52nd IEEE Conference on Decision and Control
December 10-13, 2013. Florence, Italy

Hybrid Robust Controller Design: Cyber Attack Attenuation for Cyber-Physical Systems

Cheolhyeon Kwon and Inseok Hwang

Abstract—**This paper considers controller design for Cyber-Physical Systems (CPSs) that are robust to various types of cyber attacks. While the previous studies have investigated a secure control by assuming a specific attack strategy, in this paper we propose a hybrid robust control scheme that contains multiple sub-controllers, each matched to a specific type of cyber attacks. Then the system can be adapted to various cyber attacks (including those that are not assumed for sub-controller design) by switching its sub-controllers to achieve the best performance. We propose a method for designing the secure switching logic to counter all possible cyber attacks and mathematically verify the system's performance and stability as well. The performance of the proposed control scheme is demonstrated by an example with the hybrid $H_2 - H_\infty$ controller applied to an Unmanned Aerial System (UAS).**

I. INTRODUCTION

The security issues for Cyber-Physical Systems (CPSs) against cyber attacks have emerged as an important yet challenging problem due to their close integration of the physical processes, computational resources, and communication capabilities [1]. Despite the advances in information security, such as the confidentiality, integrity, and authentication of data, these methods alone are not sufficient for CPSs to deal with various cyber attacks. In order to complement the security of the CPS from the system's perspective, *secure control theory* which studies how cyber attacks affect the physical dynamics of the system has been exploited in the last few years [2].

Within the secure control framework, our earlier work [3], [4] was focused on analyzing the system's response during cyber attacks and its vulnerabilities using information about the dynamical model of the CPS. In this paper we extend our research along this direction to develop a control scheme that alleviates the effect of cyber attacks. Most of the previous research on secure controller design is based on the game theoretical approach and/or the classical optimal control paradigms. In the game theoretical approach, the cyber attacker(s) and the protector(s) are players competing for goals in a dynamic game[5]. This has been applied to controls over a compromised network [6], electric power systems [7], etc. In the optimal control paradigms, on the other hand, different control methods such as the maximum principle [8], H_2 and H_∞ control [9], etc, have been proposed to optimize the system's performance under a specific attack model. For instance, [10] provides a secure control scheme in the presence of Denial of Service (DoS) attacks.

In all the works mentioned above, the secure control problems are subject to anticipated attack strategies, where the attack is assumed to be known a priori and can thus be treated as a parameter in the problem. However, since the attacker's intent is independent of the controller's actions and may even change during the cyber attack, the designed secure controls, although optimal under a certain attack assumption, may not be so in the case of unforeseen and arbitrary attacks. This means that their performances could degrade if the actual attack deviates from one assumed by a controller. Our work therefore studies the design of a secure control scheme with the ability of adapting the system with respect to various cyber attacks. Inspired by a hybrid system model, we propose a hybrid robust controller that consists of multiple sub-controllers, each designed to counter a specific type of cyber attacks, and can switch among them to optimize its performance against various types of cyber attacks, including those that are not assumed for sub-controller design. The main objective of this paper is to design the switching logic which enables the hybrid controller to switch to the most secure sub-controller.

For this task, we adopt the linear-quadratic performance criteria to evaluate the system and control performance. Using this criteria, it can be said that a certain controller is more secure than another if its evaluated performance is better than another under a given cyber attack. In other words, the most secure sub-controller at each time step is the one whose future performance is the best under expected future cyber attacks. Since the future attack behavior is unpredictable, we instead compute the worst-performance of each sub-controller. Once the system compares these worst-performances, the most secure sub-controller is determined and the switching to this sub-controller occurs accordingly. Such a switching logic is proved that the hybrid controller performs better than a single sub-controller and maintains its stability as well. Here, the estimated worst-performance depends on the system's current state and past attack history. Hence, unlike previous research, our hybrid control scheme incorporates the past attack information into the design of secure controls.

The rest of this paper is organized as follows: in Section II, we describe a CPS dynamics subject to cyber attacks and present a hybrid robust control framework. Section III presents a hybrid control scheme with the switching logic. More precisely, we present a cyber attack history construction method and an algorithm for the secure switching logic which can make the hybrid controller switch to the sub-controller that has the best performance under the current cyber attack. The performance of the proposed control scheme is demonstrated

Authors are with the School of Aeronautics and Astronautics, Purdue University, West Lafayette, IN, 47907 USA kwonc@purdue.edu, ihwang@purdue.edu

978-1-4673-5717-3/13/$31.00 ©2013 IEEE

with an illustrative Unmanned Aerial System (UAS) example in Section IV, where the controller is exemplified by the hybrid $H_2 - H_\infty$ controller. Conclusions are given in Section V.

II. Problem Formulation

We consider in this paper the discrete-time linear CPS model subject to a set of priori-unknown cyber attacks:

$$\begin{aligned} x_a(k+1) &= Ax_a(k) + Bu(k) + B_c a(k), \quad x_a(0) = x_0 \\ z(k) &= Cx_a(k) + Du(k) \end{aligned} \tag{1}$$

where $x_a(k) \in \mathbb{R}^n$ (the subscript 'a' means the system with cyber attacks), $u(k) \in \mathbb{R}^p$, $z(k) \in \mathbb{R}^m$ are the system's state, input, and performance output respectively. A, B, C and D are the system matrices of appropriate dimensions, and $k \in \mathcal{N}$ denotes the discrete-time index, taking values from the time horizon (possibly infinite) $\mathcal{N} = \{0, 1, 2, \cdots, N\}$. Then various cyber attacks $a(k) \in \mathbb{R}^s$ are injected into the system with the attack matrix B_c of compatible dimension.

Assumption 1. It is assumed that B_c is of full column rank and the matrix pairs (A, B) and (A, B_c) satisfy the controllability condition.

Under this assumption, we can consider the worst security problem because the attackers with partial control access to the system could only cause less trouble than those with full control access. For simplicity, let us use the following notation throughout the paper:

$$x_{[\tau_1,\tau_2]} := \left[x^{\mathrm{T}}(\tau_1)\ x^{\mathrm{T}}(\tau_1+1)\ \cdots\ x^{\mathrm{T}}(\tau_2)\right]^{\mathrm{T}}$$

Regarding the performance output $z(k)$, we assume that:

$$(i)\ \mathrm{rank}(D) = p$$
$$(ii)\ D^T C = \mathbf{0}$$

With the above assumptions, the quadratic performance criteria associated with the system under cyber attacks is given by:

$$\begin{aligned} J(u_{[\tau_1,\tau_2]}, a_{[\tau_1,\tau_2]}) :=& \|z_{[\tau_1,\tau_2]}\|^2 + x_a^{\mathrm{T}}(\tau_2+1)C^{\mathrm{T}}Cx_a(\tau_2+1) \\ =& \sum_{k=\tau_1}^{\tau_2} \left(x_a^{\mathrm{T}}(k)Qx_a(k) + u^{\mathrm{T}}(k)Ru(k)\right) \\ &+ x_a^{\mathrm{T}}(\tau_2+1)Qx_a(\tau_2+1) \end{aligned} \tag{2}$$

where $Q = C^{\mathrm{T}}C \succeq \mathbf{0}$ and $R = D^{\mathrm{T}}D \succ \mathbf{0}$.

Assumption 2. The attack sequence $a(k)$ is assumed to be *signals with bounded energy*, i.e., $\|a_{[0,N]}\| < \rho^2$ where ρ is a measurable constant.

Assumption 2 is motivated by the practical consideration that, due to the physical limitation of control units in a CPS, e.g., power capacity, operation range, etc., attacker cannot inject arbitrarily large attack sequences. Without loss of generality, we consider the control sequence as closed-loop controls such as $u(k) = \mu(x_{a[0,k]})$, where μ is a mapping function, commonly called the *control law* or *strategy*. If permissible controllers are linear, one can represent the function f via a linear state feedback formulation such that:

$$u(k) = K(k)x_a(k) \tag{3}$$

where K is a state feedback gain matrix. When the system (1) has such a controller, its closed-loop behavior is governed by:

$$x_a(k+1) = (A + BK(k))\, x_a(k) + B_c a(k) \tag{4}$$

Then, the cyber attack attenuation problem is to design a feedback gain history $K^*(k)$ which minimizes J over all energy bounded attacks:

$$\begin{aligned} \min_{\{K(k), k\in\mathcal{N}\}} \quad & J(u_{[0,N]}, a_{[0,N]}) \\ \text{Suject to :} \quad & \|a_{[0,N]}\|^2 < \rho^2 \\ & \text{System dynamics (1)} \end{aligned} \tag{5}$$

Since the attack sequence $a(k)$ is unknown a priori, an attack scenario is assumed in order to solve the above optimization problem . Therefore, the solution is optimal only if the attacker behaves as assumed by the controller. In order to improve the performance of the controller under various cyber attacks, we employ a hybrid controller $\mathcal{K}$ that consists of multiple controllers, which are given by:

$$K(k) \in \mathcal{K} = \left\{K_q^* \middle| q \in \{1, 2, \cdots, r\},\ k \in \mathcal{N}\right\} \tag{6}$$

where K_q^* denotes a controller designed for a particular attack strategy. Figure 1 illustrates a schematic of the proposed hybrid controller design. Note that the actual cyber attack may differ from these r types considered and its types can change over time. In the next section, we present how to design a switching logic which makes the hybrid controller perform safer than the nominal controller that considers a single control law only.

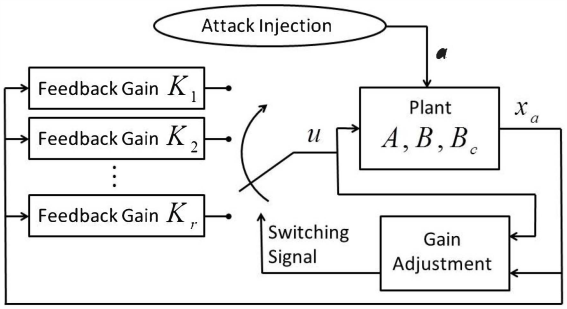

Fig. 1: Hybrid Controller Design for Various Cyber Attacks.

III. Hybrid Robust Controller Design

This section presents a robust control scheme against various cyber attacks, called discrete-time linear *Robust Hybrid Control System*, which is a collection of the following five tuples $\mathcal{H} = (\mathcal{Q}, \mathcal{X}_a, \mathcal{A}, f, G)$:

- $\mathcal{Q} = \{1, 2, \cdots, r\}$ is a finite set of the discrete state variables.
- $\mathcal{X}_a = \mathbb{R}^n$ is the continuous state space.
- $\mathcal{A} = [0, \rho^2]$ is the attack energy space.
- $f : \mathcal{Q} \times \mathcal{X}_a \to \mathcal{X}_a$ is a function that describes the evolution of the continuous state. With (6), f is defined as:

$$f(q, x) := (A + BK_q^*)x$$

Consequently, from (4), the continuous state dynamics is given by the following difference equation:

$$\begin{aligned} x_a(k+1) &= f(q(k), x_a(k)) + B_c a(k) \\ &= \left(A + BK^*_{q(k)}\right) x_a(k) + B_c a(k) \end{aligned} \tag{7}$$

- $G : \mathcal{Q} \times \mathcal{Q} \times \mathcal{N} \to 2^{\mathcal{X}_a \times \mathcal{A}}$ is a time-varying guard condition that assigns to each $(i,j) \in \mathcal{Q} \times \mathcal{Q}$ a guard $G(i,j,k) \subset \mathcal{X}_a \times \mathcal{A}$ such that:
  - $G(i,j,k)$ is a measurable subset of $\mathcal{X}_a \times \mathcal{A}$ (possibly empty, unbounded); and
  - for each $i \in \mathcal{Q}$, the set $\{G(i,j,k) | j \in \mathcal{Q}\}$ is a disjoint partition of $\mathcal{X}_a \times \mathcal{A}$, that is:

$$G(i,j,k) \cap G(i,l,k) = \emptyset, \qquad \forall j, l \in \mathcal{Q},\ j \neq l$$

and

$$\bigcup_{j=1}^{r} G(i,j,k) = \mathcal{X}_a \times \mathcal{A}, \qquad \forall j \in \mathcal{Q}$$

Let $\zeta = (q, x_a)$, where $q \in \mathcal{Q}$ and $x_a \in \mathcal{X}_a$, be the hybrid state of $\mathcal{H}$. An execution of $\mathcal{H}$ generates a discrete-time *hybrid state evolution* $\zeta(k)$ as follows:

- The evolution of the continuous state x_a in discrete-time is described by (7)
- The discrete state evolution is called as a discrete state transition and is governed by:

$$q(k) = \gamma(q(k-1), x_a(k), \|a_{[0,k-1]}\|^2, k) \tag{8}$$

where $\gamma : \mathcal{Q} \times \mathcal{X}_a \times \mathcal{A} \times \mathcal{N} \to \mathcal{Q}$ is the time-varying *discrete state transition function* defined as:

$$\gamma(i, x, \alpha^2, k) := j \quad \text{if} \quad (x, \alpha^2) \in G(i,j,k)$$

Therefore, each guard $G(i,j,k)$ describes a partition of the space $\mathcal{X}_a \times \mathcal{A}$ into a number of closed cells and its induced transition function switches the feedback gain K^*_q. Imposing the restriction on the energy of the future attack sequences $a_{[k,N]}$, we further define two functions $\bar{J} : \mathcal{Q} \times \mathcal{X}_a \times \mathcal{A} \times \mathcal{N} \to \mathbb{R}$ and $\underline{J} : \mathcal{Q} \times \mathcal{X}_a \times \mathcal{A} \times \mathcal{N} \to \mathbb{R}$ described by the following optimization problems:

$$\begin{aligned} \bar{J}(q, x, \alpha^2, k) &:= \max_{a_{[k,N]}} J(u^q_{[k,N]}, a_{[k,N]}) \\ \underline{J}(q, x, \alpha^2, k) &:= \min_{a_{[k,N]}} J(u^q_{[k,N]}, a_{[k,N]}) \\ \text{Suject to : }& \|a_{[k,N]}\|^2 < \rho^2 - \alpha^2 \\ & \text{System dynamics (1) where } x_a(k) = x \end{aligned} \tag{9}$$

where $u^q(k) = K^*_q x_a(k)$, $q \in \mathcal{Q}$. Note that $\bar{J}$ and $\underline{J}$ respectively stand for the upper bound and lower bound of the future cost from the current state with the bounded attack energy left. Using the above functions, the set of guards $\{G(i,j,k)\,| i \in \mathcal{Q}\}$ at each time k is presented as:

$$\begin{aligned} G(i,j,k) = \big\{ (x, \alpha^2) \,\big| x \in \mathcal{X}_a, \alpha^2 \in \mathcal{A}, j \in \mathcal{Q},\ l \in \mathcal{Q},\ j \neq l, \\ \bar{J}(j, x, \alpha^2, k) \leq \bar{J}(l, x, \alpha^2, k),\ \underline{J}(j, x, \alpha^2, k) \leq \underline{J}(i, x, \alpha^2, k) \big\} \end{aligned} \tag{10}$$

From (10), the discrete state transition function γ must be single-valued at all time, and thus every execution of $\mathcal{H}$ is well-defined under any possible attack sequences.

The perfomance of the hybrid control system $\mathcal{H}$ characterized by the guard condition (10) is ensured through the following theorem.

Theorem 1. *Optimality Condition* Let $J_{\mathcal{H}}$ be the cost function associated with the hybrid state response $\zeta(k)$ to an arbitrary cyber attack sequence $a(k)$, which is defined as:

$$J_{\mathcal{H}}(\zeta_{[0,N]}, a_{[0,N]}) := J(u^*_{[0,N]}, a_{[0,N]}) \tag{11}$$

where $u^*(k) = K^*_{q(k)} x_a(k)$ is determined by the hybrid state $\zeta(k)$. Then, for the cyber attacks with the bounded energy ρ, the following inequality holds:

$$\max_{a_{[\bullet,N]}} J_{\mathcal{H}}(\zeta_{[0,N]}, a_{[0,N]}) \leq \min_{\{q \in \mathcal{Q}\}} \max_{a_{[\bullet,N]}} J(u^q_{[0,N]}, a_{[0,N]}) \tag{12}$$

Proof. The theorem is proved by induction. Using (9), the right-hand side of (12) can be rewritten as:

$$\begin{aligned} &\min_{\{q \in \mathcal{Q}\}} \max_{a_{[\bullet,N]}} J(u^q_{[0,N]}, a_{[0,N]}) \\ &\qquad = \arg\min \left\{ \bar{J}(q, x_a(0), 0, 0) \middle| q \in \mathcal{Q} \right\} \end{aligned} \tag{13}$$

Under an arbitrary admissible attack sequence, the initial discrete state $q(0)$ is generated according to the guard condition (10) such that:

$$\begin{aligned} &J_{\mathcal{H}}(\zeta_{[0,0]}, a_{[0,0]}) + \bar{J}(q(0), x_a(1), \|a_{[0,0]}\|^2, 1) \\ &\quad \leq \bar{J}(q(0), x_a(0), 0, 0) = \arg\min \left\{ \bar{J}(q, x_a(0), 0, 0) \middle| q \in \mathcal{Q} \right\} \end{aligned} \tag{14}$$

And every discrete state transition at each $k = 1, 2, \cdots, N-1$ satisfies the following inequaility:

$$\begin{aligned} &J_{\mathcal{H}}(\zeta_{[0,k]}, a_{[0,k]}) + \bar{J}(q(k), x_a(k+1), \|a_{[0,k]}\|^2, k+1) \\ &\quad \leq J_{\mathcal{H}}(\zeta_{[0,k-1]}, a_{[0,k-1]}) + \bar{J}(q(k-1), x_a(k), \|a_{[0,k-1]}\|^2, k) \end{aligned} \tag{15}$$

For the final discrete state $q(N)$, the following inequality can be induced by the guard condition:

$$\begin{aligned} J_{\mathcal{H}}(\zeta_{[0,N]}, a_{[0,N]}) &\leq J_{\mathcal{H}}(\zeta_{[0,N-1]}, a_{[0,N-1]}) \\ &\quad + \bar{J}(q(N-1), x_a(N), \|a_{[0,N-1]}\|^2, N) \end{aligned} \tag{16}$$

Arranging the inequlities (14), (15), and (16) in the order of the maginitude, one can obtain (12). ■

Remark 1. Here the cost $J(u^j_{[0,N]}, a_{[0,N]})$ implies the performance of the system adopting the j^{th} controller only. Thus, if $\mathcal{H}$ is subject to the worst-case attack, Theorem 1 guarantees the performance of the hybrid controller is equivalent to or better than any individual sub-controller. Now we will show that the switching logic governed by the guard condition (10) guarantees the stability of the hybrid controller.

Theorem 2. *Stability Condition* Suppose the multiple feedback controllers individually satisfy the asymptotic stability condition, i.e.,

$$\|A + BK^*_q\| < 1, \quad \forall q \in \{1, 2, \cdots, r\} \tag{17}$$

Then the hybrid control system $\mathcal{H}$ with the sub-controllers (17) is also asymptotically stable.

Proof. Consider a collection of quadratic Lyapunov-like functions defined as:

$$V_q(x) := x^T(Q + K_q^{*T} R K_q^*)x, \quad \forall q \in \mathcal{Q} \tag{18}$$

They correspond to each discrete state q and are concatenated together to produce a time-varying Lyapunov function for $\mathcal{H}$ such that:

$$V_{\mathcal{H}}(x_a(k), k) = x_a^{\mathrm{T}}(k)(Q + K_{q(k)}^{*\mathrm{T}} R K_{q(k)}^*) x_a(k) \tag{19}$$

Note that $V_{\mathcal{H}}$ may not be monotonically decreasing along the consecutive switchings. Using (18), the cost function can be written as the sum of the Lyapunov-like functions:

$$J(u^q_{[0,N]}, a_{[0,N]}) = \sum_{k=0}^{N} V_q(x_a(k)) + x_a^{\mathrm{T}}(N+1) Q x_a(N+1) \tag{20}$$

Likewise, from (11), we know that:

$$J_{\mathcal{H}}(\zeta_{[0,N]}, a_{[0,N]}) = \sum_{k=0}^{N} V_{\mathcal{H}}(x_a(k), k) + x_a^{\mathrm{T}}(N+1) Q x_a(N+1) \tag{21}$$

With the energy bounded attack sequence along the infinite time horizon $\mathcal{N} = [0, \infty)$, the stability condition (17) yields:

$$\lim_{k \to \infty} V_q(x_a(k)) = 0, \quad \forall q \in \mathcal{Q} \tag{22}$$

On the other hand, substituting (20) and (21) for (12) gives:

$$\sum_{k=0}^{\infty} V_{\mathcal{H}}(x_a(k), k) \leq \min_{\{q \in \mathcal{Q}\}} \max_{a_{[0,\infty]}} \sum_{k=0}^{\infty} V_q(x_a(k)) \tag{23}$$

From (22), $\sum_{k=0}^{\infty} V_q(x_a(k))$ is bounded regardless of the attack sequence. Hence, $\sum_{k=0}^{\infty} V_{\mathcal{H}}(x_a(k), k)$ is also bounded, that leads to:

$$\lim_{k \to \infty} V_{\mathcal{H}}(x_a(k), k) = 0 \tag{24}$$

By the Lyapunov theorem, the existence of the positive definite Lyapunov function $V_{\mathcal{H}}$ satisfying (24) guarantees the asymptotic stability of $\mathcal{H}$. ■

Now, we leverage analytical tools for the switching logic for two reasons: Firstly, as shown in (8), the discrete state transition function γ requires the expanded information structure where the system is allowed to observe the past attack history $a_{[0,k-1]}$. This is in general an advantage to the controller, which requires an attack reconstruction procedure. Secondly, the guard condition G depends upon functions $\bar{J}$ and $\underline{J}$, both of which are based on the computationally intensive optimization problem (9). Thus, considering a number of guard sets over the whole time horizon $\mathcal{N}$, the overall computation cost could become numerically unmanageable. However, for the deterministic linear model considered in this paper, we are able to develop analytical and computationally efficient cyber attack reconstruction and switching algorithms.

Attack Reconstruction From the continuous state dynamics (7), the previous attack vector at time $k-1$ can be reconstructed as:

$$a(k-1) = B_c^+ \left(x_a(k) - (A + BK^*_{q(k)}) x_a(k-1) \right) \tag{25}$$

where $B_c^+ = (B_c^{\mathrm{T}} B_c)^{-1} B_c^{\mathrm{T}}$ denotes the Moore-Penrose pseudo inverse of matrix B_c. Since $\|a_{[0,k-1]}\|^2 = \|a_{[0,k-2]}\|^2 + \|a(k-1)\|^2$, the amount of the past attack energy can be recursively updated through the hybrid state evolution $\zeta(k)$.

Analytical Function Evaluation As a solution to (4), the state evolution to the attack sequence is given by the following convolution sums:

$$x_a(k) = \Gamma(0, k) x_a(0) + \sum_{\tau=0}^{k-1} \Gamma(\tau, k-1) B_c a(\tau) \tag{26}$$

where $\Gamma : \mathcal{N} \times \mathcal{N} \to \mathbb{R}^{n \times n}$ is the matrix function defined as:

$$\Gamma(\tau_1, \tau_2) := \begin{cases} I & \text{if } \tau_1 = \tau_2 \\ \displaystyle\prod_{\tau=\tau_1}^{\tau_2 - 1} (A + BK(\tau)) & \text{if } \tau_1 < \tau_2 \end{cases}$$

For the system controlled by the single feedback gain K_q^*, the matrix function Γ_q is:

$$\Gamma_q(\tau_1, \tau_2) := (A + BK_q^*)^{\tau_2 - \tau_1}, \quad \tau_1 \leq \tau_2 \tag{27}$$

To analytically evaluate the upper and lower bounds of the cost function, we define the following *attack correlation matrix*:

$$\Phi_q(i,j) := \begin{cases} \displaystyle\sum_{\tau=1}^{\min(i,j)} \Gamma_q^{\mathrm{T}}(\tau, i)(Q + K_q^{*\mathrm{T}} R K_q^*) \Gamma_q(\tau, j) & \\ \qquad + \Gamma_q^{\mathrm{T}}(0, i) Q \Gamma_q(0, j) & \text{if } \forall\, i, j > 0 \\ \Gamma_q^{\mathrm{T}}(0, i) Q \Gamma_q(0, j) & \text{if } \min(i,j) = 0 \end{cases} \tag{28}$$

for each discrete state q. Plugging (26) and (28) to (2), the future cost during a time interval $[k, N]$ can be transformed into the following quadratic form:

$$\begin{aligned} J(u^q_{[k,N]}, a_{[k,N]}) &= x_a^{\mathrm{T}}(k) \Phi_q(N-k, N-k) x_a(k) \\ &+ 2 a^{\mathrm{T}}_{[k,N]} \Omega_q(k,N) x_a(k) + a^{\mathrm{T}}_{[k,N]} \Psi_q(k,N) a_{[k,N]} \end{aligned} \tag{29}$$

where $\Omega_q(k,N)$ and $\Psi_q(k,N)$ are the block matrices respectively defined as:

$$\Omega_q(k,N) := \begin{bmatrix} B_c^{\mathrm{T}} \Phi_q(N-k, N-k) \\ B_c^{\mathrm{T}} \Phi_q(N-k-1, N-k) \\ B_c^{\mathrm{T}} \Phi_q(N-k-2, N-k) \\ \vdots \\ B_c^{\mathrm{T}} \Phi_q(0, N-k) \end{bmatrix}$$

$\Psi_q(k,N) :=$

$$\begin{bmatrix} B_c^{\mathrm{T}} \Phi_q(N-k, N-k) B_c & \cdots & B_c^{\mathrm{T}} \Phi_q(N-k, 0) B_c \\ \vdots & \ddots & \vdots \\ B_c^{\mathrm{T}} \Phi_q(0, N-k) B_c & \cdots & B_c^{\mathrm{T}} \Phi_q(0, 0) B_c \end{bmatrix}$$

From (29), we introduce a Lagrange multiplier $\mu \in \mathbb{R}$ and define the Lagrange function for the optimization problem (9) as:

$$L_q(a_{[k,N]},\mu) := \frac{1}{2} a_{[k,N]}^{\mathrm{T}} \Psi_q(k,N) a_{[k,N]} + a_{[k,N]}^{\mathrm{T}}\Omega_q(k,N)x_a(k) + \mu\left(\|a_{[k,N]}\|^2 - (\rho^2 - \|a_{[0,k-1]}\|^2)\right)$$

Let $(a^*_{[k,N]}, \mu^*)$ be the solution to the dual problem of the primal problem (9). The Karush-Kuhn-Tucker (KKT) condition which characterizes the solution to the dual problem can be written as:

$$\begin{cases} \mu^*\left(\|a^*_{[k,N]}\|^2 - (\rho^2 - \|a_{[0,k-1]}\|^2)\right) = 0 \\ \Omega_q(k,N)x_a(k) + \Psi_q(k,N)a^*_{[k,N]} + 2\mu^*\|a^*_{[k,N]}\|a^*_{[k,N]} = \mathbf{0} \end{cases}$$

From the above condition, the optimal attack sequences $a^*_{[k,N]}$ which satisfy the optimization problem (9) can be derived analytically. Due to the space limitation, the detailed derivations are omitted.

A cycle of the recursive hybrid state evolution $\zeta(k)$ at time k for the proposed hybrid robust control scheme is summarized as follows (see also Figure 2):

1) *Discrete state transition:* Compute the functions $\bar{J}(i, x_a(k), \|a_{[0,k-1]}\|^2, k)$, $\underline{J}(i, x_a(k), \|a_{[0,k-1]}\|^2, k)$, for all $i \in \mathcal{Q}$ using (9) and compute the discrete state $q(k)$ using (8) and (10).
2) *Continuous state evolution:* The continuous state $x_a(k+1)$ is given by (7) with an arbitrary attack sequence $a(k)$.
3) *Attack energy update:* Reconstruct the previous attack $a(k)$ using (25). Then attack energy $\|a_{[0,k]}\|$ is updated from $\|a_{[0,k-1]}\|$ and $a(k)$.

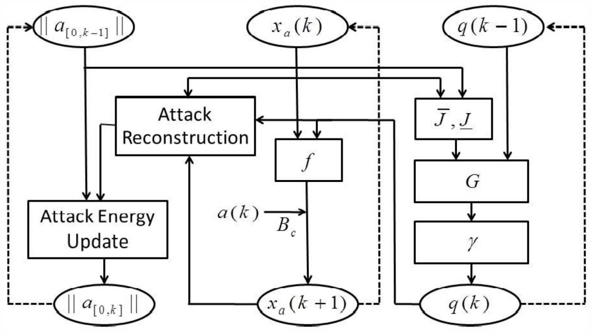

Fig. 2: Structure of Hybrid Robust Control Scheme

IV. Example: Hybrid $H_2 - H_\infty$ Controller

In this section we investigate a special class of the robust hybrid control systems that contains two optimal controllers: H_2 and H_∞ optimal controllers, each of which is derived based on an anticipated attack strategy [9], [11]. Our hybrid control scheme allows switchings between the two controllers to mitigate the effect of arbitrary attacks. The effectiveness of such a hybrid controller design is demonstrated with an example of the Unmanned Aerial System (UAS) under cyber attacks. In this example, we consider the linearized longitudinal motion of a rotorcraft, for which a detailed dynamical model can be found in [12]. Suppose the attacker has full control access, i.e., $B_c = B$. Then, the state evolution of the UAS subject to cyber attacks is captured by our framework (1), where the specific values of the system matrices A, B are given by [13]. The matrices C and D are properly chosen to reflect the performance criteria of the system under cyber attacks. The optimal feedback gains K_{H_2} and K_{H_∞} are designed accordingly by using [9] and [11].

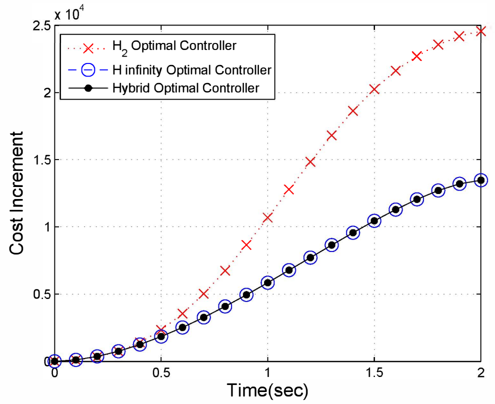

Fig. 3: Cost Increments by the H_2, H_∞, and hybrid controllers under the Worst Case Attack Sequence with Finite Time Horizon.

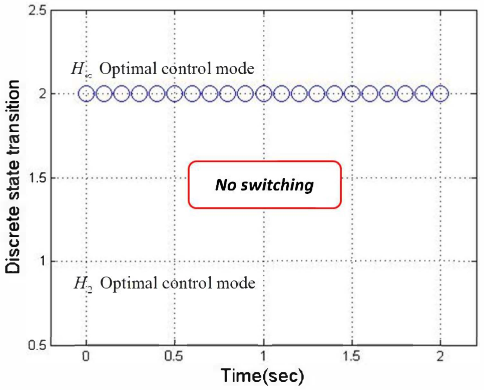

Fig. 4: Discrete State Transition of the Hybrid Controller under the Worst Case Attack Sequence with Finite Time Horizon.

For the simulations, two types of cyber attack sequences are considered: the worst-case and random attack sequences, which are the attack assumptions imposed on H_∞ and H_2 optimal controllers respectively. In the simulation, we evaluate the performance of the hybrid control scheme and compare the results with those of the single H_2 and the H_∞ optimal controllers. Under the worst-case attack sequence, Figure 3 shows the cost J for each controller with time horizon $N = 20$. Clearly, the single H_∞ optimal controller outperforms the H_2 optimal controller due to their inherent attack assumptions. As expected, the proposed hybrid controller chooses the H_∞ controller from the beginning and does not make a transition to the H_2 controller (shown in Figure 4) since H_∞ optimal controller works better the worst-case attack sequence. This demonstrates that the performance of the proposed hybrid controller is equivalent to that of a single controller designed for the worst-case attack and better for any other feasible attacks.

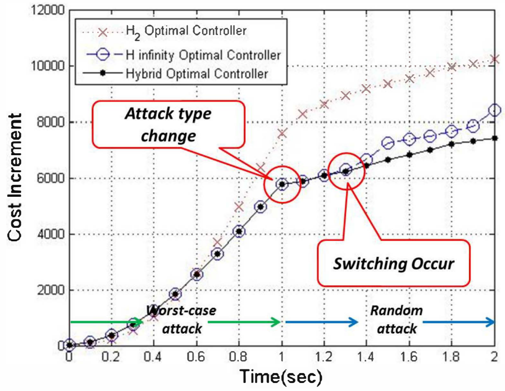

Fig. 5: Cost Increments by the H_2, H_∞, and hybrid controllers under the Worst Case Attack and Random Attack Combined Sequence 1 with Finite Time Horizon.

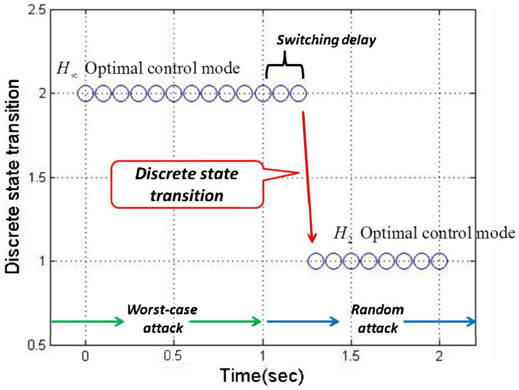

Fig. 6: Discrete State Transition of the Hybrid Controller under the Worst Case Attack and Random Attack Combined Sequence 1 with Finite Time Horizon.

Now, let us consider a combinatorial attack strategy that contains both the worst-case attack and the random attack. Here, the attacker injects the worst-case attack sequence first and then changes his attack strategy to the random attack sequence at $k = 10$. As shown in Figures 5 and 6, while each sub-controller performs poorly when it is subject to a different type of cyber attack from the one assumed for its design, the hybrid controller compensates for the attack effect by switching its sub-controller from H_∞ to H_2 optimal controller. Note that there is some switching delay due to the delay for the attack change detection. To further improve the system's performance, we need to investigate this aspect in the future research.

V. Conclusions

In this paper, we have proposed a hybrid robust control scheme which has a capability of adapting its control law with respect to various cyber attacks. The proposed hybrid controller consists of a set of multiple sub-controllers, each designed for a assumed cyber attack and it can switch among the sub-controllers. The system's robustness then can be improved by switching to the most secure sub-controller according to the reconstructed past attack sequence as well as the system's current state. In addition, we have derived an analytic algorithm to compute the guard conditions that governs the switching of the hybrid controller. To illustrate the proposed idea, we have considered a special class of the hybrid controller in which H_2 and H_∞ optimal controllers are designed as the sub-controllers. Simulation results with an Unmanned Aerial System (UAS) example demonstrate that the hybrid $H_2 - H_\infty$ controller performs better than either single H_2 or H_∞ optimal controller against various types of cyber attacks.

References

[1] A. Cardenas, S. Amin, and S. Sastry. Research challenges for the security of control systems. In *3rd USENIX Workshop on Hot topics in security*, page Article 6, Jul. 2008.

[2] A. Cardenas, S. Amin, and S. Sastry. Secure control: Towards survivable cyber-physical systems. In *First International Workshop on Cyber-Physical Systems*, Jun. 2008.

[3] W. Liu, C. Kwon, and I. Hwang. Cyber security analysis for state estimators in air traffic control systems. In *AIAA Conference on Guidance, Navigation, and Control*, Aug. 2012.

[4] C. Kwon, W. Liu, and I. Hwang. Security analysis for cyber-physical systems against stealthy deception attacks. In *AACC American Control Conference*, Jun. 2013.

[5] T. Basar and G. Olsder. Dynamic noncooperative game theory. *Society for Industrial Mathematics (SIAM) Series in Classics in Applied Mathematics*, 1999.

[6] A. Gupta, C. Langbort, and T. Basar. Optimal control in the presence of an intelligent jammer with limited actions. In *49th IEEE Conference on Decision and Control*, pages 1096–1101, Dec. 2010.

[7] Q. Zhu and T. Basar. Robust and resilient control design for cyber-physical systems with an application to power systems. In *50th IEEE Conference on Decision and Control and European Control Conference*, Dec. 2011.

[8] W. W. Lu, G. J. Bala, and E. B. Lee. Linear quadratic performance with worst case disturbance rejection. In *AACC American Control Conference*, volume 3, pages 1962–1966, Jun. 1995.

[9] G. E. Dullerud and F. Paganini. *A Course in Robust Control Theory: A Convex Approach.* Springer, 2000.

[10] S. Amin, A. Cardenas, and S. Sastry. Safe and secure networked control systems under denial-of-service attacks. In *12th International Conference on Hybrid Systems: Computation and Control*, pages 31–45, Apr. 2009.

[11] T. Basar. A dynamic games approach to controller design: Disturbance rejection in discrete-time. *IEEE Transactions on Automatic Control*, 36(8):936–952, 1991.

[12] K. S. Narenda and S. S. Tripathi. Identification and optimization of aircraft dynamics. *J. Aircraft*, 10:193–199, 1973.

[13] W. Liu and I. Hwang. Robust estimation and fault detection and isolation algorithms for stochastic linear hybrid systems with unknown fault input. *IET Control Theory and Applications*, 5(12):1353–1368, 2011.