Targeted Power System Frequency Attack via the Selection of Maliciously Controlled Inverters

Xiangyu Zou, Betelihem Ashebo, and Daniel K. Molzahn

***Abstract*—This paper studies how an adversary can execute a power system frequency attack by choosing the most effective subset of inverter-based resources (IBRs) as malicious control nodes. During the attack, the adversary controls the attacking devices to destabilize a group of designated target generators. The attack is designed by introducing an unstable oscillatory mode whose eigenvector has large components at the target generators and small components at the compromised IBRs. We formalize the optimal attacker selection problem and present an equivalent mixed-integer quadratically constrained program (MIQCP). To address this combinatorial nonconvex problem, we develop two heuristic algorithms by introducing a ranking metric. The attack process is demonstrated on a modified WSCC 179-bus system, with results verified through nonlinear dynamic simulations. We show that the proposed heuristics find optimal attacking sets in a majority of evaluated scenarios while significantly reducing the required computational time. Scenarios from the ACTIVSg500 system are used to further support our results. Finally, we discuss how selecting different eigenvalues, targets, and numbers of compromised devices impact the attack's severity.**

***Index Terms*—Cyber-physical security, inverter-based resources, stability, malicious control, mixed-integer programming.**

I. Introduction

THE power grid is undergoing a major transformation with the widespread integration of inverter-based resources (IBRs), including solar photovoltaic (PV), wind generators, and energy storage systems. Renewable sources accounted for 92.5% of new global power generation capacity in 2024, up from 85.8% in 2023 [1], with solar PV and wind accounting for 96.6% of renewable additions [2]. This expansion is expected to continue, and is projected to account for approximately 95% of global renewable capacity additions through 2030 [3]. IBRs interface with the grid through power electronics governed by digital control systems. This shift fundamentally alters power system dynamics by replacing the electromechanical response of synchronous generators with the control-determined behavior of converter-interfaced devices.

IBRs introduce distinct cybersecurity vulnerabilities, as their reliance on digital controllers, communication interfaces, and configurable software settings significantly expands the attack surface [4], [5]. Adversaries with device-level access could manipulate measurements, control logic, or setpoints, potentially causing frequency instability, voltage violations, or thermal overloading [6], [7].

A coordinated cyberattack involving multiple compromised IBRs would provide an adversary with a wider range of control actions than a single-device breach. However, compromising additional devices requires additional time, access, and resources. An attacker must therefore determine which IBRs will have the greatest grid impact when compromised and allocate resources accordingly. This work characterizes such worst-case attacks by identifying the devices most capable of destabilizing the system. Identifying these high-impact resources is important for assessing the potential consequences of coordinated attacks and prioritizing the deployment of cybersecurity protections.

Previous research has shown that coordinated malicious control can excite unstable modes that target selected generators [8], [9]. However, these studies assume that the set of compromised devices is fixed and known *a priori*. Allowing the adversary to select the compromised IBRs adds an additional degree of freedom. The effectiveness of an attack may therefore depend not only on *how* the compromised resources are controlled, but also *which* devices are under malicious control.

Accordingly, this paper introduces the problem of selecting a subset of IBRs that an adversary would prioritize to maximize the destabilizing effect on a designated set of target synchronous generators. We analyze this device-selection problem using a small-signal stability framework, which characterizes local system dynamics by linearizing the governing equations around an operating point [10], [11]. The attack is designed using an eigenvalue and eigenvector placement approach and cast into a combinatorial optimization problem.

Next, we review the literature on DER cybersecurity, small-signal analysis, malicious control, and control node selection.

A. Related work

The dependence of IBRs on digital controllers, communication links, and configurable software settings makes their control systems vulnerable to remote compromise. Surveys of the IBR attack surface describe how communication and firmware vulnerabilities may allow unauthorized changes to control parameters, setpoints, and reference signals [6], [7]. Specific inverter control functions have also been examined. Malicious alteration of an inverter's volt-var control curve can degrade system stability and performance [12]. Similarly, manipulation of the phase-locked loops of grid-following inverters can force them into off-nominal frequency operation and disturb the surrounding system [13]. Reliability authorities have also identified IBR control and protection settings as contributors

X. Zou, B. Ashebo, D.K. Molzahn are with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, USA. Email: {xy.zou, bashebo3, molzahn}@gatech.edu.

Support from the U.S. Department of Energy, Office of Science, Office of Cybersecurity, Energy Security, and Emergency Response (CESER), under DE-CR0000056 and the National Science Foundation under grant number #2112533: NSF Artificial Intelligence Research Institute for Advances in Optimization (AI4OPT).

to large-scale disturbances, underscoring the consequences of incorrect or unauthorized changes to these settings [14]. These studies show that unauthorized modification of inverter control functions is technically plausible.

The dynamic behavior exploited by these attacks can be studied through small-signal stability analysis. In this framework, the nonlinear equations governing system dynamics are linearized around a steady-state operating point, and the eigenvalues of the resulting system matrix determine the stability and damping of its oscillatory modes [10], [11]. With increasing IBR penetration, small-signal models have been extended to represent fast converter control loops [15]. IBRs commonly operate under active and reactive power droop control, which relates frequency and voltage deviations to changes in power output [16]. The associated droop gains and time constants influence system eigenvalues and may alter modal damping and coupling among IBRs [17].

Stability analysis is generally used to identify or mitigate unstable behavior. In contrast, malicious control seeks to modify the same modal structure to create instability. This idea was introduced in [8], [18], where a group of generators applies feedback control to excite an unstable mode in which designated target generators have the largest participation. The targets are driven toward their protection limits while the attacking units remain connected. Later studies considered similar attacks using demand-side loads under proportional control [19], aggregated loads providing emulated inertia [20], and active loads in islanded microgrids [9]. The system and generator information needed to construct such attacks may be obtained through insider access or information leakage. Reference [20] also showed that the attack can remain effective under uncertainty in generator parameters and network topology. The work in [21] optimizes load perturbations to move selected eigenvalues into the right-half plane, showing that deliberate destabilization can be treated as a control-design problem.

The studies discussed above assume that the compromised devices are fixed in advance, that is, the attacker is assumed to already control a particular generator, load, or inverter. In contrast, the problem considered here allows the adversary to choose which IBRs to compromise. This additional decision creates a combinatorial device-selection problem that has not been addressed in the existing malicious-control literature.

The problem is structurally related to input and actuator selection in systems control. Input/output selection determines where the inputs and outputs of a system should be placed to achieve goals of controllability and disturbance rejection [22]. Actuator-placement methods similarly select a limited set of control inputs, often through mixed-integer optimization, to achieve controllability while minimizing control effort [23]. Such selection problems are computationally difficult in general [24], and has motivated the use of controllability metrics and submodular greedy methods for tractable actuator selection [25].

These formulations, however, are designed to improve the ability to steer the system over a broad range of states. The adversary considered in this paper has a more specific objective and does not require full controllability. The goal is to introduce a single unstable mode with large modal participation at the designated target generators and limited participation at the compromised IBRs. Reference [26] provides a related formulation in which load perturbations are selected to destabilize the system through eigenvalue placement. The present problem differs by directly optimizing the relative modal participation of the target and attacking resources so that the induced instability primarily affects the intended targets while the compromised IBRs remain connected and thus capable of initiating further attacks or benefiting economically. To the best of our knowledge, this objective has not previously been posed as a device-selection problem. Section III formulates it through the direct design of the closed-loop eigenstructure.

B. Proposed Framework and Contributions

This paper extends previous research on malicious control in power systems [8], [9], [18] by formalizing the optimal cyber-physical attacker selection problem. We identify the set of devices that, when acting maliciously, has the greatest destabilizing effect on a predefined set of target generators. Several algorithms are proposed to solve the combinatorial problem, including exhaustive search, a mixed-integer optimization framework, and two ranking-based heuristics. We show that the problem greatly simplifies for certain scenarios, such as when targeting a single generator. We also demonstrate how the frequency the attack operates on, represented by a prescribed eigenvalue, impacts the attack's effectiveness.

We illustrate our methods via case studies using the Western Systems Coordination Council (WSCC) 179-bus and the ACTIVSg500 test cases [27], showing through nonlinear dynamical simulations that the compromised devices inflict unstable oscillations in the target generators.

In summary, the contributions of this work are as follows:

1) A formal optimization-based representation of the optimal attacker selection problem for inverter-based resources, where the objective is to identify a subset of devices that produces the largest destabilizing effect on specified target generators.
2) A mixed-integer quadratically-constrained program (MIQCP) reformulation that can be solved by state-of-the-art solvers such as Gurobi [28].
3) Two ranking-based heuristics to circumvent the combinatorial complexity of the optimization problem, with numerical results to support their effectiveness.
4) Intuition into how the selection of the attack's frequency influences the problem as well as how certain special cases lead to simplifications in the problem's structure.

This paper is organized as follows. Section II introduces the dynamical network model and its linearization. Section III formalizes attacker selection as a nonlinear optimization problem and presents an equivalent mixed-integer quadratically constrained program (MIQCP) form. Section IV develops a heuristic search algorithm as a computationally lighter alternative. Section V demonstrates the performance of the algorithms using an example of a successful attack. Section VI concludes the discussion with avenues for future research.

II. Dynamic Model

Section II-A presents the nonlinear model of coupled generator and IBR dynamics. Section II-B linearizes this model around a power flow solution to enable eigenvalue analysis tools used later in the paper.

A. Dynamic System Model

In a power system with b buses, g synchronous generators and h inverter-based resources, the system's response to perturbations is governed by the devices' dynamic behaviors, which are coupled by the network's power flow equations.

We adopt the one-axis (flux-decay) synchronous machine model from [29]:

$$\dot{\delta}_i = \omega_i - \omega_s, \tag{1a}$$

$$\dot{\omega}_i = \frac{\omega_s}{2H_i}(T_{M,i} + \Delta T_{M,i} - E'_{q,i} I_{q,i} - (x_{q,i} - x'_{d,i}) I_{d,i} I_{q,i} - D_i(\omega_i - \omega_s)), \tag{1b}$$

$$\dot{E}'_{q,i} = \frac{1}{T'_{do,i}}(-E'_{q,i} - (x_{d,i} - x'_{d,i}) I_{d,i} + E_{Fd,i}), \tag{1c}$$

for all $i \in \{1,\dots,g\}$. The machines have reactance parameters x_d, x'_d, and x_q, generator inertia and damping parameters H and D, d-q frame current variables I_d and I_q, internal voltage $E'_{q,i}$, and field voltage E_{Fd}. In (1a), the rotor angle δ varies when the frequency ω deviates from its nominal value ω_s. Equation (1b) models the variation in frequency when the mechanical torque T_M and electrical torque represented by the I_q terms are not balanced. Finally, (1c) defines the dynamics of the internal voltage E'_q.

Each generator is equipped with an exciter that regulates the terminal voltage V_i by adjusting the field voltage E_{Fd} in (1c), with equations

$$\dot{E}_{Fd,i} = -\frac{1}{T_{E,i}}(K_{E,i} + S_{E,i}(E_{Fd,i}))E_{Fd,i} + \frac{V_{R,i}}{T_{E,i}}, \tag{2a}$$

$$\dot{R}_{F,i} = -\frac{1}{T_{F,i}} R_{F,i} + \frac{K_{F,i}}{T^2_{F,i}} E_{Fd,i}, \tag{2b}$$

$$\dot{V}_{R,i} = -\frac{V_{R,i}}{T_{A,i}} + \frac{K_{A,i}}{T_{A,i}} R_{F,i} - \frac{K_{A,i}K_{F,i}}{T_{A,i}T_{F,i}} E_{Fd,i} + \frac{K_{A,i}}{T_{A,i}}(V_{ref,i} - V_i), \tag{2c}$$

for all $i \in \{1,\dots,g\}$. The stabilizer signal R_F and voltage regulator output V_R are defined by (2b) and (2c), respectively. These adjust the field voltage in the exciter equation (2a). The constants K_A, K_E, K_F and T_A, T_E, T_F correspond to control gains and time delays, respectively. The function $S_E(\cdot)$ models exciter saturation, and V_{ref} is the generator's voltage reference.

Finally, the governor and steam-turbine models that control the mechanical torque ΔT_M in (1b) are described by

$$\Delta \dot{T}_{M,i} = \frac{1}{T_{CH,i}}(-\Delta T_{M,i} + \Delta P_{SV,i}), \tag{3a}$$

$$\Delta \dot{P}_{SV,i} = \frac{1}{T_{SV,i}}\left(-\Delta P_{SV,i} - \frac{1}{R_{D,i}\omega_s}(\omega_i - \omega_s)\right), \tag{3b}$$

for all $i \in \{1,\dots,g\}$. Equation (3b) controls the steam valve signal ΔP_{SV}, which is an input to the first-order turbine model in (3a). The quantities T_{CH} and T_{SV} are time constants, and R_D is the inverse droop constant.

The system's IBRs use P-f droop control, where each device adjusts its active power output when the frequency of the grid deviates from its nominal value:

$$\dot{\delta}_{H,i} = \Delta\omega_{H,i}, \tag{4a}$$

$$\Delta\dot{\omega}_{H,i} = \frac{1}{T_{pf}}(-\Delta\omega_{H,i} - m_{p,i}\omega_s\gamma_{H,i}(P_{H,i} - P_{ref,i})), \tag{4b}$$

for $i \in \{1,\dots,h\}$. The droop law (4b) controls the IBR's internal angle δ_H which indirectly controls its power injection. The IBR has a time constant T_{pf} and droop constant m_p. The quantity γ_H is a unit conversion factor.

In total, there are $8g+2h$ state variables. Furthermore, the generator currents $I_{d,i}$ and $I_{q,i}$ as well as voltage magnitudes V_i and phase angles θ_i of all buses form $2g+2b$ algebraic variables that couple the ODEs. The stator algebraic equations

$$\begin{aligned} V_i \sin(\delta_i - \theta_i) - x_{q,i} I_{q,i} &= 0, \\ E'_{q,i} - V_i \cos(\delta_i - \theta_i) - x'_{d,i} I_{d,i} &= 0, \end{aligned} \tag{5}$$

and nodal power balance equations

$$\begin{aligned} P_{net,i} - \sum_{k=1}^{b} V_i V_k Y_{ik} \cos(\theta_i - \theta_k - \alpha_{ik}) &= 0, \\ Q_{net,i} - \sum_{k=1}^{b} V_i V_k Y_{ik} \sin(\theta_i - \theta_k - \alpha_{ik}) &= 0, \end{aligned} \tag{6}$$

for all $i \in \{1,\dots,b\}$, together form the algebraic equations. The (i,k)-element in the nodal admittance matrix has magnitude Y_{ik} and angle α_{ik}. The net active and reactive power injections $P_{net,i}$ and $Q_{net,i}$ depend on which devices reside at the bus. The power injections from synchronous generators are defined by

$$\begin{aligned} P_{G,i} &= I_{d,i} V_{G(i)} \sin(\delta_i - \theta_{G(i)}) + I_{q,i} V_{G(i)} \cos(\delta_i - \theta_{G(i)}), \\ Q_{G,i} &= I_{d,i} V_{G(i)} \cos(\delta_i - \theta_{G(i)}) - I_{q,i} V_{G(i)} \sin(\delta_i - \theta_{G(i)}), \end{aligned}$$

and the power injections from IBRs are defined by

$$\begin{aligned} P_{H,i} &= \frac{E_i V_{H(i)}}{x_{l,i}} \sin(\delta_{H,i} - \theta_{H(i)}), \\ Q_{H,i} &= \frac{V^2_{H(i)} - E_i V_{H(i)} \cos(\delta_H - \theta_{H(i)})}{x_{l,i}}. \end{aligned}$$

where the indexing subscripts $G(i)$ and $H(i)$ denote the bus number of the i-th synchronous generator and IBR, respectively, and E_i is the internal voltage of the i-th IBR. Active and reactive demand are treated as constant power loads.

Together, the ODEs (1)–(4) and algebraic equations (5), (6) form the system of differential-algebraic equations (DAE) that describes the nonlinear power system dynamics.

B. Linearized System Model

Linearizing the DAE model (1)–(6) around a power flow solution yields a local approximation of the system dynamics. First, the initial values of all dynamic and algebraic variables of the DAE are found. Then, new variables are defined to represent the deviation from the initial steady-state operating point. Let $x \in \mathbb{R}^{8g+2h}$ and $y \in \mathbb{R}^{2g+2b}$ represent the changes

in state and algebraic variables from their equilibrium values, respectively. By computing a first-order approximation of the dynamical equations, a linear system of the form

$$\begin{bmatrix} \dot{x} \\ 0 \end{bmatrix} = \begin{bmatrix} \mathbf{A}_{11} & \mathbf{A}_{12} \\ \mathbf{A}_{21} & \mathbf{A}_{22} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

is obtained, where the block matrices $\mathbf{A}_{11}, \mathbf{A}_{12}$ and $\mathbf{A}_{21}, \mathbf{A}_{22}$ contain coefficients of the linearized differential equations (1)–(4) and algebraic equations (5) and (6). The algebraic variables can be eliminated by Kron reduction (Schur complement) [10] to produce the linear system

$$\dot{x} = \mathbf{A}x$$

where

$$\mathbf{A} = \mathbf{A}_{11} - \mathbf{A}_{12}\mathbf{A}_{22}^{-1}\mathbf{A}_{21}$$

is the size $n = 8g + 2h$ square matrix that describes the system's dynamics around the power flow solution.

The stability of the linearized system to small disturbances is determined by the eigenvalues of $\mathbf{A}$. We focus on initially stable systems, i.e., all eigenvalues of $\mathbf{A}$ have negative real-parts. The goal of the adversary is to destabilize the system by selecting which devices to compromise and devising a malicious control strategy. The next section formalizes this goal more precisely and develops an optimization program for this process.

III. Optimization Formulation

Section III-A first describes an overview of the threat model, including the type and capability of the attack and other assumptions. Section III-B then develops an optimization program to represent the attack selection and malicious control formulation process. Despite the nonconvex and combinatorial nature of the problem, Section III-C next shows an equivalent MIQCP form that is conducive to solvers such as Gurobi [28].

A. Malicious Control Threat Model

We focus on attacks where the malicious actor gains control over several IBRs, referred to as attackers, with the goal of destabilizing a predetermined group of synchronous generators, referred to as targets. Since compromising each IBR requires time and resources, the adversary seeks to identify a subset of devices that can execute an attack most effectively. This motivates our limited-effort attack model, in which the adversary cannot compromise all IBRs and instead must select $m < h$ devices to gain control over. During an attack, the adversary manipulates the active power reference ($P_{ref,i}$ in (4)) of the m chosen devices. This introduces an external control signal u for each device that is represented by

$$\dot{x} = \mathbf{A}x + \mathbf{B}u, \tag{7}$$

where the columns of $\mathbf{B} \in \{0,1\}^{n \times m}$ are standard basis vectors corresponding to the $\Delta\omega_{H,i}$ states of the compromised devices and $u \in \mathbb{R}^m$ is the malicious reference signal that the adversary injects. The decision of which devices to compromise is represented by the matrix $\mathbf{B}$, and the formulated attack is represented by the signal u. We consider a state-feedback law of the form

$$u = -\mathbf{K}x,$$

where the gain matrix $\mathbf{K} \in \mathbb{R}^{m \times n}$ defines the control law. Although this assumes that the malicious actor has perfect state information during the attack, [20] has shown that attacks under this formulation can be extended to only requiring local data using linear state observers [30]. We refer the reader to [20] for more details, and focus on state-feedback design for the remainder of this paper.

The attack model adopts the following assumptions:

1) The linearized system analysis is valid until a machine is disconnected. Modeling the ensuing dynamics would require re-linearization around another steady state point.
2) Feedback control does not saturate the power capability of any attacking IBRs.
3) The unstable eigenvalue $\tilde{\lambda}$, introduced in Section III-B, is chosen separately from the attacking IBRs.

B. Attacker Selection Problem

With the state feedback controller, the closed-loop system is given by $\mathbf{A} - \mathbf{BK}$. Any closed-loop eigenvalue and eigenvector pair (λ_i, v_i) satisfies

$$(\mathbf{A} - \mathbf{BK})v_i = \lambda_i v_i,$$

or equivalently, by defining $w_i = \mathbf{K}v_i$,

$$(\mathbf{A} - \lambda_i \mathbf{I})v_i + \mathbf{B}w_i = 0. \tag{8}$$

To execute a successful attack, an unstable eigenvalue $\tilde{\lambda} \in \mathbb{C}$ is placed such that the target states have large components in the eigenvector $\tilde{v} \in \mathbb{C}^n$ relative to the states of the compromised IBRs. This type of attack was introduced in [8], [18], and results in a greater amplitude in the targets' unstable behavior, causing them to be disconnected by protection devices while the compromised IBRs remain connected. This idea uses eigenvector assignment to shape the system's transient behavior [31].

For any selected pair $(\tilde{\lambda}, \tilde{v})$ that satisfies (8), a corresponding gain matrix can be found. For a matrix $\mathbf{V}$ whose columns are n independent eigenvectors $\mathbf{V} = \begin{bmatrix} v_1 & \dots & v_n \end{bmatrix}$, if we compute the matrix $\mathbf{W} = \begin{bmatrix} w_1 & \dots & w_n \end{bmatrix}$ such that (8) is satisfied for all $i \in \{1, \dots, n\}$, then the gain matrix can be found as $\mathbf{K} = \mathbf{W}\mathbf{V}^{-1}$ [32].

Let the set $\mathscr{T}$ contain the indices of the ω states of the target generators. The goal of the attacker is to maximize the objective function z defined by the ratio

$$z = \frac{\sum_{i \in \mathscr{T}} v_i^H v_i}{v^H \mathbf{B}\mathbf{B}^\top v},$$

where the notation v^H represents the conjugate transpose of v. The numerator represents the participation of the target states in the unstable mode, and the denominator represents the participation of the attacker (controlled) states. A large ratio indicates that the target states have a greater amplitude in the unstable mode than the attacker and will experience more severe oscillations. In other words, maximizing z maximizes the unstable participation of the target states relative to the attacker states. In this "successful attack" scenario, the target devices will be tripped offline while the attacking devices remain online and may execute subsequent attacks. In subsequent

formations, we show the equivalent minimization of the inverse objective z^{-1} to put the binary variable $\mathbf{B}$ in the numerator.

The eigenvalue $\tilde{\lambda}$ determines the amplitude and frequency of the unstable oscillations generated by the attack and influences which targets are susceptible. Here, we assume that the complex eigenvalue $\tilde{\lambda}$ is a pre-selected constant parameter in the problem. The selection of $\tilde{\lambda}$ is discussed further in Section V-D.

For any fixed $\tilde{\lambda}$, the corresponding eigenvector $\tilde{v}$ cannot be arbitrarily set and must satisfy (8). Thus, the optimal attacker selection problem is given by

$$\begin{aligned}
\min_{v,w,\mathbf{B}_{\text{ibr}}} \quad & z^{-1} = \frac{v^H \mathbf{B}\mathbf{B}^\top v}{\sum_{i\in\mathscr{T}} v_i^H v_i} && \text{(9a)}\\
\text{s.t.} \quad & (\mathbf{A}-\tilde{\lambda}\mathbf{I})v + \mathbf{B}w = 0, && \text{(9b)}\\
& \mathbf{B}^\top \mathbf{1}_n = \mathbf{1}_m, && \text{(9c)}\\
& \mathbf{B} = \begin{bmatrix} \mathbf{0}_{(n-h)\times m} \\ \mathbf{B}_{\text{ibr}} \end{bmatrix}, \quad \mathbf{B}_{\text{ibr}} \in \{0,1\}^{h\times m}, && \text{(9d)}\\
& v \in \mathbb{C}^n,\ w \in \mathbb{C}^m, && \text{(9e)}
\end{aligned}$$

where $\mathbf{1}_n$ is the n-dimensional vector of ones. Equations (9c) and (9d) define the structure of the matrix $\mathbf{B}$, whose m columns are constrained to the standard basis vectors of the final h states. In previous works, the matrix $\mathbf{B}$ is assumed to be known, i.e., the attacking devices are specified rather than being a decision variable. References [8] and [9] have shown that for any fixed $\mathbf{B}$, (9) resolves to a generalized eigenvalue problem with a closed-form solution. We will notate this solution as

$$z^* = f(\mathbf{B}), \tag{10}$$

where the function f returns the inverse of the optimal objective of the minimization problem described by (9) with a fixed $\mathbf{B}$ matrix. When $\mathbf{B}$ is a decision variable, as in the attacker selection problem we propose in this paper, the cross-terms between binary variables in $\mathbf{B}$ and complex continuous variables v significantly increase the problem's complexity.

The first candidate solution approach is to iterate through all possible combinations of m devices, computing the optimal objective for each using (10), and selecting the best performing set. However, this brute-force search scales poorly when h and m are large, as there are $\binom{h}{m}$ total combinations.

C. MIQCP Attacker Selection

The optimization problem (9) is nonlinear with a rational objective and cross-terms in the equality constraint (9b). These complexities render it prohibitive for even state-of-the-art mixed-integer solvers. However, we can reformulate (9) into an equivalent MIQCP which solvers such as Gurobi allow.

Instead of treating the matrix $\mathbf{B}$ as a decision variable, let $x \in \{0,1\}^n$ represent which states are compromised, where x_i indicates whether the i-th state is maliciously controlled. The number of attacking devices must equal m, and only the frequency states of the IBRs can be selected. Thus, we have

$$\mathbf{1}_n^\top x = m, \tag{11}$$

$$x = \begin{bmatrix} \mathbf{0}_{n-h}^\top & x_{\text{ibr}}^\top \end{bmatrix}^\top. \tag{12}$$

An interpretation of constraint (9b) is that the matrix-vector product $(\mathbf{A}-\tilde{\lambda}\mathbf{I})v$ lies in the subspace spanned by the columns of $\mathbf{B}$. Since $\mathbf{B}$ is only comprised of standard basis vectors corresponding to the attacker states, the subspace constraint can be written as the equivalent relation

$$(\mathbf{I}-\mathbf{X})(\mathbf{A}-\tilde{\lambda}\mathbf{I})v = 0, \tag{13}$$

with the notation $\mathbf{X} = \mathsf{diag}(x)$, which states that all unselected entries of $(\mathbf{A}-\tilde{\lambda}\mathbf{I})v$ must be zero. The objective function is scale-invariant in v, and the denominator can be removed by fixing its magnitude to 1. Furthermore, the matrix $\mathbf{B}$ can be replaced by observing that $\mathbf{B}\mathbf{B}^\top = \mathbf{X}$. This intermediate reformulation with the new variable x is expressed as

$$\begin{aligned}
\min_{v,x_{\text{ibr}}} \quad & v^H \mathbf{X} v\\
\text{s.t.} \quad & \sum_{i\in\mathscr{T}} v_i^H v_i = 1,\\
& (\mathbf{I}-\mathbf{X})(\mathbf{A}-\tilde{\lambda}\mathbf{I})v = 0,\\
& \mathbf{1}_n^\top x = m, \quad x = \begin{bmatrix} \mathbf{0}_{n-h}^\top & x_{\text{ibr}}^\top \end{bmatrix}^\top,\\
& x_{\text{ibr}} \in \{0,1\}^h,\ v \in \mathbb{C}^n. && \text{(14)}
\end{aligned}$$

Each component of the eigenvector contributes to the new objective function its squared magnitude if the component corresponds to a compromised state, and zero otherwise. This relation can instead be written as a logical constraint. By introducing $c_i = x_i v_i^H v_i$, the objective becomes $\sum_i^n c_i$, and the constraints

$$c_i \geq 0, \quad c_i \geq v_i^H v_i - M(1-x_i),$$

are added for all $i \in \{1,\dots,n\}$, where M is a large (big-M) constant. The binary-continuous products are thus replaced by a linear objective and mixed-integer convex inequalities. Similarly, the subspace constraints (13) can be rewritten as linear big-M constraints as

$$-M(1-x) \leq (\mathbf{A}-\tilde{\lambda}\mathbf{I})v \leq M(1-x). \tag{15}$$

With this, the problem in (14) is transformed into the MIQCP

$$\begin{aligned}
\min_{v,x_{\text{ibr}},c} \quad & \sum_{i=1}^n c_i && \text{(16a)}\\
\text{s.t.} \quad & \sum_{i\in\mathscr{T}} v_i^H v_i = 1, && \text{(16b)}\\
& -M(1-x) \leq (\mathbf{A}-\tilde{\lambda}\mathbf{I})v \leq M(1-x), && \text{(16c)}\\
& \mathbf{1}_n^\top x = m, \quad x = \begin{bmatrix} \mathbf{0}_{n-h}^\top & x_{\text{ibr}}^\top \end{bmatrix}^\top, && \text{(16d)}\\
& c_i \geq v_i^H v_i - M(1-x_i), && \text{(16e)}\\
& c_i \geq 0, \qquad \forall i \in \{1,\dots,n\} && \text{(16f)}\\
& x_{\text{ibr}} \in \{0,1\}^h,\ v \in \mathbb{C}^n,\ c \in \mathbb{R}^n, && \text{(16g)}
\end{aligned}$$

with the normalization condition (16b) remaining the sole nonconvex constraint. When only one machine is designated as the target, (16b) is resolved and the problem is simplified to a mixed-integer convex program. We elaborate on this special but nontrivial case and provide a discussion of target selection in Section V-D.

The values of the big-M constants must be set somewhat arbitrarily, as the values of v are otherwise unbounded. However, the normalization constraint on the target states of v informs

reasonable values of M, since the attackers would like those states to have the largest magnitudes in the vector.

For some systems, the problem in (16) can be directly solved by state-of-the-art solvers such as Gurobi [28]. However, for larger systems with many candidate compromisable IBRs, both the combinatorial optimization problem (16) and brute-force searching may not be computationally practical. In the next section, we present a heuristic selection approach based on the special case of selecting a single attacker.

IV. Attack Capability Ranking Heuristic

This section discusses a special case in which only one attacking device is selected from the system's h IBRs, that is, the attack budget $m = 1$. Section IV-A shows how the attack selection problem in this special case simplifies to comparing the ratios of matrix diagonal terms. Building on this, Section IV-B develops a heuristic algorithm for the general problem based on the attacking capability of each IBR when working independently.

A. Single Attacker Scenario

In the initial formulation (9) when $m = 1$, the input matrix $\mathbf{B}$ is an n-dimensional vector that we will notate as $\mathbf{b} \in \{0,1\}^n$, and w is a complex scalar. Thus, (9) reduces to

$$\min_{v,w,\mathbf{b}_{\text{ibr}}} \quad z^{-1} = \frac{v^H \mathbf{b}\mathbf{b}^\top v}{\sum_{i\in\mathscr{T}} v_i^H v_i} \tag{17a}$$

$$\text{s.t.} \quad (\mathbf{A} - \tilde{\lambda}\mathbf{I})v + \mathbf{b}w = 0, \tag{17b}$$

$$\mathbf{b}^\top \mathbf{1}_n = 1, \tag{17c}$$

$$\mathbf{b} = \begin{bmatrix} \mathbf{0}_{(n-h)}^\top & \mathbf{b}_{\text{ibr}}^\top \end{bmatrix}^\top, \quad \mathbf{b}_{\text{ibr}} \in \{0,1\}^h, \tag{17d}$$

$$v \in \mathbb{C}^n,\ w \in \mathbb{C}. \tag{17e}$$

For simplicity of notation, let $\hat{\mathbf{A}} = (\mathbf{A} - \tilde{\lambda}\mathbf{I})^{-1}$, and define the matrix $\mathbf{C} = [\hat{\mathbf{e}}_i]_{i\in\mathscr{T}}$ that selects the target states of v. The denominator in (17a) can be rewritten as $v^H\mathbf{C}\mathbf{C}^\top v$. By substituting v in the objective using (17b), both v and w can be eliminated from the problem, leaving only binary variables. Furthermore, constraints (17c) and (17d) restrict $\mathbf{b}$ to a subset of standard basis vectors. The problem thus simplifies to

$$\min_{b} \quad \frac{(\mathbf{b}^\top \hat{\mathbf{A}}^H \mathbf{b})(\mathbf{b}^\top \hat{\mathbf{A}} \mathbf{b})}{\mathbf{b}^\top \hat{\mathbf{A}}^H \mathbf{C}\mathbf{C}^\top \hat{\mathbf{A}} \mathbf{b}} \tag{18a}$$

$$\text{s.t.} \quad \mathbf{b} \in \{\hat{\mathbf{e}}_{n-h+1}, \ldots, \hat{\mathbf{e}}_n\}. \tag{18b}$$

The product $\hat{\mathbf{e}}_i^\top \mathbf{X} \hat{\mathbf{e}}_i$ extracts the i-th diagonal value of $\mathbf{X}$. Thus, the optimal ratio z^* and reciprocal of the solution to (18) is given by the unconstrained maximization problem

$$z^* = \max_{i\in\{n-h+1,\ldots,n\}} \frac{(\hat{\mathbf{A}}^H \mathbf{C}\mathbf{C}^\top \hat{\mathbf{A}})_{ii}}{\hat{\mathbf{A}}_{ii}^H \hat{\mathbf{A}}_{ii}}, \tag{19}$$

which can be solved efficiently by comparing h ratios of matrix diagonal terms. The ratio $z_i = \frac{(\hat{\mathbf{A}}^H \mathbf{C}\mathbf{C}^\top \hat{\mathbf{A}})_{ii}}{\hat{\mathbf{A}}_{ii}^H \hat{\mathbf{A}}_{ii}}$ is a metric of how effectively IBR i can carry out a malicious attack alone.

B. The Row-Search Heuristic

We return to the general case of multiple compromised devices. Extending the single-attacker case, one natural strategy may be to control the m attackers that perform best individually. We term this the "single best" heuristic, with an attacking set $\mathscr{C}_1$ that contains the indices of the m best devices as

$$\mathscr{C}_1 = \{i : z_i \in \max_m(z_1, \ldots, z_h)\}. \tag{20}$$

The corresponding input matrix is formulated as $\mathbf{B} = [\hat{\mathbf{e}}_i]_{i\in\mathscr{C}_1}$.

In practice, this heuristic may perform sub-optimally, as the most effective IBRs at attacking alone may not be the optimal choices when attacking as a group. The interactions between the attacking devices are not captured by (19), which, when considering multiple attackers, includes expressions of the off-diagonal terms of the matrices. Alternatively, $\mathscr{C}_1$ can be used as an initial candidate set to be refined using a partial search, as shown in Algorithm 1.

Algorithm 1 Row Search Heuristic

```
Given: A, unstable eigenvalue λ̃, and target matrix C
Compute Â = (A − λ̃I)^{-1}
Initialize C_alg = C_1 from (20), and formulate B
Initialize z_best = f(B)
swapped = TRUE
while swapped = TRUE do
    swapped = FALSE
    for j ∈ C_alg do
        for k = {n−h+1, ..., n} \ C_alg do
            C = k ∪ (C_alg \ j)
            Solve (10) for z* using B = [ê_i]_{i∈C}
            if z* > z_best then
                Set C_best = C, z_best = z*
                swapped = TRUE
            end if
        end for
    end for
    C_alg = C_best, z_alg = z_best
end while
Output the refined set C_alg and objective value z_alg
```

Algorithm 1 begins with the set of IBRs obtained from (20), with an initial objective value of $f(\mathbf{B})$. The algorithm then considers swapping out any member of the current set with an unselected device. If any swap improves the objective value, the device is marked as a candidate. After all swaps have been considered, the best swap is executed, and the algorithm continues until no new swaps occur.

The algorithm is guaranteed to converge, as the objective value monotonically increases with each iteration. When h and m are large, Algorithm 1 provides an efficient alternative to brute-force searching and the MIQCP (16). The search process evaluates a much smaller subset of combinations than the exhaustive brute-force approach. While the heuristic is not guaranteed to give an optimal attacking set, Section V empirically shows that the algorithm performs exceptionally well while significantly reducing the computational burden.

V. Case Study

This section demonstrates the entire attacker selection and attack formulation process and illustrates its effect via nonlinear dynamical simulations. The main case study is conducted on the WSCC 179-bus system, with additional supporting results from the ACTIVSg500 system. We show that the heuristic algorithms produce near-optimal attacking sets for a variety of scenarios while dramatically reducing the required computational time. Finally, we discuss how the selection of targets and unstable eigenvalue affect the attack's potency.

A. Test Systems

The primary case study uses a modified version of the WSCC 179-bus system shown in Figure 1. In addition to the original 29 synchronous generators, 16 IBRs are introduced at various buses in the system with the circuit model described in [33]. The dynamic parameters of the generators are based on those of [20], and the IBR droop coefficients and time constants are selected within reasonable ranges [33]. The parameters of all network components and the initial operating point are provided in [27].

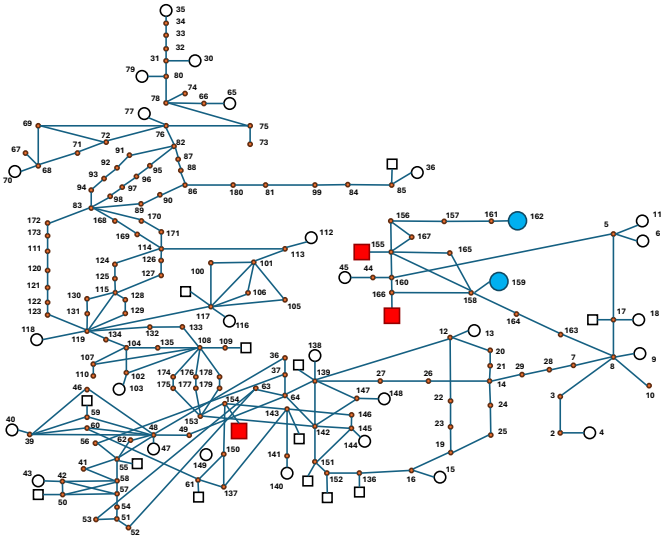

Fig. 1. Modified WSCC 179-bus System. Blue: target generators, red: compromised IBRs in the example attack.

The system is linearized around a stable operating point to obtain the state matrix $\mathbf{A} \in \mathbb{R}^{264\times264}$. States 30-58 and 249-264 represent the frequency variables of the synchronous generators and IBRs, respectively. The matrix has 86 real eigenvalues and 89 complex eigenvalue pairs. The oscillatory modes between the generators range from 2.5 to 9.4 rad/s (0.4 to 1.5 Hz).

We also utilize ACTIVSg500, a 500-bus synthetic system of South Carolina. The system contains 60 synchronous generators and is modified to include 30 vulnerable IBRs. We adopt the dynamic model (1)–(6) and set dynamic parameters to values within their typical ranges as provided in [27].

B. Example Attack

We illustrate the attack formulation process from start to finish on the WSCC 179-bus system. The target states are selected as $\mathscr{T} = \{57, 58\}$ and the unstable eigenvalue is chosen as $\tilde{\lambda} = 0.2 + j5.12$. We devise an attack in which $m = 3$ IBRs can be compromised.

TABLE I
Closed-loop eigenvector components of select states

State	v	$\lvert v\rvert$
57 (t1)	$-0.3742 - j0.0671$	0.380
58 (t2)	$-0.5679 - j0.1093$	0.578
262 (a1)	$0.0408 - j0.1715$	0.176
263 (a2)	$0.0221 - j0.1479$	0.150
264 (a3)	$0.0302 - j0.1448$	0.148
$z^* = \sum_{i\in\mathscr{T}} \lvert v_i\rvert^2 \div \sum_{j\in\mathscr{C}} \lvert v_j\rvert^2 = 6.357$		

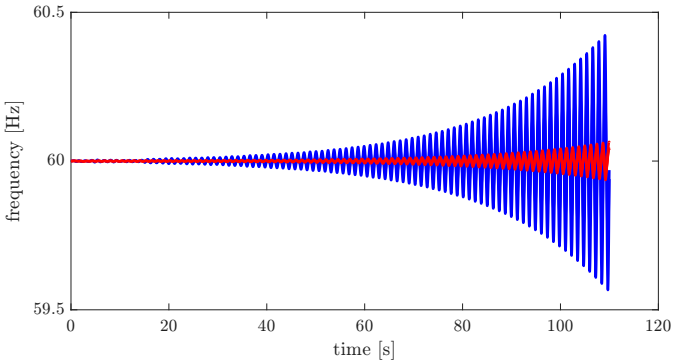

Fig. 2. DAE simulation of the WSCC 179-bus system with optimally selected attackers. Blue: target frequency states. Red: attacker frequency states.

By solving the MIQCP in (16), the best attacking set is found as $\mathscr{C} = \{262, 263, 264\}$. The target and attacker devices are shown in green and blue in Figure 1, respectively. The optimal objective of $z^* = 6.357$ indicates that the aggregated participation of the target machines is z^* times greater than that of the attacking devices. This can also be seen in the optimal eigenvector, the target and attacker components of which are shown in Table I.

The state feedback matrix $\mathbf{K} \in \mathbb{R}^{3\times264}$ is derived by replacing an existing mode with the unstable mode $(\tilde{\lambda}, \tilde{v})$. To verify that the system is destabilized by the attack, the nonlinear DAE described by (1)–(6) in Section II is simulated with malicious feedback control at the chosen IBRs. The system is subjected to a temporary 2-second line outage, and the attack begins when the line is restored. Figure 2 shows the frequency states of the target synchronous generators (blue) and the attacking IBRs (red). The simulation ends when the rate of change of a target generator's frequency (ROCOF) exceeds 2 Hz/s, the threshold adopted by [20] at which protective devices will disconnect a synchronous generator. This value is supported by [34], which found that synchronous generators generally cannot maintain stability with a ROCOF greater than 2 Hz/s.

As expected, the electrical frequency states of both the attacking devices and target generators exhibit growing oscillations at a frequency around $\mathrm{Im}(\tilde{\lambda}) = 5.12$ rad/s. The amplitude of the targets' swings is much greater than that of the attackers. The ratio of summed squared amplitudes matches the value predicted by the optimal objective function $z^* = 6.357$. The attack results in the disconnection of generator 29, which will subject the network to further dynamic transients. The linearized system may not accurately represent the system's

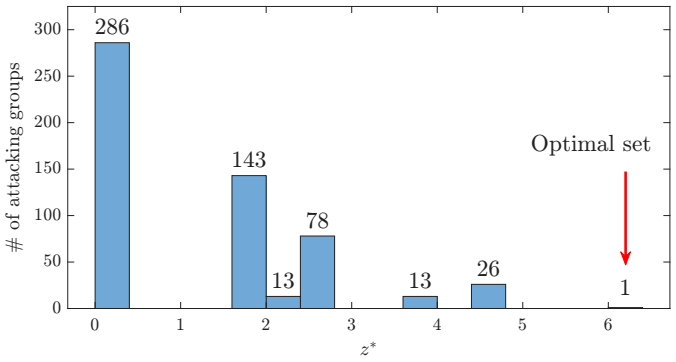

Fig. 3. Histogram of the performance of all 3-member attacking sets. The optimal set with $z^* = 6.357$ performs much better than all others.

TABLE II
PERFORMANCE METRICS OF HEURISTIC ALGORITHMS

Algorithm	Find optimal set	$\zeta \geq \zeta_{\text{optimal}}$	Avg. time (s)
WSCC-179: 2 targets (406 scenarios)			
Brute search	100%	100%	0.0120
Single best (20)	87.44%	99.59%	0.0073
Row-search (Alg. 1)	99.75%	$\sim 100\%$	0.0092
MIQCP (Eq. (16))	100%	100%	23.044
WSCC-179: 3 targets (3654 scenarios)			
Brute search	100%	100%	0.0141
Single best (20)	82.40%	99.43%	0.0090
Row-search (Alg. 1)	99.78%	$\sim 100\%$	0.0099
MIQCP (Eq. (16))	100%	100%	43.962
ACTIVSg500: 2 targets (1770 scenarios)			
Brute search	100%	100%	0.0637
Single best (20)	98.98%	99.99%	0.0401
Row-search (Alg. 1)	100%	100%	0.0415
MIQCP (16)	100%	100%	112.526

dynamics following the removal of a generator, which alters the original nonlinear system. How the system evolves and how a continued attack may ensue thereafter is a subject of future work.

To illustrate the importance of optimally selecting the attacking devices, the greatest attainable objective value for each set of $m = 3$ attackers is plotted in a histogram in Figure 3.

As this figure shows, the optimal set, whose attack is illustrated in Figure 2, out-performs all other three-device combinations by a wide margin. A majority of attacking groups can only achieve a ratio less than 1, which indicates that affecting the target synchronous generators requires these groups to inflict a more severe instability onto themselves, rendering such attacks ineffective. Thus, these results highlight that not all groups of compromised IBRs can execute a successful attack for a set of designated targets. The choice of which IBRs to compromise directly determines the level of threat an adversary may pose to the system.

C. Evaluation of Attacker Selection Heuristics

Three metrics are used to evaluate the effectiveness of the heuristic algorithms:

1) Does the heuristic identify the optimal control set?
2) How well does the heuristic attacking set perform compared to the optimal one?
3) Does the heuristic reduce the computational time of the problem?

To show the effectiveness of the heuristic selection algorithms from Section IV, we solve the problem for every combination of two and three synchronous generators as targets for the WSCC 179-bus system, and two synchronous generators as targets for the ACTIVSg500 system. In each case, a suitable eigenvalue $\tilde{\lambda}$ is first selected, and the optimization problem (16) and Algorithm 1 are used to find the best group of $m = 3$ IBRs as attackers. The aggregated results are shown in Table II, along with the brute force approach, which searches through all possible solutions.

As Table II shows, the single best heuristic is able to identify the optimal attacking set in a majority of the scenarios. On average, its solutions perform well compared to the optimal solution, even when it does not find the optimal set. The row search heuristic improves upon this, obtaining the optimal set in almost every single scenario at a small additional computational cost. Both heuristics reduce the computational time compared to the optimal methods, a reduction that becomes greater for larger values of m. Figure 4 shows this trend, comparing the average computational times of 50 2-target scenarios from the ACTIVSg500 system.

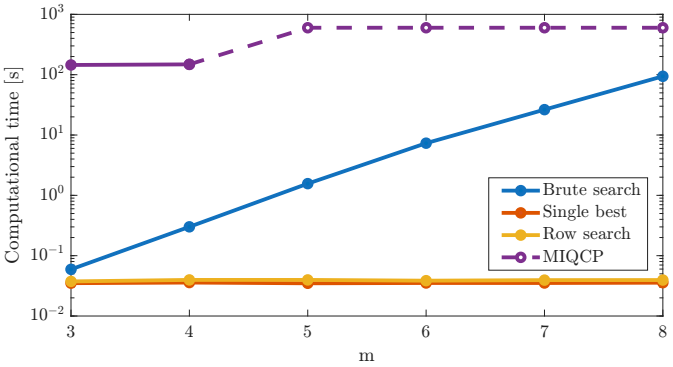

Fig. 4. A 10-minute limit was enforced for the MIQCP, with unfilled markers indicating time limit was reached. The optimal methods scale poorly while the heuristics use around the same amount of time.

For greater values of m, the brute search method slows down significantly, having to check more combinations. In contrast, the heuristic algorithms require about the same amount of time to complete as they consider only a small subset of combinations. Furthermore, the heuristics continue to identify near-optimal solutions akin to the results in Table II, showing the effectiveness of the proposed heuristics.

The MIQCP approach solves the problem optimally, but is much slower than even brute search. This may be caused by the higher dimensionality of the formulation. The brute force method solves (10) for all permissible values of the input matrix $\mathbf{B}$. However, the generalized eigenvalue problem described by (10) is m-dimensional. In contrast, the MIQCP in (16) contains n-dimensional variables and cannot be simplified to a lower dimension. Thus, when $n \gg m$, the MIQCP is outperformed by brute search. However, we present the MIQCP as a basis for future work which is elaborated upon in Section VI.

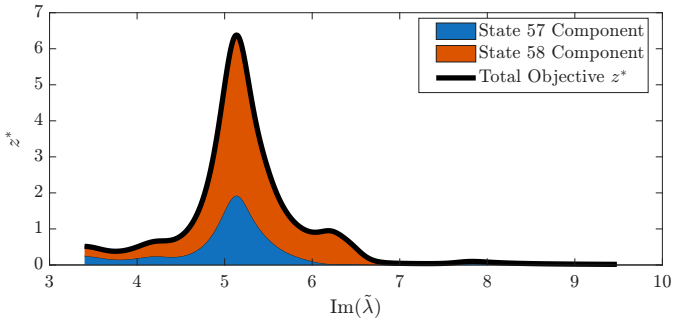

Fig. 5. Optimal objective function for the case study in V-B with various values of the placed eigenvalue's imaginary part $\mathrm{Im}(\tilde{\lambda})$.

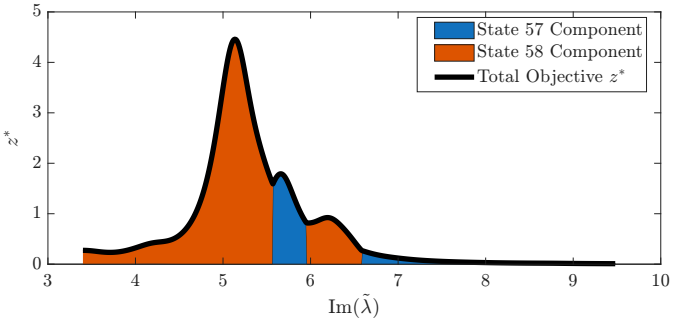

Fig. 6. Optimal objective function for the target set $\mathscr{T} = \{53, 58\}$ with various values of the placed eigenvalue $\tilde{\lambda}$.

D. Target and Eigenvalue Selection

This section examines how the selection of the targets and the unstable eigenvalue affect attack severity. We use examples from the WSCC 179-bus system to show how the unstable eigenvalue affects the attack's severity and how each machine in the target set is affected. We present an intuition-based method to select the eigenvalue and leave a more rigorous analysis as a subject of future work.

The real and imaginary components of the eigenvalue dictate the exponential rate of growth and frequency of the injected unstable mode, respectively. To set the value of real component, the adversary must consider how quickly the instability must grow to disconnect the target(s). The longer an attack continues, the more likely it is to be detected. The choice of the imaginary component plays a major role in the attack's effectiveness. Numerical simulations show that the best value lies close to the frequency of an existing oscillatory mode. Therefore, these frequencies provide candidate values for the eigenvalue's imaginary component. As a heuristic, we propose solving the attacker selection problem with each candidate value to identify the best choice for the eigenvalue's imaginary component.

From the case study in Section V-B with the target set $\mathscr{T} = \{57, 58\}$, the eigenvalue of the attack was selected as $\tilde{\lambda} = 0.2 + j5.12$. Figure 5 shows the optimal objective of (9) for different choices of $\mathrm{Im}(\tilde{\lambda})$ with a fixed $\mathrm{Re}(\tilde{\lambda}) = 0.2$. The black curve shows the variation of the optimal objective function, and the colors underneath show how each target state contributes to it. The optimal objective changes as the imaginary component varies. The peak occurs at $j5.12$, the value from the case study, at which both target states contribute substantially to the objective z^*. The participation factors of the original system show that both target machines participate in a mode with frequency $j5.14$. This indicates that generators are more susceptible to attacks close to their natural modes of oscillation, but not necessarily their most participated mode.

In the next example, the target set is altered to be $\mathscr{T} = \{53, 58\}$, and the optimal objective is plotted again for various $\mathrm{Im}(\tilde{\lambda})$ with a fixed $\mathrm{Re}(\tilde{\lambda}) = 0.2$ in Figure 6. The objective function peaks at $j5.14$, but despite the high overall objective value, only state 58 is significantly affected by the attack. A smaller peak at $j5.69$ affects only state 53. This shows that although the optimization framework in (9) maximizes the aggregated magnitudes of v in the target states, it is agnostic

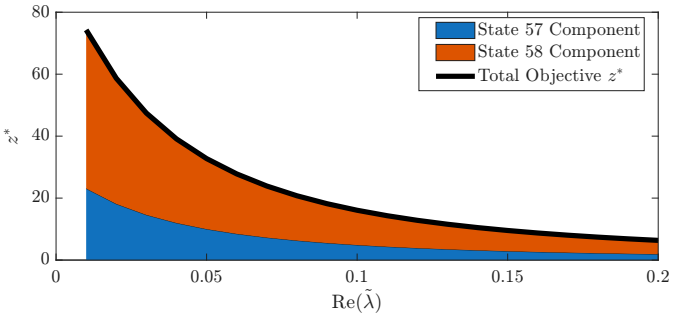

Fig. 7. Optimal objective function for the case study in V-B with various values of the placed eigenvalue's real part $\mathrm{Re}(\tilde{\lambda})$.

of how each target is affected. When multiple targets are designated, the formulated attack may affect all of them, as in Figure 5, or focus on a subset as in Figure 6.

The eigenvalue's real part controls the unstable oscillation's growth rate. To show its effect, the problem is computed with the target set $\mathscr{T} = \{57, 58\}$, with the eigenvalue's imaginary component fixed at $\mathrm{Im}(\tilde{\lambda}) = j5.12$ in Figure 7. As the real part of $\tilde{\lambda}$ is increased, the optimal objective decreases, indicating a trade-off between the rate of unstable growth and the participation of the targets relative to the attackers. The malicious actor can choose this value to balance the two factors to influence how quickly the attack unfolds.

Finally, Figure 8 shows the effect of increasing the number of devices m that can be compromised. Although compromising more IBRs increases the potency of an attack, there is diminishing value in every additional device compromised. In this case, the adversary sees negligible improvement when compromising more than three IBRs. This further reinforces our limited effort model, indicating that the selection of compromised devices is a much greater factor to a successful attack than their number.

VI. Conclusion

This paper investigated how different sets of compromised IBRs can destabilize a prescribed set of target generators. This is cast as a combinatorial optimization program that selects both which devices to compromise and how they should be maliciously controlled. An alternative MIQCP formulation and a row-search heuristic are also presented. The adopted solution approach depends on the problem's scale and desired optimality guarantees. The attacker selection process is demonstrated in

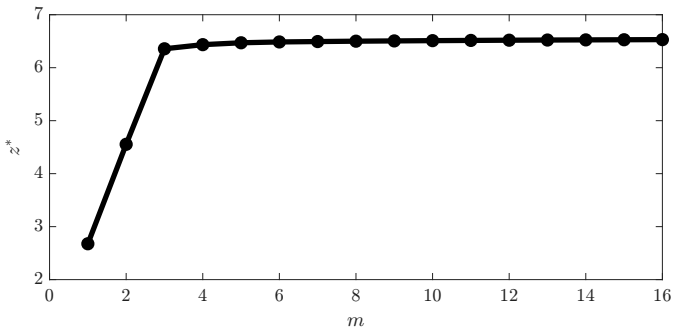

Fig. 8. Optimal objective function for the case study in Section V-B with various sizes of the attacking (controlled) set.

detail using the WSCC 179-bus network, with supplementary results for the ACTIVSg500 system. The results show that many combinations of compromised devices are unable to successfully execute an attack, highlighting the importance for an adversary to select the most potent group. We further show how the problem is influenced by the selection of the unstable eigenvalue, target set, and number of compromised IBRs. By understanding which devices may contribute to a cyber-physical attack, the goal of this work is to uncover the vulnerabilities of a system and inform where cybersecurity protection systems are most crucial.

Future work may investigate relaxation or decomposition approaches to resolve the nonconvex normalization constraint (16b) that remains in the MIQCP formulation (16). Although this formulation can be solved by commercial solvers, eliminating the nonconvex constraint would greatly simplify the problem and improve its computational time.

Another future direction is to explore the system dynamics after a synchronous generator is disconnected. Our analysis relies on a linearization around an operating point, an approximation that may break down when the system changes substantially, like when one or more generators are removed. Increasing scope to consider system behavior after an attack successfully causes generator disconnections would model an even more sophisticated attacker than considered in this paper.

REFERENCES

[1] "Digitalisation and AI for power system transformation: Perspectives for the G7," tech. rep., International Renewable Energy Agency, 2025. https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2025/Oct/IRENA_INN_Digitalisation_AI_for_power-systems_2025.pdf.

[2] "Renewable capacity highlights 2025," tech. rep., International Renewable Energy Agency, 2025. https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2025/Mar/IRENA_DAT_RE_Capacity_Highlights_2025.pdf.

[3] "Renewables 2024: Analysis and forecast to 2030," tech. rep., International Energy Agency, 2024. https://www.iea.org/reports/renewables-2024.

[4] T. Reynolds, "Cyber-physical challenges and opportunities for securing inverter-based resources," tech. rep., National Renewable Energy Laboratory, 2025. https://docs.nlr.gov/docs/fy25osti/95985.pdf.

[5] W. Hupp, D. Saleem, J. T. Peterson, and K. Boyce, "Cybersecurity certification recommendations for interconnected grid edge devices and inverter based resources," tech. rep., National Renewable Energy Laboratory, 2021. https://www.osti.gov/biblio/1832209.

[6] N. D. Tuyen, N. S. Quan, V. B. Linh, V. Van Tuyen, and G. Fujita, "A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy," *IEEE Access*, vol. 10, pp. 35846–35875, 2022.

[7] B. Ahn, T. Kim, S. Ahmad, S. K. Mazumder, J. Johnson, H. A. Mantooth, and C. Farnell, "An overview of cyber-resilient smart inverters based on practical attack models," *IEEE Trans. Power Electron.*, vol. 39, no. 4, pp. 4657–4673, 2024.

[8] C. L. DeMarco, "Design of predatory generation control in electric power systems," in *31st Hawaii Int. Conf. Syst. Sci.*, vol. 3, pp. 32–38, 1998.

[9] C. Roberts, U. Markovic, D. Arnold, and D. S. Callaway, "Malicious control of an active load in an islanded mixed-source microgrid," in *IEEE Madrid PowerTech*, pp. 1–6, 2021.

[10] P. M. Anderson and A. A. Fouad, *Power System Control and Stability*. Wiley, 2nd ed., 2003.

[11] H. Saadat, *Power System Analysis*. PSA Pub., 2010.

[12] A. M. Saber, A. Youssef, D. Svetinovic, H. Zeineldin, and E. El-Saadany, "Learning-based detection of malicious Volt-VAr control parameters in smart inverters," in *49th Annu. Conf. IEEE Ind. Electron. Soc.*, 2023.

[13] A. Bamigbade, Y. Dvorkin, and R. Karri, "Cyberattack on phase-locked loops in inverter-based energy resources," *IEEE Trans. Smart Grid*, vol. 15, no. 1, pp. 821–833, 2023.

[14] "Inverter-based resource performance issues report," tech. rep., North American Electric Reliability Corporation, 2023. https://www.nerc.com/globalassets/our-work/reports/white-papers/nerc_inverter-based_resource_performance_issues_public_report_2023.pdf.

[15] T. He, S. Li, S. Wu, and K. Li, "Small-signal stability analysis for power system frequency regulation with renewable energy participation," *Math. Probl. Eng.*, vol. 2021, no. 1, p. 5556062, 2021.

[16] B. Bahrani, M. H. Ravanji, B. Kroposki, D. Ramasubramanian, X. Guillaud, T. Prevost, and N.-A. Cutululis, "Grid-forming inverter-based resource research landscape: Understanding the key assets for renewable-rich power systems," *IEEE Power Energy Mag.*, vol. 22, no. 2, pp. 18–29, 2024.

[17] Z. Yang, M. Zhan, D. Liu, C. Ye, K. Cao, and S. Cheng, "Small-signal synchronous stability of a new-generation power system with 100% renewable energy," *IEEE Trans. Power Syst.*, vol. 38, no. 5, pp. 4269–4280, 2023.

[18] C. L. DeMarco, J. V. Sariashkar, and F. Alvarado, "The potential for malicious control in a competitive power systems environment," in *IEEE Int. Conf. Control Appl.*, pp. 462–467, 1996.

[19] S. Amini, H. Mohsenian-Rad, and F. Pasqualetti, "Dynamic load altering attacks in smart grid," in *IEEE PES Innov. Smart Grid Tech. Conf.*, 2015.

[20] H. E. Brown and C. L. Demarco, "Risk of cyber-physical attack via load with emulated inertia control," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 5854–5866, 2018.

[21] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2862–2872, 2016.

[22] M. van de Wal and B. de Jager, "A review of methods for input/output selection," *Automatica*, vol. 37, no. 4, pp. 487–510, 2001.

[23] P. V. Chanekar, N. Chopra, and S. Azarm, "Optimal actuator placement for linear systems with limited number of actuators," in *Proc. ACC*, pp. 334–339, IEEE, 2017.

[24] A. Olshevsky, "Minimal controllability problems," *IEEE Control Netw. Syst.*, vol. 1, no. 3, pp. 249–258, 2014.

[25] T. H. Summers, F. L. Cortesi, and J. Lygeros, "On submodularity and controllability in complex dynamical networks," *IEEE Control Netw. Syst.*, vol. 3, no. 1, pp. 91–101, 2015.

[26] V. Katewa and F. Pasqualetti, "Optimal dynamic load-altering attacks against power systems," in *Proc. ACC*, pp. 4568–4573, IEEE, 2021.

[27] X. Zou, "Power system dynamic test cases." https://github.com/13zouhar/Power-System-Dynamic-Test-Cases, 2026.

[28] Gurobi Optimization, LLC, *Gurobi Optimizer Reference Manual*, 2023. https://www.gurobi.com.

[29] P. Sauer and M. Pai, *Power System Dynamics and Stability*. Prentice Hall, 1998.

[30] C.-T. Chen, *Linear System Theory and Design*, vol. 301. Holt, Rinehart and Winston New York, 1984.

[31] G. Klein and B. Moore, "Eigenvalue-generalized eigenvector assignment with state feedback," *IEEE Trans. Autom. Control*, vol. 22, no. 1, pp. 140–141, 1977.

[32] P. Subrahmanyan and D. Trumper, "Eigenvector assignment," in *Proc. ACC*, vol. 4, pp. 2238–2243, IEEE, 1999.

[33] W. Du, "Model specification of droop-controlled, grid-forming inverters (REGFM_A1)," tech. rep., Pacific Northwest National Laboratory, 2023. https://www.osti.gov/biblio/2229442.

[34] W. Uijlings, D. Street, and S. London, "An independent analysis on the ability of generators to ride through rate of change of frequency values up to 2 Hz/s," *EirGrid, London, UK, Rep*, vol. 16010927, 2013.