2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Robust and Scalable Game-theoretic Security Investment Methods for Voltage Stability of Power Systems

Lu An, Pratishtha Shukla, Aranya Chakrabortty, and Alexandra Duel-Hallen

Abstract— **We develop investment approaches to secure electric power systems against load attacks where a malicious intruder (the attacker) covertly changes reactive power setpoints of loads to push the grid towards voltage instability while the system operator (the defender) employs reactive power compensation (RPC) to prevent instability. Extending our previously reported Stackelberg game formulation for this problem, we develop a robust-defense sequential algorithm and a novel genetic algorithm that provides scalability to large-scale power system models. The proposed methods are validated using IEEE prototype power system models with time-varying load uncertainties, demonstrating that reliable and robust defense is feasible unless the operator's RPC investment resources are severely limited relative to the attacker's resources.**

Index Terms— **Power Systems, Voltage stability, Load attacks, Game Theory, Security investment, Robust defense**

I. Introduction

Over the past decade, significant research has been performed on cybersecurity of electric power systems [1], including security against various kinds of attacks on both generation and loads. With the proliferation of demand response and direct load control programs by utility companies across the United States, load attacks are becoming more common. Malicious attackers, for instance, can easily hack into the thermostats of domestic customers and covertly change their active and reactive power setpoints. When a large number of loads are manipulated in this way, the transmission grid can face a voltage collapse. In the literature so far, these attacks have mostly been studied from the point of view of detection and control [2]. Our objective in this paper is to formulate a RPC investment strategy that power system operators can adopt to secure the grid from this class of attacks, which may result in severe degradation of voltage stability [3].

Game-theoretic methods, including Stackelberg games, have been widely applied to study security and optimization for wide ranges of cyber-physical systems, including power systems [4]. However, most game-theoretic investment approaches employ repeated games [4], which are not suitable when long-term, fixed security investment is desired. To address this issue, in [5] we developed a cost-based Stackelberg game (CBSG) to strategically allocate the players' long-term security investment resources. The cost-based Stackelberg equilibrium (CBSE) of this game not only optimizes the load attacker's and the system operator's payoffs, i.e., the increase and reduction of the voltage instability index [3], respectively, but also saves their costs.

However, in [5] we assumed complete knowledge of the opponent's resources, which is idealistic for the defender, who acts first. In this paper, we develop and validate a robust-defense (i.e. robust-RPC) sequential method. Moreover, we assumed fixed values of constant-power loads in [5] while in this paper we consider a practical case of *time-varying* loads. Finally, the algorithm in [5] requires traversal search that has exponential complexity in the number of target loads. To address scalability of the CBSG, we develop an iterative, evolutionary, bidirectional, genetic algorithm (GA)-based method to find a CBSE, which improves upon previously investigated evolutionary methods for finding a Stackelberg equilibrium (SE) [6], [7] by utilizing parallel evolution for both players. We evaluate performance of the proposed methods on IEEE 9-bus and 39-bus power system models and show that reliable and robust defense is feasible unless the operator's RPC investment resources are severely limited relative to the load attacker's resources.

The rest of the paper is organized as follows. Section II summarizes the power system and the CBSG based on [5]. A bidirectional evolutionary algorithm is introduced in Section III. A robust-defense method is proposed in Section IV. Numerical results for IEEE prototype models are contained in Section V, and Section VI concludes the paper.

II. Power System Model and Cost-based Stackelberg Game

We consider a power system with $G \geq 1$ generators and $K \geq 1$ constant power loads, where the load buses are indexed as the first K buses, followed by G generator buses. Let us denote the steady-state voltage magnitudes at the load buses as $\boldsymbol{V}_L = [V_1, \cdots, V_K] \in \mathbb{R}^K$ and at the generator buses as $\boldsymbol{V}_G = [V_{K+1}, \cdots, V_{K+G}] \in \mathbb{R}^G$. The admittance matrix of the network is denoted as $\boldsymbol{Y} = \boldsymbol{G} + j\boldsymbol{B}$. We partition the susceptance matrix $\boldsymbol{B} \in \mathbb{R}^{(K+G)\times(K+G)}$ into four block matrices as

$$\boldsymbol{B} = \begin{pmatrix} \boldsymbol{B}_{LL} & \boldsymbol{B}_{LG} \\ \boldsymbol{B}_{GL} & \boldsymbol{B}_{GG} \end{pmatrix} \tag{1}$$

where $\boldsymbol{B}_{LL}$ contains the interconnections among loads and $\boldsymbol{B}_{LG} = \boldsymbol{B}_{GL}{}^T$ represents the interconnections between loads and generators. Following the derivations in [3], one can then define the open-circuit load voltage vector as $\boldsymbol{V}_L^* = -\boldsymbol{B}_{LL}^{-1}\boldsymbol{B}_{LG}\boldsymbol{V}_G$, and, subsequently, the symmetric stiffness matrix as

$$\boldsymbol{Q}_{crit} \triangleq \frac{1}{4}\mathrm{diag}(\boldsymbol{V}_L^*) \cdot \boldsymbol{B}_{LL} \cdot \mathrm{diag}(\boldsymbol{V}_L^*), \tag{2}$$

Dr. Lu An is with NVIDIA Corporation. Dr. Pratishtha Shukla is with Oak Ridge National Lab. Dr. Aranya Chakrabortty and Dr. Alexandra Duel-Hallen are with ECE Department, North Carolina State University. (e-mail: lan4@alumni.ncsu.edu, pshukla@alumni.ncsu.edu, achakra2@ncsu.edu, sasha@ncsu.edu)

979-8-3503-0123-6/23/$31.00 ©2023 IEEE

TABLE I

CBSG DESCRIPTION BASED ON [5]

Term	Definition
$\boldsymbol{a} = [a_k : k \in \{1, \cdots, K\}] \in \mathbb{R}^K$	Actions of the load attacker
$a_k \in \{0, 1/(L_a-1), 2/(L_a-1), \cdots, 1\}$	Attacker's investment level on load k (chance of success)
L_a	The number of attacker's investment levels
$q_a^k \leq q_a^{k,\max}, \forall k$	Covertness constraint for the attacker on load k
$\boldsymbol{O}^j = [o_1^j, \cdots, o_k^j, \cdots, o_K^j], \forall j = 1, \cdots, 2^K$	The j^{th} outcome of attack at all loads
$P_{\boldsymbol{a}}(\boldsymbol{O}^j) = \prod_{k:\forall o_k^j = 1} a_k \prod_{k:\forall o_k^j = 0} (1 - a_k)$	The probability of outcome $\boldsymbol{O}^j$
$\boldsymbol{q}_a^j = \boldsymbol{O}^j \odot \boldsymbol{q}_a$	The incremental reactive power demand for $\boldsymbol{O}^j$
γ_a	The scaled cost of the attack on load k at full effort level
$C_a = \gamma_a \|\|\boldsymbol{a}\|\|_1 \leq 1$	The total cost of the attacker
$\boldsymbol{d} = [d_k : k \in \{1, \cdots, K\}] \in \mathbb{R}^K$	RPC actions of the defender
$d_k \in \{0, 1/(L_d-1), 2/(L_d-1), \cdots, 1\}, \forall k \in \mathscr{L}_{ctrl}$	Defender's investment (RPC) level on the control device of load k
L_d	The number of defender's investment levels
$q_d^{k,\max}$	The maximum reactive power the defender can compensate on load $k \in \mathscr{L}_{ctrl}$
$q_d^k = d_k q_d^{k,\max}$	The defender's compensation on load $k \in \mathscr{L}_{ctrl}$
γ_d	The scaled investment cost of RPC per protected load
$C_d = \gamma_d \|\|\boldsymbol{d}\|\|_1 \leq 1$	The defender's total investment cost
$\boldsymbol{Q}_L^j = \boldsymbol{Q}_L^n + \boldsymbol{q}_a^j - \boldsymbol{q}_d$	Tthe reactive power demand vector for the j^{th} outcome $\boldsymbol{O}^j$ given actions $\boldsymbol{a}$ and $\boldsymbol{d}$
$U_j(\boldsymbol{q}_a^j, \boldsymbol{q}_d) = Clip\left(\left\|\boldsymbol{Q}_{crit}^{-1}\boldsymbol{Q}_L^j\right\|_\infty ; (\Delta^n, 1)\right)$	The voltage instability index (3) restricted to $[\Delta^n, 1]$ for the j^{th} outcome $\boldsymbol{O}^j$ and actions $\boldsymbol{a}$, $\boldsymbol{d}$
$U^a(\boldsymbol{a}, \boldsymbol{d}) = \sum_j^{2^K} P_{\boldsymbol{a}}(\boldsymbol{O}^j) U_j(\boldsymbol{q}_a^j, \boldsymbol{q}_d)$	The attacker's expected utility given actions $\boldsymbol{a}$ and $\boldsymbol{d}$
$U^d(\boldsymbol{a}, \boldsymbol{d}) = -U^a(\boldsymbol{a}, \boldsymbol{d})$	The defender's utility given actions $\boldsymbol{a}$ and $\boldsymbol{d}$
$(\boldsymbol{a}_o^*, \boldsymbol{d}_o^*)$	Cost-based Stackelberg equilibrium (CBSE)

where $\operatorname{diag}(\cdot)$ denotes the diagonal matrix.

Let $\boldsymbol{Q}_L = [Q_1, \cdots, Q_K] \in \mathbb{R}^K$ denote the K-dimensional real vector that represents the *reactive power setpoints* at the load buses. Using (2), the *voltage instability index* of the system is defined as

$$\Delta = ||\boldsymbol{Q}_{crit}^{-1}\boldsymbol{Q}_L||_\infty, \tag{3}$$

which is easily computable and accounts for the structure of the entire grid topology. The k^{th} entry of the matrix-vector product $\boldsymbol{Q}_{crit}^{-1}\boldsymbol{Q}_L$ captures the stability stress on load k, with $||\cdot||_\infty$ identifying the maximally stressed node. According to Theorem 1 in [3], the power flow equation will have a unique, stable solution if $\Delta < 1$. Equivalently, $\Delta \geq 1$ indicates that at least one load bus in the model i is overly stressed and can be responsible for a voltage collapse. We refer to $1 - \Delta$ as the *voltage stability margin* [8]. The larger the value of Δ, the narrower the stability margin is and the closer the power system is to a voltage collapse. Finally, let $\boldsymbol{Q}_L^n$ denote the system's *nominal reactive power setpoint vector*. Then the *nominal voltage instability index* Δ^n is computed as the value of Δ (3) using $\boldsymbol{Q}_L^n$.

As proven in [3, Supp. 6] and [5], the voltage instability index Δ increases as the reactive power demands of the loads grow. The attacker can attempt to increase the reactive power demands at the load buses by breaking into the loads and adding an incremental vector

$$\boldsymbol{q}_a = [q_a^1, \cdots, q_a^K] \in \mathbb{R}^K \tag{4}$$

to $\boldsymbol{Q}_L^n$, thus driving Δ towards 1. Moreover, the attacker can make such load attacks covert by designing the entries of $\boldsymbol{q}_a$ small enough that they maintain the load bus voltages to be within their usual allowable range of 0.9 per unit (pu) to 1.1 pu while sill pushing Δ towards 1. As the attack is at the device level rather than at the system level, the state estimator placed at the local substation might be unable to detect it. To prepare for possible future attacks, the operator, or the defender, can switch on pre-installed voltage control devices, such as shunt capacitors and power electronic converters, to compensate for the potential increase in consumption in advance. We assume generators provide reactive power support as usual to maintain power balance, but extra support required to compensate for the attacks is provided by the control devices installed at a set of the load buses denoted $\mathscr{L}_{ctrl} = \{l_n : n = \{1, \cdots, N\}\}$, where l_n is the load bus index and $N \leq K$. Thus, the K-dimensional RPC vector for all loads can be denoted as

$$\boldsymbol{q}_d = [q_d^1, \cdots, q_d^K] \in \mathbb{R}^K, \tag{5}$$

where $q_d^k = 0, \forall k \notin \mathscr{L}_{ctrl}$. If an attack is successful at each load, the overall reactive power balance becomes $\boldsymbol{Q}_L = \boldsymbol{Q}_L^n + \boldsymbol{q}_a - \boldsymbol{q}_d$. The goal of the system operator (defender) is to strategically compensate for the attacker's actions and to avoid the voltage collapse by maintaining Δ as close as possible to the nominal Δ^n.

The zero-sum CBSG in this paper is based on the CBSG in [5]. It is summarized in Table I. The attacker's and the operator's utilities are given by the expected value of Δ (3) restricted to $[\Delta^n, 1]$ and its opposite, respectively. The Cost-Based Backward Induction (CBBI) in [5] computes a CBSE, i.e., the load attack and RPC investment pair that provides the same players' payoffs as any SE but saves the attacker's and defender's costs. Theorem I in [5], [9] and [10, Appx.B] demonstrates existence of CBSE and other CBSG properties.

Finally, we assumed in [5] that the system model is given by the *nominal* model. However in practice, the reactive power setpoint vector $\boldsymbol{Q}_L$ is time-variant and is uncertain a priori. Consider a set of possible uncertain models $\{\mathscr{M}_i \mid i = 1, \cdots, M\}$ due to the fluctuation of real-time power consumption. When the nominal model is used by the operator and the attacker to compute their investment strategies $(\boldsymbol{a}_o^*, \boldsymbol{d}_o^*)$, there is a mismatch with the actual CBSE of the model $\mathscr{M}_i$. To evaluate the fractional difference of the utilities of the nominal model and uncertain model $\mathscr{M}_i$ at a CBSE of the nominal model, we

$$\mu_i\% = \left|\frac{U^a(\boldsymbol{a}_o^*, \boldsymbol{d}_o^*) - U_i^a(\boldsymbol{a}_o^*, \boldsymbol{d}_o^*)}{U^a(\boldsymbol{a}_o^*, \boldsymbol{d}_o^*)}\right| \times 100\%, \tag{6}$$

where the payoffs of the system operator and the load attacker at $(\boldsymbol{a}_o^*, \boldsymbol{d}_o^*)$ are given by $U_i^a(\boldsymbol{a}_o^*, \boldsymbol{d}_o^*) = -U_i^d(\boldsymbol{a}_o^*, \boldsymbol{d}_o^*)$, which are obtained from the ideal players' utilities in Table I by substituting the *nominal* reactive power vector $\boldsymbol{Q}_L^n$ of the nominal model by the *i^{th} model's nominal reactive power vector* $\boldsymbol{Q}_L^{n,i}$ and replacing Δ^n by $\Delta^{n,i}$, the nominal voltage instability index of the i^{th} model. Note that $\mu_{nom} = 0$.

III. A Bidirectional Evolutionary Method for Computing a CBSE

The CBBI algorithm in [5] is a traversal searching method with the complexity of $\mathcal{O}\left(L_a^K L_d^N\right)$. To reduce the computational complexity, we employ the following bidirectional parallel evolutionary GA-based (BPEGA) method (Algorithm 1). In Algorithm 1, the population sizes of the each generation of the attacker's and defender's strategies are represented by even non-negative integers S_a and S_d, respectively. In Step 2 of Algorithm 1, in each generation, each player determines the fitness value (performance metric) of the current population. For the defender's strategy candidate $\boldsymbol{d} \in POP_d^t$ where POP_d^t denotes the defender's current strategy population, an attacker's best response within its strategy population POP_a^t is given by $g_{tmp}(\boldsymbol{d}) = \underset{\boldsymbol{a} \in POP_a^t}{\arg\max}\, U^a(\boldsymbol{a}, \boldsymbol{d})$. Thus, the fitness value of each $\boldsymbol{d} \in POP_d^t$ is given by

$$fit_d(\boldsymbol{d}) = U^d(g_{tmp}(\boldsymbol{d}), \boldsymbol{d}), \forall \boldsymbol{d} \in POP_d^t. \tag{7}$$

Suppose that $\boldsymbol{d}' \in POP_d^t$ has the highest fitness value within the current population

$$\boldsymbol{d}' = \underset{\boldsymbol{d} \in POP_d^t}{\arg\max}\, fit_d(\boldsymbol{d}). \tag{8}$$

For each value of $\boldsymbol{d}'$ that satisfies (8), the attacker assigns the fitness value to all $\boldsymbol{a} \in POP_a^t$ as

$$fit_a(\boldsymbol{a}) = U^a(\boldsymbol{a}, \boldsymbol{d}'), \forall \boldsymbol{a} \in POP_a^t. \tag{9}$$

In Step 6, if several individuals have the same fitness value and cost, the individuals who were selected in an earlier generation are placed ahead of those selected later. Since the "combine and sort" process guarantees that the individual with the highest fitness value among the members of the current generation and of the feasible children set is selected for the next generation, the proposed BPEGA algorithm is an elitist GA [12].

Algorithm 1: Bidirectional Parallel Evolutionary Genetic Algorithm

```
Parameter Initialization: Population sizes $S_a$ and
  $S_d$, crossover probability $P_c$, mutation rate $P_m$,
  maximum number of generations $T$. Current
  generation $t = 0$;
Step 1. Population Initialization: Randomly
  selected feasible initial populations for both players
  $POP_a^0 = \{\boldsymbol{a}_1, \cdots, \boldsymbol{a}_{S_a}\}$ and
  $POP_d^0 = \{\boldsymbol{d}_1, \cdots, \boldsymbol{d}_{S_d}\}$, where $\forall \boldsymbol{a} \in POP_a^0$ and
  $\forall \boldsymbol{d} \in POP_d^0$ which satisfy the attacker's and
  defender's cost constraints, respectively;
while the termination criteria are not satisfied, do
    Step 2. Evaluation: The defender and attacker
      compute $U^d(\boldsymbol{a}, \boldsymbol{d})$ and $U^a(\boldsymbol{a}, \boldsymbol{d})$ for all
      $\boldsymbol{d} \in POP_d^t$ and $\boldsymbol{a} \in POP_a^t$ and evaluate all
      individuals in the current generation to compute
      their fitness values based on (7) and (9);
    for Attacker and Defender do
        Step 3. Selection: Select $S_a/2$ (or $S_d/2$)
          pairs of parents $tmp_P^a$ (or $tmp_P^d$) using the
          Roulette Wheel selection method [11];
        Step 4. Reproduction: Apply crossover with
          probability $P_c$ and mutation operation with
          rate $P_m$ [11] to generate $S_a$ (or $S_d$) children
          $tmp_c^a$ (or $tmp_c^d$);
        Step 5. Check feasibility: For each
          individual in $tmp_c^a$ (or $tmp_c^d$), check if it is a
          feasible solution to attacker's (or defender's)
          cost constraint. Include all feasible children
          in the set $tmp_{c,f}^a$ (or $tmp_{c,f}^d$);
        Step 6. Combine and sort: Combine the
          current generation $POP_a^t$ (or $POP_d^t$) with
          the set of feasible children $tmp_{c,f}^a$ (or
          $tmp_{c,f}^d$). Sort by the fitness value in the
          descending order. Sort the individuals with
          the same fitness values by their investment
          cost in ascending order. The $S_a$ (or $S_d$)
          individuals with the highest ranking are
          selected as the next generation $POP_a^{t+1}$ (or
          $POP_d^{t+1}$);
    end
    $t \leftarrow t + 1$
end
Step 7. Apply the CBBI algorithm [5] to the final
  generation $POP_a^T$ and $POP_d^T$ to determine
  $(\boldsymbol{a}_o^*, \boldsymbol{d}_o^*)$;
```

The iteration will stop when either of the following two conditions is satisfied: (1) For each player, all individuals in the current population are identical, i.e. $\boldsymbol{a}_i = \boldsymbol{a}_j, \forall \boldsymbol{a}_i, \boldsymbol{a}_j \in POP_a^t$ and $\boldsymbol{d}_i = \boldsymbol{d}_j, \forall \boldsymbol{d}_i, \boldsymbol{d}_j \in POP_d^t$; (2) The iteration has reached the preset maximum iteration number T.

Finally, a GA converges when a sequence of objective function evaluations approaches the maximum of the objective function as the number of iterations T tends to infinity [6]. Since BPEGA employs parallel evolution of both players, the convergence result of [7], which assumes only the defender's evolution, is not applicable to Algorithm 1.

Proposition 1. *Assume a crossover probability $P_c > 0$ and* *a mutation rate $P_m > 0$. As the number of iterations T tends to infinity, both players' expected utilities generated by the BPEGA (Algorithm 1) converge to the utilities at any SE and the strategy pair selected by the BPEGA has the lowest players' costs among all SEs of the CBSG.*

Proof. The proof is based on [9], [10, Prop.5.1] and is omitted due to the space constraints. □

The computational complexity of the BPEGA is $\mathcal{O}(TS_aS_d) \ll \mathcal{O}(L_a^K L_d^N)$, the complexity of the CBBI algorithm, when the system size is large and $TS_aS_d \ll L_a^K L_d^N$. In practice, power systems with different system sizes might require different T values to achieve convergence as discussed in Sec.V.

IV. Robust Defense against Load Attacks

In the CBBI algorithm of [5] or the BPEGA Algorithm 1, the load attacker does not require the knowledge of the operator's cost per load γ_d to determine its best response since it is the follower and thus observes the defender's RPC strategy before acting. However, the system operator acts first and thus relies on the knowledge of γ_a. When the defender does not have complete information about the attacker's resources, the proposed CBSG (Table I) is unsuitable. In the *robust-defense (RD)* algorithm described below, the defender employs a lower bound γ_a^{est} on the attacker's actual cost γ_a, where $0 \leq \gamma_a^{est} \leq \gamma_a$, to compute its RPC strategy.

Step 1: (a) For each defender's RPC action $\boldsymbol{d}$ that satisfies the cost constraint, the defender estimates the set of attacker's best responses (i.e., load attack strategies) $\mathcal{G}(\gamma_a^{est}, \boldsymbol{d})$, where $g(\gamma_a^{est}, \boldsymbol{d}) \in \mathcal{G}(\gamma_a^{est}, \boldsymbol{d})$ if

$$\begin{aligned} g(\gamma_a^{est}, \boldsymbol{d}) &= \arg\max_{\boldsymbol{a}} U^a(\boldsymbol{a}, \boldsymbol{d}), \\ \text{s.t.} \quad & \gamma_a^{est}||\boldsymbol{a}||_1 \leq 1, \; q_a^k \leq q_a^{k,\max}, \forall k. \end{aligned} \tag{10}$$

(b) For each $\boldsymbol{d}$, the *smallest-cost* estimated best response is

$$g_o(\gamma_a^{est}, \boldsymbol{d}) = \operatorname*{arg\,min}_{g(\gamma_a^{est},\boldsymbol{d}) \in \mathcal{G}(\gamma_a^{est},\boldsymbol{d})} ||g(\gamma_a^{est}, \boldsymbol{d})||_1. \tag{11}$$

Step 2: (a) The defender (operator) determines the set of its RPC strategies $\mathcal{D}_{est}$ where $\boldsymbol{d}_{RD}^* \in \mathcal{D}_{est}$ if

$$\begin{aligned} \boldsymbol{d}_{RD}^* &= \arg\max_{\boldsymbol{d}} U^d(g_o(\gamma_a^{est}, \boldsymbol{d}), \boldsymbol{d}), \\ \text{s.t.} \quad & \gamma_d||\boldsymbol{d}||_1 \leq 1. \end{aligned} \tag{12}$$

(b) A strategy in (12) with the *smallest cost* is chosen

$$\boldsymbol{d}_{RD}^o = \operatorname*{arg\,min}_{\boldsymbol{d}_{RD}^* \in \mathcal{D}_{est}} ||\boldsymbol{d}_{RD}^*||_1. \tag{13}$$

Step 3: (a) By observing the defender's RPC action $\boldsymbol{d}_{RD}^o$, the attacker finds its actual set of best responses $\mathcal{G}(\gamma_a, \boldsymbol{d}_{RD}^o)$, where the load attack strategy $\boldsymbol{a}_{RD}^* \in \mathcal{G}(\gamma_a, \boldsymbol{d}_{RD}^o)$ if

$$\begin{aligned} \boldsymbol{a}_{RD}^* = g(\gamma_a, \boldsymbol{d}_{RD}^o) &= \arg\max_{\boldsymbol{a}} U^a(\boldsymbol{a}, \boldsymbol{d}_{RD}^o), \\ \text{s.t.} \quad \gamma_a||\boldsymbol{a}||_1 \leq 1; & \, q_a^k \leq q_a^{k,\max}, \forall k, \end{aligned} \tag{14}$$

(b) If multiple solutions exist in $\mathcal{G}(\gamma_a, \boldsymbol{d}_{RD}^o)$, the attacker chooses a load attack strategy with the *smallest cost*

$$\boldsymbol{a}_{RD}^o = g_o(\gamma_a, \boldsymbol{d}_{RD}^o) = \operatorname*{arg\,min}_{\boldsymbol{a}_{RD}^* \in \mathcal{G}(\gamma_a, \boldsymbol{d}_{RD}^o)} ||\boldsymbol{a}_{RD}^*||_1. \tag{15}$$

A strategy pair $(\boldsymbol{a}_{RD}^o, \boldsymbol{d}_{RD}^o)$ is a *cost-based RD solution*. Note that the actual defender's payoff differs from its estimate $U^d(g_o(\gamma_a^{est}, \boldsymbol{d}_{RD}^o), \boldsymbol{d}_{RD}^o)$ and is given by $U^d(\boldsymbol{a}_{RD}^o, \boldsymbol{d}_{RD}^o)$.

Theorem 1.
In the proposed RD method (steps 1∼3 above):
(a) *The actual utility of the defender is at least as large as its estimated utility, i.e.*

$$U^d(\boldsymbol{a}_{RD}^o, \boldsymbol{d}_{RD}^o) \geq U^d(g_o(\gamma_a^{est}, \boldsymbol{d}_{RD}^o), \boldsymbol{d}_{RD}^o). \tag{16}$$

(b) *The defender's actual payoff $U^d(\boldsymbol{a}_{RD}^o, \boldsymbol{d}_{RD}^o)$ increases with its estimate of the attacker's cost γ_a^{est} and approaches its payoff $U^d(\boldsymbol{a}_o^*, \boldsymbol{d}_o^*)$ at a CBSE of the CBSG in Table I as γ_a^{est} tends to the actual γ_a value.*

Proof. The proof is referred to [13] and is omitted due to the space constraints. □

Remark 1. *Theorem 1(a) demonstrates that assuming the worst-case attack scenario provides robust RPC when the system operator is uncertain about the load attacker's resources. Moreover, from Theorem 1(b), we conclude that as the operator's knowledge of the attacker's cost improves, the defender's actual payoff of the RD solution increases and approaches the payoff of the ideal game.*

To evaluate the defender's utility loss due to its uncertainty about the attacker's budget, we compute the mismatch (loss) of actual defender's utility using the RD method relative to that at a CBSE of the ideal CBSG. For each set of γ_a^{est}, γ_a, and γ_d values, this mismatch is computed as

$$\mu_{RD}\% = \left| \frac{U^d(\boldsymbol{a}_{RD}^o, \boldsymbol{d}_{RD}^o) - U^d(\boldsymbol{a}_o^*, \boldsymbol{d}_o^*)}{U^d(\boldsymbol{a}_o^*, \boldsymbol{d}_o^*)} \right| \times 100\%. \tag{17}$$

Finally, the evolutionary Algorithm 1 can be easily modified to perform the RD method and shown to converge to an RD solution. Moreover, as for the CBSG, the RD method is developed assuming the nominal model, but can be applied to any uncertain model i and evaluated using a metric similar to (6). The details are omitted for brevity.

V. Numerical Results

In Sec.V-A, we validate computationally efficient BPEGA method proposed in Sec.III by comparing its performance with the traversal algorithm for the IEEE 9-bus system. Then in Sec.V-B, we employ GA methods to analyze performance of the IEEE 39-bus system.

A. IEEE 9-bus System

The IEEE 9-bus system has 6 load buses, which are all potential targets for the attacker. We assume that the set of buses with control devices installed is $\mathscr{L}_{ctrl} = \{4, 5, 6, 8\}$. In the simulation, $q_a^{k,\max}$ is determined by the covertness constraint, and we set $q_d^{k,\max} = 2$ pu, $\forall k$. It was verified that these compensations do not violate the $[0.9, 1.1]$ pu voltage range for any bus. The M load-uncertain models are created by adding independent zero-mean Gaussian random variables to the components of the nominal reactive power setpoint vector $\boldsymbol{Q}_L^n$, i.e., the i^{th} model's nominal reactive power setpoint vector is given by $\boldsymbol{Q}_L^{n,i} = \boldsymbol{Q}_L^n(1+\boldsymbol{\epsilon}^i)$, where $\boldsymbol{\epsilon}^i \sim N(0, \sigma^2)$, $i = \{1, \cdots, M\}$, and the standard deviation $\sigma = 0.1$ [14]. Note that the number of models $M = 20$, which satisfies the criteria for the sample size given the margin of error (MOE) of 0.05 and the confidence interval (CI) of 95%.

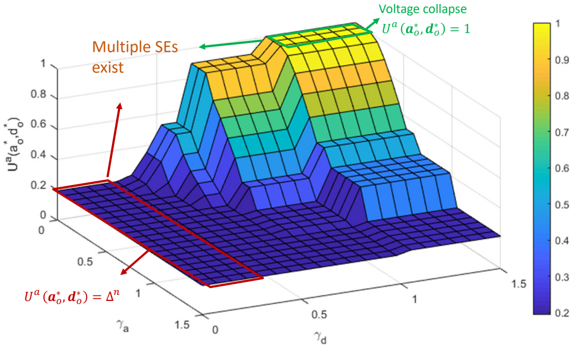

Fig. 1. Attacker's expected utility at CBSE vs. γ_a and γ_d for $L_a = L_d = 3$, IEEE 9-bus system

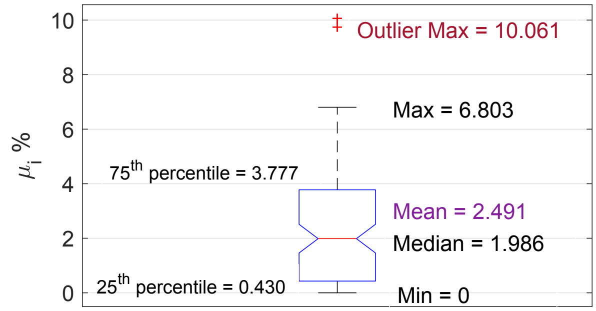

Fig. 2. Boxplot of the utility difference $\mu_i\%$ (6) over the randomly generated set of 20 models and 5 cost pairs (γ_a, γ_d): (0.1, 0.1), (0.1, 1.5), (0.75, 0.75), (1.5, 0.1), (1.5, 1.5); $L_a = L_d = 3$; the IEEE 9-bus system

Fig. 1 shows the attacker's expected utility $U^a(\boldsymbol{a}_o^*, \boldsymbol{d}_o^*)$ at a CBSE for varying γ_a and γ_d assuming a fixed nominal model. These trends are consistent with Theorem 1 in [5]. In particular, each player's utility improves as that player's cost decreases while the opponent's cost is fixed, and both players target "important" loads with the greatest impact on Δ_0, but the attacker tends to avoid the loads protected by the defender [5]. Fig. 2 represents the utility difference (6) statistics for five different cost pairs. We observe that most uncertain models experience modest utility differences from the CBSE shown in Fig. 1, demonstrating robustness of CBSG to load uncertainty in the IEEE 9-bus power system.

Next, we validate convergence of BPEGA Algorithm 1. We set $S_a = 30$, $S_d = 20$, $P_c = 0.85$, $P_m = 0.05$, and $T = 30$. These initialization parameters are selected experimentally and reflect a trade-off between convergence and computational complexity for the IEEE 9-bus system. For the nominal system model, Fig. 3 shows that the BPEGA Algorithm 1 converges to a CBSE obtained by the traversal CBBI algorithm in fewer than 15 iterations, thus confirming Proposition 1. Similar results were obtained for other cost pairs, demonstrating fast convergence of the BPEGA Algorithm 1 [10].

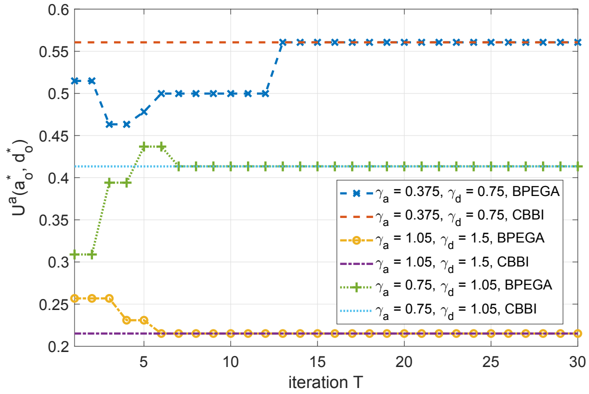

Fig. 3. Convergence of the attacker's utility in the BPEGA Algorithm 1 with $L_a = L_d = 3$; the IEEE 9-bus system

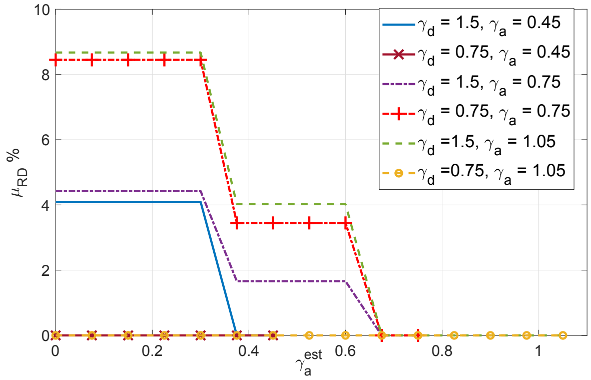

Fig. 4. The mismatch $\mu_{RD}\%$ (17) for varying γ_a^{est} given $\gamma_a = \{0.45, 0.75, 1.05\}$, and $\gamma_d = \{0.75, 1.5\}$; $L_a = L_d = 3$; the IEEE 9-bus system

Finally, we compare the performance of the RD method for the nominal-model IEEE 9-bus system to that of the ideal CBSG by measuring the mismatch $\mu_{RD}\%$ (17) in Fig. 4 for varying costs γ_a^{est} estimated by the system operator given selected γ_a and γ_d values. We observe that the mismatch reduces as the worst-case cost estimate γ_a^{est} approaches the actual γ_a value as shown in Theorem 1(b). We also found that the mismatch is zero for *all* γ_a^{est} values in many cases, e.g. when $(\gamma_a, \gamma_d) = (0.75, 0.45)$ or $(0.75, 1.05)$. Moreover, even when the most powerful attacker is assumed ($\gamma_a^{est} = 0$) while the actual γ_a values are in the range $0 \leq \gamma_a \leq 1.5$ and $\gamma_d \in \{0.45, 0.75, 1.5\}$, the mismatch (17) for most cost pairs was less than 1% with median of $\mu_{RD} = 0$ and 75% percentile = 0.575, indicating that the RD method is robust to the system operator's uncertainty about the load attacker's resources. On the other hand, the defender's cost of the RD solution is at least as large as the defender's cost of a CBSE of the ideal CBSG. When the actual γ_a is large, $\gamma_a^{est} = 0$, and γ_d is relatively small, e.g. $\gamma_a \geq 1.05$ and $\gamma_d \leq 0.225$, the defender's overpayment using the RD method compared to the ideal CBSG can be as high as 300% since the defender grossly overestimates the attacker's budget in the RD method. However, the defender's excess cost of the RD solution reduces as its cost per load γ_d increases and γ_a^{est} approaches the actual γ_a value. Finally, the attacker's investment cost is the same in both methods.

B. IEEE 39-bus system

Next, we apply the proposed methods to the IEEE 39-bus system, which contains 29 loads. We assume that the set of buses with control devices installed is $\mathscr{L}_{ctrl} = \{5, 6, 7, 8, 10, 11, 13\}$. This set includes both players' five most important loads [5]. The $M = 20$ load-uncertain models were created using the same method for the IEEE 9-bus system (Sec.V-A).

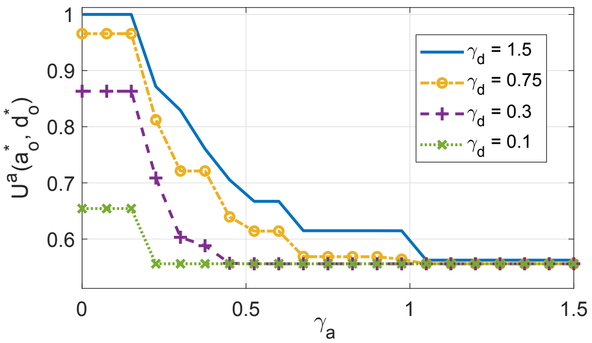

Fig. 5. Attacker's utility at a CBSE found by the BPEGA algorithm with $L_a = L_d = 3$; the IEEE 39-bus system

For levels of investment $L_a = L_d = 3$, the complexities of the CBBI algorithm and the BPEGA Algorithm 1 are $\mathcal{O}\left(3^{29} \times 3^7\right)$ and $\mathcal{O}(TS_aS_d) = \mathcal{O}(30 \times 30 \times 20) = \mathcal{O}(18000)$, respectively. Since the former complexity is too high, we apply the BPEGA Algorithm 1 and the RD method for IEEE 39-bus system in Fig. 5 and 6. We observe the same performance trends as in Fig. 1. Note that voltage collapse occurs only when the attacker has very small cost γ_a while the defender's cost $\gamma_d \gg \gamma_a$. We conclude that voltage collapse can be successfully prevented in both IEEE 9-bus and 39-bus systems unless the defender's security resources are disproportionately limited relative to the attacker's budget.

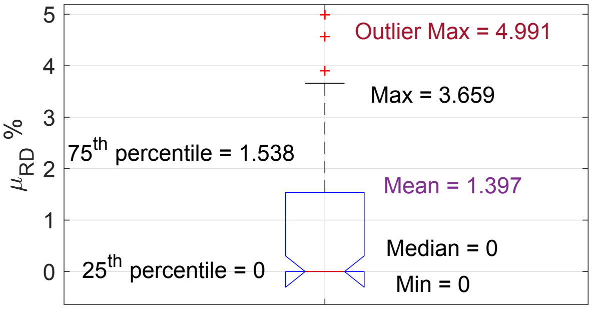

Fig. 6. Boxplot of the mismatch μ_{RD}% (17) of the RD solution for $\gamma_a^{est} = 0$ over the cost pairs: $\gamma_a = [0 : 0.075 : 1.5]$, $\gamma_d = \{0.45, 0.75, 1.5\}$; $L_a = L_d = 3$; the IEEE 39-bus system

Moreover, we found that for the IEEE 39-bus system, most uncertain models experience slight utility differences (6) ranging from 0% to 1.836%, confirming the robustness of proposed CBSG to load uncertainty. Furthermore, Fig. 6 shows the boxplot for the mismatch (17) of the defender's utilities of the RD solution for selected defender's costs when the most powerful attacker is assumed ($\gamma_a^{est} = 0$) and the actual γ_a values are in the range $0 \leq \gamma_a \leq 1.5$. We observe that the mismatch for most cost pairs is modest, confirming that the RD solution is robust to imperfect knowledge of the attacker's budget by the defender. Finally, for both IEEE 9-bus and 39-bus systems, we found that the RD method is robust to model uncertainty, with statistics similar to those in Fig. 2.

VI. Conclusion

We investigated scalable, robust game-theoretic investment solutions for securing electric power systems from load attacks and associated voltage collapse. To address the scalability of the proposed methods to large power systems, a bidirectional, parallel, evolutionary generic algorithm (BPEGA) was developed. Moreover, we proposed a robust-defense (RD) method to address realistic scenarios where the defender lacks full information about the attacker's budget. It is demonstrated that the system operator is able to preserve voltage stability for both load- and/or information-uncertain scenarios unless its reactive power compensation resources are much more limited than the load attacker's resources.

References

[1] S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, "A systems and control perspective of CPS security," *Annual Reviews in Control*, vol. 47, pp. 394 – 411, 2019.

[2] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2862–2872, July 2018.

[3] J. W. Simpson-Porco, F. Dörfler, and F. Bullo, "Voltage collapse in complex power grids," *Nature communications*, vol. 7, p. 10790, 2016.

[4] S. Etesami and T. Basar, "Dynamic games in Cyber-Physical security: An overview," *Dynamic Games and Applications*, pp. 1–30, 2019.

[5] L. An, A. Chakrabortty, and A. Duel-Hallen, "A Stackelberg security investment game for voltage stability of power systems," in *2020 IEEE 59th Conference on Decision and Control (CDC)*, 2020.

[6] E. D'Amato, E. Daniele, L. Mallozzi, and G. Petrone, "Equilibrium strategies via GA to Stackelberg games under multiple follower's best reply," *International Journal of Intelligent Systems*, vol. 27, no. 2, pp. 74–85, 2012.

[7] T. Vallée and T. Başar, "Off-line computation of Stackelberg solutions with the genetic algorithm," *Computational Economics*, vol. 13, no. 3, pp. 201–209, 1999.

[8] T. Van Cutsem and C. Vournas, *Voltage stability of electric power systems*. Springer Science & Business Media, 2007.

[9] P. Shukla, L. An, A. Chakrabortty, and A. Duel-Hallen, "A robust Stackelberg game for cyber-security investment in networked control systems," *IEEE Transactions on Control Systems Technology*, vol. 31, no. 2, pp. 856–871, 2023.

[10] L. An, "Game-theoretic methods for cost allocation and security in Smart Grid," 2020, Ph.D. thesis. [Online]. Available: https://repository.lib.ncsu.edu/handle/1840.20/38411

[11] B. Liu, "Stackelberg-Nash equilibrium for multilevel programming with multiple followers using genetic algorithms," *Computers & Mathematics with Applications*, vol. 36, no. 7, pp. 79–89, 1998.

[12] K. Deb, A. Pratap, S. Agarwal, and T. Meyarivan, "A fast and elitist multiobjective genetic algorithm: NSGA-II," *IEEE transactions on evolutionary computation*, vol. 6, no. 2, pp. 182–197, 2002.

[13] L. An, P. Shukla, A. Chakrabortty, and A. Duel-Hallen, "Supplementary material for: Robust and scalable game-theoretic security investment methods for voltage stability of power systems," 2023, supplementary document. [Online]. Available: https://tinyurl.com/supp-doc-cdc23-an

[14] R. Bo and F. Li, "Probabilistic LMP forecasting considering load uncertainty," *IEEE Transactions on Power Systems*, vol. 24, no. 3, pp. 1279–1289, 2009.