2019 American Control Conference (ACC)
Philadelphia, PA, USA, July 10-12, 2019

Switching for Unpredictability: A Proactive Defense Control Approach

Aris Kanellopoulos, *Student Member, IEEE,* Kyriakos G. Vamvoudakis, *Senior Member, IEEE*

***Abstract*— In this paper, we consider the problem of securely operating a cyber-physical system in an adversarial environment. The defending mechanism we introduce is proactive in nature and employs the principles of moving target defense. The defense implementation utilizes a switching structure to persistently and stochastically alter the behavior of the system with respect to both its actuators and its sensors. Thus, the ability of an adversary to successfully scan the system in preparation for the attack is decreased. The unpredictability of the system's operation is quantified by an entropy metric which is subsequently optimized. Theorems are presented that show stability of the system under proactive switching. Simulations show the efficacy of the proposed approach on a simplified aircraft model.**

***Index Terms*— Cyber-physical security, proactive defense, moving target defense, switched systems.**

I. Introduction

The widespread use of low cost embedded controllers, communication and computational devices, has resulted in the physical and digital worlds being more intertwined than ever. From the simple programmable logic controllers found in industrial production systems, to the large-scale complex networks of the Internet of Things and modern cyber-physical systems (CPS), both civilian and military applications now depend on the smooth cooperation of sensing and actuating devices with the underlying information layer [1], [2]. Owing to the complexity of those systems, an attribute that makes them difficult to monitor, as well as the ease of access to malicious software, CPS are ofter required to operate in adversarial and unknown environments.

Examples of attacks in CPS are numerous. In experimental settings, researchers have demonstrated the ability to gain access to the operation of a pacemaker through its wireless protocols [3]. Similarly, several researchers have showcased the exploitation of various attack surfaces in modern vehicles, mainly through their wireless data acquisition subsystems [4], [5]. Moreover, there has been a plethora of cyber-attacks in real world CPS. One such case, was the downing of a military U.S. drone [6], where a two-pronged attack was launched. Initially, the communication bus between the drone and the human operator was jammed, and subsequently, the adversary spoofed the drone's GPS to alter its trajectory. However, such incidents are not limited to critical or military infrastructure. A German Steel Mill was severely damaged when an attacker, with knowledge of the system's structure, gained access to the network through a spear phising email, causing critical component failure [7].

Until recently, although the control subsystem is an essential component of a CPS, security concerns were ignored. Most defense mechanisms were applied solely on the software level. This changed by the introduction of various intrusion detection and mitigation mechanisms that employ control-theoretic concepts to 'robustify' the system under attacks. The development of detection algorithms gives away the reactive nature of most defense schemes. The prevalent design paradigm assumes that the system is oblivious to the possibility of attacks until one has already affected it. A different approach, one extensively utilized in computer networks, sees the system modifying its behavior in order to deter the potential attackers or preemptively guarantee that most attacks would be unsuccessful. This approach to proactive defense is called moving target defense (MTD).

Related Work

The need for system-wide approaches to security, rather than solely software-oriented, was first suggested in [8]. In [9], the security of the system was defined in terms of trust between the interconnected components of a network. The authors in [10], employed game-theoretic concepts to predict and mitigate the behavior of an intelligent attacker trying to jam the network's communication links. In [11], the principles of fault-diagnosis are utilized, without taking into account the malicious nature of the attacker. Several detection schemes for adversarial inputs have been proposed in the literature. In [12], the authors use a hypothesis testing technique based on the output of a Kalman filter to detect an attack. The authors of [13], use the fused information from all the system's sensors to mitigate any measurement compromises. Proactive security algorithms have been outside the scope of the aforementioned works.

Previous work on proactive defense systems, and MTD in particular, has mostly revolved around computer security systems [14]. In [15], a scheme in which constantly rotating Internet Protocol version 6 (IPv6) addresses are used for deception purposes. Similarly, in [16], an algorithm for IP mutation is introduced, called OpenFlow Random host mutation. However, these approaches only consider the underlying software of a system. In the context of control theory, the authors in [17] augment the state space of a linear system to introduce stochasticity, while the authors in [18], formulate the MTD as a game. Recent attempts have also focused on formalizing the framework of MTD, leading to [19] and

A. Kanellopoulos and K. G. Vamvoudakis are with the Daniel Guggenheim School of Aerospace Engineering, Georgia Tech, Atlanta, GA, 30332, USA e-mail: (ariskan@gatech.edu, kyriakos@gatech.edu).

This work was supported in part, by NATO under grant No. SPS G5176, by ONR Minerva under grant No. $N00014-18-1-2160$, by an NSF CAREER, and by NAWCAD under grant No. $N00421-16-2-0001$.

especially [20], where the MTD entropy hypothesis was stated.

Contribution

The contributions of the present work are threefold. Initially, after formulating the CPS as a linear system with redundant actuators and sensor, and defining the controllable and observable subsets, we design multiple optimal controllers for the admissible actuation subsets. Then, we introduce a probabilistic switching scheme that optimizes a weighted sum of the overall optimality and unpredictability of the system. Finally, we employ an optimal-control based observer design to show the use of MTD for secure state estimation.

Notation: The notation used here is standard. $\mathbb{R}$ is the set of real numbers. $\bar{\lambda}(A)$ is the maximum eigenvalue of the matrix A and $\underline{\lambda}(A)$ is its minimum eigenvalue. $\|\cdot\|$ denotes the Euclidean norm of a vector and the Frobenius norm of a matrix. The superscript $\star$ is used to denote the optimal trajectories of a variable. $(\cdot)^{\mathrm{T}}$ denotes the transpose of a matrix. ∇_x and $\frac{\partial}{\partial x}$ are used interchangeably and denote the partial derivative with respect to a vector x. The cardinality of a set, i.e. the number of elements contained in the set, is denoted by $\text{card}(\cdot)$. 2^A denotes the power set of a set A, i.e., the set containing all subsets of A, including the empty set and the A itself.

II. Problem Formulation

Consider the following linear time-invariant continuous time system,

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t), \\ y(t) &= Cx(t), \end{aligned} \tag{1}$$

where $x(t) \in \mathbb{R}^n$ is the state, $u(t) \in \mathbb{R}^m$ is the input of the system, $y(t) \in \mathbb{R}^p$ is the output, $A \in \mathbb{R}^{n\times n}$ is the plant matrix, $B \in \mathbb{R}^{n\times m}$ is the input matrix, and $C \in \mathbb{R}^{p\times n}$ is the output matrix.

We can rewrite (1) as,

$$\dot{x} = Ax + \sum_{i=1}^{m} b_i u_i, \tag{2}$$

$$y_j = c_j x \ , \ j \in \{1, \dots, p\}, \tag{3}$$

where b_i is a column vector corresponding to the i-th actuator, u_i is the value of the input signal associated with this actuator, and y_j is the output given by a specific sensor c_j corresponding to the j-th row of the output matrix.

Assumption 1. In order to offer a greater degree of freedom for deception purposes and to mitigate the effect of potential attacks, we will consider systems with redundant actuating and sensing components. □

III. Defense Against Actuator Attacks

In this section, we will focus our attention to the case of actuator attacks. Let $\mathcal{B}$ denote the set containing the actuators of the system by the vectors $b_i, i \in \{1, \dots, m\}$. The power set of $\mathcal{B}$, denoted as $2^{\mathcal{B}}$, contains all possible combinations of the actuators acting on the system. Each of these combinations is expressed by the input matrix B_j, $j \in \{1, \dots, 2^m\}$ whose columns are the appropriate vectors b_i.

The set of the candidate actuating modes $\mathcal{B}_c$ is defined as the set of the actuator combinations that renders the system (1) fully controllable,

$$\mathcal{B}_c = \left\{ B_j \in 2^{\mathcal{B}} : \text{rank}(\begin{bmatrix} B_j & AB_j & \dots & A^{n-1}B_j \end{bmatrix}) = n \right\}. \tag{4}$$

The system (1) with the actuating mode B_i can be rewritten as,

$$\dot{x} = Ax + B_i u_i, \ i \in \{1, \dots, \text{card}(\mathcal{B}_c)\}. \tag{5}$$

Remark 1. Note that, we do not require different actuating modes to share common actuators. Moreover, while a single actuating mechanism might be able to control a system, two different - less potent - mechanisms might need to work cooperatively to control the same system. All these modes will belong to the set (4). □

A. Optimal Controllers Design

For each actuating operating mode B_i, $i \in \{1, \dots, \text{card}(\mathcal{B}_c)\}$, we denote the candidate control law $u_i(t)$.

We are interested in deriving optimal controllers for each of these modes. Towards that, we define an infinite horizon integral cost functional and the associated optimization,

$$\begin{aligned} V_i^\star(x(t_0)) &= \min_{u_i} \int_{t_0}^{\infty} r_i(x, u_i) d\tau \\ &\equiv \min_{u_i} \int_{t_0}^{\infty} (x^{\mathrm{T}} Q_i x + u_i^{\mathrm{T}} R_i u_i) \mathrm{d}\tau, \ \forall x(t_0), \end{aligned} \tag{6}$$

where $Q_i \succeq 0$, $R_i \succ 0$ $\forall i \in \{1, \dots, \text{card}(\mathcal{B}_c)\}$.

Assumption 2. We assume that each pair $(A, \sqrt{Q_i})$ is detectable. □

The Hamiltonian associated with (5) and (6) is,

$$H_i(x, u_i, \nabla V_i) = \nabla V_i^{\mathrm{T}}(Ax + B_i u_i) + x^{\mathrm{T}} Q_i x + u_i^{\mathrm{T}} R_i u_i, \ \forall x, u_i, \tag{7}$$

with V_i denoting the value function, not necessarily the optimal.

Applying the stationarity conditions $\frac{\partial H_i(x, u_i, \nabla V_i)}{\partial u_i} = 0$, yields,

$$u_i^\star = -R_i^{-1} B_i^{\mathrm{T}} \nabla V_i. \tag{8}$$

The optimal value functions $V_i^\star(\cdot)$ must satisfy the Hamilton-Jacobi-Bellman equation,

$$x^{\mathrm{T}} Q_i x + \nabla V_i^{\star\mathrm{T}}(Ax) - \frac{1}{2} \nabla V_i^{\star\mathrm{T}} B_i R_i^{-1} B_i^{\mathrm{T}} \nabla V_i^\star = 0. \tag{9}$$

Since all systems (5) are linear and the cost (6) is quadratic, all value functions will be quadratic in the state, i.e., $V_i^\star(x) = x^{\mathrm{T}} P_i x$. Substituting this expression into (9) and (8), yields the feedback controller with optimal gain K_i,

$$u_i^\star(x) = -K_i x \equiv -R_i^{-1} B_i^{\mathrm{T}} P_i x, \tag{10}$$

where P_i are the solutions to the following Riccati equations,

$$A^{\mathrm{T}}P_i + P_iA - P_iB_i^{\mathrm{T}}R^{-1}B_i^{\mathrm{T}}P_i + Q_i = 0. \quad (11)$$

We introduce the set containing all K_i, denoted $\mathcal{K}$, with the understanding that $\mathrm{card}(\mathcal{K}) = \mathrm{card}(\mathcal{B}_c)$. For ease of exposition, with some abuse of notation we consider K_i to mean both an element in the set of optimal controllers, as well as the respective Kalman gain. Also, we will use $\mathcal{K}$ to denote the set of controllers, as well as the set of the appropriate indexes.

Fact 1. Due to (4) and Assumption 2, for each B_i, the solution exists and is unique. □

Fact 2. Each K_i, with input given by (8) guarantees that (1) has an asymptotically stable equilibrium point. □

B. Switching-Based MTD framework

We will now develop a framework to facilitate deception of potential attackers based on the principles of MTD.

1) Maximization of Unpredictability: To formally define the switching law, we need to introduce the *probability simplex* $\mathbf{p} = \begin{bmatrix} p_1 & p_2 & \dots & p_N \end{bmatrix}$ which denotes the probability that controller K_i is active.

To incorporate ideas from the framework of MTD, we propose a switching rule that optimizes over the minimum cost that each controller is able to attain, as well as an unpredictability term quantified by the information entropy produced by the switching probability simplex $\mathbf{p}$. This way we achieve the desired trade-off between overall optimality and unpredictability. The use of information entropy is standard practice in MTD design [19].

Theorem 1. Suppose that (1), is controlled by $N = \mathrm{card}(\mathcal{K})$ candidate controllers with associated cost given by (6). Then, the probability p_i that the controller K_i is active is given by,

$$p_i = e^{\left(-\frac{V_i}{\epsilon} - 1 - \epsilon \log\left(e^{-1}\sum_1^N e^{(\frac{V_i}{\epsilon})}\right)\right)}, \quad (12)$$

with $\epsilon \in \mathbb{R}^+$ denoting the certain level of unpredictability which constitutes a design parameter.

Proof. We formulate the following optimization problem,

$$\min_{\mathbf{p}}(\mathbf{V}^{\star\mathrm{T}}\mathbf{p} - \epsilon\mathcal{H}(\mathbf{p}))$$
$$\text{subject to:}$$
$$\|\mathbf{p}\|_1 = 1 \text{ and } \mathbf{p} \geq 0,$$

where $\mathbf{V}^\star = \begin{bmatrix} V_1^\star & \dots & V_N^\star \end{bmatrix}^{\mathrm{T}} = \begin{bmatrix} x(t_0)^{\mathrm{T}}P_1x(t_0) \dots x(t_0)^{\mathrm{T}}P_Nx(t_0) \end{bmatrix}^{\mathrm{T}}$, with $x(t_0)$ the given initial state, denotes a column vector containing the value function of each candidate controller, $\mathcal{H}(\mathbf{p}) = -\mathbf{p}^{\mathrm{T}}log(\mathbf{p})$ is the information entropy produced by the simplex. Furthermore, for the decision vector $\mathbf{p}$ to constitute a probability simplex we constrain it to the nonnegative orthant (i.e. $p_i \geqslant 0$, $\forall i \in \{1 \dots N\}$) and we require its l_1 norm to satisfy $\|p\|_1 = \sum_{i=1}^N \|p_i\| = 1$.

The entropy of a probability is a concave function [21] and therefore, the cost index, being a sum of a linear function of the probability and the negative entropy, is convex. We define the Lagrangian of the optimization problem as,

$$\begin{aligned} L &= \mathbf{V}^{\star\mathrm{T}}\mathbf{p} - \epsilon\mathcal{H}(\mathbf{p}) + \lambda(\mathbf{1}^{\mathrm{T}}\mathbf{p} - 1) + \boldsymbol{\beta}^{\mathrm{T}}\mathbf{p} \\ &= \mathbf{V}^{\star\mathrm{T}} + \epsilon\mathbf{p}^{\mathrm{T}}\log(\mathbf{p}) + \lambda(\mathbf{1}^{\mathrm{T}}\mathbf{p} - 1) + \boldsymbol{\beta}^{\mathrm{T}}\mathbf{p}, \quad (13) \end{aligned}$$

where $\mathbf{1}$ denotes a vector consisting of ones and λ,$\boldsymbol{\beta}$ are the Karush-Kuhn-Tucker (KKT) multipliers.

The KKT conditions for the problem are,

$$\nabla L = \mathbf{V}^\star + \epsilon\mathbf{1} + \epsilon\log(\mathbf{p}) + \lambda\mathbf{1} + \boldsymbol{\beta}, \quad (14)$$

and the complementarity conditions on the optimal solution $\mathbf{p}^\star$ are,

$$\boldsymbol{\beta}^{\mathrm{T}}\mathbf{p}^\star = 0. \quad (15)$$

Note that if there $\exists i : p_i = 0$, then $log(p_i)$ is undefined. Consequently, for the optimization to be feasible, one of the following must hold,

- $\epsilon\log(p_i) = 0, \forall i \Rightarrow \epsilon = 0 \Rightarrow \mathbf{p}^\star = \begin{bmatrix} \mathbf{0}_{i-1} \dots 1 \dots \mathbf{0}_{N-i} \end{bmatrix}^{\mathrm{T}}$, where the K_i controller is the optimal one.
- $\boldsymbol{\beta} = 0$.

We consider now the nontrivial case, i.e., $\boldsymbol{\beta} = 0$, which yields,

$$\nabla L = \mathbf{V}^\star + \epsilon\log(\mathbf{p}) + \epsilon\mathbf{1} + \lambda\mathbf{1} = 0. \quad (16)$$

The N equations for each controller are independent, leading to the system of equations,

$$V_i^\star + \epsilon\log(p_i) + \epsilon + \lambda = 0 \ , \forall i \in \{1, \dots, N\}. \quad (17)$$

Solving now for the optimal probabilities p_i, yields,

$$p_i = e^{\left(-\frac{V_i^\star}{\epsilon} - \frac{\lambda}{\epsilon} - 1\right)} \ , \forall i \in \{1, \dots, N\}. \quad (18)$$

We take into account that,

$$\|\mathbf{p}\|_1 = 1 \Rightarrow \sum_{i=1}^N p_i = 1 \Rightarrow \sum_{i=1}^N e^{\left(-\frac{V_i^\star}{\epsilon} - \frac{\lambda}{\epsilon} - 1\right)} = 1.$$

Solving for λ, we get,

$$\lambda = \epsilon\log\left(e^{-1}\sum_{i=1}^N e^{(-\frac{V_i^\star}{\epsilon})}\right) \quad (19)$$

and after substituting (19) in (18) one has the required result. □

2) Switching-based MTD scheme: In order to analyze the behavior of the system under the proposed MTD framework, we shall formulate a switched system consisting of the different operating modes. First, we introduce the switching signal $\sigma(t) = i$, $i \in \{1, \dots, \mathrm{card}(\mathcal{K})\}$, which denotes the active controller as a function of time. This way, the system is,

$$\dot{x}(t) = \tilde{A}_{\sigma(t)}x(t), \quad (20)$$

where $\tilde{A}_{\sigma(t)} := A - B_{\sigma(t)}R^{-1}_{\sigma(t)}B^{\mathrm{T}}_{\sigma(t)}P_{\sigma(t)}$ denotes the closed-loop subsystem when the controller $K_{\sigma(t)}$ is active.

Remark 2. Since the actual switching sequence is different under the designer's choice for unpredictability, we will constrain the switching signal to have a predefined average dwell time. This way, the stability of the overall system will be independent of the result of the optimization. Intuitively, as was initial shown in [22], a system with stable subsystems is stable if the switching is slow enough on an average sense. □

Remark 3. By augmenting the linear system with the stochastic multi-controller, whose transition probabilities are predefined, we develop a Markov jump system. Consequently, one could examine the stability properties of the system with appropriate techniques from stochastic systems. However, it is known that the properties of such a system depend on the corresponding probability transition matrix [23]. While relaxing the requirement for dwell time, a design based on Markov jump systems could produce switching systems that fail to converge based on the level of entropy in the optimization algorithm. To ensure that the two subsystems, the entropy optimizer, and the switching system, operate independently, we utilize the dwell time approach. □

Definition 1. A switching signal has an average dwell time τ_D if over any time-interval $[t, T]$, the number of switches $S(T, t)$ is bounded above as,

$$S(T,t) \leqslant S_0 + \frac{T-t}{\tau_D},$$

where S_0 is an arbitrary chatter bound and τ_D is the dwell time. □

Theorem 2. Consider the system (1) in the absence of attacks. The switched system defined by the piecewise continuous switching signal $\sigma(t) = i,\ i \in \mathcal{K}$ denoting the active controller K_i and the continuous flow (5) with optimal input (8) which satisfies (11) is asymptotically stable for every switching signal $\sigma(t)$ if the average dwell time bounded by,

$$\tau_D > \frac{\max_{q,p\in\mathcal{K}} \frac{\bar{\lambda}(P_p)}{\underline{\lambda}(P_q)}}{\min_{p\in\mathcal{K}} \frac{\underline{\lambda}(Q_p + P_p B_p R_p^{-1} B_p^{\mathrm{T}} P_p)}{\underline{\lambda}(P_p)}}, \tag{21}$$

with an arbitrary chatter bound $S_0 > 0$.

Proof. The proof is based on the method of multiple Lyapunov functions, as presented in [24]. It has been omitted due to space limitations and will be presented in the journal version of the work. □

IV. Defense Against Sensor Attacks

In this section we show how the methods developed can be applied to the proactive defense of CPS against sensor attacks by employing sensor redundancy.

A. Candidate Sensors Sets

Similarly to the proposed framework for the actuators, we introduce the set of all sensors, denoted by $\mathcal{C}$, and the elements of its power set $\mathcal{C}_i \in 2^{\mathcal{C}}$, where $C_i \in \mathcal{C}_i$ is a combination of the different rows of C.

The set of candidate sensing modes $\mathcal{S}_o$ is defined as the set of the sensor combinations that renders the system (1) fully observable,

$$\mathcal{S}_o = \left\{ C_j \in 2^{\mathcal{C}} : \operatorname{rank} \left(\begin{bmatrix} C_j \\ C_j A \\ \vdots \\ C_j A^{n-1} \end{bmatrix} \right) = n \right\}.$$

The system utilizing the sensor combination C_i is,

$$\begin{aligned} \dot{x} &= Ax + Bu, \\ y_i &= C_i x. \end{aligned}$$

Remark 4. We note the distinction between the set of sensors $\mathcal{C}$ and the set of sensing modes $\mathcal{S}_o$. The set of sensors contains the different physical components that measure parts of the system's behavior. On the other hand, the set of sensing modes contains those cooperating sensors together with an observer scheme that reconstruct an estimate of the system state. □

B. Optimal Observers Design

In order to incorporate concepts from optimal control into state estimation, we follow the work of [25]. The observer of (1) will be now designed as a dynamic system sharing the same structural properties,

$$\begin{aligned} \dot{\hat{x}} &= A\hat{x} + Bu + B\bar{u}_i, \\ \hat{y}_i &= C_i \hat{x}, \end{aligned} \tag{22}$$

where $\hat{x} \in \mathbb{R}^n$, $\hat{y}_i \in \mathbb{R}^p$ are the estimates of the state and the output respectively, $\bar{u}_i \in \mathbb{R}^m$ denotes a "fictional" input, i.e., a correction term which forces the observer to track the actual system.

Remark 5. The state estimate $\hat{x}$ is independent of the active sensing mode. On the other hand, the output $\hat{y}_i$ and "fictional" input $\bar{u}_i$ are not. □

To design the optimal $\bar{u}_i$, we define the optimization problem based on the following cost function $\forall t \geqslant 0$,

$$U_i^\star(\hat{x}) = \min_{\bar{u}_i} \int_t^\infty \left[(\hat{y}_i - y_i)^{\mathrm{T}} Q_i (\hat{y}_i - y_i) + \bar{u}_i^{\mathrm{T}} R_i \bar{u}_i \right] \mathrm{d}\tau.$$

Defining the Hamiltonian of the system as,

$$\begin{aligned} H_i(\hat{x}, \bar{u}_i^\star, U_i^\star) &= (\hat{y}_i - y_i)^{\mathrm{T}} Q_i (\hat{y}_i - y_i) + \bar{u}_i^{\star\mathrm{T}} R_i \bar{u}_i^\star \\ &\quad + \nabla U_i^{\star\mathrm{T}} (A\hat{x} + Bu + B\bar{u}_i^\star) = 0. \end{aligned} \tag{23}$$

We can now find the optimal control from the stationarity conditions $\frac{\partial H_i(\hat{x}, \bar{u}_i^\star, U_i^\star)}{\partial \bar{u}_i^\star} = 0$. This leads to,

$$\bar{u}_i^\star = -R_i^{-1} B^{\mathrm{T}} \nabla U_i^\star(\hat{x}).$$

Due to the quadratic structure of the cost functional and the linear structure of the dynamic system, we assume that the value function is quadratic in $\hat{x}(t)$, i.e., $U_i^\star(\hat{x}) = \hat{x}^{\mathrm{T}} G_i \hat{x}$, which means that the optimal 'input' is,

$$\bar{u}_i^\star = -R_i^{-1} B^{\mathrm{T}} G_i \hat{x}. \tag{24}$$

In this section, we show how the same techniques introduced and analyzed in the previous sections can be applied to detect and mitigate sensor attacks.

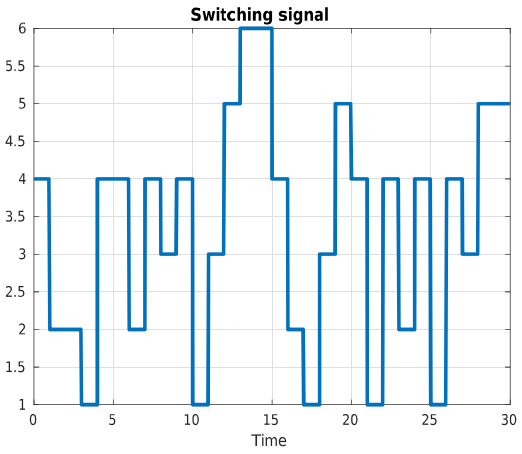

Fig. 1. The evolution of the MTD switching signal that guarantees actuator proactive security. It can be seen that controller with index 4 is preferred since it is the most optimal.

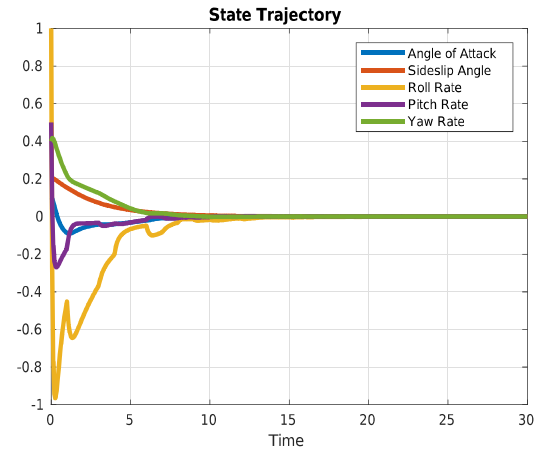

Fig. 2. The evolution of the MTD state that guarantees actuator proactive security. With the appropriate dwell-time, the system remains stable.

C. MTD for Sensor Attacks

Theorem 3. The state estimation scheme utilizing optimal observers as described by (22), for every sensing mode in $\mathcal{S}_o$ has an asymptotically stable equilibrium point under a switching-based MTD mechanism given that the switching signal has the average dwell time,

$$\tau_D > \frac{\max_{q,p\in\mathcal{S}_o} \frac{\bar{\lambda}(G_p)}{\underline{\lambda}(G_q)}}{\min_{p\in\mathcal{S}_o} \frac{\underline{\lambda}(C_i^{\mathrm{T}} Q_p C_i + G_p B_p R_p^{-1} B_p^{\mathrm{T}} G_p)}{\bar{\lambda}(G_p)}}.$$

Proof. The proof follows closely Theorem 2 for the switched observer comprised of different sensing modes and by taking into account the optimal control problem formulated in this section by (24) and (23). □

Remark 6. The optimization problem solved in subsection III-C is identical for the case of sensor switching. As a result, the probability that a certain sensing mode S_i is active, obeys (12). □

V. Simulation

In order to show the effectiveness of our approaches we will use a linearized 5-dimensional model of the ADMIRE benchmark aircraft [26]. The model has 7 redundant actuators and 2 redundant sensors. Initially, we present results for the problem of controlling the plant in an adversarial environment. Figure 1 shows the switching signal for the MTD framework applied to actuator attacks. Figure 2 shows convergence of the states under actuator MTD.

Although the advantages of most intrusion detection mechanism can be seen when the system is under attack, due to its proactive nature the success or failure of an MTD system is not easily obvious. Furthermore, the optimality loss induced by the use of non-overall-optimal controllers must be examined. The optimality loss was assessed as the difference between the actual cost during the system run, and the value function of the most optimal controller. To obtain some first validation results for our MTD algorithm, random attack

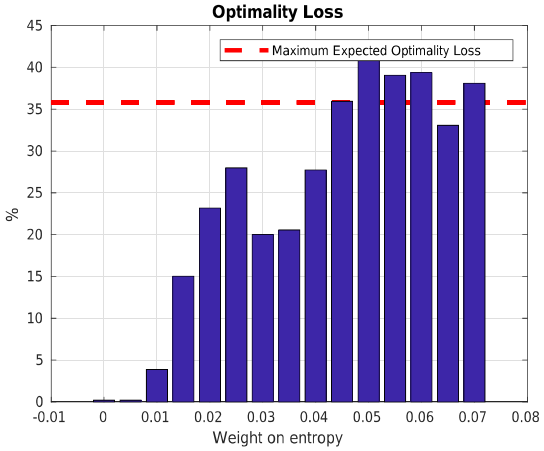

Fig. 3. Optimality loss induced by the unpredictable controllers for different entropy levels. By increasing the weight on the entropy, we reach a maximum optimality loss in the case of the uniform distribution.

vectors where considered for multiple runs of the system. In Figure 3, we present the average cost of the system as the unpredictability increases. We can see that the cost converges to a maximum value for uniform distribution over all the available controllers. In Figure 4, the compromise between security against attacks and optimality is highlighted.

VI. Conclusion and Future Work

In this work, we developed a defense mechanism for control systems that operate in adversarial environments. This scheme employs the principles of MTD, to introduce unpredictability on the system's operation. The MTD was implemented through a stochastic switching mechanism. Convex optimization techniques were utilized to guarantee unpredictability maximization, while Lyapunov methods were used to show stability of the proposed algorithm. Simulations on linearized models of a benchmark aircraft showcased the efficacy of our method.

Future efforts will focus on, complementing the proactive mechanism with an appropriate intrusion detection system to

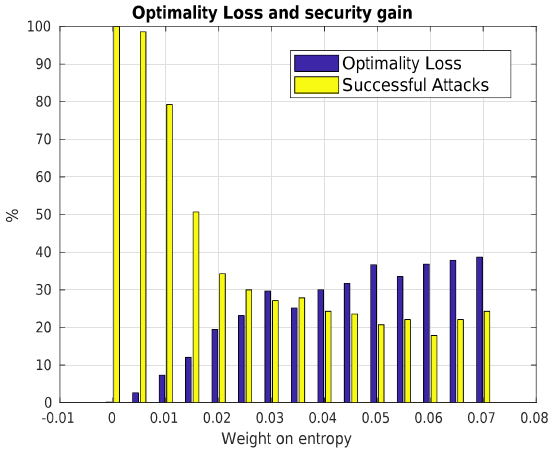

Fig. 4. Optimality loss and rate of successful attacks as a function of the entropy. Increase of unpredictability leads to less optimal controllers but manages to secure the system from attacks.

secure the system even further, as well as on the development of realistic models of the attackers to analyze the efficiency of proactive defense schemes.

REFERENCES

[1] R. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: the next computing revolution," in *Proceedings of the 47th design automation conference*. ACM, 2010, pp. 731–736.

[2] I. Lee and O. Sokolsky, "Medical cyber physical systems," in *Design Automation Conference (DAC), 2010 47th ACM/IEEE*. IEEE, 2010, pp. 743–748.

[3] N. Leavitt, "Researchers fight to keep implanted medical devices safe from hackers," *Computer*, vol. 43, no. 8, pp. 11–14, 2010.

[4] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno *et al.*, "Comprehensive experimental analyses of automotive attack surfaces." in *USENIX Security Symposium*. San Francisco, 2011.

[5] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham *et al.*, "Experimental security analysis of a modern automobile," in *Security and Privacy (SP), 2010 IEEE Symposium on*. IEEE, 2010, pp. 447–462.

[6] D. P. Shepard, J. A. Bhatti, T. E. Humphreys, and A. A. Fansler, "Evaluation of smart grid and civilian uav vulnerability to gps spoofing attacks," in *Proceedings of the ION GNSS Meeting*, vol. 3, 2012, pp. 3591–3605.

[7] R. M. Lee, M. J. Assante, and T. Conway, "German steel mill cyber attack," *Industrial Control Systems*, vol. 30, p. 62, 2014.

[8] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on*. IEEE, 2008, pp. 495–500.

[9] G. Theodorakopoulos and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks," *IEEE Journal on selected areas in Communications*, vol. 24, no. 2, pp. 318–328, 2006.

[10] S. Bhattacharya and T. Başar, "Game-theoretic analysis of an aerial jamming attack on a uav communication network," in *American Control Conference (ACC), 2010*. IEEE, 2010, pp. 818–823.

[11] M. Maki, J. Jiang, and K. Hagino, "A stability guaranteed active fault-tolerant control system against actuator failures," *International Journal of Robust and Nonlinear Control*, vol. 14, no. 12, pp. 1061–1077, 2004.

[12] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on scada systems," *IEEE Transactions on Control Systems Technology*, vol. 22, no. 4, pp. 1396–1407, 2014.

[13] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic Control*, vol. 59, no. 6, pp. 1454–1467, 2014.

[14] S. Jajodia, A. K. Ghosh, V. Swarup, C. Wang, and X. S. Wang, *Moving target defense: creating asymmetric uncertainty for cyber threats*. Springer Science & Business Media, 2011, vol. 54.

[15] M. Dunlop, S. Groat, W. Urbanski, R. Marchany, and J. Tront, "Mt6d: A moving target ipv6 defense," in *Military Communications Conference, 2011-Milcom 2011*. IEEE, 2011, pp. 1321–1326.

[16] J. H. Jafarian, E. Al-Shaer, and Q. Duan, "Openflow random host mutation: transparent moving target defense using software defined networking," in *Proceedings of the first workshop on Hot topics in software defined networks*. ACM, 2012, pp. 127–132.

[17] S. Weerakkody and B. Sinopoli, "Detecting integrity attacks on control systems using a moving target approach," in *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*. IEEE, 2015, pp. 5820–5826.

[18] Q. Zhu and T. Başar, "Game-theoretic approach to feedback-driven multi-stage moving target defense," in *International Conference on Decision and Game Theory for Security*. Springer, 2013, pp. 246–263.

[19] H. Okhravi, T. Hobson, D. Bigelow, and W. Streilein, "Finding focus in the blur of moving-target techniques," *IEEE Security & Privacy*, vol. 12, no. 2, pp. 16–26, 2014.

[20] R. Zhuang, S. A. DeLoach, and X. Ou, "Towards a theory of moving target defense," in *Proceedings of the First ACM Workshop on Moving Target Defense*. ACM, 2014, pp. 31–40.

[21] T. M. Cover and J. A. Thomas, *Elements of information theory*. John Wiley & Sons, 2012.

[22] J. P. Hespanha and A. S. Morse, "Stability of switched systems with average dwell-time," in *Decision and Control, 1999. Proceedings of the 38th IEEE Conference on*, vol. 3. IEEE, 1999, pp. 2655–2660.

[23] M. Mariton, *Jump linear systems in automatic control*. M. Dekker New York, 1990.

[24] D. Liberzon, *Switching in systems and control*. Springer Science & Business Media, 2012.

[25] J. Na, G. Herrmann, and K. G. Vamvoudakis, "Adaptive optimal observer design via approximate dynamic programming," in *American Control Conference (ACC), 2017*. IEEE, 2017, pp. 3288–3293.

[26] X. Yu and J. Jiang, "Hybrid fault-tolerant flight control system design against partial actuator failures," *IEEE Transactions on Control Systems Technology*, vol. 20, no. 4, pp. 871–886, 2012.

[27] G. Zhai, B. Hu, K. Yasuda, and A. N. Michel, "Stability analysis of switched systems with stable and unstable subsystems: an average dwell time approach," *International Journal of Systems Science*, vol. 32, no. 8, pp. 1055–1061, 2001.