A Stackelberg Game for Robust Cyber-Security Investment in Network Control Systems

Pratishtha Shukla, Aranya Chakrabortty, Senior Member, IEEE, and Alexandra Duel-Hallen Fellow, IEEE

Abstract—We present a resource-planning game for cyber-security of network control systems (NCS). The NCS is assumed to be operating in closed-loop using a linear state-feedback $H_2$ controller. A zero-sum, two-player Stackelberg game (SG) is developed between an attacker and a defender for this NCS. The attacker aims to disable communication of selected nodes and thereby render the feedback gain matrix to be sparse, leading to degradation of closed-loop performance. The defender, on the other hand, aims to prevent this loss by investing in protection of targeted nodes. Both players trade their $H_2$-performance objectives for the costs of their actions. The standard backward induction method is modified to determine a cost-based Stackelberg equilibrium (CBSE) that provides the optimal performance payoffs to both players while saving their individual costs. We analyze the dependency of a CBSE on the relative budgets of the players as well as on the “important” network nodes, which must be preserved to achieve a reliable $H_2$-performance. Additionally, we consider NCS models with uncertainties, and develop robust, long-term security investment games based on this cost-based SG. The proposed games are validated using an example of wide-area control electric power systems, where it is demonstrated that reliable and robust defense is feasible unless the defender is much more resource-limited than the attacker.

Index Terms—Cyber-Security, Game theory, Stackelberg game, Backward Induction, Resource Allocation, Network Control Systems, Wide-Area control, Power systems

I. INTRODUCTION

Cyber-physical security of network control systems (NCSs) is a critical challenge for the modern society [1]–[4]. While research on NCS security has focused on false data injection and intermittent denial-of-service (DoS) attacks [2]–[7], malicious destruction of communication hardware (e.g. circuit boards, memory units, and communication ports) [1] or persistent distributed DoS (DDoS) attacks (where selected targets are flooded with messages and are unable to perform their services) [8] have received relatively less attention. In reality, these attacks can cause more severe damage to the communication network of an NCS compared to data tampering and intermittent jamming as they tend to disable communication, and thus prevent feedback control, for an extended period of time, requiring expensive repairs or recovery efforts [1,8].

A legitimate question, therefore, is how can network operators invest money for securing the important assets in an NCS against attacks that disable communication permanently under a limited budget? The same question applies to attackers in terms of targeting the best set of devices whose failure to communicate will maximize damage. These types of questions are best answered using game theory, which has been used as a common tool for modeling and analyzing cybersecurity problems as it effectively captures conflicting goals of attackers and defenders [6,7,9]. However, game-theoretic research for security investments in NCS is often unrelated to the physical system model [10] and usually employs dynamic games where the players repeatedly update their investment strategies in response to the actions of their opponents in real time [5,6]. The latter approach, however, might not be practical when long-term, fixed security investment is desired. Recently a mixed-strategy (MS) investment game for mitigation of hardware attacks on an NCS was presented in [11]. However, MS games [6,7,12] are also unsuitable for realistic, long-term security investment since they have randomized strategies and must be played many times to realize the expected payoffs. A long-term security investment game has been proposed in [13] recently, but this game does not address any kind of dynamic performance, nor does it address model uncertainties.

In this paper, we develop a Stackelberg game [14] for persistent malicious attacks on NCSs, where fixed, non-randomized investment strategies are determined for both players. The NCS is assumed to be operating in closed-loop using a state-feedback $H_2$ controller. The actions of the players are modeled as discrete investment levels into the network nodes. These levels indicate the chances of success for attack or protection at a given node. The need for feedback control in the model guides the selection of the levels of attack and security investment at each node. The attacker aims to disable communication to/from a set of selected nodes, which makes the feedback gain matrix sparse, thereby degrading the closed-loop $H_2$-performance. The defender, on the other hand, invests in tamper-resistant devices [3], intrusion monitoring, threat management systems that combine firewalls and anti-spam techniques [4], devices or software that ensure authorized and authenticated access via increased surveillance [15], etc. to prevent the attacks and maintain the optimal $H_2$-performance. A Stackelberg Equilibrium (SE) [14] of this game describes an optimal resource allocation of the two players given their respective budgets. Moreover, we develop an algorithm for computing a cost-based SE (CBSE), which saves the players’ costs without compromising their payoffs, and analyze the dependency of the players’ payoffs at CBSE on the budgets and numbers of investment levels.

Furthermore, we develop robust game-theoretic investment approaches for NCS with model uncertainties. The model parameters of an NCS usually vary over time due to changes in operating conditions, thereby making the NCS model uncertain [16]. Modifying the security investment as these changes occur can be time-consuming, expensive and infeasible if the model is unknown for the upcoming time interval. Thus, unlike in repeated dynamic games [6], we seek fixed, long-term...
investment that provides robust $H_2$-performance over a set of future uncertain models. We propose and analyze the trade-offs of two SG designs for uncertain model sets, based on the average-payoff and nominal-model payoff criteria.

The proposed games are validated using an example of wide-area control for the IEEE 39-bus model, which represents the New England power system. First, we show that as the cost of defense per node increases, CBSEs of the proposed cost-based Stackelberg game (CBSG) reveal the “important” physical nodes [11,17] that need higher levels of protection. Second, we demonstrate that reliable control performance can be maintained unless the defender’s resources are much more limited than the attacker’s. Third, we perform a statistical payoff comparison to examine the trade-offs of the SGs proposed for uncertain model sets and demonstrate feasibility of robust, long-term protection for power systems with load uncertainty.

The main contributions of this paper are:

- Development of a Stackelberg security investment game for hardware or persistent DDoS attacks on communication equipment of NCSs.
- Formulation and analysis of robust, long-term Stackelberg security investment games for NCSs with uncertain dynamic models.

The rest of the paper is organized as follows. In Section II, we present an NCS model as well as attack and defense models. The proposed CBSG and investment games for uncertain system models are formulated in Section III. Numerical results are provided in Section IV. Section V concludes the paper.

II. System Model and Attack and Defense Models

We consider an NCS with $n$ nodes. Each node may be characterized by multiple states and control inputs, as shown in Fig. 1. At the $i^{th}$ node, the state vector is denoted as $x_i \in \mathbb{R}^{m_i}$, with the total number states $m = \sum_{i=1}^n m_i$, and the control input is denoted as $u_i \in \mathbb{R}^r_i, i = 1, \ldots, n$, with the total number of control inputs $r = \sum_{i=1}^n r_i$. The state-space model of the network is written as

$$\dot{x}(t) = Ax(t) + Bu(t) + Dw(t),$$

where $x(t) = (x_1^T(t), \ldots, x_n^T(t))^T \in \mathbb{R}^{m 	imes 1}$, $u(t) = (u_1^T(t), \ldots, u_n^T(t))^T \in \mathbb{R}^{r 	imes 1}$, $w(t) \in \mathbb{R}^{q \times 1}$ is the disturbance and $A \in \mathbb{R}^{m \times m}, B \in \mathbb{R}^{m \times r}, D \in \mathbb{R}^{m \times q}$ are the state, input, and disturbance matrices, respectively. The control input $u(t)$ is designed using linear state-feedback

$$u(t) = -Kx(t),$$

where $K \in \mathbb{R}^{r \times m}$ is the feedback gain matrix:

$$K = 
\begin{bmatrix}
K_{11} & K_{12} & \cdots & K_{1n} \\
K_{21} & K_{22} & \cdots & K_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
K_{n1} & K_{n2} & \cdots & K_{nn}
\end{bmatrix}.$$  

(3)

From (3) it follows that

$$u_j(t) = -K_{jj}x_i$$

(4)

i.e. the $r_i \times m_j$ block matrix $K_{ij}$ represents the topology of the communication network needed to transmit the state of node $i$ to the controller at node $j$. The diagonal blocks $K_{ii}$ correspond to the local, or self-links, while the off-diagonal blocks $K_{ij}, i \neq j$ indicate the inter-node communication links, respectively, as shown in Fig. 1.

The objective is to find the feedback matrix $K$ that minimizes the $H_2$-performance cost function

$$J(K) = \text{trace}(D^TPD)$$

subject to

$$\sum_{i=1}^n (A - BK_i)x = 0$$

$$J_p = \sum_{i=1}^n (A - BK_i)x = 0$$

$$\text{trace}(K^TRK)$$

where $p$ is the closed-loop observability Gramian, $Q = Q^T \geq 0 \in \mathbb{R}^{r \times r}$ and $R = R^T > 0 \in \mathbb{R}^{r \times r}$ are design matrices that denote the state and control weights, respectively. With standard assumptions, $(A, B)$ is stabilizable and $(A, Q^{1/2})$ is detectable [17].

In Fig 1, the nodes directly communicate with each other, following the connectivity dictated by $K$ in (3). Another option, which is becoming more common in NCSs to ensure data privacy, is a third-party cloud network that emulates the communication layer, with a virtual machine (VM) created in the cloud layer for each physical node. The physical nodes transmit their measured states to their respective VMs. The VMs then communicate with each other following the connectivity of $K$ in (3) to exchange the state information and compute the control inputs, which are then transmitted back to their respective physical nodes for actuation [18].

In the remainder of this paper, we consider attacks and protection for both communication network models discussed above. In both cases, communication equipment of individual nodes can be targeted. Moreover, in the second option above, attacker can break into the cloud and launch attacks on selected VMs. In both cases, the hardware or persistent DDoS attacks can prevent the affected nodes or their VMs from sharing their state information and compromise their control inputs, thereby inducing sparsity in $K$ (3) and degrading the closed-loop $H_2$-performance (i.e. resulting in a suboptimal value of $J$ in (5)). The attacker invests as per its budget into selected nodes (or VMs) to increase the value of $J$ in (5) while the defender aims to protect against attacks by installing tamper-resistant devices and/or intrusion monitoring software. Note that the defender does not know when and where an attack might happen, so it acts proactively by selecting a set of nodes (or VMs) and the protection levels to maintain $J$ as low as possible within the defense budget in case of a future attack. Since the proposed game applies to both direct communication and cloud-based networks, we formulate a single game, referring to either the

\begin{figure}[h]
\centering
\includegraphics[width=0.8\textwidth]{system_topology.png}
\caption{System topology}
\end{figure}
nodes in Fig. 1 or their VMs as “nodes” for the rest of the paper.

III. COST-BASED STACKELBERG INVESTMENT GAME

We employ the Stackelberg [14] investment game where the attacker and defender invest into disabling and protecting the communication capabilities of selected system nodes, respectively. The attacker’s actions \( a \) and the defender’s actions \( d \) indicate the levels of investment into the system nodes, which measure the chances of successful attack and protection at these nodes, respectively. Both players have budget constraints and also aim to reduce their costs of attack or protection.

The players have opposite control performance goals — the attacker aims to increase the \( \mathcal{H}_2 \)-performance cost in (5) while the defender tries to keep it as close to the optimal value as possible, resulting in the payoffs \( U^a(a, d) \) and \( U^d(a, d) \) for the attacker and the defender, respectively. Given a pair of investment strategies \((a, d)\), \( U^d(a, d) = -U^a(a, d) \), resulting in a zero-sum game [19].

As in many SGs for security [5,9,13], the defender is the leader and chooses the investment profile first. Given a defender’s action \( d \), the attacker follows by a best-response to \( d \), given by \( a = g(d) = \arg \max U^a(a, d) \). Thus, the defender chooses a strategy \( d \) that maximizes its payoff given the attacker’s best responses to its actions. A resulting Stackelberg Equilibrium (SE) [14] specifies a pair of strategies \((a^*, d^*)\), which optimizes the payoffs of the players in an SG. Finally, we augment the standard SG described above by selecting an SE that reduces the players’ costs [13]. The resulting game is termed cost-based Stackelberg game (CBSG).

A. Player’s Actions and Cost Constraints

The actions of the players are given by \( n \)-dimensional investment vectors into the system nodes, denoted as
\[
a = (a_1, a_2, \ldots, a_n), \quad d = (d_1, d_2, \ldots, d_n)
\]  
(6)

for the attacker and the defender, respectively. A higher value of \( a_k \) (or \( d_k \)) corresponds to a larger attack (or protection) investment level at node \( k \). The levels \( a_k \) in (6) are chosen from the set \( \{0, \frac{1}{L_a}, \frac{2}{L_a}, \ldots, 1\} \) where \( L_a + 1 \) is the total number of attacker’s investment levels. Similarly, \( d_k \in \{0, \frac{1}{L_d}, \frac{2}{L_d}, \ldots, 1\} \) where \( L_d + 1 \) is the number of defender’s investment levels. Given the actions \( a \) and \( d \), the probability of successful attack at node \( k \) is given by
\[
P_k(a, d) = a_k (1 - d_k).
\]  
(7)

The set of possible attack outcomes at all nodes is represented by a set of \( 2^n \) sparsity patterns, or binary \( n \)-tuples,
\[
s_m = (s_{m}^1, \ldots, s_{m}^n)
\]  
(8)

where \( s_{m}^k = 0 \) indicates an attack is successful at node \( k \) while \( s_{m}^k = 1 \) means that either protection is successful at node \( k \) or node \( k \) is not attacked. From (7), the probability that the sparsity pattern \( s_m \) occurs given the strategy pair \((a, d)\) is
\[
P_{s_m}(a, d) = \prod_{k, \ s_{m}^k = 0} P_k(a, d) \prod_{k, \ s_{m}^k = 1} (1 - P_k(a, d)).
\]  
(9)

Finally, the players’ budgets are as follows. Let \( \gamma_a \) and \( \gamma_d \) denote the cost of attack and protection of node \( i \) at full effort, i.e., when \( a_i \) (or \( d_i \)) = 1, respectively. Scaling this cost by the level of effort and summing over all nodes, the actions of the players are cost-constrained as
\[
\sum_{i=1}^{n} \gamma_a a_i \leq 1, \quad \sum_{i=1}^{n} \gamma_d d_i \leq 1.
\]  
(10)

Remark 1. In (10), we have assumed without loss of generality that the total cost of each player is bounded by 1. Thus, \( \gamma_a \) and \( \gamma_d \) are scaled costs per node \( i \) for the attacker and the defender, respectively.

Assumption 1. In this paper, we assume that the opponent’s budget and the number of investment levels are known to each player. Moreover, we assume that the players have the same (symmetric) knowledge of the system model and model uncertainty. These idealistic assumptions justify the zero-sum game property and result in a baseline game performance characterization. Extensions to the asymmetric system knowledge and uncertainty about the opponent’s action set will be addressed in future work.

B. Structural Sparsity and Players’ Payoffs

When a sparsity pattern \( s_m \) (8) occurs, all communication to/from each node \( k \) for which \( s_{m}^k = 0 \) is disabled. Thus, the corresponding feedback matrix \( \mathbf{K} \) in (3) has the sub-blocks \( \mathbf{K}_{kp} = 0 \) and \( \mathbf{K}_{pk} = 0 \) for all \( p = 1, 2, \ldots, n \), \( q = 1, 2, \ldots, n \), imposing the structural sparsity constraint [20] on the matrix \( \mathbf{K} \). For example, Fig. 2 shows the scenario where communication is disabled within and to/from node 3 and the resulting structural sparsity of the feedback matrix \( \mathbf{K} \).

Next, given \( s_m \), we define the \( \mathcal{H}_2 \)-performance loss vector \( \Delta \) with the elements
\[
\Delta_{s_m} = J(I_{s_m}^*) - J(K_{s_m}^*) \quad i = 0, \ldots, 2^n - 1
\]  
(11)

where \( K_{s_m}^* \) and \( I_{s_m}^* \) optimize the \( \mathcal{H}_2 \)-performance objective function in (5) without and with the structural sparsity constraint imposed by \( s_m \), respectively. The latter can be computed using the structured \( \mathcal{H}_2 \) optimization algorithm in [20]. The loss corresponding to the sparsity pattern \( s_0 = (0, \ldots, 0) \) represents the open-loop loss given by
\[
\Delta_{OL} = J_{OL} - J(I_{s_m}^*)
\]  
(12)

where \( J_{OL} \) is \( \mathcal{H}_2 \)-performance of the open-loop system.

Given \( a \) and \( d \), the attacker’s payoff is
\[
U^a(a, d) = \sum_{m=0}^{2^n-1} P_{s_m}(a, d) \Delta_{s_m}
\]  
(13)
The following properties hold for the proposed CBSG:

(a) A CBSE exists and has the same payoff as any other SE.
(b) Given $L_a$ and $L_d$, the payoff of each player is non-increasing with its cost per node when the opponent’s cost per node is fixed.
(c) Given $L_a$ and $L_d$, there exist $\epsilon > 0$ and $\theta > 0$ such that when $\gamma_a < \epsilon$ while $\gamma_d > \theta$, the attacker’s payoff at CBSG $U^a(a^*, d^*) = \Delta_{\text{OL}}$ (the open-loop loss (12)). Moreover, there exists an $\alpha > 0$ such that when $\gamma_d < \alpha$, the attacker’s payoff at CBSG $U^a(a^*, d^*) = 0$ (i.e. the optimal $H_2$-performance is achieved).
(d) When $L_d$ (or $L_a$) is increased to $L_{d}'$ (or $L_{a}'$) that satisfies $L_{d}' = L_{d}^\eta(L_d)$ (or $L_{a}' = L_a^\eta(L_a)$), where $\eta$ is a positive integer, the defender’s (or attacker’s) payoff does not decrease if the costs per node of both players and the opponent’s number of investment levels $L_a$ (or $L_d$) are fixed.

The proof is similar to the proof of Theorem 1 in [13] and is omitted for brevity.

### D. Robust Investment for Systems with Model Uncertainty

The CBSG developed above assumes a fixed system model in (1), which we refer to as a nominal model $M_{\text{nom}}$. In practice, the model varies with time. We denote the set of possible system models over a long time interval by $\mathcal{M} = \{M_i = \{A_i, B_i\}, i = 1, ..., M\}$, where $A_i$ and $B_i$ are the state and input matrices in (1) of the nominal model ($i = 1$) and $M - 1$ uncertain models.

If a CBSE $(a_{\text{nom}}^*, d_{\text{nom}}^*)$ of the SG designed for $M_{\text{nom}}$ is employed as an investment strategy for any model $M_i \in \mathcal{M}$, the resulting game is termed the “nominal-model” SG. The payoff of this game can be mismatched since $(a_{\text{nom}}^*, d_{\text{nom}}^*)$ might be a suboptimal investment strategy when $i \neq 1$. The resulting mismatch $\mu_{\text{i,nom}}\%$ is given by

$$
\mu_{\text{i,nom}}\% = \left| \frac{U^a_{M_i}(a_{\text{nom}}^*, d_{\text{nom}}^*) - U^a_{M_i}(a_{i}^*, d_{i}^*)}{U^a_{M_i}(a_{i}^*, d_{i}^*)} \right| \times 100\% 
$$

(20)

where $U^a_{M_i}(a, d)$ is the attacker’s payoff (13) when the actual model is $M_i$ and $(a_{i}^*, d_{i}^*)$ is a CBSE of the SG designed for model $M_i$. Note that $\mu_{1,nom} = 0$. A similar game can be designed based on an initial model $M_1$, $i \neq 1$, instead of $M_{\text{nom}}$.

The design of the above game does not take into account the knowledge of the uncertain model set. In the following robust game, the payoffs are modified to account for the system variation while the action sets and the cost constraints are the same as in the fixed-model game. In this “average-payoff” SG, the attacker’s payoff is defined as the expectation of the losses of all possible system models in $\mathcal{M}$ as

$$
U^a_{\text{avg}}(a, d) = \sum_{j=1}^{M} \phi_{M_j} U^a_{M_j}(a, d) 
$$

(21a)

$$
= \sum_{m=0}^{2^n-1} P_{s_m}(a, d) \left[ \sum_{j=1}^{M} \phi_{M_j} \Delta_{s_m} \right] 
$$

(21b)
where \( P_{\phi_{M_j}}(a, d) \) is given by (9), \( \phi_{M_j} \) is the probability of occurrence of the model \( M_j \), \( \sum_{j=1}^{M} \phi_{M_j} = 1 \), and \( \Delta_{s_m}^M_{-\ell} \) is the loss in (11) associated with the model \( M_j \) for the sparsity pattern \( s_m \) in (8). The expression (21b) saves computation relative to (21a) since in the latter \( M \) payoff matrices must be computed while only one such matrix is needed in the former, based on the expected loss \( E(M_j) = \sum_{j=1}^{M} \phi_{M_j} \Delta_{s_m}^M_{-\ell} \). Note that (21) represents an unbiased estimate of the attacker’s expected payoff over the set \( M \). The mismatch \( \mu_{i,\text{avg}}(\%) \) of this game’s payoff when the actual system model is \( M_i \) is computed as

\[
\mu_{i,\text{avg}} \% = \frac{\| U_{M_i}^\ast(a_{\text{avg}}^i, d_{\text{avg}}^i) - U_{M_i}^\ast(a_{\text{avg}}^i, d_{\text{avg}}^i) \|}{\| U_{M_i}^\ast(a_{\text{avg}}^i, d_{\text{avg}}^i) \|} \times 100 \%
\]

(22)

where \( (a_{\text{avg}}^i, d_{\text{avg}}^i) \) is a CBSE of the average-payoff SG (21).

Note that the average-payoff SG in (21) requires more information than the nominal-model SG in (20). In particular, the latter just needs the knowledge of the nominal system model at the time of investment planning. On the other hand, the former game requires the knowledge of the payoffs and their distributions for all models in \( M \). We also note that the computation complexity of both games in this section is similar to that of the fixed-case game (see Remark 3).

Remark 4. Both games in this section are zero-sum. The zero-sum property of the average-payoff game stems from Assumption I on symmetric system knowledge by the two players.

IV. NUMERICAL RESULTS FOR WIDE-AREA CONTROL OF ELECTRIC POWER SYSTEMS

A. Power system model

To demonstrate the performance of the proposed investment games, we consider one of the most important and safety-critical example of an NCS, namely, an electric power system. The linear static state-feedback controller to be designed is referred to as wide-area control [21], which helps in damping system-wide oscillations of power flows by minimizing the \( H_2 \) performance function in (5). Before discussing the game, we first briefly overview the dynamic model of the system.

Consider a power system network with \( n \) synchronous generators and \( \ell \) loads. We assume the \( i \)-th generator to consist of \( m_i \) states \( \xi_i = [\delta_i, \omega_i, x_{i,\text{rem}}] \in \mathbb{R}^{m_i} \) (where \( x_{i,\text{rem}} \) is the vector of all non-electromechanical states), one scalar control input \( \Gamma_i \), and \( \sum_{i=1}^{n} m_i = m \) (total number of states). All the loads in the system are considered as constant power loads without any dynamics. Let the pre-disturbance equilibrium of the \( i \)-th generator be \( \xi_i^0 \). The differential-algebraic model of the entire system, consisting of the generator models and the load models together with the power balance in the transmission lines, is converted to a state-space model using Kron reduction (for details, please see [22]) and linearized about \( \xi_i^0, i = 1, 2, ..., n \). The small-signal state of generator \( i \) (or node \( i \)) is defined as \( x_{i}(t) = \xi_i(t) - \xi_i^0 \). The small-signal model is thereafter written in the form of (1). The small-signal control input is given by \( u_i(t) = \Delta \Gamma_i \).

To evaluate the performance of the games for uncertain models, we consider the uncertainties arising from the \( \ell \) loads. The load active and reactive power setpoints are gradually increased to a critical level until the power flow solution fails to converge. The load powers are then slightly lowered from their failing values. By repeating this process for each load, we thus create \( \ell \) uncertain models. We then linearize each model around its operating point to produce a model \( M_j = \{ A_j, B_j \} \) in the set \( M \) in section III.D. The total number of models in \( M = \ell + 1 \) where the “nominal” model \( M_{\text{nom}} \) is generated using the default load settings of the 39-bus model. Since the matrices \( B \) and \( D \) in (1) are independent of the load, we assume that they are the same for all uncertain models.

For the wide-area control design, \( R \) is chosen as the identity matrix while \( Q = \text{diag}(\hat{\mathcal{L}}, I_n, I_{m-2n}) \), so that all generators arrive at a consensus in their small-signal changes in the phase angles. Here, \( \hat{\mathcal{L}} = nI_n - 1_n \cdot 1_n^T \) [23], where \( 1_n \in \mathbb{R}^{n \times 1} \) is the column vector of all ones, \( I_n \) is an \( n \times n \) identity matrix and \( I_{m-2n} \) is an \( m - 2n \times m - 2n \) identity matrix.

We assume all states to be available, either from direct measurement using Phasor Measurement Units (PMUs) or via generator-wise state estimation using decentralized Kalman filters [24]. The states of the generators are communicated to the VMs to exchange \( \xi_i \) and compute \( u_i \) using (2) within the cloud [18]. The attack model for this network is detailed in Section II, with VMs of individual generators playing the roles of the nodes.

B. SG performance for fixed system model

We employ the IEEE 39-bus power model, which consists of 10 synchronous generators and 19 loads, to evaluate the performance of the proposed SGs. Generator 1 is modeled by 7 states, generators 2 through 9 are modeled by 8 states each while generator 10 is an equivalent aggregated model for the part of the network that we do not have control over, modeled by 4 states. Therefore, \( n = 9 \). The dimension of the state vector in (1) is \( m = 75 \), i.e. \( A \in \mathbb{R}^{75 \times 75} \), with the total number of control inputs \( r = 9 \), resulting in \( B \in \mathbb{R}^{75 \times 9} \) and \( K \in \mathbb{R}^{9 \times 75} \). We assume that \( D \in \mathbb{R}^{75 \times 9} \) is a matrix with all elements zero except for the ones corresponding to the acceleration equation of all generators. The 19 load buses result in 19 uncertain models as discussed above, along with one nominal system model. The data set for the IEEE 39-bus system along with uncertain models can be found in [25]. We make a practical assumption that all 20 models are equally likely, i.e. \( \phi_{M_j} = \frac{1}{20} \) in (21).

In this section the game is evaluated for the fixed nominal model available in [25]. Table I illustrates the fractional control performance losses \( \frac{\Delta_{s_m}^M_{-\ell}}{\Delta_{s_m}^M_{-\ell}^0} (\%) \) (see (11)) for the sparsity patterns where only one element of \( s_m \) in (8) is zero, i.e. only one generator is disabled. The highest loss is observed for the disabled generator 9, followed by the generators 8, 4, 7, 5, 3, 2, 6, 1, imposing the “importance” ranking of the generators, or nodes. From Table I, we observe that when only the inter-node communication links are disabled while the self-links are intact (see Fig. 1), the losses are greatly reduced, confirming that retaining the self-links is critical for
Fig. 3 shows the fractional attacker’s payoff (13) (relative to $J(K^a_{L_d})$) at CBSE versus the players’ costs while Fig. 4 illustrates the players’ strategies and payoffs at CBSE. In both Figures, we assume that all nodes of each player have the same cost per node in (10), i.e., $\gamma_a = \gamma_d$, $\gamma_d = \gamma_d$ for all $i = 1, \ldots, n$. We observe the performance trends are consistent with Theorem 1(a)–(c).

In general, multiple SEs are possible for any choice of SG settings. In this example, they occur in the outlined regions of Fig. 3. The cost pair boundaries of these regions depend on the parameters $n = 9$ and $L_a = L_d = 3$. First, multiple SEs exist when $\gamma_d \leq \frac{1}{2}$, i.e., the defender is capable of protecting all nodes, resulting in $U^a(a^*, d^*) = 0$ (no loss) while the attacker chooses not to act at CBSE since it cannot change its payoff as shown in the first row of Fig. 4. The second region of multiple SEs corresponds to $\gamma_a > 3$ where the expected loss is zero since the attacker does not have resources to attack in this region. In the example, a CBSE occurs when the defender also chooses not to act (see the second row of Fig. 4). Finally, multiple SEs exist when $\gamma_a \leq \frac{1}{2}$ while $\gamma_a < \gamma_d \leq 3$ where the attacker is able to attack all nodes fully but both players choose cost-saving strategies. For example, in the third row of Fig. 4, the attacker saves its cost by not investing into node 9 at CBSE since the defender fully protects this most “important” node.

In the fourth row of Fig. 4, the defender is very resource-limited and thus does not act while the attacker attacks all nodes, resulting in the open-loop system, which occurs in the region $\gamma_a \leq \frac{1}{2}$, $\gamma_d > 3$ shown in Fig. 3. The last three rows of Fig. 4 illustrate the scenarios where one or both players are resource-limited, and thus choose from the “important” nodes (Table I) to optimize their payoffs strategically. In the fifth row, the defender invests into the most “important” node 9 at the level $d_9 = \frac{1}{3}$ while the attacker has sufficient resources to invest fully into both “important” nodes 9 and 8, thus raising the expected system loss above 50%. When $\gamma_a = 2$, $\gamma_d = 1$ (sixth row), the defender invests into the “important” nodes 9 and 8 while the attacker chooses the unprotected, but still “important”, node 4 since it has low chance of affecting the outcome for the more “important” nodes due to its limited budget. The resulting attacker’s payoff is low in this case. Finally, in the last row, the defender is more resource-limited than the attacker, and both players target node 9 at the levels dictated by their cost constraints in (10), with the resulting payoff increasing relative to the sixth row.

![Multiple SEs](image)

**Fig. 3:** Attacker’s fractional payoff at CBSE vs. costs per node $\gamma_a$ of the attacker and $\gamma_d$ of the defender; $L_a = L_d = 3$

![Players’ strategies and attacker’s fractional payoff at CBSE](image)

**Fig. 4:** Players’ strategies and the attacker’s fractional payoff at CBSE for several $(\gamma_a, \gamma_d)$ pairs; $L_a = L_d = 3$

While we assumed that all nodes have the same costs $\gamma_a$ or $\gamma_d$ for the attacker and defender, respectively, in some systems, the cost of attacking or protecting a certain node (e.g. an “important” node) might be higher than that for other nodes. For example, we found that when a player’s cost of the most “important” node 9 increases significantly relative to the costs of the other nodes, that player avoids investing into node 9, and thus it’s payoff decreases.

In Fig. 5, we illustrate the players’ fractional payoffs for $\gamma_a = \gamma_d = 1.5$ (which characterize moderate resources of both players) as a player’s number of investment levels varies while its opponent’s number of investment levels is fixed.

### Table I: Ranking of node “importance” according to the fractional loss $\Delta_{OL}$ (%)

| Node Rank | Node | Disabled generator | Fract. loss % (local links disabled) | Fract. loss % (local links intact) |
|-----------|------|--------------------|-------------------------------------|-----------------------------------|
| 1         | 9    | 40.7               | 0.07                                | 8.41                              |
| 2         | 8    | 17.96              | 0.06                                | 14.64                             |
| 3         | 4    | 17.67              | 0.06                                | 13.47                             |
| 4         | 7    | 16.29              | 0.057                               | 16.26                             |
| 5         | 5    | 16.26              | 0.057                               | 18.12                             |
| 6         | 2    | 14.63              | 0.045                               | 17.96                             |
| 7         | 3    | 14.63              | 0.045                               | 17.67                             |
| 8         | 6    | 13.41              | 0.04                               | 13.47                             |
| 9         | 1    | 3.79               | 0.01                                | 13.47                             |

Open-loop 1,2,3,4,5,6,7,8,9 181.92 0.4

---

Fract. loss

exist when $\gamma_a \leq \frac{1}{2}$, resulting in the open-loop fractional loss shown. The open-loop fractional loss is also shown.

...
Similar simulations were performed for other cost pairs, and the results are consistent with Theorem 1(d). We observe that setting a player’s number of levels to three provides a near-optimal payoff for that player for any fixed opponent’s number of levels. Thus, \( L_a = L_d = 3 \) is used in the numerical results throughout the paper.

Finally, we compare the proposed game with individual optimization (IO), where the attacker aims to degrade the system performance by increasing the \( \mathcal{H}_2 \)-performance cost \( J \) in (5), while the defender aims to decrease it. Both players act under their individual budget constraint and without taking into account the opponent’s possible actions. While each player always targets its “important” nodes in IO, in the game the players’ strategies affect each other and the attacker often prefers to avoid the nodes protected by the defender as illustrated in Fig. 4. We found that each player’s payoff can be up to 50% lower when using IO relative to playing the game for some cost pairs \((\gamma_a, \gamma_d)\). Moreover, the players’ costs can be significantly lower when playing the proposed CBSG than in IO since the CBBH algorithm in Section III.C selects an SE with the lowest cost while in IO each player invests fully up to its budget constraint.

### C. Performance of SGs for uncertain systems

In this section, we simulate the games for the uncertain model set of the 39-bus system, created by varying the loads from their nominal values as discussed in Section IV.A and further detailed in [25]. In this section \( J_{M_i}(\mathbf{K}^*_i, \mathcal{H}_2) \) denotes the optimal \( \mathcal{H}_2 \)-performance (5) for the system \( M_i \in \mathcal{M} \). First, to assess the degree of uncertainty among the models in \( \mathcal{M} \), we applied the optimal controller designed for the nominal model \( \mathbf{K}^*_{\text{nom}, \mathcal{H}2} \) to each model \( M_i \in \mathcal{M} \). We found that this mismatched controller can have up to 13.71% worse performance than the optimal controller \( \mathbf{K}^*_i, \mathcal{H}2 \) designed for the model \( M_i \in \mathcal{M} \), thus confirming large diversity of the model set \( \mathcal{M} \) [25].

In Fig. 6, we demonstrate that the payoff of the SG designed for model \( M_i \in \mathcal{M} \) (at its CBSE) follows the trends of the nominal model (Fig. 3, 4). Note that the payoff difference between the models \( M_i \in \mathcal{M} \) is at most 5%. Moreover, we found that for all 20 systems, node 9 is the most “important”, but the order of “importance” of the remaining nodes varies. Thus, the players’ strategies at CBSEs of the SGs designed for these models differ significantly.

The payoffs of the games for uncertain models discussed in Section III.D are compared in Fig. 7 for two different cost pairs (chosen to reflect moderate resources of both players) and five actual system models. The fractional payoffs of the nominal-model SG \( U_{M_i}^{\gamma}(\mathbf{a}^*_{\text{nom}}, \mathbf{d}_i^{\gamma}_{\text{nom}}) \) (20), the average-payoff SG \( U_{M_i}^{\gamma}(\mathbf{a}^*_{\text{avg}}, \mathbf{d}_i^{\gamma}_{\text{avg}}) \) (21), and the ideal SG \( U_{M_i}^{\gamma}(\mathbf{a}^*_i, \mathbf{d}^*_i) \) with respect to \( J_{M_i}(\mathbf{K}^*_i, \mathcal{H}_2) \) are illustrated. We observe that the fractional payoffs and their differences vary with the cost pair. Similar comparisons were performed for other cost pairs and models in \( \mathcal{M} \), and we found that the fractional payoffs of the two SGs proposed in Section III.D are within 4% of the payoffs of the ideal SG for each model \( M_i \in \mathcal{M} \).

Fig. 8 represents a comparison of the mismatch statistics for the nominal-model (20) and the average-payoff (22) SGs, each averaged over possible actual models in \( \mathcal{M} \) and all cost pairs. Note that the average-payoff SG has a lower mean mismatch and a much tighter mismatch distribution than the nominal-model SG. Thus, the average-payoff game is a robust choice when the uncertain models and their distribution are known to both players. On the other hand, the nominal-model game is an acceptable approach to security investment in NCS when future uncertainty is difficult to model, thus demonstrating inherent robustness of the proposed SG for security investment. Note that both SGs in Fig. 8 have zero minimum mismatch since both games match some models for selected cost pairs, e.g., the average-payoff game matches \( M_8 \).
in Fig. 7a, and the nominal-payoff game matches $M_{\text{nom}}$ for all cost pairs.

Finally, we summarize the computational requirements of the games analyzed in section IV. The computation of the loss vector corresponding to all sparsity patterns in (8) is dominated by the structured $H_2$ optimization algorithm in [20]. This vector can be computed in under 900 seconds. Further, the payoff matrix (13) must be computed for all actions that satisfy (10). This computation scales with the number of feasible actions or payoffs (Remark 3), which is bounded by $4^{18}$ for the SG designed for the IEEE 39-bus system model with $L_a = L_d = 3$. The payoff computation for one matrix entry, i.e. for a pair of actions $(a, d)$, takes 20 seconds. Note that the above computations can be shared if investment for more than one cost pair is of interest. Finally, for each cost pair, the CBBI algorithm in Section IIIC needs to be executed to find a CBSE. The running time of this algorithm depends on the cost pair. For example, for moderate costs $\gamma_a = \gamma_d = 1$, the running time is under 450 seconds. While the overall complexity of the game can be high for large systems, it solves a long-term resource-planning problem and is implemented offline, so the computation complexity does not significantly impact its implementation. Nevertheless, numerical approaches to reduce the computational complexity of the proposed game will be explored in our future work.

V. CONCLUSION

A Stackelberg security investment game between an attacker and a defender of a NCS, which allocates the players’ resources in a cost-efficient manner, is proposed. Cost-based Stackelberg Equilibria of the game reveal the “important” nodes of the system, whose communication is critical for maintaining satisfactory control performance. Moreover, long-term game-theoretic investment approaches are proposed for NCSs with model uncertainty. Using an example of wide-area control of power systems applied to the IEEE 39-bus test model with uncertain loads, we demonstrated that successful defense is feasible unless the defender is much more resource-limited than the attacker.

The experiments are run using MATLAB on Windows 10 with 64-bit operating system, 3.4 GHz Intel core i7 processor, and 16GB memory.

REFERENCES

[1] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A. Sadeghi, M. Maniotakis, and R. Karri, “The Cybersecurity Landscape in Industrial Control Systems,” Proceedings of the IEEE, vol. 104, pp. 1039–1057, May 2016.
[2] S. Dibaji, M. Pirani, D. Flamolboz, A. Annaswamy, K. Johansson, and A. Chakrabortty, “A systems and control perspective of CPS security,” in Annual Reviews in Control, vol. 47, pp. 394–411, 2019.
[3] Y. Mo, T. Kim, K. B. D. D. H. Lee, A. Perrig, and B. Sinopoli, “Cyber-physical security of a smart grid infrastructure,” Proceedings of the IEEE, vol. 100, no. 1, pp. 195–209, 2012.
[4] Y. Yuan, H. Yang, L. Guo, and F. Sun, Analysis and Design of Networked Control Systems under Attacks. Boca Raton: CRC Press, 2019.
[5] Y. Li, D. Shi, and T. Chen, “False Data Injection Attacks on Networked Control Systems: A Stackelberg Game Analysis,” IEEE Transactions on Automatic Control, vol. 63, no. 6, pp. 1959–1964, 2018.
[6] S. Etesami and T. Basar, “Dynamic Games in Cyber-Physical Security: An Overview,” Dynamic Games and Applications, vol. 9, pp. 884–913, 12 2019.
[7] Q. Zhu and T. Basar, “Game-Theoretic Methods for Robustness, Security, and Resilience of Cyberphysical Control Systems: Games-in-Games Principle for Optimal Cross-Layer Resilient Control Systems,” IEEE Control Systems Magazine, vol. 35, pp. 46–65, Feb 2015.
[8] Cybersecurity Infrastructure Security Agency (CIS), DDoS Quick Guide, 2014. https://us-cert.cisa.gov/security-publications/DDoS-Quick-Guide.
[9] H. Yuan, Y. Xia, J. Zhang, H. Yang, and M. S. Mahmoud, “Stackelberg-Game-Based Defense Analysis Against Advanced Persistent Threats on Cloud Control System,” IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 1571–1580, 2020.
[10] S. Amin, G. Schwartz, and S. Sastry, “Security of interdependent and identical networked control systems,” Automatica, vol. 49, no. 1, pp. 186–192, 2013.
[11] P. Shukla, A. Chakrabortty, and A. Duel-Hallen, “A Cyber-Security Investment Game for Networked Control Systems,” American Control Conference (ACC), pp. 2297–2302, 2019.
[12] M. Balcan, A. Blum, N. Haghitalab, and A. Procaccia, “Commitment without regrets: online learning in Stackelberg security games,” ACM conference on economics and computation, pp. 61–78, 2015.
[13] L. An, A. Chakrabortty, and A. Duel-Hallen, “A Stackelberg Security Investment Game for Voltage Stability of Power Systems,” 2020. https://arxiv.org/abs/2006.11665.
[14] R. Amir and I. Grilo, “Stackelberg versus Cournot Equilibrium,” Games and Economic Behavior, vol. 26, no. 1, pp. 1 – 21, 1996.
[15] “European Network and Information Security Agency (ENSA), Protecting Industrial Control systems-Recommendations for Europe and member states,” 2011. https://www.enisa.europa.eu.
[16] D. Huang and S. Nguang, “Robust Control for Uncertain Networked Control Systems with Random Delays,” Springer Publishing Company, Incorporated, 1st ed., 2009.
[17] F. Dörfler, M. R. Jovanović, M. Chertkov, and F. Bullo, “Sparsity-promoting optimal wide-area control of power networks,” IEEE Transactions on Power Systems, vol. 29, no. 3, pp. 2281–2291, 2014.
[18] D. Soudakovich, A. Chakrabortty, and A. M. Annaswamy, “A delay-aware cyber-physical architecture for wide-area control of power systems,” in Control Engineering Practice, vol. 60, pp. 171–182, March 2017.
[19] M. J. Osborne and A. Rubinstein, A course in game theory. MIT press, 1994.
[20] M. Fardad, F. Lin, and M. Jovanovic, “Design of Optimal Sparse Feedback Gains via the Alternating Direction Method of Multipliers,” IEEE Trans. Automat. Control, vol. 58, pp. 2426–2431, 2013.
[21] A. Chakrabortty and P. P. Khargonekar, “Introduction to wide-area monitoring and Economic Behavior,” in Annual Reviews in Control, vol. 60, pp. 171–182, March 2017.
[22] F. Lian, A. Chakrabortty, and A. Duel-Hallen, “A Stackelberg Game for Robust Cyber-Security Investment in Networked Control Systems,” 2020. https://github.com/Husky-hp/Stackel-Game-for-robust-cyber-sec-invest-in-Netw-Contr-Sys.