HIOA-CPS: Combining Hybrid Input-Output Automaton and Game Theory for Security Modeling of Cyber-Physical Systems

Mustafa Abdallah, Sayan Mitra, Shreyas Sundaram, and Saurabh Bagchi

2021 IEEE Security and Privacy Workshops (SPW) | 978-1-6654-3732-5/20/$31.00 ©2021 IEEE | DOI: 10.1109/SPW53761.2021.00044

***Abstract*—A Cyber-Physical System (CPS) is usually composed of subnetworks where each subnetwork is under ownership of one defender. Security threats on such CPS can be represented by an attack graph where the defenders are required to invest wisely their limited budget in order to protect their critical assets from being compromised. We model such CPS using hybrid input/output automaton (HIOA) where each subnetwork is represented by a HIOA module. We first establish the building blocks needed in our setting. We then present our model that characterizes the continuous time evolution of the investments and discrete transitions between different system's states (where each state represents a different condition within the system). Finally, we provide a representative real-world CPS to validate our modeling and show its benefit for CPS security.**

***Index Terms*—Cyber-Physical Systems, Hybrid Input/Output Automaton, Game Theory, Attack Graphs.**

I. Introduction

Cyber-physical systems (CPS) demand a high degree of criticality, i.e., safety, security, and reliability [1]–[3]. However, such CPS are increasingly facing sophisticated attacks which motivates the fundamental problem we set out to solve — how to create such CPS out of the inherently unreliable building blocks. In this context, significant research has been performed on understanding how to better secure CPS [4]–[6]. This research involved both mathematical and applied frameworks that have been developed in order to precisely model the security of CPS.

There exist several challenges that have not been tackled for modeling CPS's security precisely [7], [8]. One main challenge is the dynamic nature of CPS that represents the change of the state of the system with time has not been considered. For example, the state of an autonomous vehicle model has to include variables representing physical quantities like position, velocity, and angular speed of wheels, etc., as well as variables representing the state of the software modules used for perception, planning, and control [9]. Moreover, a CPS model has two broad kinds of such variables: continuous variables, such as security mechanisms that can be modeled as continuous variables (e.g., the fraction of traffic that is monitored for malicious packets on a network link) and discrete variables (e.g., the number of security personnel to deploy to a given site). Therefore, the question that needs to be answered is how to create a security model for CPS that involves both these types of variables.

In addition to defining the state variables, a CPS model also has to describe how the values of system variables can change. Such changes are naturally described by programs and the natural language for describing the laws of the physical world is the language of ordinary differential equations (ODE). Bringing together discrete and continuous variables, programs, and ODEs within the same mathematical model gives rise to the so-called *hybrid models*. There are several different model classes that fall under the umbrella term hybrid systems, such as hybrid automata [10], hybrid input/output automata [11], hybrid dynamical systems [12], and switched systems [13].

In all of these works, there exist two fundamental gaps between the goal of modeling resilient CPS precisely and the current state-of-the-art, in the areas of modeling, security, and distributed algorithms for CPS. First, the models typically do not capture all the facets required to answer the two modeling requirements (e.g., they may focus on detailed element-level modeling or only the static modeling that can inform only the deployment decision). Second, most of the security algorithms that consider interdependent systems are oblivious to the requirements that arise due to the legacy nature of assets or the presence of multiple stakeholders (defenders).

Exceptions include the recent works [2], [14] that studied the interdependency between multiple stakeholders with a security game setting, and provided a method to calculate the optimal investments by the defenders to minimize their loss. However, they did not model the continuous time nature of the system and the transitions between different system states. In other words, they only solved (partially) the second gap in the state-of-the-art for precisely securing CPS.

In this paper, we combine hybrid input/output automaton modeling with game theory — to the best of our knowledge, this hybrid has never been attempted before. We demonstrate that this hybrid can be put to good use to model CPS involving multiple defenders who are responsible for defending interdependent subnetworks within the system. Fundamentally, our hybrid modeling enables us to model both continuous and discrete transitions of large-scale CPS together. Specifically, we build-up our modeling framework based on the hybrid I/O automata (HIOA) of [11]. We choose this framework because it explicitly identifies input/output variables and actions of the automata, which makes it particularly suitable for defining externally visible interfaces across different types of modules (or players) in the CPS in a precise manner. We show the applicability and benefits of our proposed framework via a representative CPS. In particular, our model captures the evolution of resources allocation unlike previous works and can lead to better resource utilization. The differences between our proposed hybrid model and the related work is shown in Table I.

An implicit, but crucial factor that can enable our modeling is the availability of enormous amounts of data. Such data

Mustafa Abdallah, Shreyas Sundaram, and Saurabh Bagchi are with the School of Electrical and Computer Engineering at Purdue University. Email: {abdalla0,sundara2,sbagchi}@purdue.edu. Sayan Mitra is with the School of Electrical and Computer Engineering at the University of Illinois at Urbana-Champaign. Email: mitras@illinois.edu.

DOI 10.1109/SPW53761.2021.00044

TABLE I: Comparison between the prior related work and HIOA-CPS in terms of the available features.

System	Multiple Defenders	Interdependent subnetworks	Analytical Framework	CPS Security	Dynamics Modeling
TAC03 [10], MIT07 [11]	✗	✗	✓	✗	✓
S&P09 [15], EC18 [16]	✗	✗	✗	✓	✗
JDA17 [17], CDC19 [6]	✗	✗	✓	✓	✗
TCNS20 [14], AsiaCCS21 [2]	✓	✓	✓	✓	✗
HIOA-CPS	✓	✓	✓	✓	✓

would be needed to fit the state changes of the discrete as well as continuous variables. The fidelity of our modeling approach and consequently its utility depends on such "big data" being collected and then synthesized to generate the model parameters (see Section III).

In summary, this paper makes the following contributions:

- We propose a hybrid modeling that incorporates both game-theory and HIOA modeling for precisely modeling security investments in dynamic interdependent systems. Our system model captures both continuous variables and discrete modes of such systems.
- We propose a first effort to incorporate both adversarial and stochastic choices withing HIOA model for security analysis. This model can be applied to different applications, e.g., CPS, and autonomous driving.
- We validate our hybrid model via a representative real-world CPS and show its benefits for precise security modeling.

The remainder of this paper is organized as follows. We introduce the preliminaries of our framework in Section II, followed by the proposed HIOA hybrid framework in Section III. In Section IV, we apply our framework to a real-world CPS. Section VI presents the related literature. We discuss the applicability of our model and associated challenges in Section V. We conclude the paper in Section VII.

II. Preliminaries and Notations

Now, we introduce the notations of our framework, including the HIOA framework, and the game-theoretic setup.

A. Hybrid Input/Output Automaton (HIOA)

A hybrid automaton is a useful model of a system that displays continuous-time behavior interleaved with discrete jumps. Hybrid automata with inputs and outputs allow exogenous time-varying inputs, and observable outputs.

A hybrid input/output automaton (HIOA) $\mathcal{A}$ is defined as a tuple $(\mathcal{L}, \mathcal{X}, \mathcal{U}, \mathcal{M}, \mathcal{G}, \mathcal{R}, \Delta, \mathcal{T}, \mathcal{Y}, \mathcal{I})$, where

- $\mathcal{L}$ is a finite set of system's discrete modes.
- $\mathcal{X} = \{x_1, x_2, \ldots, x_n\}$ is a finite set of n state variables, and X denotes the set of all valuations of $\mathcal{X}$. We denote any particular vector of states by $\mathbf{x} = (x_1, x_2, \ldots, x_n)$. Thus, the hybrid state space is a subset of the set $\mathcal{L} \times X$.
- $\mathcal{U} = \{u_1, u_2, \ldots, u_m\}$ denotes the set of m typed input variables. We emphasize that these variables can be of different types (e.g., Real ($\mathbb{R}$), Integers ($\mathbb{Z}$), or Boolean). We denote $\mathbf{u} = (u_1, u_2, \ldots, u_m)$ as the the input vector.
- $\mathcal{M}$ maps each mode $l \in \mathcal{L}$ with a mode invariant $M(l) \in X \times \mathcal{U}$.
- $\mathcal{G}$ is a set of predicates over $X \times \mathcal{U}$.
- $\mathcal{R}$ is a set of functions from $X \times \mathcal{U}$ to X.
- $\Delta \in \mathcal{L} \times \mathcal{G} \times \mathcal{R} \times \mathcal{L}$ is a finite set of transitions. For each transition $\delta \in \Delta$, $g \in \mathcal{G}$ is its guard predicate, and $r \in \mathcal{R}$ is its reset map.
- $\mathbb{T} \in \mathbb{R}_{\geq 0}$ represent the domain of time values.
- A trajectory $\tau(\mathcal{X}, \mathcal{U})$ is a function from $\mathbb{T}$ to $(X \times \mathcal{U})$ that describes the valuations of the input variables and state variables over time. A trajectory is often a sequence of alternating flows (within modes) and resets (consistent with mode transitions).
- The set of all trajectories for the set of variables V is denoted by $trajs(V)$ where $\mathcal{T} \subseteq trajs(V)$.
- $\mathcal{Y} \in \mathcal{X}$ denotes the set of typed output variables.
- $\mathcal{I} \in \mathcal{L} \times X$ is the set of possible initial discrete modes and valuations of the state variables.

Note that for a given mode l the flow within l is typically the solution trajectory $\mathbf{x}(\cdot)$ of an initial value problem as described by ODE $\dot{\mathbf{x}} = f_l(\mathbf{x}, \mathbf{u})$ with the initial condition $v(\mathbf{x}) = \mathbf{x}_0$ at $t = t_0$. In addition, $\mathcal{A}$ satisfies the following axioms:

$\mathbf{E_1}$ (Input transition enabled) For every $l \in \mathcal{L}$ and $a \in \Delta$, there exists $l' \in \mathcal{L}$ such that $l \xrightarrow{a} l'$.

$\mathbf{E_2}$ (Input trajectory enabled) For every $l \in \mathcal{L}$ and every $v \in trajs(\mathcal{U})$, there exists $\tau \in \mathcal{T}$, such that $\tau.fstate = l$, $\tau \downarrow \mathcal{U} \leq v$, and either (a) $\tau \downarrow \mathcal{U} = v$, or (b) τ is closed and some $l \in \mathcal{L}$ is enabled in $\tau.lstate$.[1]

B. Properties of HIOA

A large CPS is typically composed of smaller modules where putting the modules together creates increasingly larger and more complex pieces until we build the whole system. For instance, operators of large-scale CPS have subordinates operating subsystems of this CPS. In this context, we exploit powerful properties of HIOA to represent large-scale CPS. In this context, we introduce one main property of HIOA that are useful in our setting of modeling CPS security.

Closure under decomposition: We build large HIOA models from smaller modules, using the *composition* operation which is denoted by $||$. Composing two HIOA $\mathcal{A}_1$ and $\mathcal{A}_2$ results in a new object $\mathcal{A} = \mathcal{A}_1 || \mathcal{A}_2$. The compatibility conditions (axioms $\mathbf{E_1}$ and $\mathbf{E_2}$) ensure that $\mathcal{A}$ is also a valid HIOA. This property is called *closure under composition*. For example, consider a cyber attack scenario involving a networked CPS such as the smart grid in Section IV, where each different subnetwork is managed by a different defender. In the HIOA framework, each of these components would be represented as an automaton and composition leads to the whole smart grid.

C. Game Theoretic Framework

1) Attack Graph: We represent the assets in a CPS as nodes of a directed graph $G = (V, \mathcal{E})$ where each node $v_i \in V$ represents an asset. A directed edge $(v_i, v_j) \in \mathcal{E}$ means that if node v_i is successfully compromised, it can be used to

[1]Note that $\tau.fstate$ and $\tau.lstate$ are the first state and last state of a trajectory τ, respectively. Also, $a \downarrow b$ denotes the restriction of the function a into the set b [11].

launch an attack on node v_j. We assume that the success of attacks across different edges in the network are captured by independent random variables. Each edge $(v_i, v_j) \in \mathcal{E}$ has an associated weight $p^0_{i,j} \in (0, 1]$, denoting the probability of successfully attacking asset v_j starting at v_i (in the absence of any security investments). The graph contains a designated source node v_s, which is used by the attacker to initiate her attack on the network. For a general asset $v_t \in V$, we define $\mathcal{P}_t$ to be the set of directed paths from the source v_s to v_t on the graph, where a path $P \in \mathcal{P}_t$ is a collection of edges $\{(v_s, v_1), (v_1, v_2), ..., (v_k, v_t)\}$. The attacker can choose any path from the multiple attack paths in $\mathcal{P}_t$ to attack v_t. Figure 2 shows an example of attack graph modeling of CPS.

2) Strategic Defenders: Let $\mathcal{D}$ be the set of all defenders of the network. Each defender $D_k \in \mathcal{D}$ is responsible for defending a subnetwork (i.e., a set $V_k \subseteq V \setminus \{v_s\}$ of assets). For each compromised asset $v_m \in V_k$, the defender D_k will incur a financial loss $L_m \in \mathbb{R}_{\geq 0}$. To reduce the attack success probabilities on edges interconnecting assets inside the network, a defender can allocate security resources on these edges, subject to the constraints described below.

Let $\mathcal{E}_k \subseteq \mathcal{E}$ be the subset of edges that defender D_k can allocate security resources on. We assume that each defender D_k has a security budget $B_k \in \mathbb{R}_{\geq 0}$. Thus, we define the defense strategy space of each defender $D_k \in \mathcal{D}$ by

$$X_k \triangleq \{x^k_{i,j} \in \mathbb{R}_{\geq 0}, (v_i, v_j) \in \mathcal{E}_k : \sum_{(v_i,v_j)\in\mathcal{E}_k} x^k_{i,j} \leq B_k\}. \quad (1)$$

We denote any particular vector of investments by defender D_k by $x_k \in X_k$.[2]

Under a joint defense strategy, the total investment on edge (v_i, v_j) is $x_{i,j} := \{\sum_{D_k\in\mathcal{D}} x^k_{i,j} : (v_i, v_j) \in \mathcal{E}_k\}$. Let $p_{i,j} : \mathbb{R}_{\geq 0} \to [0, 1]$ be a function mapping the total investment $x_{i,j}$ to an attack success probability, and with $p_{i,j}(0) = p^0_{i,j}$.

The goal of each defender D_k is to choose her investment vector x_k in order to best protect her assets from being attacked. In this paper, we consider the scenario where each defender minimizes the highest probability path to each of her assets; and thus the defender seeks to make the most vulnerable path to each of her assets as secure as possible. Mathematically, this is captured via the cost function

$$C_k(\mathbf{x}) = \sum_{v_m\in V_k} L_m \Big(\max_{P\in P_m} \prod_{(v_i,v_j)\in P} p_{i,j}(x_{i,j}) \Big) \quad (2)$$

subject to $x_k \in X_k$. Note that $C_k(\mathbf{x})$ is a function of the investments of all defenders, and thus we denote the cost by $C_k(x_k, \mathbf{x}_{-k})$ where $\mathbf{x}_{-k}$ is the vector of investments by defenders other than D_k. Each defender chooses her investment vector $x_k \in X_k$ to minimize the cost $C_k(x_k, \mathbf{x}_{-k})$, given the investments $\mathbf{x}_{-k}$ by the other defenders.

Remark 1. *For each HIOA module, we will consider the investments of other defenders as part of the inputs to that HIOA module. Thus, within specific modes, the valuation of the internal state variables will be calculated via the best response notion that we define below.*

[2]Each element in this investment vector represent the security effort by the operators to reduce the probability of successful attack on an edge which arises from the associated vulnerability that is represented by that edge in the attack graph (see Table II for examples for such vulnerabilities).

Definition 1. *The best response of player D_k at a given investment profile $\mathbf{x}_{-k}$ by other defenders is the set $\mathbf{x}^*_k \triangleq \operatorname{argmin}_{\mathbf{x}_k\in X_k} C_k(\mathbf{x}_k, \mathbf{x}_{-k})$.*

The recent works [14], [18] studies the above security game setting, and provides a method to calculate the optimal investments by the defenders with respect to the cost function (2). However, they did not model the continuous time nature of the system and the transitions between different modes (states). In the next section, we will combine HIOA with this game theoretic framework to model large-scale CPS. To the best of our knowledge, our proposed model is the first effort to model both adversarial and stochastic choices for security analysis.

III. The Proposed HIOA framework for modelling interdependent system with multiple defenders

Having introduced the notations of multiple-defender setup and the HIOA framework, we now present our hybrid model to capture the modes and the continuous time evolution of variables (within each mode) where the interdependent system contains different subnetworks with one defender responsible for defending each subnetwork (as shown earlier in Section II).

To the best of our knowledge, our work is the first step in the direction of developing this extension of the framework and applying it for security analysis of the target applications by introducing the notion of rewards (or utility functions).

We now introduce the model's main components: the modes of operation, the variables, the trajectories, and valuations.

A. Modes of Operation

We assume that each HIOA has four modes of operation.

- *Startup mode*: This mode represents the initial state of each subnetwork (defender).
- *Normal mode*: In this mode, each subnetwork should be in a normal operation status where the defender is allocating the investments by best responding to other defenders' optimal investments.
- *Alternate mode*: This mode represents the state in which the defender alternates her investments from the normal mode. This can happen due to any external event (e.g., detecting attacks) or when one of the other defenders change her security investments.
- *Fail mode*: This mode represents one or more node failures (i.e., when one of the subnetwork components is successfully compromised).

We emphasize the reachability of each mode from some other modes via triggering specific events. For example, the "normal" mode is reachable from "alternate" mode by external stability event. We acknowledge that in a real system, it is certainly possible for the system to encounter a failure in startup mode, however we choose not to model this scenario for simplicity in modeling and analysis.

B. Input, State, and Output Variables

In our model, each subnetwork (managed by defender $D_k \in \mathcal{D}$) can be viewed as a HIOA module with the following inputs, outputs and internal states:

- The set of state variables $\mathcal{X}$ is $\{\mathbf{x}_k, \tau, \mathbf{p}_k^0\}$, where $\mathbf{x}_k$ is the defender's defense investment vector over the edges and $\mathbf{p}_k^0$ is the vector of initial attack probabilities.
- The set of input variables $\mathcal{U}$ is {Attack_Risk, Fail_Event, $\mathbf{x}_{-k}$}, where Attack_Risk is an indicator of the risk on the subnetwork and has a value of 0 if there is no attack incident and non-zero otherwise, Fail_Event represents the triggering event of failure (or compromise) and $\mathbf{x}_{-k}$ is the investment of all defenders except defender D_k.
- The set of output variables is $\{\mathbf{p}_k, \mathbf{x}_k\}$.

Remark 2. *The estimation of model's parameters (e.g., the Attack_Risk) can be inferred from the alerts provided by intrusion detection sensors deployed in various parts of the CPS's subnetworks. Such collection of data have been a challenging issue, however, there are recent efficient algorithms for collecting this data for a large-scale CPS (e.g., smart agriculture [19] and Cyber attacks [20]). Thus, it becomes feasible for us to collect such parameters to build our model.*

C. Trajectories and Valuations

Now, we provide the trajectories that describe the relations between the different variables, the guards, and reset functions.

- For any trajectory in $\mathcal{T}$, the flow function for the trajectory in any mode is described by the ODE $\dot{\mathbf{x}}_k = 0$.
- For each mode $l \in \mathcal{L}$, $\mathcal{M}$ maps l to the negation of the conjunction of all the guards on its outgoing transitions.
- The set of guards is {Fail_Event = true, $\tau = \tau_I$}.
- The set of reset functions is a union of two functions $g(\cdot)$ and $g_o(\cdot)$ that are given in our update formulas.
- The transitions are as depicted in Figure 1. These transitions between different modes are represented by directed arrows. Note that the valuations functions are given in (3). Such valuation gives the probability of successful attack $\mathbf{p}_k(t)$, and the investments $\mathbf{x}_k(t)$ that minimize the cost in each mode (given by (2)) throughout the time horizon.
- The set of initial states is the singleton set: {(startup, $\mathbf{p}_k^0 \to 0$, $\tau \to 0$, $\mathbf{p}_k \to 0$)}. Noe that these set of initial states can be chosen arbitrarily for different CPS models based on the initial conditions of that CPS.

A summary of our HIOA module is given below.

HIOA: Subnetwork of defender D_k

Variables

input: Attack_Risk: Boolean, investment of other defenders ($\mathbf{x}_{-k}$): Float.

internal: Defense investments ($\mathbf{x}_k$): Real vector, Initial Success Prob. ($\mathbf{p}_k^0$): Real vector.

output: Probability of Successful attack ($\mathbf{p}_k(t)$).

Real trajectories

$$\mathbf{p}_k(t) = \mathbf{p}_k^0 \; f(\mathbf{x}_k(t)) \tag{3}$$

$$\mathbf{x}_k(t) = \begin{cases} 0 & \text{if } Att\_Risk = 0 \\ min_{\mathbf{x}_k \in X_k} \; C_k(\mathbf{x}_k(l), \mathbf{x}_{-k}(l)) & Otherwise \end{cases}$$

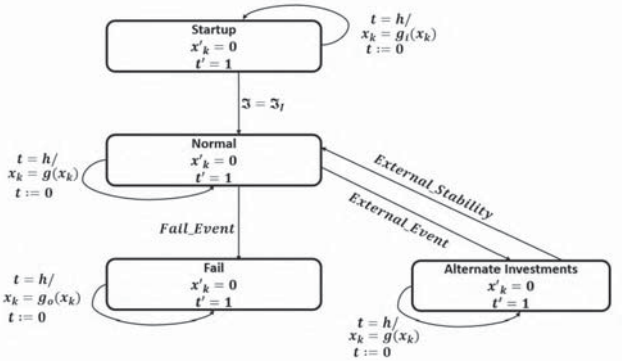

Fig. 1: An HIOA module for one subnetwork. This HIOA module has four modes and the transitions between different modes are represented by directed arrows (where the corresponding conditions for such transitions are given above each arrow). The ODEs that represent the continuous time evolution of internal variables inside each mode are represented inside the four modes. h denotes the sample period for the decision, where $t = mh$, and $m \in \mathbb{R}_{\geq 0}$ is a sample number.

Update Functions

Startup Mode Dynamics: We assume that a timer is used by the system to count up to τ_I seconds. The update function $g_i(\cdot)$ (in Figure 1) consists of two update equations given by

$$\begin{aligned} \mathbf{p}_k[m+1] &= \mathbf{p}_k[m] + \mathbf{p}_k^2[m], \\ \tau[m+1] &= \tau[m] + h. \end{aligned} \tag{4}$$

Normal and Alternate Modes Dynamics: Here, we assume that the update function depends on the best response to other defenders' investments and previous state. Note that the timer is not used in these modes, thus we have $\tau[m+1] = 0$. The update function $g(\cdot)$ is given by

$$\begin{aligned} \mathbf{x}_k[m+1] &= \frac{1}{2}\left(\mathbf{x}_k[m-1] + \mathbf{x}_k^*[m]\right), \\ \tau[m+1] &= 0. \end{aligned} \tag{5}$$

Note that $\mathbf{x}_k^*[m] \in argmin_{\mathbf{x}_k | m|} \; C_k(\mathbf{x}_k[m], \mathbf{x}_{-k}[m])$.

Fail Mode Dynamics: In this mode, we assume that the system goes into failure where the probability of successful attack goes to one. Again, note that timer is not used in this mode, thus the update function $g_o(\cdot)$ in fail mode is given by

$$\begin{aligned} \mathbf{p}_k[m+1] &= \mathbf{1}, \\ \tau[m+1] &- 0. \end{aligned} \tag{6}$$

Now, we introduce the parallel decomposition result that enables us composing subnetworks of different defenders to represent the whole large-scale CPS.

D. Parallel Decomposition

Lemma 1. *Given two HIOA $\mathcal{A}_1$ and $\mathcal{A}_2$, where $\mathcal{A}_i$ is defined as the tuple $(\mathcal{L}_i, \mathcal{X}_i, \mathcal{U}_i, \mathcal{M}_i, \mathcal{G}_i, \mathcal{R}_i, \Delta_i, \mathcal{T}_i, \mathcal{Y}_i, \mathcal{I}_i)$ for $i \in \{1, 2\}$, we say that $\mathcal{A}_1$ and $\mathcal{A}_2$ are compatible if $\mathcal{X}_1 \cap \mathcal{X}_2 = \phi$, $\mathcal{Y}_1 \cap \mathcal{Y}_2 = \phi$, $\mathcal{Y}_1 \subseteq \mathcal{U}_2$, and $\mathcal{Y}_2 \subseteq \mathcal{U}_1$.*

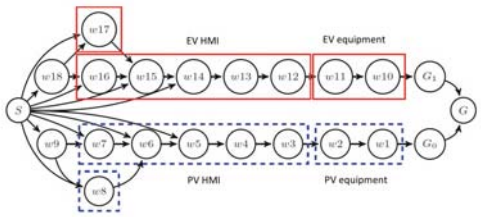

Fig. 2: An attack graph of a DER.1 failure scenario adapted from [14]. It shows stepping-stone attack steps that can lead to the compromise of PV (i.e., G_0) or EV (i.e., G_1).

IV. Evaluating Hybrid Model on Real-world CPS

In this section, we use our proposed hybrid HIOA and game theory model to model a real-world CPS to validate our hybrid model idea and show the flexibility of such idea in modeling large-scale CPS. We first describe the real-world CPS and then we show how to apply our hybrid model for such CPS in an experimental setting with considering related parameters.

A. DER.1 system description:

The US National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group has proposed a framework for evaluating the risks of cyber attacks on the smart electric grid [21]. A distributed energy resource (DER) is described as a cyber-physical system consisting of entities such as generators, storage devices, and electric vehicles, that are part of the energy distribution system [21]. The DER.1 failure scenario has been identified as the riskiest failure scenario affecting distributed energy resources according to the NESCOR ranking. Here, there are two critical equipment assets: a PhotoVoltaic (PV) generator and an electric vehicle (EV) charging station. Each piece of equipment is accompanied by a Human Machine Interface (HMI), the only gateway through which the equipment can be controlled. The DER.1 failure scenario is triggered when the attacker gets access to the HMI. The vulnerability of the system may arise due to various reasons, such as hacking of the HMI, or an insider attack. Once the attacker gets access to the system, she changes the DER settings and gets physical access to the DER equipment. Through this manipulation, the attacker can cause physical damage to the system.

B. Experimental Setup

Attack Graph: To analyze the above system within our HIOA model, we follow the model proposed by [14], which maps the above high level system overview into an attack graph as shown in Figure 2. In this attack graph, node labels starting with "w" are used to denote the non-critical assets/equipment used as part of the attack steps, and G_0, G_1, and G represent the critical assets which are the attacker's goals. For the attacker's goals, G_0 represents a physical failure of the PV system, G_1 represents a physical failure of the EV system, and G means that a failure of either type has occurred. The goal G may signify non-physical losses (e.g., reputation losses) for the DER operator as a result of a successful compromise. The first defender is responsible for defending the critical asset G_0, the second defender for defending G_1. Both defenders share the common asset G.

TABLE II: Baseline probability of successful attack for the vulnerabilities in the DER.1 failure scenario.

Vulnerability (CVE-ID)	Edge(s)	Attack Vector	Score
DER.1 application			
Physical access (CVE-2017-10125)	(w_9, w_7),(w_{18}, w_{16})	Physical	0.71
Network access (CVE-2019-2413)	(w_9, w_8),(w_{18}, w_{17})	Network	0.61
Software access (CVE-2018-2791)	(w_7, w_6),(w_8, w_6)	Network	0.82
Sending cmd (CVE-2018-1000093)	(w_6, w_5),(w_{15}, w_{14})	Network	0.88

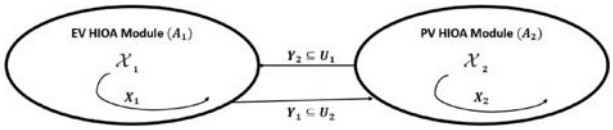

Fig. 3: An Example HIOA module for the real-world CPS system (DER.1) composed of two subnetworks. Each subnetwork is represented by a HIOA module.

Baseline Probabilities of successful attack: Each edge in the attack graphs represents a real vulnerability within the CPS. To create the baseline probability of attack on each edge (i.e., without any security investment), we first create a table of CVE-IDs (from real vulnerabilities reported in the CVE database for 2000-2020). We then followed [20], [22] to convert the main attack's metrics (i.e., attack vector (AV), attack complexity (AC)) to a baseline probability of successful attack. Table II illustrates such process for our DER.1 failure scenario.

Hybrid modeling of DER.1: Here, we show the modeling of DER.1 using our hybrid model. Figure 3 shows such modeling example where each CPS physical component and its HMI can be represented by a HIOA module. Note that the dynamics and the transitions of each subnetwork are encapsulated in its HIOA hybrid model. We emphasize that the compatibility condition (in Lemma 1) is satisfied since the output variables of each module (i.e., the investment of the defender of the corresponding subnetwork) is the input to the other hybrid HIOA module. We now present the variables of each HIOA module.

- The set of state variables of EV subnetwork module is $\mathcal{X}_1 = \{\mathbf{x}_1, \tau, \mathbf{p}_1^0\}$. On the other hand, the set of state variables of PV subnetwork module is $\mathcal{X}_2 = \{\mathbf{x}_2, \tau, \mathbf{p}_2^0\}$, where $\mathbf{p}_k^0$ is the vector of initial successful attack probabilities over the corresponding edges within the attack graph.
- The set of output variables for EV module is $\{\mathbf{p}_1, \mathbf{x}_1\}$. The set of output variables for PV module is $\{\mathbf{p}_2, \mathbf{x}_2\}$.
- The set of input variables of EV module $\mathcal{U}_1 = \{Attack\_Risk, Fail\_Event, \mathbf{x}_{-1} = \mathbf{x}_2\}$ and similarly $\mathcal{U}_2 = \{Attack\_Risk, Fail\_Event, \mathbf{x}_{-2} = \mathbf{x}_1\}$.

The update functions (that captures the dynamics as explained earlier in Section III) are calculated using Equations (4)–(6) and the trajectories by Equation (3).

Experimental Results: We assume that there is no attack risk on the startup time as mentioned earlier. Then, we calculate the dynamics of the investments for both our hybrid

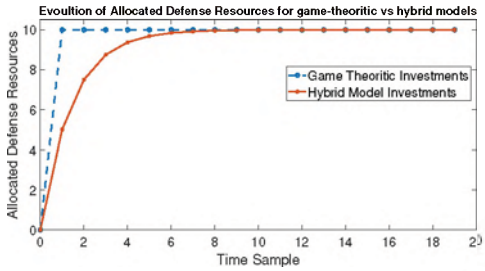

Fig. 4: Comparison of evolution of defense resources allocation in game-theoretic-only (dashed blue line) vs our hybrid model (red solid line). Our model is more efficient on security resources utilization.

model and the game-theoretic only model. Figure 4 shows such comparison on normal and alternate modes.[3] We emphasize that our model is more efficient on security resources utilization since it takes account both current investments from the game and the memory given by investments in the previous time sample. On the contrary, the game-theoretic only model does not take account of such memorization. Another merit from our hybrid model is that it can give the dynamic nature of the system's security state and the evolution of the allocation process. On the other hand, existing works with only game-theoretic investments (e.g., [2], [14]) for attack graph consider only repeated single shot and do not consider any dynamic nature of the CPS and do not study alternation between different modes. We believe that these two main distinctions along with the utilization of security resources make our proposed hybrid model more efficient in modeling dynamics of CPS compared to those works.

V. Discussion

A. Applicability of the proposed hybrid model

We emphasize that our modeling can effectively model any interdependent CPS that can be represented by attack graphs (e.g., SCADA [14], IEEE 300 BUS [2], E-Commerce [23], and VOIP [2]). A second application domain that seems a natural fit to our hybrid modeling formulation is embedded systems that are often the core of autonomous systems like autonomous driving. Thus, we believe that our work can have a crucial role in improving the security modeling of autonomous systems.

B. Computing investments under hybrid modeling for unknown costs

Note that the existing literature does not effectively capture the significantly more complex scenarios that we are considering as part of this paper, involving a mix of static and dynamical nodes. Thus, filling this critical gap is essential when the defenders' costs are unknown. One particular approach that can be pursued is to leverage simulation based optimization (SO) techniques into a broader optimization framework for computing optimal security deployments.

[3]Note that the two approaches would give same insights under full failure (fail mode). We omit the details of such experiment in the interest of space.

Such SO techniques have been widely applied for optimizing complex systems [24], but their use in the broader context of security policies for interdependent CPS is lacking in the literature. SO techniques involve iteratively tuning the optimization parameters based on evaluations of the objective function through a simulator, but face challenges due to the difficulty of evaluating gradients, and in the time taken to run each simulation. Such challenges can be tackled via the use of approximations to the objective functions (i.e., $f(\cdot)$ and $C_k(\cdot)$ in our context) (learned via regression), and by switching between multiple simulators at different levels of resolution, depending on the operating points that are being evaluated [24]. Note that creating a systematic approach to integrate such techniques into an optimization framework for computing security deployments for CPS would be an avenue for future work.

VI. Related Work

A. Security in interdependent systems

There exist several prior works that have studied the problem of securing systems with interdependent assets [23], [25]. These works have a common theme of modeling the stepping-stone attacks in which the successful attack of one asset can lead to compromise a dependent asset. The popular abstraction notion for modeling such stepping-stone attacks is attack graphs [20]. We follow such works for creating attack graphs, however we do not rely only on investments from the attack graph game but we model the dynamics evolution of the investments with time, from the hybrid model, which has not been studied in all of these works.

B. Game-theoretic modeling of security

The interaction between defenders and attackers is an important aspect when securing interdependent systems since it affects the security state of the system. Such interaction has been modeled using game theory by modeling the interaction between one defender and one attacker [6], [26], one defender and multiple attackers [27], [28]. Our work differs from these works in that we consider the interdependencies between multiple defenders in an interdependent network. The exceptions that provide a theoretical treatment of multiple defenders in interdependent security games include [2], [5], [14]. These works, however, do not consider the more realistic attack scenarios that we consider, do not consider the evolution of investments by, HIOA hybrid model, and do not involve HIOA with game theory in one framework that we consider in our current work.

C. HIOA (hybrid) modeling

The combination of discrete-continuous variables, programs, and ODEs within the same mathematical model to describe the dynamics of control systems (e.g., controlling valves) have been handled in the literature via the language of hybrid models that can have different structure (e.g., hybrid automata [10], hybrid input/output automata [11], hybrid dynamical systems [12], and the switched systems [13]). In

contrast to those works, we extend this framework and apply it to CPS security where stochastic and adversary notations are considered. We also incorporate game-theory within the update functions for each hybrid module.

VII. Conclusion and Future Work

This paper presented a hybrid framework that combined HIOA and game theory for modeling interdependent system with multiple defenders, who place their investments to protect the target assets. We first established the objective function of each defender and then provided the HIOA hybrid model; in particular, we modeled the continuous time evolution of the investments within the CPS and the transitions between different system's states. We then validated our model using a real-world CPS, a smart grid system. We showed that our hybrid model captures the evolution of resource allocation in CPS and can lead to better resource utilization. We emphasize that our model can be applied to model the resource allocation in different domains that are represented via large-scale interdependent systems. A future avenue of research would be using simulation based techniques for computing security deployments for complex CPS with unknown costs aided by our combined (hybrid) modeling scheme. Moreover, exploring the effect of human decision-making on our proposed hybrid model (similar to the recent works [5], [29] on game-theoretic formulations of interdependent systems using attack graphs) would be another avenue for future research.

VIII. Acknowledgements

We thank the anonymous reviewers for their valuable comments to improve the quality of this paper. This material is based in part upon work supported by the National Science Foundation under Grant Number CNS-1718637, Wabash Heartland Innovation Network (WHIN) project from Lilly Endowment Inc. NSF CCF-1919197, and Army Research Lab under Contract number W911NF-2020-221. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the sponsors.

References

[1] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security – a survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, 2017.

[2] M. Abdallah, D. Woods, P. Naghizadeh, I. Khalil, T. Cason, S. Sundaram, and S. Bagchi, "Morshed: Guiding behavioral decision-makers towards better security investment in interdependent systems," *arXiv preprint arXiv:2011.06933*, 2020.

[3] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions," *Computers & Security*, vol. 68, pp. 81–97, 2017.

[4] A. Laszka, M. Felegyhazi, and L. Buttyan, "A survey of interdependent information security games," *ACM Computing Surveys (CSUR)*, vol. 47, no. 2, p. 23, 2015.

[5] A. Sanjab, W. Saad, and T. Başar, "Prospect theory for enhanced cyber-physical security of drone delivery systems: A network interdiction game," in *IEEE International Conference on Communications (ICC)*, 2017, pp. 1–6.

[6] M. Abdallah, P. Naghizadeh, T. Cason, S. Bagchi, and S. Sundaram, "Protecting assets with heterogeneous valuations under behavioral probability weighting," in *2019 IEEE 58th Conference on Decision and Control (CDC)*, 2019, pp. 5374–5379.

[7] D. Garlan, "Modeling challenges for cps systems," in *2015 IEEE/ACM 1st International Workshop on Software Engineering for Smart Cyber-Physical Systems*. IEEE, 2015, pp. 1–1.

[8] S. Weyer, T. Meyer, M. Ohmer, D. Gorecky, and D. Zühlke, "Future modeling and simulation of cps-based factories: an example from the automotive industry," *Ifac-Papersonline*, vol. 49, no. 31, pp. 97–102, 2016.

[9] B. Chen, Z. Yang, S. Huang, X. Du, Z. Cui, J. Bhimani, X. Xie, and N. Mi, "Cyber-physical system enabled nearby traffic flow modelling for autonomous vehicles," in *2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC)*. IEEE, 2017, pp. 1–6.

[10] J. Lygeros, K. H. Johansson, S. N. Simic, J. Zhang, and S. S. Sastry, "Dynamical properties of hybrid automata," *IEEE Transactions on automatic control*, vol. 48, no. 1, pp. 2–17, 2003.

[11] S. Mitra, "A verification framework for hybrid systems," Ph.D. dissertation, Massachusetts Institute of Technology, 2007.

[12] R. Goedel, R. G. Sanfelice, and A. R. Teel, "Hybrid dynamical systems: modeling stability, and robustness," 2012.

[13] D. Liberzon, *Switching in systems and control*. Springer Science & Business Media, 2003.

[14] M. Abdallah, P. Naghizadeh, A. R. Hota, T. Cason, S. Bagchi, and S. Sundaram, "Behavioral and game-theoretic security investments in interdependent systems modeled by attack graphs," *IEEE Transactions on Control of Network Systems*, 2020.

[15] A. Acquisti, "Nudging privacy: The behavioral economics of personal information," *IEEE security & privacy*, vol. 7, no. 6, 2009.

[16] E. M. Redmiles, M. L. Mazurek, and J. P. Dickerson, "Dancing pigs or externalities?: Measuring the rationality of security decisions," in *Proceedings of the 2018 ACM Conference on Economics and Computation*. ACM, 2018, pp. 215–232.

[17] P. Guan, M. He, J. Zhuang, and S. C. Hora, "Modeling a multitarget attacker–defender game with budget constraints," *Decision Analysis*, vol. 14, no. 2, pp. 87–107, 2017.

[18] M. Abdallah, P. Naghizadeh, A. R. Hota, T. Cason, S. Bagchi, and S. Sundaram, "The impacts of behavioral probability weighting on security investments in interdependent systems," in *2019 American Control Conference (ACC)*. IEEE, 2019, pp. 5260–5265.

[19] B. Chatterjee, D. H. Seo, S. Chakraborty, S. Avlani, X. Jiang, H. Zhang, M. Abdallah, N. Raghunathan, C. Mousoulis, A. Shakouri, S. Bagchi, D. Peroulis, and S. Sen, "Context-aware collaborative intelligence with spatio-temporal in-sensor-analytics for efficient communication in a large-area iot testbed," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

[20] J. Homer, S. Zhang, X. Ou, D. Schmidt, Y. Du, S. R. Rajagopalan, and A. Singhal, "Aggregating vulnerability metrics in enterprise networks using attack graphs," *Journal of Computer Security*, vol. 21, no. 4, pp. 561–597, 2013.

[21] A. Lee, "Electric sector failure scenarios and impact analyses-draft," *National Electric Sector Cybersecurity publisher Resource (NESCOR) Technical Working Group*, vol. 1, 2013.

[22] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing, "Automated generation and analysis of attack graphs," in *Proceedings 2002 IEEE Symposium on Security and Privacy*. IEEE, 2002, pp. 273–284.

[23] G. Modelo-Howard, S. Bagchi, and G. Lebanon, "Determining placement of intrusion detectors for a distributed application through bayesian network modeling," in *International Workshop on Recent Advances in Intrusion Detection*. Springer, 2008, pp. 271–290.

[24] C. Osorio and M. Bierlaire, "A simulation-based optimization framework for urban transportation problems," *Operations Research*, vol. 61, no. 6, pp. 1333–1345, 2013.

[25] P. Xie, J. H. Li, X. Ou, P. Liu, and R. Levy, "Using Bayesian networks for cyber security analysis," in *Dependable Systems and Networks (DSN), 2010 IEEE/IFIP international conference on*. IEEE, 2010, pp. 211–220.

[26] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*. IEEE, 2010, pp. 1–10.

[27] G. Yan, R. Lee, A. Kent, and D. Wolpert, "Towards a bayesian network game framework for evaluating ddos attacks and defense," in *Proceedings of the 2012 ACM conference on Computer and communications security (CCS)*, 2012, pp. 553–566.

[28] T. Alpcan and T. Baar, *Network Security: A Decision and Game-Theoretic Approach*, 1st ed. New York, NY, USA: Cambridge University Press, 2010.

[29] D. Woods, M. Abdallah, S. Bagchi, S. Sundaram, and T. Cason, "Network defense and behavioral biases: An experimental study," 2020.