

Asymptotic Security of Control Systems by Covert Reaction: Repeated Signaling Game with Undisclosed Belief

Hampei Sasahara¹, Serkan Sarıtaş², and Henrik Sandberg¹

Abstract—This study investigates the relationship between resilience of control systems to attacks and the information available to malicious attackers. Specifically, it is shown that control systems are guaranteed to be secure in an asymptotic manner by rendering reactions against potentially harmful actions covert. The behaviors of the attacker and the defender are analyzed through a repeated signaling game with an undisclosed belief under covert reactions. In the typical setting of signaling games, reactions conducted by the defender are supposed to be public information and the measurability enables the attacker to accurately trace transitions of the defender’s belief on existence of a malicious attacker. In contrast, the belief in the game considered in this paper is undisclosed and hence common equilibrium concepts can no longer be employed for the analysis. To surmount this difficulty, a novel framework for decision of reasonable strategies of the players in the game is introduced. Based on the presented framework, it is revealed that any reasonable strategy chosen by a rational malicious attacker converges to the benign behavior as long as the reactions performed by the defender are unobservable to the attacker. The result provides an explicit relationship between resilience and information, which indicates the importance of covertness of reactions for designing secure control systems.

I. INTRODUCTION

Modern cyber-physical systems are facing malicious actions by sophisticated adversaries because of increasing interconnectivity of the cyber and physical layers. In fact, various incidents on cyber attacks on physical systems have been reported, which cover a broad range of applications such as an attack on an uranium enrichment plant, attacks on Ukrainian power plants, remote car hacking, and unmanned aerial vehicle hacking [1]–[4]. Thus, analysis and synthesis of resilient cyber-physical systems have become a crucial topic in our community.

There are numerous studies discussing resilience of cyber-physical systems based on control theory, in which several definitions of resilience have been proposed thus far; see [5]–[13]. In the existing studies, the control system to be defended is supposed to be protected with an attack-detection scheme. Accordingly, the behavioral principle of malicious attackers is given as maximizing impacts on behavior of the control system through attacks without being detected. In this framework, behaviors of the system, the attacker, and the defender after an alarm are not concerned. An implicit premise is that effects of malicious attacks can immediately

be eliminated or an excessive reaction, e.g., terminating the entire system, is performed once an alarm rings.

In actual systems, however, the post-alarm process should carefully be analyzed because root-cause analysis of anomalies is difficult and also suspension of whole parts of the system is undesirable due to false alarms and costs. An approach to cope with attacks more flexibly is to choose a proper reaction against potentially executed harmful actions depending on the level of confidence on existence of a malicious attacker. An example can be provided for networked systems, in which disconnecting some components that are presumed to be attacked is more acceptable than simply terminating the entire network when the operator’s confidence is not firm. The technical problem here is that, under this scenario sophisticated attackers choose their actions according to their measurement on the state of the system as well as defender’s reactions. Thus we can no longer employ the existing frameworks for resilience assessment because it is now required to handle interactions between attacker’s actions and defender’s reactions unlike the case where the attacker simply avoids being detected.

This study investigates the relationship between *resilience* of control systems and *information* available to malicious attackers under the setting above motivated by the following consideration. Suppose that a malicious attacker can fully observe reactions executed by the defender. When observing aggressive reactions, the attacker recognizes that the confidence on existence of a malicious attacker is fairly firm and then a reasonable behavior of the attacker is to stay calm. Conversely, if a non-aggressive reaction is observed, the attacker is allowed to execute an offensive action. This discussion leads to the expectation that leak of information on the reactions implemented by the defender causes serious damage to the system, and conversely, also that resilience is enhanced by rendering reactions covert. A naturally arising question here is how, and how much, the resilience is strengthened by covertness of reactions.

In order to give an answer to the question, we analyze the situation using game theory. In particular, we formulate behaviors of the decision makers as a repeated signaling game [14]. In a signaling game, there are two players, one of which, referred to as a sender, has private information called *type* and chooses her action based on her preference depending on her type [15], [16]. The action has a role as signaling to the other player, referred to as a receiver, who forms a belief on the sender’s type based on received signals and chooses a reasonable reaction under the belief. A widely employed solution concept is perfect Bayesian

¹ Hampei Sasahara and Henrik Sandberg are with the Division of Decision and Control Systems, KTH Royal Institute of Technology, Stockholm, Sweden, {hampei, hsan}@kth.se.

² Serkan Sarıtaş is with the Division of Information Science and Engineering, KTH Royal Institute of Technology, Stockholm, Sweden, saritas@kth.se.

Nash equilibria, on which both player's strategies are best responses to each other and the belief of the receiver is updated based on Bayes' rule. Typically, the reasonable actions of the players are supposed to be given as one of the equilibria on the premise that the prior belief and its transition are public information. In our case, however, the exact value of the belief is undisclosed to the attacker owing to covertness of reactions and hence her reasonable strategies cannot be determined using the usual concept. Because the accurate value of the belief is unknown, the attacker has to estimate the belief, i.e., "belief of belief" is required for determining the attacker's reasonable actions. To handle this situation, we introduce a novel framework, under which the estimated belief is specifically given as the conditional expected value of the true belief. Based on the framework, we can determine well-posed reasonable attacker's actions.

Our analysis under the presented framework reveals that *asymptotic security* is achieved by covert reaction for general control systems. Specifically, it is shown that any reasonable strategy chosen by a rational malicious attacker converges to the benign behavior as time proceeds. The finding is based on the fact that the estimated belief from the attacker is a monotonically non-decreasing function whatever strategy the attacker chooses. From the monotonicity, the estimated belief is eventually large as the game proceeds. When the belief is sufficiently increased the reasonable action is restricted to the most unsuspecting behavior, which is given by the benign behavior. The obtained result gives an explicit relationship between resilience and information and suggests that covertness of reactions is an essential requirement for designing secure control systems.

Existing literature considering control systems under Bayesian games where some players do not have exact values of other players' beliefs can be found [17]–[20]. Typically, the situation emerges with *asymmetric information*, i.e., some information of the game is assumed to be private. The approach for handling the situation in [17]–[19] is based on the idea that the belief of all players are constructed only with common information. It is shown in [20] that if the game is a linear quadratic game then the true belief is constructed only with each player's local information. Analysis of system security based on signaling game is studied in [21], the modeling in which is similar to ours. The main difference compared to this study is that the belief is assumed to be known to both players and a single stage game is considered in [21]. In economics literature, games without knowledge of actions performed by players are categorized into a Bayesian game with imperfect information, in which the solution concept is given as sequential equilibria [22]–[24]. Our solution concept differs from sequential equilibria from the perspective that our concept is given with the sender's belief about the receiver's belief while sequential equilibria are given with the sender's belief about all variables in the game on each information set. Furthermore, the notion of hierarchies of beliefs is proposed for treating the "belief of belief" concept in the general setup [25], [26].

The organization of this paper is as follows. In Section II,

we first show a motivating example for our analysis. Then we give the model of the system to be defended and behaviors of a malicious attacker and the defender based on a repeated signaling game formulation. Section III provides an analysis of the formulated game and reveals that asymptotic security is achieved by covert reaction. The theoretical findings are verified through a numerical example in Section IV and Section V draws conclusion.

Notation

Let \mathbb{Z}_+ and \mathbb{R} denote the sets of nonnegative integers and real numbers, respectively. Let $\mathfrak{P}(\mathcal{X})$ denote the power set of a set \mathcal{X} . The probability space considered in this paper is denoted by $(\Omega, \mathfrak{F}, \text{Prob})$. We use upper case letters for random variables and lower case letters for their realizations. The expected value of X is denoted by $\mathbb{E}[X]$. For a random variable $X : \Omega \rightarrow \mathcal{X}$, we use $X \in \mathcal{X}$ for representing its codomain. For discrete random variables X and Y , let $p(x)$ and $p(y|x)$ denote the probability mass function of X and the conditional probability mass function of Y given $X = x$, respectively. Similarly, $\mathbb{E}[Y|x]$ denotes the conditional expected value of Y given $X = x$. Let $x_{0:k}$ denote a tuple (x_0, \dots, x_k) of the sequence x_0, \dots, x_k .

II. CONTROL SYSTEM WITH COVERT REACTION

A. Motivating Example

Consider the networked system shown in Fig. 1. The upstream process and the downstream process are interconnected through a network over an overt channel. The overt channel is possibly under man-in-the-middle attack where the adversary can receive and alter the signal on the channel. To cope with the attack, the system operator equips a redundant secure channel, called covert channel [27], through which secret information can be transferred being unrecognized by other third parties. A covert channel is typically regarded as a vulnerability of communication [28] but can proactively be used for enhancing reliability [29]. Although the subsystems can securely communicate through the covert channel, the overt channel is preferable to use if no attacks are executed since communication over the covert channel requires an unusual protocol and would cause a high cost or performance degradation. Moreover, the operator utilizes the model-based anomaly detection scheme [30] with which the defender can observe the residual obtained as the difference between the actual signal through the overt channel and the ideal signal calculated through a model of the system. Basically, the residual is not always zero owing to noise but is small without attacks and hence large residual encourages the operator to use the covert channel. The objective of the operator is to achieve an efficient operation by properly choosing the channel used for the communication at each time step based on the measured residual. Conversely, the objective of the adversary is to disturb the downstream process by choosing proper signals on the overt channel.

We now explain the idea of "covert reaction" with this example. Let us suppose that no data is transferred through the overt channel when the covert channel is used. Then the

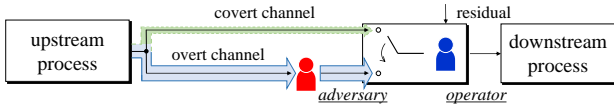


Fig. 1. Example: A networked system with an overt channel under man-in-the-middle attack and a secure covert channel that would cause a costly communication or performance degradation.

adversary can recognize the channel used for each communication, which corresponds to the case of *overt reaction*. If usage of the overt channel is observed, which indicates that presence of the attacker is not suspected, then large disturbance can be injected. If no data through the over channel is observed, the attacker tries to lurk by stopping injection of attacks. Hence, in the case of overt reaction, the adversary can choose a reasonable action according to the observed scenario. A possible approach that inhibits this strategy is to transfer data through both the channels when the covert channel is used for actual communication. Then, because the overt channel is used in both cases, the true scenario cannot be identified from the attacker's perspective, which corresponds to the case of *covert reaction*. Thus, in the case of covert reaction, the adversary has to take an alternative strategy, under which the damage on the system would be less harmful. From this discussion, we expect that covert reaction can enhance resilience of control systems.

This example motivates us to thoroughly analyze resilience of control systems with covert reaction. In the next subsection, we provide a model of the control system to be defended for mathematical analysis.

B. System Description

Consider a control system being possibly under attack shown in Fig. 2. Let $U_k \in \mathcal{U}$ and $X_k \in \mathcal{X}$ denote the input signal and the state of the system at the time step $k \in \mathbb{Z}_+$, respectively. The input signals are assumed to be mutually independent, i.e., U_i and U_j are independent for any $i, j \in \mathbb{Z}_+$. There is a party, called a *sender*, who can alter the behavior of the system through an *action* $a_k \in \mathcal{A}$. Let $\theta \in \Theta = \{\theta_b, \theta_m\}$ denote the *type* of the sender, where the symbols θ_b and θ_m imply that the sender is benign or malicious, respectively. The case $\theta = \theta_b$ corresponds to the control system under normal operation where effects of the action a_k can be ignored, e.g., $a_k = 0$ if \mathcal{A} is the Euclidean space. We denote the map of the system by $\Sigma_k : \mathcal{U}^{k+1} \times \mathcal{A} \rightarrow \mathcal{X}$. Then the k th state is determined according to the relationship $x_k = \Sigma_k(u_{0:k}, a_k)$ with given input signals and an action where effects of the initial value of the state are ignored because the analysis in this paper is independent of the initial value. Note that we assume that the state is affected only by the instantaneous action. This property is favorable to the attacker in terms of avoidance of detection because there are no lingering effects of an attack. In this sense, we consider a severe situation for defending the control system.

To detect the existence of a malicious sender and cope with potentially malicious actions, we consider a commonly

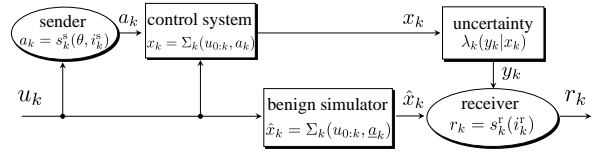


Fig. 2. Signal-flow diagram of the system under potentially malicious actions and the defense architecture for detection and reaction.

used detection and reaction architecture shown in Fig. 2. The basic idea of the defense mechanism is to compare the actual signal and the ideal signal under the normal operation and to perform a proper reaction based on the result of the detection process. Let $Y_k \in \mathcal{Y}$ denote the measurement output which is obtained through an uncertain environment, e.g., noisy measurement and modeling error. The characteristic of the uncertainty is modeled by a memoryless channel $\lambda_k(y_k|x_k) := p(y_k|x_k) = p(y_k|x_{0:k})$. The memoryless property is also favorable to the attacker for the same reason as the one of the control system. Let $\hat{X}_k \in \mathcal{X}$ denote the ideal state at the k th step under the benign operation generated through the benign simulator $\hat{x}_k = \Sigma_k(u_{0:k}, \underline{a}_k)$ where \underline{a}_k is the action that is performed if the sender is benign. Note that \underline{a}_k is known to the players owing to Assumption 3 shown below. Based on the measurement, the other party, called a *receiver*, chooses an action $r_k \in \mathcal{R}$ at each time step. We henceforth refer to r_k as a *reaction* for emphasizing that r_k denotes a counteraction against potentially malicious attacks.

For avoiding trivial discussions, we make an assumption that guarantees validity of the defense architecture.

Assumption 1 (Valid Defense Architecture) The defense architecture is valid, i.e.,

- 1) For any $u_{0:k}$, if $x_k = \hat{x}_k$ then $a_k = \underline{a}_k$.
- 2) Let $I(X_k; Y_k)$ denote the mutual information of X_k and Y_k [31]. Then $\inf_{k \in \mathbb{Z}_+} I(X_k; Y_k) > 0$ holds.

The first assumption means that the system is input observable [32], i.e., any malicious attack is immediately noticeable if there is no uncertainty in the measurement process. Owing to this assumption, we disregard attacks that are impossible to detect even with the most powerful detection tool, such as covert attacks [33] and zero-dynamics attacks [34]. The second assumption simply states that the measurement signal has nonzero information on the state, which means that the channel is valid for attack detection including the limit.

Moreover, for simplicity, the following technical assumption is made.

Assumption 2 (Discrete Variables) The sets of signals and actions, namely, $\mathcal{U}, \mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{R}$ are finite sets.

Assumption 2 makes all random variables discrete. Then it suffices to consider only probability mass functions.

C. Game Description

Based on the system description, we provide each player's decision policy about her actions through a repeated game

formulation. For the formulation, the notions of *strategy*, *utility*, *belief*, and *best response* are needed.

The sender chooses an action at each time step based on the type and available information. Let $s_k^s \in \mathcal{S}_k^s$ denote the *strategy* of the sender at the k th step. Suppose that the sender uses *pure strategies*. Then the space of the k th sender's strategies is given by $\mathcal{S}_k^s = \{s_k^s : \Theta \times \mathcal{I}_k^s \rightarrow \mathcal{A}\}$ where \mathcal{I}_k^s denotes the set of the k th sender's available information, which consists of signals measured by the sender at the k th step. The elements of \mathcal{I}_k^s , referred to as information sets in game theory, are explicitly determined in the next subsection (see Assumption 4). Similarly, let $s_k^r \in \mathcal{S}_k^r$ denote the strategy of the receiver at the k th step. The receiver uses pure strategies as well and then the space of the k th receiver's strategies is given by $\mathcal{S}_k^r = \{s_k^r : \mathcal{I}_k^r \rightarrow \mathcal{R}\}$ where \mathcal{I}_k^r denotes the set of the k th receiver's available information.

Utilities are employed for representing players' preferences. Let $\mathbf{U}_k^s : \Theta \times \mathcal{X} \times \mathcal{A} \times \mathcal{R} \rightarrow \mathbb{R}$ denote an immediate utility function for the sender such that $\mathbf{U}_k^s(\theta, x_k, a_k, r_k)$ gives the utility that she receives when her type is θ , the sender plays the action a_k , and the receiver chooses the reaction r_k . Similarly, let $\mathbf{U}_k^r : \Theta \times \mathcal{X} \times \mathcal{A} \times \mathcal{R} \rightarrow \mathbb{R}$ denote the receiver's utility function such that $\mathbf{U}_k^r(\theta, x_k, a_k, r_k)$ gives her payoff under the same scenario.

As a preparation for analysis, we put an assumption on preferences of the benign sender. We suppose that the system is optimally controlled without any specific actions of the sender and then actions plays the role only to disturb the system. Since the benign sender has no motivation to disturb the system, doing nothing becomes the optimal action. The following assumption is made.

Assumption 3 (Benign Sender's Preference) There exists $a_b \in \mathcal{A}$ such that $\mathbf{U}_k^s(\theta_b, x_b, a_b, r) > \mathbf{U}_k^s(\theta_b, x, a, r')$ where $x_b := \sum_k(u_{0:k}, a_b)$ and $x := \sum_k(u_{0:k}, a)$ for any $a \in \mathcal{A} \setminus \{a_b\}$, $u_{0:k} \in \mathcal{U}^{k+1}$, $r, r' \in \mathcal{R}$, $k \in \mathbb{Z}_+$.

In Assumption 3, the benign action a_b means that the sender does not perform any particular active operations. We do not put any assumptions on the utilities of the malicious sender and the receiver at this moment. Instead, we make an alternative assumption that dominates their preferences in the next section (see Assumption 5 in Section III).

When some variables of the utilities are unavailable to the players, *expected utilities* are used for choosing a reasonable strategy instead of the utility itself. Let $\bar{\mathbf{U}}_k^s : \Theta \times \mathcal{A} \times \mathcal{I}_k^s \times \mathcal{S}_k^r \rightarrow \mathbb{R}$ denote the sender's expected utility at the k th step under a fixed sender's strategy with a realization of her available information for a given receiver's strategy such that $\bar{\mathbf{U}}_k^s(\theta, a_k, i_k^s, s_k^r) := \mathbb{E}[\mathbf{U}_k^s(\theta, X_k, a_k, s_k^r(I_k^r)) | i_k^s]$.

Similarly, we define the receiver's expected utility. However, since θ is not a random variable, the expected value cannot be taken in the normal sense. Thus, the receiver prepares a *belief* $\pi_k \in \Pi$ such that $\pi_k : \Theta \rightarrow (0, 1)$ represents the possibility of the type of the sender for each time step from the viewpoint of the receiver. Let $\bar{\mathbf{U}}_k^r : \mathcal{R} \times \mathcal{I}_k^r \times \mathcal{S}_k^s \times \Pi \times \mathcal{S}_{0:k}^s \rightarrow \mathbb{R}$ denote the receiver's

expected utility at the k th step under the belief such that $\bar{\mathbf{U}}_k^r(r_k, i_k^r, s_k^s, \pi_k, \sigma_{0:k}^s) := \mathbb{E}[\mathbf{U}_k^r(\theta_k, X_k, s_k^s(\theta_k, I_k^s), r_k) | i_k^r]$ where $\theta_k \in \Theta$ is a random variable obeying the probability distribution obtained by the belief π_{k+1} in (1), shown below, and $\sigma_{0:k}^s \in \mathcal{S}_{0:k}^s$ is a profile of sender's strategies used for calculation of π_{k+1} . Note that we use the symbol $\sigma_{0:k}^s$ instead of $s_{0:k}^s$ for emphasizing that the strategies $\sigma_{0:k}^s$ are not the strategies that are actually chosen by the sender but the estimated strategies from the perspective of the receiver.

The receiver updates her belief based on her observation as the time proceeds according to Bayes' rule, which is given by $\text{Prob}(\mathcal{E}_1 | \mathcal{E}_2) = \text{Prob}(\mathcal{E}_1 \cap \mathcal{E}_2) / \text{Prob}(\mathcal{E}_2) = \text{Prob}(\mathcal{E}_2 | \mathcal{E}_1) \text{Prob}(\mathcal{E}_1) / \text{Prob}(\mathcal{E}_2)$ for two events \mathcal{E}_1 and \mathcal{E}_2 . The dynamics of the belief obeys

$$\pi_{k+1} = f(\pi_k, i_k^r, \sigma_{0:k}^s) \quad (1)$$

with an initial belief $\pi_0 \in \Pi$ such that $\pi_0(\theta_b) + \pi_0(\theta_m) = 1$ and $\pi_0(\theta_b), \pi_0(\theta_m) \in (0, 1)$ where $f : \Pi \times \mathcal{I}_k^r \times \mathcal{S}_{0:k}^s \rightarrow \Pi$ represents Bayes' rule under a given sender's strategy given by

$$f(\pi, i_k^r, \sigma_{0:k}^s)(\theta) := \frac{p_{\sigma_{0:k}^s}(i_k^r | \theta) \pi(\theta)}{\sum_{\theta' \in \Theta} p_{\sigma_{0:k}^s}(i_k^r | \theta') \pi(\theta')} \quad (2)$$

where $\sigma_{0:k}^s \in \mathcal{S}_{0:k}^s$ represents a profile of estimated sender's strategies used for calculating the posterior belief and $p_{\sigma_{0:k}^s}(\cdot)$ represents the corresponding probability under $A_i = \mathcal{S}_i^s(\theta, I_i^s)$ for $i = 0, \dots, k$.

A reasonable choice of each player's strategies is given by a *best response* provided that the opponent's strategy is given. A sender's strategy s_k^s is said to be a best response for a given receiver's strategy s_k^r under the type θ when s_k^s satisfies the condition $s_k^s(\theta, i_k^s) \in \arg \max_{a_k \in \mathcal{A}} \bar{\mathbf{U}}_k^s(\theta, a_k, i_k^s, s_k^r)$ for any $i_k^s \in \mathcal{I}_k^s$, where it is supposed that the best response depends only on the immediate utility for simplicity. To ease notation, we let $\text{BR}_k^s : \Theta \times \mathcal{S}_k^r \rightarrow \mathfrak{P}(\mathcal{S}_k^s)$ denote the set-valued function of all sender's best responses for a given receiver's strategy. Similarly, a receiver's strategy s_k^r is said to be a best response for a given s_k^s with the estimated sender's strategies $\sigma_{0:k}^s$ under the belief π_k when s_k^r satisfies the condition $s_k^r(i_k^r) \in \arg \max_{r_k \in \mathcal{R}} \bar{\mathbf{U}}_k^r(r_k, i_k^r, s_k^s, \pi_k, \sigma_{0:k}^s)$ for any $i_k^r \in \mathcal{I}_k^r$. Let $\text{BR}_k^r : \mathcal{S}_k^s \times \Pi \times \mathcal{S}_{0:k}^s \rightarrow \mathfrak{P}(\mathcal{S}_k^r)$ denote the set-valued function of all receiver's best responses.

Finally, all models of the game and the initial belief are assumed to be known to both players.

Basically, the players choose their own strategies along the path generated by the best response. The best response of the malicious sender is influenced by the receiver's belief through the receiver's strategy. Thus the malicious sender is allowed to execute aggressive actions when she recognizes that the belief $\pi_k(\theta_m)$ is small. This discussion leads us to the expectation that, the more information on the belief is leaked, the more serious the damage caused by the attack is, and vice versa. From this perspective, we analyze the behaviors of the players under *covert reactions* formulated in the subsequent subsection.

D. Best Response Strategies under Undisclosed Belief

Consider the case where the receiver successfully conceals information on the belief from the sender, namely, the case of covert reaction. The following assumption is made.

Assumption 4 (Covert Reaction) The available information of the sender at the k th step is given by $i_k^s = \{u_{0:k}, a_{0:k-1}\}$. The available information of the receiver is given by $i_k^r = \{u_{0:k}, \hat{x}_{0:k}, y_{0:k}, r_{0:k-1}\}$.

Note that i_k^s does not include $y_{0:k}$ and $r_{0:k-1}$. If $r_{0:k-1}$ is available to the sender, the region of the belief can be computed and hence $r_{0:k-1}$ should be covert. Further, since \hat{x}_k can be computed from $u_{0:k}$, for keeping the belief undisclosed the receiver necessarily conceals $y_{0:k}$, with which the transition of the belief can completely be calculated.

One difficulty for the analysis of the game under Assumption 4 is that a commonly used equilibrium concept, such as perfect Bayesian Nash equilibrium, cannot be employed because the players are unable to compute the equilibria for deciding reasonable actions. To handle this situation, we introduce a novel framework in the following discussion.

From the perspective of the sender, one approach for choosing a reasonable strategy without the exact value of the belief is to estimate the belief only with available information. We suppose that the sender uses the conditional expected value given a sender's strategy and the available information as an estimation of the belief. Let $\hat{\pi}_k \in \Pi$ denote the estimated belief given by $\hat{\pi}_{k+1} = \text{EX}_k^\pi(\theta, s_{0:k}^s, i_k^s, s_{0:k}^r, \sigma_{0:k}^s)$ with $\text{EX}_k^\pi : \Theta \times \mathcal{S}_{0:k}^s \times \mathcal{I}_k^s \times \mathcal{S}_{0:k}^r \times \mathcal{S}_{0:k}^s \rightarrow \Pi$ defined by $\text{EX}_k^\pi(\theta, s_{0:k}^s, i_k^s, s_{0:k}^r, \sigma_{0:k}^s)(\theta') := \mathbb{E}[\pi_{k+1}(\theta') | \theta, s_{0:k}^s, i_k^s, s_{0:k}^r, \sigma_{0:k}^s]$ where $\sigma_{0:k}^s$ is the estimated sender's strategy profile from the receiver's side used for the Bayesian inference (2). With the estimation, the sender can choose s_k^{s*} according to

$$\begin{cases} s_k^{s*} \in \text{BR}_k^s(\theta, s_k^{r*}) \\ s_k^{r*} \in \text{BR}_k^r(s_k^{s*}, \hat{\pi}_k, \sigma_{0:k}^s) \\ \hat{\pi}_k = \text{EX}_{k-1}^\pi(\theta, s_{0:k-1}^s, i_{k-1}^s, s_{0:k-1}^{r*}, \sigma_{0:k-1}^s) \end{cases} \quad (3)$$

provided that $\sigma_{0:k}^s$ is known.

Since the exact values of $\sigma_{0:k}^s$ are private information of the receiver, however, the sender has to estimate the estimated sender's strategies to obtain a reasonable strategy as well. Let $\hat{\sigma}_{0:k}^s$ denote the estimation of the estimated strategies $\sigma_{0:k}^s$. Because sender's strategies must be chosen to be reasonable, the conditions

$$\begin{cases} \hat{\sigma}_i^s \in \text{BR}_i^s(\theta, \hat{\sigma}_i^r) \\ \hat{\sigma}_i^r \in \text{BR}_i^r(\hat{\sigma}_i^s, \hat{\pi}_i, \hat{\sigma}_{0:i}^s) \\ \hat{\pi}_i = \text{EX}_{i-1}^\pi(\theta, \hat{\sigma}_{i-1}^s, i_{i-1}^s, \hat{\sigma}_{0:i-1}^r, \hat{\sigma}_{0:i-1}^s) \end{cases}$$

for any $i = 0, \dots, k$ are expected to hold under another estimated sender's strategy $\hat{\sigma}_{0:k}^s$. Likewise, further estimations are required over and over and the same procedure is performed infinitely many times.

In this paper, we suppose that the sender uses the true strategies $s_{0:k}^s$ as the estimated strategies $\sigma_{0:k}^s$ for truncating

the infinite chain of estimations. Then we can define reasonable sender's strategies based on best responses as follows.

Definition 1 (Best Response Strategy) A sender's strategy profile $\{s_k^s\}_{k \in \mathbb{Z}_+}$ is said to be a sender's best response strategy profile when there exists $\{s_k^r\}_{k \in \mathbb{Z}_+}$ such that

$$\begin{cases} s_k^s \in \text{BR}_k^s(\theta, s_k^r) \\ s_k^r \in \text{BR}_k^r(s_k^s, \hat{\pi}_k, s_{0:k}^s) \\ \hat{\pi}_k = \text{EX}_{k-1}^\pi(\theta, s_{0:k-1}^s, i_{k-1}^s, s_{0:k-1}^r, s_{0:k-1}^s) \end{cases}$$

holds for any $k \in \mathbb{Z}_+$, $\theta \in \Theta$, $i_{k-1}^s \in \mathcal{I}_{k-1}^s$.

Definition 1 is obtained by simply substituting $s_{0:k}^s$ to $\sigma_{0:k}^s$ in (3). Note that, although we can define receiver's best response strategies in a similar way, we do not explicitly state the definition because it is unnecessary for our analysis.

The main objective of this study is to investigate the benefit induced by the confidentiality of the reactions on the resilience of the control systems. More precisely, we aim at analyzing the reasonable behavior of the malicious sender under covert reactions. Based on the preparation, we mathematically analyze sender's best response strategies in the next section.

III. ANALYSIS: ASYMPTOTIC SECURITY

In this section, we reveal that the control system can be guaranteed to be secure in an asymptotic manner through covert reaction, which results in *asymptotic security*.

A. Definition of Asymptotic Security

First of all, we claim that the benign sender always chooses a_b under any best response strategies at any time.

Proposition 1 (Benign Sender's Strategy) Under Assumption 3, any sender's best response strategy profile satisfies $s_k^s(\theta_b, I_k^s) = a_b$ almost surely for any $k \in \mathbb{Z}_+$.

Proof: Assumption 3 directly leads to the claim. \square

To clearly state the resilience achieved through covert reaction, we define a notion of security as follows.

Definition 2 (Asymptotic Security) The control system is said to be *asymptotically secure* when any sender's best response strategy profile satisfies $s_k^s(\theta_m, I_k^s) \rightarrow a_b$ almost surely as $k \rightarrow \infty$.

Definition 2 means that the reasonable strategy of the malicious sender converges to the benign one regardless of her available information. Note that in Definition 2 the limit in \mathcal{A} is taken in the following sense: A sequence of actions $a_k \in \mathcal{A}$ for $k \in \mathbb{Z}_+$ converges to $a \in \mathcal{A}$ when there exists $N \in \mathbb{Z}_+$ such that $a_k = a$ for any $k > N$, which is obtained by giving the discrete topology [35] on \mathcal{A} .

B. Asymptotic Security by Covert Reaction

While the preference of the benign sender is determined in Assumption 3, we have made no assumptions on preferences of the malicious sender and the receiver. We here make a reasonable assumption that should be satisfied by sender's best response strategies instead of making an assumption on their utilities themselves.

Assumption 5 (Players' Preference) Any sender's best response strategy profile satisfies $\text{Prob}(\mathcal{E}_{\{s_k^s\}}) = 1$ where

$$\mathcal{E}_{\{s_k^s\}} := \left\{ \omega : \limsup_{k \in \mathbb{Z}_+} \pi_{m,k}(\omega) < 1 \text{ under } \{s_k^s\} \right\},$$

which belongs to \mathfrak{F} , with $\pi_{m,k} := \pi_k(\theta_m)$.

Assumption 5 means that any possible belief does *not* approach one if the sender's strategy is given by best responses. In other words, rational malicious senders avoid the situation where the receiver has a firm belief on existence of the malicious sender. This assumption can be regarded as a replacement of an assumption on the utilities of the malicious sender and the receiver for determining their preferences. Although it is more desirable to derive the statement in Assumption 5 from an appropriate assumption on the utilities, we treat the claim as an assumption in this paper.

Based on the preparation, the following theorem, the main result of this paper, holds.

Theorem 1 (Asymptotic Security) Let Assumptions 1 to 5 hold. Then the control system is asymptotically secure.

Essentially, Theorem 1 is derived from the monotonicity of the estimated belief shown in the following lemma.

Lemma 1 (Monotonicity of Estimated Belief) Assume that $\{s_k^s\}_{k \in \mathbb{Z}_+}$ is a sender's best response strategy profile. Then under Assumptions 1 to 5

$$\hat{\pi}_{k+1}(\theta_m) \geq \hat{\pi}_k(\theta_m)$$

almost surely, where the equality holds if and only if $s_k^s(\theta_m, i_k^s) = a_b$.

For the proofs of Lemma 1 and Theorem 1, see Appendix.

Lemma 1 implies that the estimated belief on existence of a malicious sender does *not* decrease regardless of what strategy the malicious sender chooses at the k th step. Furthermore, the estimated belief is invariant only if she chooses the benign action, which is the most unsuspecting behavior. Because of the monotonicity of the estimated belief, strategies that can be chosen by the malicious sender are eventually restricted as the time proceeds. When the expected belief becomes sufficiently large, the possible strategy becomes the benign one alone, which is the claim of Theorem 1.

Theorem 1 implies that the control system is guaranteed to be secure in an asymptotic manner if the receiver's belief is kept to be undisclosed through covert reactions. The result clarifies the relationship between secrecy of the defender's

belief and the resilience of the control system to be defended. What should be emphasized here is that no particular assumptions are made on the structure of the control system and the sender's utility function except for Assumption 5, under which the sender avoids having the receiver have a firm belief on existence of a malicious attacker. In other words, the finding is irrelevant to the control system and the objective of the attacker. In this sense, the result implies that covertness of reactions is an essential requirement for enhancing resilience of control systems.

IV. NUMERICAL EXAMPLE

We confirm the validity of the theoretical results through a simple numerical example. Suppose that all sets of signals and actions are binary, i.e., $\mathcal{X} = \mathcal{Y} = \mathcal{U} = \mathcal{A} = \mathcal{R} = \{0, 1\}$. The input signals U_k are supposed to be independent and identically distributed with $\text{prob}(U_k = 0) = \text{prob}(U_k = 1) = 0.5$. The system is given by $\Sigma_k(u_{0:k}, 0) = u_k$ and $\Sigma_k(u_{0:k}, 1) = 1 - u_k$. The channel characteristic is given by $\lambda_k(0|0) = \lambda_k(1|1) = \lambda$ with a given $\lambda \in (0, 1) \setminus \{0.5\}$. The utility of the benign sender is given by $\mathbf{U}_k^s(\theta_b, x, 0, r) = 1$ and $\mathbf{U}_k^s(\theta_b, x, 1, r) = 0$. The other utilities are given by

$$\mathbf{U}_k^s(\theta_m, x, a, r) = \begin{cases} 3, & \text{if } a = 1, r = 0, \\ 2, & \text{if } a = 0, r = 0, \\ 1, & \text{if } a = 0, r = 1, \\ 0, & \text{if } a = 1, r = 1, \\ 1, & \text{if } \theta = \theta_b, r = 0, \\ \alpha, & \text{if } \theta = \theta_m, r = 1, \\ 0, & \text{otherwise,} \end{cases}$$

where α is determined such that $\alpha\bar{\pi} = 1 - \bar{\pi}$ with a given $\bar{\pi} \in (0, 1)$. The numbers 0 and 1 mean a nonaggressive action and an aggressive action, respectively. The utility functions infer that the malicious sender prefers the aggressive action and the nonaggressive action when the receiver chooses the nonaggressive action and the aggressive action, respectively, and the receiver chooses the aggressive reaction when the sender is doubtful. Specifically, the malicious sender's best responses are given by $a = 0$ if $r = 1$ and $a = 1$ if $r = 0$. The receiver's best response is given by $r = 1$ when $\pi_k(\theta_m) \geq \bar{\pi}$ and otherwise $r = 0$.

In Fig. 3, the curves represent the malicious sender's estimated belief, two sample paths of the receiver's exact belief, and the empirical mean of the exact belief obtained under twenty trials where the broken line represents the boundary $\bar{\pi}$. The curves are obtained under $\lambda = 0.55$ and $\bar{\pi} = 0.85$ with the initial belief $\pi_0(\theta_m) = 0.15$. Because the sample path of $\hat{\pi}_k(\theta_m)$ is independent of the elementary event under this setting, only the unique path is drawn. The receiver's belief in the result is calculated with the true sender's best response. As observed in the figure, the curve of the estimated belief $\hat{\pi}_k(\theta_m)$ monotonically increases as the time proceeds in contrast to the exact beliefs $\pi_k^{(1)}(\theta_m)$ and $\pi_k^{(2)}(\theta_m)$. When the estimated belief exceeds $\bar{\pi}$, the malicious sender's best response becomes the benign one and subsequently the estimated belief is kept to be invariant. Moreover, it can be confirmed that the analytic mean $\hat{\pi}(\theta_m)$

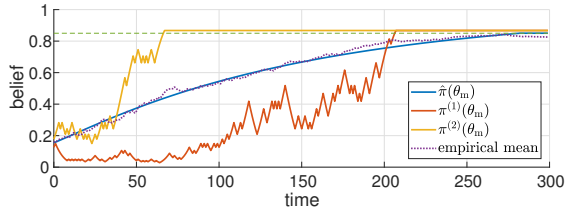


Fig. 3. The time sequence of the sender's estimated belief $\hat{\pi}_k(\theta_m)$, two sample paths of the exact receiver's belief $\pi(\theta_m)$, and the empirical mean.

is close with the empirical mean, represented by the dotted line. The result numerically indicates the asymptotic security of the control system guaranteed in the theoretical findings.

V. CONCLUSION

In this paper, we have considered a defense mechanism for resilient control systems with reactions. The behaviors of a malicious attacker and the defender have been analyzed through a repeated signaling game. It has theoretically been discovered that asymptotic security is achieved by covert reaction. The result indicates the importance of covertness of reactions for enhancing resilience of control systems.

One important future research direction is to consider cumulative utilities and strategies with memory instead of the immediate utilities used for deciding the players' best responses. In the current setting, because the sender does not care about future transition of receiver's belief, the malicious sender tends to choose an aggressive action even if it leads to a rapid rise of the belief, which could be unreasonable in practical situations. Another direction is to consider the case where there is a feedback from the reaction to the system state. It is expected that the same results hold if we can make the effects secret to the sender by utilizing the internal structure of the control system. Moreover, analyzing "transient security" in the proposed framework is an open problem. The difficulty arises from computational complexity of best responses for general control systems. Finally, this paper is built on the premise that the sender uses her own strategy as the strategy estimated by the receiver for truncating the infinite chain of estimations. Analysis of the case where multiple estimations are used for determining reasonable strategies is included in future work.

APPENDIX

Proof of Lemma 1

Fix an elementary event and consider corresponding realizations. All probabilities in the proof are taken with $A_k = s_k^s(\theta_m, I_k^s)$. Since $\{s_k^s\}$ is a sender's best response strategy profile, with $\sigma_{0:k}^s = s_{0:k}^s$ we have $\hat{\pi}_{k+1}(\theta_m) = \sum_{i_k^r \in \mathcal{I}_k^r} f(\pi_k, i_k^r, s_{0:k}^s)(\theta_m) p(i_k^r | \theta_m, i_k^s)$. Since $p(i_k^r | i_{k-1}^r) = 0$ if $i_{k-1}^r \notin i_k^r$, we have

$$\begin{aligned} p(i_k^r | \theta_m, i_k^s) &= \sum_{i_{k-1}^r \in \mathcal{I}_{k-1}^r} p(i_k^r | \theta_m, i_k^s, i_{k-1}^r) p(i_{k-1}^r | \theta_m, i_k^s) \\ &= p(i_k^r | \theta_m, i_k^s, i_{k-1}^r) p(i_{k-1}^r | \theta_m, i_k^s) \end{aligned}$$

where $i_{k-1}^r \subset i_k^r$. Because $\{U_k\}_{k \in \mathbb{Z}_+}$ are mutually independent and a_{k-1} is uniquely determined from i_{k-1}^s with the given sender's strategy profile, it turns out that $p(i_{k-1}^r | \theta_m, i_k^s) = p(i_{k-1}^r | \theta_m, i_{k-1}^s, u_k, a_{k-1}) = p(i_{k-1}^r | \theta_m, i_{k-1}^s)$, which yields

$$\begin{aligned} \hat{\pi}_{k+1}(\theta_m) &= \sum_{i_k^r \in \mathcal{I}_k^r} \frac{p(i_k^r | \theta_m, i_{k-1}^r) \pi_k(\theta_m)}{\sum_{\theta' \in \Theta} p(i_k^r | \theta', i_{k-1}^r) \pi_k(\theta')} \\ &\quad \cdot p(i_k^r | \theta_m, i_k^s, i_{k-1}^r) p(i_{k-1}^r | \theta_m, i_{k-1}^s). \end{aligned}$$

We will reduce the index variable of the summation. Because the control system is a deterministic system, \hat{x}_k is uniquely determined once $u_{0:k}$ is fixed. Hence, from Assumption 4, if $u_k, \hat{x}_k \notin i_k^r$ for $u_k \in i_k^s$ and $\hat{x}_k = \Sigma_k(u_{0:k}, a_b)$, then $p(i_k^r | \theta, i_k^s, i_{k-1}^r) = 0$. Thus we have

$$\begin{aligned} \hat{\pi}_{k+1}(\theta_m) &= \sum_{y_k \in \mathcal{Y}} \sum_{i_{k-1}^r \in \mathcal{I}_{k-1}^r} \frac{p(y_k | \theta_m, i_{k-1}^r, u_k, \hat{x}_k) \pi_k(\theta_m)}{\sum_{\theta' \in \Theta} p(y_k | \theta', i_{k-1}^r, u_k, \hat{x}_k) \pi_k(\theta')} \\ &\quad \cdot p(y_k | \theta_m, i_k^s, i_{k-1}^r) p(i_{k-1}^r | \theta_m, i_{k-1}^s). \end{aligned}$$

Since the estimated state \hat{x}_k is uniquely determined from i_{k-1}^r , we have $p(y_k | \theta_m, i_{k-1}^r, u_k, \hat{x}_k) = p(y_k | \theta_m, i_k^s, i_{k-1}^r)$, which we denote by $p_m(y_k, i_{k-1}^r)$. With the similar notation $p_b(y_k, i_{k-1}^r) := p(y_k | \theta_b, i_k^s, i_{k-1}^r)$, we have

$$\begin{aligned} \hat{\pi}_{k+1}(\theta_m) &= \sum_{y_k \in \mathcal{Y}} \sum_{i_{k-1}^r \in \mathcal{I}_{k-1}^r} \frac{p_m(y_k, i) \pi_k(\theta_m) p(i | \theta_m, i_{k-1}^s)}{p_b(y_k, i) \pi_k(\theta_b) + p_m(y_k, i) \pi_k(\theta_m)} \end{aligned}$$

where i is used instead of i_{k-1}^r for simplifying the expression. The equation can be rewritten as

$$\hat{\pi}_{k+1}(\theta_m) = \sum_{i \in \mathcal{I}_{k-1}^r} G_k(i) \pi_k(\theta_m) p(i | \theta_m, i_{k-1}^s) \quad (4)$$

where $G_k(i) := \sum_{y \in \mathcal{Y}} \frac{p_m(y_k, i)^2}{p_b(y_k, i) \pi_k(\theta_b) + p_m(y_k, i) \pi_k(\theta_m)}$.

We investigate the exact lower bound of $G_k(i)$ for a fixed i . Omitting the notation i and k , we let $m_y := p_m(y_k, i)$ and $b_y := p_b(y_k, i)$, which satisfy $\sum_{y \in \mathcal{Y}} m_y = \sum_{y \in \mathcal{Y}} b_y = 1$. Define $g(\alpha, m, b) := \sum_{y \in \mathcal{Y}} \frac{m_y^2}{\alpha m_y + (1-\alpha)b_y}$ where m and b contain all m_y and b_y , respectively, and $\alpha \in (0, 1)$. Since

$$\frac{m_y^2}{\alpha m_y + (1-\alpha)b_y} = \frac{m_y}{\alpha} - \frac{1-\alpha}{\alpha} \cdot \frac{m_y b_y}{\alpha m_y + (1-\alpha)b_y},$$

we have

$$g(\alpha, m, b) = \frac{1}{\alpha} \sum_{y \in \mathcal{Y}} m_y - \frac{1-\alpha}{\alpha} \cdot \underbrace{\sum_{y \in \mathcal{Y}} \frac{m_y b_y}{\alpha m_y + (1-\alpha)b_y}}_{=: h(\alpha, m, b)}.$$

From the weighted arithmetic mean–geometric mean inequality, it turns out that

$$\begin{aligned} h(\alpha, m, b) &\leq \sum_{y \in \mathcal{Y}} \frac{m_y b_y}{m_y^{\alpha} b_y^{1-\alpha}} = \sum_{y \in \mathcal{Y}} m_y^{1-\alpha} b_y^{\alpha} \\ &\leq \sum_{y \in \mathcal{Y}} \{(1-\alpha)m_y + \alpha b_y\} = 1. \end{aligned}$$

By using this inequality, we have $g(\alpha, m, b) \geq \frac{1}{\alpha} \sum_{y \in \mathcal{Y}} m_y - \frac{1-\alpha}{\alpha} = 1$. Since $G_k(i) = g(\pi_k(\theta_b), m, b)$, we have $G_k(i) \geq 1$, where the equality holds if and only if $m_y = b_y$ for any $y \in \mathcal{Y}$.

From the lower bound of $G_k(i)$, we have $\hat{\pi}_{k+1}(\theta_m) \geq \sum_{i \in \mathcal{I}_{k-1}^r} \pi_k(\theta_m) p(i|\theta_m, i_{k-1}^s) = \hat{\pi}_k(\theta_m)$ where the equality holds if and only if $p(y_k|\theta_b, i_k^s, i_{k-1}^r) = p(y_k|\theta_m, i_k^s, i_{k-1}^r)$ for any $y_k \in \mathcal{Y}$, $i_{k-1}^r \in \mathcal{I}_{k-1}^r$. Since $p(y_k|\theta, i_k^s, i_{k-1}^r) = \lambda_k(y_k|\Sigma_k(u_{0:k}, s_k^s(\theta, i_k^s)))$, the positivity of the mutual information in Assumption 1 yields $\Sigma_k(u_{0:k}, s_k^s(\theta_b, i_k^s)) = \Sigma_k(u_{0:k}, s_k^s(\theta_m, i_k^s))$. Thus, from the input observability in Assumption 1, $s_k^s(\theta_b, i_k^s) = s_k^s(\theta_m, i_k^s)$. From Proposition 1, the claim holds. \square

Proof of Theorem 1

Fix an elementary event in $\mathcal{E}_{\{s_k^s\}}$ and consider corresponding realizations. Because $\{\hat{\pi}_k(\theta_m)\}_{k \in \mathbb{Z}_+}$ is bounded above, Lemma 1 implies that there exists $\hat{\pi}_m^* \in [0, 1]$ such that $\hat{\pi}_k(\theta_m) \rightarrow \hat{\pi}_m^*$ as $k \rightarrow \infty$.

We show that there exists $N \in \mathbb{Z}_+$ such that $\hat{\pi}_k(\theta_m)$ is identical for $k > N$ by contradiction. Assume that $\hat{\pi}_{k+1}(\theta_m) > \hat{\pi}_k(\theta_m)$ for any $k \in \mathbb{Z}_+$. Then for any $\epsilon > 0$ there exists $N \in \mathbb{Z}_+$ such that $\hat{\pi}_m^* - \epsilon < \hat{\pi}_k(\theta_m) < \hat{\pi}_m^*$ for any $k > N$. From the uniform boundedness of the mutual information in Assumption 1, $\limsup_{k \rightarrow \infty} \max_{y \in \mathcal{Y}, i \in \mathcal{I}_{k-1}^r} |p_m(y_k, i) - p_b(y_k, i)| > 0$. Because $G_k(i)$, defined in (4), is a continuous function with respect to $p_m(y_k, i)$ and $p_b(y_k, i)$ and $\hat{\pi}_m^* < 1$ from Assumption 5, we have $\limsup_{k \rightarrow \infty} \max_{i \in \mathcal{I}_{k-1}^r} G_k(i) > 1$. Then there exists $\epsilon > 0$ and $k \in \mathbb{Z}_+$ such that $\hat{\pi}_{k+1}(\theta_m) > \hat{\pi}_m^*$ holds when $\hat{\pi}_m^* - \epsilon < \hat{\pi}_k(\theta_m)$, which leads to a contradiction.

Therefore, there exists $N \in \mathbb{Z}_+$ such that $\hat{\pi}_k(\theta_m)$ is identical for $k > N$. Hence, from Lemma 1, $s_k^s(\theta_m, i_k^s) = a_b$ for $k > N$, which proves the claim. \square

REFERENCES

- [1] D. Kushner, "The real story of Stuxnet," *IEEE Spectrum*, vol. 50, no. 3, pp. 48–53, Mar. 2013.
- [2] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, 2016, [ONLINE] Available: <https://ics.sans.org/media/E-ISAC.SANS.Ukraine.DUC.5.pdf>.
- [3] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," 2015, [ONLINE] Available: <http://illmatix.com/Remote%20Car%20Hacking.pdf>.
- [4] D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Drone hack: Spoofing attacks demonstration on a civilian unmanned aerial vehicle," *GPS World*, vol. 23, no. 8, pp. 30–33, 2012.
- [5] A. Teixeira, K. C. Sou, H. Sandberg, and K. H. Johansson, "Secure control systems: A quantitative risk management approach," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 24–45, Feb 2015.
- [6] Y. Mo and B. Sinopoli, "On the performance degradation of cyber-physical systems under stealthy integrity attacks," *IEEE Trans. Autom. Control*, vol. 61, no. 9, pp. 2618–2624, Sep. 2016.
- [7] J. Milošević, T. Tanaka, H. Sandberg, and K. H. Johansson, "Analysis and mitigation of bias injection attacks against a Kalman filter," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 8393–8398, 2017, 20th IFAC World Congress.
- [8] C.-Z. Bai, F. Pasqualetti, and V. Gupta, "Data-injection attacks in stochastic control systems: Detectability and performance tradeoffs," *Automatica*, vol. 82, pp. 251–260, 2017.
- [9] D. Umsonst, H. Sandberg, and A. A. Cárdenas, "Security analysis of control system anomaly detectors," in *Proc. 2017 American Control Conference (ACC)*, May 2017, pp. 5500–5506.
- [10] E. Kung, S. Dey, and L. Shi, "The performance and limitations of ϵ -stealthy attacks on higher order systems," *IEEE Trans. Autom. Control*, vol. 62, no. 2, pp. 941–947, Feb. 2017.
- [11] Y. Chen, S. Kar, and J. M. F. Moura, "Optimal attack strategies subject to detection constraints against cyber-physical systems," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 3, pp. 1157–1168, Sep. 2018.
- [12] Z. Guo, D. Shi, K. H. Johansson, and L. Shi, "Worst-case stealthy innovation-based linear attack on remote state estimation," *Automatica*, vol. 89, pp. 117–124, 2018.
- [13] J. Milošević, H. Sandberg, and K. H. Johansson, "Estimating the impact of cyber-attack strategies for stochastic networked control systems," *IEEE Trans. Control Netw. Syst.*, 2019, early access.
- [14] A. Kaya, "Repeated signaling games," *Games and Economic Behavior*, vol. 66, no. 2, pp. 841–854, 2009.
- [15] V. P. Crawford and J. Sobel, "Strategic information transmission," *Econometrica*, vol. 50, no. 6, pp. 1431–1451, 1982.
- [16] D. M. Kreps and J. Sobel, "Chapter 25 signalling," in *Handbook of Game Theory with Economic Applications*. Elsevier, 1994, vol. 2, pp. 849–867.
- [17] A. Gupta, A. Nayyar, C. Langbort, and T. Başar, "Common information based Markov perfect equilibria for linear-Gaussian games with asymmetric information," *SIAM Journal on Control and Optimization*, vol. 52, no. 5, pp. 3228–3260, 2014.
- [18] A. Nayyar, A. Gupta, C. Langbort, and T. Başar, "Common information based Markov perfect equilibria for stochastic games with asymmetric information: Finite games," *IEEE Trans. Autom. Control*, vol. 59, no. 3, pp. 555–570, Mar. 2014.
- [19] D. Vasal, A. Sinha, and A. Anastasopoulos, "A systematic process for evaluating structured perfect Bayesian equilibria in dynamic games with asymmetric information," *IEEE Trans. Autom. Control*, vol. 64, no. 1, pp. 81–96, Jan. 2019.
- [20] N. Heydaribeni and A. Anastasopoulos, "Linear equilibria for dynamic LQG games with asymmetric information and dependent types," in *Proc. the IEEE 58th Annual Conference on Decision and Control (CDC)*, 2019, pp. 5971–5976.
- [21] J. Pawlick, E. Colbert, and Q. Zhu, "Modeling and analysis of leaky deception using signaling games with evidence," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 7, pp. 1871–1886, July 2019.
- [22] D. M. Kreps and R. Wilson, "Sequential equilibria," *Econometrica*, vol. 50, no. 4, pp. 863–894, 1982.
- [23] D. Fudenberg and J. Tirole, "Perfect Bayesian equilibrium and sequential equilibrium," *Journal of Economic Theory*, vol. 53, no. 2, pp. 236–260, 1991.
- [24] H. L. Cole and N. Kocherlakota, "Dynamic games with hidden actions and hidden states," *Journal of Economic Theory*, vol. 98, no. 1, pp. 114–126, 2001.
- [25] J. Mertens and S. Zamir, "Formulation of Bayesian analysis for games with incomplete information," *International Journal of Game Theory*, vol. 14, pp. 1–29, 1985.
- [26] T. Börgers, *An Introduction to the Theory of Mechanism Design*. Oxford University Press, 2005.
- [27] B. W. Lampson, "A note on the confinement problem," *Commun. ACM*, vol. 16, no. 10, pp. 613–615, 1973.
- [28] S. Zander, G. Armitage, and P. Branch, "A survey of covert channels and countermeasures in computer network protocols," *IEEE Commun. Surveys Tuts.*, vol. 9, no. 3, pp. 44–57, 2007.
- [29] J. Kaur, S. Wendzel, O. Eissa, J. Tonejc, and M. Meier, "Covert channel-internal control protocols: Attacks and defense," *Security and Communication Networks*, vol. 9, no. 15, pp. 2986–2997, 2016.
- [30] S. X. Ding, *Model-Based Fault Diagnosis Techniques Design Schemes, Algorithms and Tools*, 2nd ed., ser. Advances in Industrial Control. Springer, 2013.
- [31] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley-Interscience, 2006.
- [32] M. Hou and R. Patton, "Input observability and input reconstruction," *Automatica*, vol. 34, no. 6, pp. 789–794, 1998.
- [33] R. S. Smith, "Covert misappropriation of networked control systems: Presenting a feedback structure," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 82–92, Feb. 2015.
- [34] F. Pasqualetti, F. Dorfler, and F. Bullo, "Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 110–127, Feb. 2015.
- [35] J. Munkres, *Topology*, 2nd ed. Pearson, 2000.