and nodes 6, 18, 21, 24, and 30 (blue) are connected to DGs. Other nodes have a load but no generation. Red boxes represent the supernodes that meet the conditions in Definition III.1, which reduced the number of nodes from 33 to 25. Since all normally operating lines (except line 1-2) are in E^a, all lines within the supernodes were removed from the attack set. Therefore, the size of E^a after topology reduction is reduced from 31 to 23, an over 25% reduction of the set.

Loss Computation: Table I shows the maximin losses and the computation time (in terms of iteration count) of the network with and without topology reduction for different r^a. As expected, the attacker's achievable loss increases with the attacking lines. Losses are also the same for both original and reduced networks, displaying that the attacker's optimal disconnection set did not contain lines within supernodes. The number of scenarios in Table I counts all combinations of

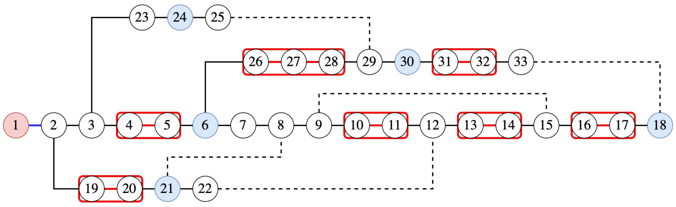


Fig. 3: Topology of 33-bus system and supernode formations.

two players' actions, which is larger in the original topology than in the reduced topology, and the gap grows as r^a increases. However, the main computational bottleneck is the OPF computation required for the loss. Some defender actions may violate radiality and thus are not valid actions. Hence, the number of loss evaluations was also counted and is shown in Table I. The number of scenarios and loss evaluations grows exponentially as r^a, with the size of E^a (and E^d) as the base. As the attack size increases, the impact of topology reduction becomes more significant, reducing the number of scenarios and loss evaluations for the 4-line attack by about 71.8%.

TABLE I: Losses and computation steps of 33-bus system.

r^a **value**		1	2	3	4
Loss (MW)	**Original**	0	0.615	0.745	1.105
	Reduced	0	0.615	0.745	1.105
Scenarios	**Original**	186	7,440	116,870	975,415
	Reduced	138	4,048	46,046	274,505
Loss eval.	**Original**	90	2,992	49,472	489,949
	Reduced	66	1,604	19,370	138,216

B. 119-Bus System

Network Description and Topology Reduction: The network consisted of 118 normally operating lines and 15 NOPs with a total active load of 22.710 MW. Seven controllable DGs were included in the network, in which the locations and capacities were taken from [13]. All NOPs were in E^d, and E^a included all normally operating lines, except for the line that connects the network to the power grid. Supernode generation resulted in a reduced network of 73 nodes. Moreover, E^a was also reduced from 117 lines to 72 lines, about a 38.5% reduction.

Loss Computation: Table II shows the maximin losses and the computation time. The maximin loss between the original and reduced topology remained unchanged for all tested r^a values. Additionally, both the number of scenarios and the total loss evaluations are cut significantly for the reduced topology, over 76% reduction for the 3-line attack.

TABLE II: Losses and computation steps of 119-bus system.

r^a **value**		1	2	3
Loss (MW)	**Original**	1.733	3.861	7.696
	Reduced	1.733	3.861	7.696
Scenarios	**Original**	1,872	821,106	149,834,880
	Reduced	1,152	309,276	34,352,640
Loss eval.	**Original**	357	57,855	5,676,439
	Reduced	222	22,349	1,359,578

V. Conclusion

We introduced a topology reduction technique to minimize the search space of the worst-case adversarial line disconnections by identifying groups of nodes through their topological characteristics. The simulation results of 33- and 119-bus systems showed that the introduced method reduced the set of available lines by the attacker by over 25% and 38%, respectively. The effect was amplified with larger attack sizes where potential scenarios grow exponentially, reducing the required computation by over 71% for the 4-line attack on the 33-bus system and over 76% for the 3-line attack on the 119-bus system. This demonstrates a slower growth in the number of potential disconnecting sets needed to identify the worst-case attack compared to the original network. For future work, the topology reduction to different network structures, such as meshed networks, will be considered. Furthermore, it would be interesting to apply the reduction technique as a pre-processing step on existing MILP models that also take worst-case attacks into account, as in [3], [6], which would reduce the number of variables.

References

[1] D. U. Case, "Analysis of the cyber attack on the Ukrainian power grid," *Electricity information sharing and analysis center (E-ISAC)*, vol. 388, no. 1-29, p. 3, 2016.

[2] X. Liu and Z. Li, "Local topology attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2617–2626, 2017.

[3] Y. Lin and Z. Bie, "Tri-level optimal hardening plan for a resilient distribution system considering reconfiguration and DG islanding," *Appl. Energy*, vol. 210, pp. 1266–1279, 2018.

[4] V. Vita, S. Lazarou, C. A. Christodoulou, and G. Seritan, "On the determination of meshed distribution networks operational points after reinforcement," *Appl. Sci.*, vol. 9, no. 17, 2019.

[5] J. Noh, W. Chae, W. Kim, and S. Choi, "A study on meshed distribution system and protection coordination using HILS system," in *13th Int. Conf. Inform. and Commun. Technol. Convergence (ICTC)*, 2022, pp. 344–346.

[6] L. Ma, L. Wang, and Z. Liu, "Soft open points-assisted resilience enhancement of power distribution networks against cyber risks," *IEEE Trans. Power Syst.*, vol. 38, no. 1, pp. 31–41, 2023.

[7] H. Wang, S. Wang, L. Yu, and P. Hu, "A novel planning-attack-reconfiguration method for enhancing resilience of distribution systems considering the whole process of resiliency," *Int. Trans. Electr. Energy Syst.*, vol. 30, no. 2, 2020.

[8] S. Cremers, I. Semertzis, M. van Dijk, and H. La Poutré, "Game-theoretical modeling of sequential topology attacks in radially operated distribution networks," 2025, to appear in Proc. of IEEE PowerTech 2025, Accepted version available at https://ir.cwi.nl/pub/35174.

[9] H. Ghoreishi, H. Afrakhte, and M. Jabbari Ghadi, "Optimal placement of tie points and sectionalizers in radial distribution network in presence of DGs considering load significance," in *2013 Smart Grid Conf. (SGC)*, 2013, pp. 160–165.

[10] W. Zhang, X. Meng, R. Li, H. Chen, Y. Gu, Y. Zhang, and J. Zhang, "Open capacity model of medium voltage transmission line in distribution network based on load data," in *J. Phys.: Conf. Ser.*, vol. 2378, no. 1. IOP Publishing, 2022, p. 012069.

[11] S. Diamond and S. Boyd, "CVXPY: A Python-embedded modeling language for convex optimization," *J. Mach. Learn.*, vol. 17, no. 83, pp. 1–5, 2016.

[12] A. A. Hagberg, D. A. Schult, and P. J. Swart, "Exploring network structure, dynamics, and function using NetworkX," in *Proc. 7th Conf. Python in Sci.*, Pasadena, CA USA, 2008, pp. 11 – 15.

[13] K. Devabalaji and K. Ravi, "Optimal size and siting of multiple DG and DSTATCOM in radial distribution system using bacterial foraging optimization algorithm," *Ain Shams Eng. J.*, vol. 7, no. 3, pp. 959–971, 2016.