Game-Theoretical Modeling of Sequential Topology Attacks in Radially Operated Distribution Networks

Sho Cremers*†, Ioannis Semertzis†, 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, i.semertzis@tudelft.nl

***Abstract*—While the digitalization of the power system has its merit, it also introduced emerging cyber attack threats. Once the attacker has access to the control of the system, they can cause significant damage to infrastructure and society as a whole. Game-theoretical models that allow the decision-making of multiple actors have been previously studied to assess the impact of such attacks and potential responses. In this study, we present a novel and generalized incident response game against topology attacks in radially operated distribution networks. The introduced model allows for sequential interactions between the attacker and defender over multiple waves of attacks. Within this new framework, we propose a simplified model called the associated single-round game to efficiently compute the lower-bound load loss attainable by the adversary. Finally, a case study on the IEEE 33-bus system showed that the multi-round game framework can be used to determine and compare optimal sequences of actions. Moreover, the single-round game required less computation while achieving the same maximum loss by the attacker against an optimal defender, indicating a tight bound.**

***Index Terms*—Topology attack, Cyber attack, Game theory, Incident response, Sequential game**

I. Introduction

Increasing digitalization of the power system in recent years has caused a surge in cyber attacks targeting the system. Cyber-physical attacks on critical infrastructure can have serious consequences that have a physical impact on society as a whole and may also endanger human lives. One example is the attack on the Ukrainian distribution network in 2015. Once the hackers had remote access to the system, they successfully caused power disruption to about 225,000 consumers [1].

To assess the risks and impacts of cyber attacks on the power system, researchers have utilized game-theoretical models. Such models can capture the complex interactions and behaviors of multiple decision-makers with opposing objectives, providing insights into the resilience of the network, as well as the response strategies. A common representation of cyber-physical attacks in the power system that are often analyzed with game-theoretical models is by so-called topology attacks [2], [3]. With such attacks, the network is represented as a graph, where the buses are abstracted to nodes and the power lines to edges. Attacks are represented by altering the elements of the graph such as removing edges to indicate power line disconnection, causing power outages on consumers and/or economic loss to the network operator [4], [5]. Here, we make an important distinction between cyber-physical attacks and localized physical attacks on the network. While physical attacks are limited by geographical constraints, cyber-physical attacks may be launched at multiple locations across a wide area with minimal delay once the attacker gains remote access to the system.

Medium-voltage (MV) distribution networks are often modeled to have a network topology of a meshed structure, though it is commonly operated radially [4]. The benefit of radial operation as opposed to meshed operation includes simpler fault protection and control, as well as lower installation costs [6], [7]. However, a short circuit on just one line can significantly impact the rest of the system, dividing the network into multiple components. Normally open points (NOPs) are distribution lines that are not in use during normal operation but can be closed when faults occur elsewhere. These NOPs can be utilized for topology reconfiguration and provide increased resilience to the network. Furthermore, integration of distributed generation (DG) in the network can provide further reliability and tolerance against faults [8]. Hence, game theoretical models on topology attacks in the distribution network have considered the defender's response actions as reconfiguration of the network topology and the adaptation of power outputs from generation sources. These models often combine the defender's action of infrastructure planning performed before the attack, modeling them as tri-level defender-attacker-defender (DAD) optimization problems. For example, the model by [4] determined the optimal line hardening plan in the top level, while the second and the third level consisted of line disconnections and network reconfiguration, respectively. Similarly, [9] modeled the optimal placements of soft open points (SOPs) to enhance resilience against cyber attacks, where the second and third layers of their model once again represented line disconnections and network reconfiguration. The game-theoretical model by [5] not only considered immediate load recovery but also the longer-term restoration plan.

Though previous studies provide valuable insights into possible defense strategies against topology attacks in radially operated networks, to our knowledge, they have only modeled such attacks as single-time, simultaneous line disconnections. Since radial networks are well equipped to limit the spread of faults, the impact of sequential line disconnections (in which

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

multiple lines are disconnected over a period of time) is often overlooked compared to meshed networks. However, we argue that sequential attacks in radial networks are also a concern that should be addressed. First, it is realistic that the attacker may not perform all the attacks at once but instead launch attacks serially due to their available resources (such as cost, access options, and information). Second, the attacker may prefer to disconnect lines in waves, so that they can observe the operator's responses before launching successive attacks. This may induce the defender's actions in the middle that are not optimal at the end. Finally, sequential interactions may raise additional constraints for the operator, as frequent switching operations could shorten the lifespan of switches and potentially cause high surge voltages [10]. Therefore, a new game theoretical model that can represent the interactions across multiple rounds in the response stage is necessary.

In this study, we present an incident response game against topology attacks between the remote attacker and the grid operator in a radially operated MV distribution network.

- First, we propose a new and general mathematical model to represent multi-round, sequential interactions between the attacker and the defender. This general model further allows the user a high level of customization by parameterizing the number of rounds of attack and defense as well as constraints on their actions. Furthermore, the players' utilities to maximize can be defined by the user so that different objectives between the two players can be encoded, though we mainly focus on the load loss of the final topology state. The newly proposed game can help users analyze the resilience of the network against various capabilities of attacks and prepare for ever-increasing threats. While this game allows for the modeling of complex interactions that may occur in a realistic attack, it also raises the computational complexity for determining optimal solutions.
- Second, to overcome the computational challenge while providing a reasonable indication of the attack impact, we propose to translate the multi-round game into a simplified version called the associated single-round game, where the same number of total actions are replicated in one round. We mathematically prove the maximum loss of the attacker against the optimal defense in the single-round game is also achievable in the multi-round game; therefore, it is the lower bound of an optimal attack in the multi-round game.
- Third, we provide a case study of the sequential game on the IEEE 33-bus system and compare the solutions and computational results between the original multi-round game and the single-round game. The results show the tightness of the lower bound can be achieved (i.e., a better lower bound can only be achieved by different network structures and properties).

The remainder of the paper is organized as follows. Background for the game model is introduced in Section II. The sequential game is proposed in Section III. Then, its associated single-round game is described in Section IV and the theorem is proved. Section V presents the case study and simulation results. Finally, Section VI concludes the paper.

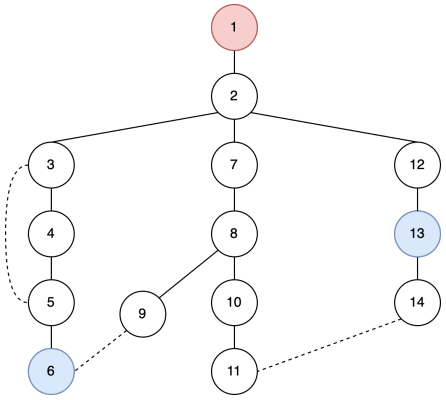

Fig. 1. Graph representation of an example network.

II. Network and Actor Models

A. Distribution Network Representation

The topology of a MV distribution network is represented as an undirected graph $G = (V, E)$ where the set of nodes V represents buses in the network, and the set of edges E represents the distribution lines. At least one node is assumed to be connected to the power grid, which acts as a power generator large enough to supply the total load of the network. Other nodes may also have generation by being connected to DGs. Each node in the network $x \in V$ has a power demand that should be met. Loads across the network are supplied by generation available in the network (by the grid or DGs) while adhering to the constraints described below.

In general, distribution lines are considered to be active. However, the NOPs, a subset of distribution lines in E, are inactive during normal operation [11]. Furthermore, the active distribution network is assumed to be connected and to have a radial structure during normal operation. After unplanned line disconnections, the network may separate into several connected components. To reduce load loss caused by such line disconnections, NOPs may be closed and hence added to the active network to reconnect the components. The operator may also leave them to operate independently using local power generation. In either case, it is assumed to keep the network radially operated, i.e., each component in the network is a tree. Additionally, to ensure safe operation of the network, the operators follow operational constraints at every time step. To model such constraints, we apply the Linearized DistFlow model as in [4].

Fig. 1 shows an example of the topology of a distribution network. Solid lines represent distribution lines that are normally operated, whereas the dotted lines represent NOPs. All nodes have loads to be met. Node 1 (in red) is connected to the power grid, and nodes 6 and 13 (in blue) are connected to DGs; hence, the three nodes have power generation. Note that there are no cycles when only considering the solid lines. Therefore, it is radially operated in normal conditions.

B. Attack & Defense Model

In this study, the attacker is assumed to perform breaker-jammer attacks [9], where the attacker disconnects a distribution line by manipulating the circuit breaker and jams the communication to the affected breaker such that the distribution line cannot be easily reconnected. The attacker's actions are modeled by removing these lines from the active network topology. Due to limited resources, levels of protection, and/or capabilities, the attacker actions may be restricted to a subset of lines, denoted $E^a \subset E$.

On the other hand, the defender may close NOPs to reduce power interruption to the consumers during the disturbance. While adhering to the operational and radiality constraints, the defender can close any NOPs, modeled as adding such lines to the active network. Hence, the action space of the defender is all NOPs in the network, denoted $E^d \subset E$.

C. Loss Function

Let $\mathbb{P}(G')$ be the set of constraints from the Linearized DistFlow model [4], along with the associated variables and parameters, given some active network topology $G' = (V, E')$. Then, the operator performs redispatch when a change in network topology occurs from player actions. The optimization problem given a (radial) network topology G' is shown as

$$l(G') = \min_{\mathbb{P}(G')} \sum_{x \in V} P_{shed,x}, \tag{1}$$

where the variable $P_{shed,x}$ is the lost load at bus x from the DistFlow constraints. The solution minimizes the sum of active power load loss that occurs across the network. The computed load loss will be used as the loss function to quantify the effectiveness of actions by both the attacker and the defender.

III. Game Model

In this section, we define the sequential game in which the two players take actions in an alternating manner, consisting of N rounds. The number of rounds represents the capabilities of the players, indicating how long the attack can last or until the attacker is neutralized. Prior to the physical attack, the attacker is assumed to be undetected by the defender. Thus, the attacker takes the initial move, followed by the defender's NOP connections. These actions are repeated N times.

A. Sequential Game

Given the full topology G, we define the sequential game.

Definition III.1. A sequential incident response game in the radially operated distribution network G that consists of two players has a tuple $\langle G, N, E^a, E^d, \mathbb{A}, \mathbb{D}, u_a, u_d, l \rangle$. The parameter N is the total number of rounds, and E^a and E^d are the action spaces of the attacker and the defender, respectively. $\mathbb{A}$ and $\mathbb{D}$ represent the set of constraints on the attacker and the defender actions. Functions u_a and u_d represent the utility functions of the attacker and the defender, respectively. The loss function l represents the loss caused by changes in the network topology and its operational constraints.

The utility functions can be derived from l and composed such that the objectives of the players are to maximize their utilities. Note that other effectiveness measures could be applied, though, in this study, we restrict ourselves to load loss caused (as in (1)) after every round. Given the above-defined game, the attacker and the defender construct their strategies.

B. Player Strategies & Action Constraints

The actions of the players are outputted by their probabilistic polynomial-time algorithms $\mathcal{A}$ and $\mathcal{D}$, which represent the attacker and defender strategies, respectively. At each round, the attacker is aware of all attacker and defender actions taken up to the previous round. As the follower, the defender observes all actions in the previous rounds, as well as the attacker's action in the current round. The algorithms are defined as the following for every round $1 \leq j \leq N$:

$$A_j \leftarrow \mathcal{A}(A_1, \ldots, A_{j-1}; D_1, \ldots, D_{j-1}), \text{ s.t. } \mathbb{A}, \tag{2}$$
$$D_j \leftarrow \mathcal{D}(A_1, \ldots, A_j; D_1, \ldots, D_{j-1}), \text{ s.t. } \mathbb{D}. \tag{3}$$

Here, A_j and D_j represent the actions taken by the players, where A_j is the set of lines disconnected at round j, and D_j is the set of NOPs connected. Note that because $\mathcal{A}$ is a probabilistic algorithm, the action A_j is selected from all possible actions with some probability given the previous actions of both players; similarly, D_j is selected by $\mathcal{D}$ in the same manner. These actions impact the topology of the active network, specifically the set of active edges in the topological graph. The attack A_j removes $(A_j \cap E^a)$ from the active lines at time j. The intersection with E^a ensures that the disconnected lines A_j are also in the attacker's action space. In contrary, D_j adds $(D_j \cap E^d) \setminus [(\bigcup_{i=1}^{j} A_i) \cap E^a]$ to the set of active lines at time j. The set of lines $(D_j \cap E^d)$ ensures that the lines closed by the defender are NOPs. Furthermore, any NOP that was attacked in previous time steps $[(\bigcup_{i=1}^{j} A_i) \cap E^a]$ cannot be connected by the defender.

To represent the topological changes over time, let us denote the active topology after round j as $G_j = (V, E_j)$, where the set of lines E_j represents the connected lines after round j. Recall that during initial operation, the distribution network is connected and operated radially while all NOPs are disconnected, i.e., $G_0 = (V, E \setminus E^d)$ is a tree. Given the initial state of the network and repeated disconnections and connections of lines at each round of attack and defense, by abuse of nation, we denote $E(A_1, \ldots, A_j, D_1, \ldots, D_j)$ as the set of active edges at time $j > 0$ as a function of action history:

$$\begin{aligned} E_j =& E(A_1, \ldots, A_j, D_1, \ldots, D_j) \\ =& \left[(E \setminus E^d) \cup \left((\bigcup_{i=1}^{j} D_i) \cap E^d \right) \right] \setminus \left[(\bigcup_{i=1}^{j} A_i) \cap E^a \right]. \end{aligned} \tag{4}$$

It can be seen from (4) that attacked lines are removed from the union of originally active lines and NOPs closed by the defender up to round j. If an NOP is disconnected by the attacker (given that E^a contains NOPs), the line is considered to be inactive for the rest of the game, whether the NOP line is connected by the defender in the previous rounds or not.

The set of constraints $\mathbb{A}$ and $\mathbb{D}$, which are to be complied with at every round, represents the capabilities of the players. These constraints can be adjusted according to the type of attacker or defender to the designer's preferences, but certain constraints are assumed to always be included. One such constraint in $\mathbb{A}$ is that the attacker always disconnects at least one line at every round, such that there is no empty attack. Additionally, the attacker may be limited in the number of disconnections in each round. Hence, $\mathbb{A}$ includes the following:

$$1 \leq |A_j| \leq r_j^a, \quad \forall j \in \{1, \ldots, N\}, \tag{5}$$

where r_j^a is the maximum number of line disconnection by the attacker at round j. Finally, the attacker can only disconnect lines that are in its action space E^a. However, such a constraint is not included in $\mathbb{A}$, as any line selected outside of E^a will not affect the topology, as shown in (4).

An important and compulsory constraint for the defender is the radiality constraint. It has to be satisfied at every round, and hence, the following constraint is included in $\mathbb{D}$:

$$G_j = (V, E_j) \text{ is a forest}, \quad \forall j \in \{1, \ldots, N\}, \tag{6}$$

where E_j is defined by (4). Furthermore, the defender's capability may be limited by the number of NOPs that can be closed in each round. Hence $\mathbb{D}$ also includes the following:

$$|D_j| \leq r_j^d, \quad \forall j \in \{1, \ldots, N\}, \tag{7}$$

where r_j^d is the maximum number of NOPs the defender can connect at round j.

C. Utility Functions and Optimization Problem

For the sake of readability, let us denote $G_j(\mathcal{A}, \mathcal{D})$ for graph $G_j = (V, E_j)$ as a function of $\mathcal{A}$ and $\mathcal{D}$ after round j, where E_j is given as (4). Suppose the defender is assumed to have a singular objective of achieving the smallest load loss at the end of the game. In that case, the defender minimizes the expression $\mathbb{E}[l(G_N(\mathcal{A}, \mathcal{D}))]$ given the developing knowledge about the attacker strategy $\mathcal{A}$. Since the output of $\mathcal{A}$ and $\mathcal{D}$ is considered to be probabilistic, the defender minimizes the expectation over coin flips in $\mathcal{A}$ and $\mathcal{D}$ for probabilistic actions. (Note that probabilistic algorithms do not exclude deterministic outputs. The reader can refer to [12] for details on probabilistic algorithms.) On the other hand, the attacker may want to maximize the loss at the end of the game against the defender, especially against one that minimizes the loss. This results in an optimization problem for the attacker defined by a max-min expression, which we denote as

$$\boxed{\max_{\mathcal{A}}} \boxed{\min_{D}} \mathbb{E}\big[l(G_N(\mathcal{A}, \mathcal{D}))\big] \tag{8}$$

over coin flips. Note that while $\mathcal{A}$ and $\mathcal{D}$ represent separate sequences in (8), in reality, they cannot be optimized successively as the optimal actions of the defender are dependent on the attacker's actions and vice versa. In this paper, we simplify the notation as stated in (8) to represent that the attacker aims to maximize the expected loss given that the defender chooses its actions to minimize the load loss. We denote $\boxed{\max}$ and $\boxed{\min}$ for maximizing and minimizing their strategies, to differentiate them from the classical maxima and minima of a function or a set.

If the players' objectives are determined solely by the loss associated with the final active topology, the defender may prefer to wait until the last round to take actions (if the constraints allow) in order to minimize the loss, having observed the attacker's full set of actions beforehand, i.e., the operator waits to respond until it is confirmed that the attacker has been neutralized and can no longer disconnect additional lines. More generally, however, the defender may want to minimize the loss across different times. For example, consider a scenario in which each round of the game represents a time. In such a case, minimizing loss at an earlier time may be preferred. The attacker may also have variations in their preference as to when a large loss should occur, also considering the defender's (cyber) security capabilities. In order to take into account different preferences, we define two utility functions of the defender and the attacker, u_d and u_a in N variables,

$$u_d \in \mathbb{R}^N \to \mathbb{R} \text{ and } u_a \in \mathbb{R}^N \to \mathbb{R}. \tag{9}$$

The utilities take the loss at each time step as inputs. Both players aim to maximize the utilities, and given that both $\mathcal{A}$ and $\mathcal{D}$ are probabilistic, the optimization problems of the players are defined as

$$\boxed{\max_{\mathcal{D}}} \mathbb{E}\big[u_d\big(l(G_1(\mathcal{A}, \mathcal{D})), \ldots, l(G_N(\mathcal{A}, \mathcal{D}))\big)\big], \tag{10}$$

$$\boxed{\max_{\mathcal{A}}} \mathbb{E}\big[u_a\big(l(G_1(\mathcal{A}, \mathcal{D})), \ldots, l(G_N(\mathcal{A}, \mathcal{D}))\big)\big]. \tag{11}$$

The exact formulations of the utility functions may be up to the design and capabilities of the players. We do, however, assume that the utility of the attacker increases with the loss, whereas the utility of the defender decreases. Generalized definitions of utilities as in (9) allow the modeling of separate objectives between the players, which can result in a representation of more complex optimization problems.

While we have defined the algorithms $\mathcal{A}$ and $\mathcal{D}$ as probabilistic, the following property can be proven.

Lemma III.1. *If a player's probabilistic strategy maximizes its utility given the opponent's strategy in the game (Def. III.1), then there is a deterministic strategy that also achieves the maximum utility against the same opponent strategy.*

The proof is provided in Appendix A. Essentially, Lemma III.1 indicates that a best response to the opponent's strategy can be found from the set of deterministic strategies. Therefore, we restrict both the defender's and attacker's strategies to be deterministic in the rest of the paper, which reduces the computational complexity of determining an optimal strategy (with the knowledge of the opponent). Given deterministic strategies, we can drop the expectation from optimization problems of the defender and the attacker in (10)

and (11), and hence:

$$\boxed{\max_{\mathcal{D}}}\big[u_d\big(l(G_1(\mathcal{A},\mathcal{D})),\ldots,l(G_N(\mathcal{A},\mathcal{D}))\big)\big], \quad (12)$$

$$\boxed{\max_{\mathcal{A}}}\big[u_a\big(l(G_1(\mathcal{A},\mathcal{D})),\ldots,l(G_N(\mathcal{A},\mathcal{D}))\big)\big]. \quad (13)$$

Similarly, the max-min expression in (8) can also drop the expectation when limiting to deterministic strategies. This expression is the maximum final loss achievable by the attacker against a defender that also minimizes the final loss, which we denote as *maximin loss*. Given that strategies are deterministic, we formally define the maximin loss as the following.

Definition III.2. The maximin loss of an N-round sequential game is the largest final loss (after N rounds) achievable by the attacker, while the defender also minimizes the final loss. Mathematically, the maximin loss is denoted as

$$\boxed{\max_{\mathcal{A}}}\boxed{\min_{\mathcal{D}}} l(G_N(\mathcal{A},\mathcal{D})) \quad (14)$$
$$= \max_{A_1}\min_{D_1}\ldots\max_{A_N}\min_{D_N} l\big((V,E(A_1,\ldots,A_N,D_1,\ldots,D_N))\big),$$

with the set of active lines at the end of the game derived from (4) given the action history. The attacker and defender actions are restricted by their sets of constraints $\mathbb{A}$ and $\mathbb{D}$, respectively.

Note that if both players' utilities are defined strictly by the final loss, i.e.,

$$u_a\big(l(G_1(\mathcal{A},\mathcal{D})),\ldots,l(G_N(\mathcal{A},\mathcal{D}))\big) = l(G_N(\mathcal{A},\mathcal{D})) \text{ and} \quad (15)$$

$$u_d\big(l(G_1(\mathcal{A},\mathcal{D})),\ldots,l(G_N(\mathcal{A},\mathcal{D}))\big) = -l(G_N(\mathcal{A},\mathcal{D})), \quad (16)$$

then the optimization problem can be defined as (14). Hence, the maximin loss is used as a measurement of the attacker's capability in inducing loss against an optimal defender.

IV. Associated Single-Round Game

While a multi-round sequential game may allow for modeling more realistic and complex interactions between the actors, it also increases the computation required to find the optimal strategies with the network size and the number of rounds. Here, we provide a simplified game model that helps to reduce the computation while providing a meaningful analysis of the original multi-round game. Essentially, the simplified game models all the actions taken by a player during N-rounds into a single-round action. By doing so, the player actions' sequential relationship is ignored. We denote such a model as the *associated single-round game* of the N-round sequential game. Formally, it is defined as the following for any sequential game with $N > 1$.

Definition IV.1. The associated single-round game of a sequential game $\langle G, N, E^a, E^d, \mathbb{A}, \mathbb{D}, u_a, u_d, l\rangle$ is defined by a tuple $\langle G, 1, E^a, E^d, \mathbb{A}^{one}, \mathbb{D}^{one}, u_a^{one}, u_d^{one}, l\rangle$, where the network topology G and attacker and defender action spaces E^a and E^d are equivalent to the original sequential game. The sets of constraints $\mathbb{A}^{one}$ and $\mathbb{D}^{one}$ are related to $\mathbb{A}$ and $\mathbb{D}$ of the N-round game, as they have the same limit on the total number of line (dis)connections. Hence, constraint (5) in $\mathbb{A}$ is defined in $\mathbb{A}^{one}$ as

$$N \le |A_j^{one}| \le \sum_{j=1}^{N} r_j^a. \quad (17)$$

The defender's constraint is similarly defined in $\mathbb{D}^{one}$ with constraint (7) in $\mathbb{D}$ (without a constraint on minimum number of NOP connections). The utility functions of the attacker and the defender in the single-round game, u_a^{one} and u_d^{one}, are only dependent on the final loss of the game as it only considers one sequence of attack and defense. Given the set of attacked lines A_1^{one} and the set of closed NOP lines D_1^{one} after one (and the only) round, the utilities of the players are defined as

$$u_a^{one} = l\big((V,E(A_1^{one},D_1^{one}))\big), \quad (18)$$

$$u_d^{one} = -l\big((V,E(A_1^{one},D_1^{one}))\big). \quad (19)$$

Note that since we assume utilities are derived from l, (18) and (19) are the only possible choices of utility functions in the single-round game. A (deterministic) attacker algorithm in the associated game, denoted as $\mathcal{A}^{one}$, outputs a set of lines A_1^{one} to be disconnected from E^a, given no prior knowledge. A defender algorithm $\mathcal{D}^{one}$ then outputs a set of NOPs D_1^{one} to be connected from E^d given the attacker's action A_1^{one}.

Fig. 2 illustrates the interactions of players in the N-round game and its associated single-round game. It can be seen that the total line disconnections and NOP connections are equivalent in both games. Since the defender can observe the complete attacking lines in the single-round game, it has greater capabilities than in the N-round game, and therefore, we show in the below theorem that the maximin loss of the single-round game is at most the maximin loss of the N-round game. However, we also show that there is an attacker strategy in the N-round game that is guaranteed to achieve single-round maximin loss.

Theorem IV.1. *Consider an N-round sequential game $\langle G, N, E^a, E^d, \mathbb{A}, \mathbb{D}, u_a, u_d, l\rangle$ with $N > 1$ and utility functions u_a and u_d derived from a loss function l, defined as* (15) *and* (16) *respectively. Then, the maximin loss achieved by player strategies $\mathcal{A}^{one}$ and $\mathcal{D}^{one}$ in the associated single-round game $\langle G, 1, E^a, E^d, \mathbb{A}^{one}, \mathbb{D}^{one}, u_a^{one}, u_d^{one}, l\rangle$ (Definition IV.1) can at least be achieved by the attacker in the N-round game (lower-bound load loss).*

For the detailed proof, the reader may refer to Appendix B. Theorem IV.1 shows that the single-round game's maximin loss can indicate an optimal attacker's capability in sequential interactions. The use of a single-round game can improve the computational efficiency for determining a pair of opponent strategies that achieves the maximin loss compared to the N-round game, especially as N increases. Note that we have strictly looked at maximizing/minimizing the final loss, not the utilities of the players. However, utility functions are possibly derived from the loss function, and hence, the maximin loss can still provide valuable insights on potential strategies.

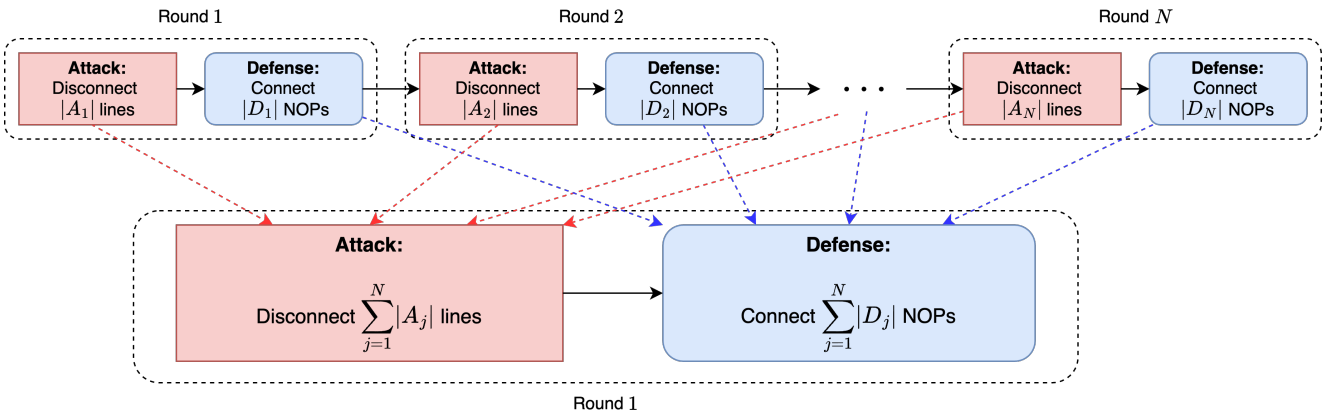

Fig. 2. Comparison of the sequential N-round game and its associated single-round game.

V. Case Study

A. Setup

To simulate the N-round game and compare the results with its associated single-round game, the modified IEEE 33-bus system from [4] was adopted. The network contained 32 normally operating distribution lines and 5 NOPs. The total active load of the network was 3.715 MW. The 5 controllable distributed generators connected to the network had a maximum capacity of 0.6 MW each.

For the case study, N was set to 3. The attacker's action space E^a was restricted to normally operating lines except for one line that connects the power grid to the rest of the network. In this game, the attacker was limited to 1 line disconnection per round. The defender was also constrained to at most 1 NOP connection at each round, while satisfying the radiality. The objective of the attacker was to maximize the loss of the final topology, whereas the defender's objective was to minimize the final loss. As intermediate losses were ignored, the maximin loss (Definition III.2) was the final loss achieved when both players took optimal actions. Its associated single-round game allowed at most 3 line disconnections by the attacker and 3 NOP connections by the defender in one round.

All of the experimental code was written in Python (version 3.10.13). The electrical network data was loaded from pandapower [13] (version 2.10.13), and DistFlow constraints and its optimization problem was modeled using CVXPY [14] (version 1.4.1) and GLPK-MI solver for determining the load loss. The network's radiality was verified with a depth-first search algorithm from NetworkX [15] (version 3.2.1).

B. Results

In the N-round game described above, the maximin loss of 0.745 MW was achieved by the attacker, which was about 20% of the total load. In total, there were 84 action sequences that resulted in the maximin loss at the end. Fig. 3 shows the intermediate losses (after each action) of one sequence that obtained the maximin loss. It can be seen that after the attacker's first and second disconnections, the defender is able to recover the lost load by closing the NOPs. After the attacker's third disconnection, however, the defender has no NOP that can recover the lost load.

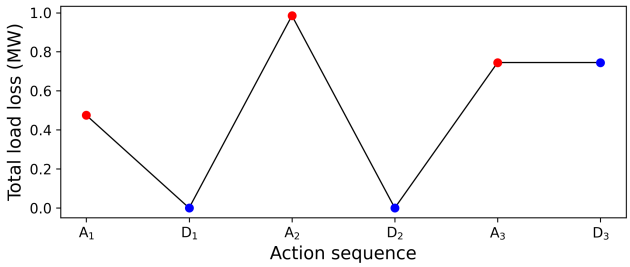

Fig. 3. Intermediate losses of the 3-round game achieving the maximin loss.

Table I shows the comparison of maximin loss values and the computational results between the N-round game and its associated single-round game. It can be seen that the single-round game resulted in the same maximin loss, indicating a tight bound can be attained. The total number of computations, on the other hand, shows a significant difference. In Table I, the number of scenarios indicates the number of possible combinations of two players' action histories. The number of possible sequences in the N-round game is significantly larger than in the single-round game. However, loss computation (which is the bottleneck of computation) is unnecessary for all sequences, as the radiality constraint not being satisfied in at least one round is considered an invalid defense. Therefore, the actual number of loss evaluations was also counted and is shown in Table I. The N-round game required over 15 times more loss computations compared to the single-round game, once again showing the efficiency of the simplified game.

TABLE I
Maximin Loss Values and Computational Results

	Loss (MW)	Scenarios	Loss Eval.
N- Round	0.745	3,667,920	756,957
Single-Round	0.745	116,870	49,472

VI. Conclusion

In this study, we introduced a new and generalized game-theoretical model on topology attacks in a radially operated distribution network. The proposed game was able to incorporate multiple stages of attacks and responses by modeling sequential interactions between the actors. To counter the large computation required to determine the optimal solution, we also proposed the associated single-round game to model the multi-round interactions into a single round. The results showed that the single-round game was able to significantly reduce the potential outcomes of the game, presenting an example case of a tight lower bound. This means that we need to restrict ourselves to a subset of network structures/graphs defined by some properties in order to improve the lower bound. This is left for future research. Another important future work will be to demonstrate the lower bound for more generalized utility functions beyond the final load loss.

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] J. Kim and L. Tong, "On topology attack of a smart grid: Undetectable attacks and countermeasures," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1294–1305, 2013.

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

[4] 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.

[5] W. Ji, T. Tu, and N. Ma, "A novel defender-attacker-defender model for resilient distributed generator planning with network reconfiguration and demand response," *Energy Engin.*, vol. 121, no. 5, pp. 1223–1243, 2024.

[6] 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.

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

[8] T. Zhao, B. Chen, S. Zhao, J. Wang, and X. Lu, "A flexible operation of distributed generation in distribution networks with dynamic boundaries," *IEEE Trans. Power Syst.*, vol. 35, no. 5, pp. 4127–4130, 2020.

[9] 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.

[10] C. Wang, K. Pang, M. Shahidehpour, F. Wen, and S. Duan, "Two-stage robust design of resilient active distribution networks considering random tie line outages and outage propagation," *IEEE Trans. Smart Grid*, vol. 14, no. 4, pp. 2630–2644, 2023.

[11] 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.

[12] R. Motwani and P. Raghavan, *Randomized Algorithms*. Cambridge University Press, 1995.

[13] L. Thurner, A. Scheidler, F. Schäfer, J. Menke, J. Dollichon, F. Meier, S. Meinecke, and M. Braun, "pandapower – an open-source python tool for convenient modeling, analysis, and optimization of electric power systems," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6510–6521, Nov 2018.

[14] 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.

[15] 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.*, G. Varoquaux, T. Vaught, and J. Millman, Eds., Pasadena, CA USA, 2008, pp. 11 – 15.

[16] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.

Appendix A
Proof of Lemma III.1

Proof. Let be given that $\mathcal{A}^*$ is a probabilistic attack strategy that maximizes the expected utility according to a certain utility function u_a against a (probabilistic) defense strategy $\mathcal{D}$. If $\mathcal{A}^*$ has multiple lines assigned a non-zero probability as its action A_j at time j given a history of actions $(A_1, D_1, \ldots, A_{j-1}, D_{j-1})$, then the expected utility of choosing any of the lines with non-zero probability must be the same (since if that is not the case, $\mathcal{A}^*$ is not optimal as selecting a line with the highest expected utility with 100% probability yields a higher expected utility than $\mathcal{A}^*$). Therefore, swapping the probabilistic action to the deterministic action of selecting any of the lines that are assigned non-zero probability is also an optimal strategy. We can make the same argument for any other history at time j, and subsequently for any time j. Therefore, if there is an optimal probabilistic attack strategy that maximizes the expected utility against a defense strategy, there is also an optimal deterministic attack strategy with the same expected utility against the same defense strategy. We make the same reasoning for the defender strategy. □

Appendix B
Proof of Theorem IV.1

Proof. Consider attack and defense strategies $\mathcal{A}$ and $\mathcal{D}$ in an N-round sequential game $\langle G, N, E^a, E^d, \mathbb{A}, \mathbb{D}, u_a, u_d, l\rangle$, with its maximin loss defined as (14). By repeatedly applying the max-min inequality [16] to a pair of adjacent maxima and minima in (14), the following inequality can be derived:

$$
\begin{aligned}
&\boxed{\max_{\mathcal{A}}}\boxed{\min_{\mathcal{D}}} l(G_N(\mathcal{A},\mathcal{D})) \\
&= \max_{A_1}\min_{D_1}\max_{A_2}\min_{D_2}\ldots\max_{A_N}\min_{D_N} l\big((V, E(A_1,\ldots,A_N,D_1,\ldots,D_N))\big) \\
&\geq \max_{A_1}\ldots\max_{A_N}\min_{D_1}\ldots\min_{D_N} l\big((V, E(A_1,\ldots,A_N,D_1,\ldots,D_N))\big) \\
&= \max_{A_1,\ldots,A_N}\min_{D_1,\ldots,D_N} l\big((V, E(A_1,\ldots,A_N,D_1,\ldots,D_N))\big). \qquad (20)
\end{aligned}
$$

Intuitively, the right-hand side of expression (20) represents a scenario in which the attacker optimizes the full sequence of attacks $(A_1, \ldots, A_N)$ against a defender that minimizes the final loss by selecting defense sequence $(D_1, \ldots, D_N)$ after having observed the attacker's sequence. In such a case (where each player's full action sequence is optimized at once), the loss is at most as large as the maximin loss of the N-round game on the left-hand side of (20). Though the order of the optimization is changed, it will not impact whether all constraints in $\mathbb{A}$ and $\mathbb{D}$ are satisfied. First, the attacker's constraints are independent of the defender's actions, and hence the full attack sequence can be selected without violating any constraints in $\mathbb{A}$. Next, the defender's set of constraints $\mathbb{D}$ contains the radiality constraints for each round

which are dependent on the attacker's past actions. However, since the full attack sequence is known, the defender can construct the defender action D_j at each round j without violating the radiality. Now, take any deterministic attack strategy $\overline{\mathcal{A}}$ in the N-round game. Naturally, we have the following inequality:

$$\begin{aligned}&\max_{A_1,\ldots,A_N}\min_{D_1,\ldots,D_N} l\big((V,E(A_1,\ldots,A_N,D_1,\ldots,D_N))\big)\\&\geq \min_{D_1,\ldots,D_N} l\big((V,E(\overline{A}_1,\ldots,\overline{A}_N,D_1,\ldots,D_N))\big).\end{aligned} \tag{21}$$

Next, we will show that an attack strategy in the N-round game that achieves the maximin loss of the associated single-round game can be realized. From Definition III.2, the maximin loss of the associated single-round game $\langle G,1,E^a,E^d,\mathbb{A}^{one},\mathbb{D}^{one},u_a^{one},u_d^{one},l\rangle$ is given as

$$\boxed{\max_{\mathcal{A}^{one}}}\boxed{\min_{\mathcal{D}^{one}}} l(G_1(\mathcal{A}^{one},\mathcal{D}^{one})) = \max_{A_1^{one}}\min_{D_1^{one}} l\big((V,E(A_1^{one},D_1^{one}))\big), \tag{22}$$

where A_1^{one} and D_1^{one} are subject to $\mathbb{A}^{one}$ and $\mathbb{D}^{one}$, respectively. The final active topology $(V,E(A_1^{one},D_1^{one}))$ used for computing the loss is dependent on the actions of the two players. Similarly to the N-round game, the set of active edges after the game can be derived using (4). Given an attacker action A_1^{one} and defender action D_1^{one}, the set of edges after the single-round game is

$$E(A_1^{one},D_1^{one}) = \Big[(E\setminus E^d)\cup(D_1^{one}\cap E^d)\Big]\setminus\Big[A_1^{one}\cap E^a\Big]. \tag{23}$$

Now, let us denote a pair of deterministic attacker and defender actions in the associated single-round game that achieves the maximin loss as A_1^{one*} and D_1^{one*}, i.e.,

$$l\big((V,E(A_1^{one*},D_1^{one*}))\big) = \boxed{\max_{\mathcal{A}^{one}}}\boxed{\min_{\mathcal{D}^{one}}} l(G_1(\mathcal{A}^{one},\mathcal{D}^{one})). \tag{24}$$

Given this, we can construct an attack strategy in the N-round game that disconnects the same lines as in A_1^{one*} by the end of the game. Let us denote such a strategy in the N-round game as $\overline{\mathcal{A}}$ with the following properties:

$$\overline{A}_i \subset A_1^{one*}, \quad \forall i\in\{1,\ldots,N\}, \text{ and} \tag{25}$$

$$\bigcup_{i=1}^{N}\overline{A}_i = A_1^{one*}. \tag{26}$$

Since the N-round and the single-round games share the same maximum (and minimum) line disconnections in the game (as shown in (17)), $\overline{\mathcal{A}}$ can be constructed without violating constraint (5) in $\mathbb{A}$, and therefore, it is a valid attack strategy in the N-round game.

Given $\overline{\mathcal{A}}$ above, the guaranteed final loss achievable by the attacker (against a defender that minimizes the final loss) can be obtained. By substituting (4) for the final topology and (26) for the attacker's disconnected lines during N rounds, the loss is derived as

$$\begin{aligned}&\min_{D_1,\ldots,D_N} l\big((V,E(\overline{A}_1,\ldots,\overline{A}_N,D_1,\ldots,D_N))\big) \qquad (27)\\&= \min_{D_1,\ldots,D_N} l\Big((V,\Big[(E\setminus E^d)\cup((\bigcup_{i=1}^{N}D_i)\cap E^d)\Big]\setminus\Big[(\bigcup_{i=1}^{N}\overline{A}_i)\cap E^a\Big]\Big)\Big)\\&= \min_{D_1,\ldots,D_N} l\Big((V,\Big[(E\setminus E^d)\cup((\bigcup_{i=1}^{N}D_i)\cap E^d)\Big]\setminus\Big[A_1^{one*}\cap E^a\Big]\Big)\Big).\end{aligned}$$

Since both the N-round game and its associated single-round game have the same maximum number of NOP closings by the defender, we can see that the optimal set of NOP connections to minimize the final loss against such an attack is to connect all NOPs in D_1^{one*}. In the N-round game, however, the radiality constraint (6) has to be satisfied at every round, not only at the end. Given the additional restrictions in the N-round game for the defender due to the radiality constraint and maximum number constraint on every round, the defender may not be able to connect all NOPs in D_1^{one*} in the N-round game. Therefore, a set of NOPs connecting D_1^{one*} is a lower-bound loss in the sequential game, as no set of closed NOPs in the N-round game $(\bigcup_{i=1}^{N}D_i)$ can achieve smaller loss than D_1^{one*} against the attack A_1^{one*}. This is the case for any pair of attacker and defender actions that achieves the maximin loss in the single-round game. Hence, we can derive the following inequality:

$$\begin{aligned}&\min_{D_1,\ldots,D_N} l\Big((V,\Big[(E\setminus E^d)\cup((\bigcup_{i=1}^{N}D_i)\cap E^d)\Big]\setminus\Big[(\bigcup_{i=1}^{N}\overline{A}_i)\cap E^a\Big]\Big)\Big)\\&\geq l\Big((V,\Big[(E\setminus E^d)\cup(D_1^{one*}\cap E^d)\Big]\setminus\Big[A_1^{one*}\cap E^a\Big]\Big)\Big)\\&= \boxed{\max_{\mathcal{A}^{one}}}\boxed{\min_{\mathcal{D}^{one}}} l(G_1(\mathcal{A}^{one},\mathcal{D}^{one})).\end{aligned} \tag{28}$$

Note that the left-hand side of the expression is subject to $\mathbb{D}$, including the radiality constraint on every round, whereas the right-hand side is subject to $\mathbb{A}^{one}$ and $\mathbb{D}^{one}$.

Finally, from (20), (21), (27), and (28), we can derive that

$$\begin{aligned}&\boxed{\max_{\mathcal{A}}}\boxed{\min_{\mathcal{D}}} l(G_N(\mathcal{A},\mathcal{D}))\\&\geq \max_{A_1,\ldots,A_N}\min_{D_1,\ldots,D_N} l\big((V,E(A_1,\ldots,A_N,D_1,\ldots,D_N))\big)\\&\geq \min_{D_1,\ldots,D_N} l\big((V,E(\overline{A}_1,\ldots,\overline{A}_N,D_1,\ldots,D_N))\big)\\&\geq \boxed{\max_{\mathcal{A}^{one}}}\boxed{\min_{\mathcal{D}^{one}}} l(G_1(\mathcal{A}^{one},\mathcal{D}^{one})),\end{aligned} \tag{29}$$

showing that the maximin loss of the associated single-round game is the lower bound to the maximin loss of the original N-round game. □