2011 American Control Conference
on O'Farrell Street, San Francisco, CA, USA
June 29 - July 01, 2011

Stackelberg-game analysis of correlated attacks in cyber-physical systems

Minghui Zhu and Sonia Martínez

Abstract— **This paper studies a resilient control problem for discrete-time, linear time-invariant systems subject to state and input constraints. State measurements and control laws are transmitted over a communication network and could be corrupted by human adversaries. In particular, we consider a class of human adversaries, namely correlated jammers, who are modeled as rational decision makers and whose strategies are highly correlated to the control system operator. The coupled decision making process is modeled as a two-level receding-horizon dynamic Stackelberg (leader-follower) game. We propose a receding-horizon Stackelberg control law for the operator, and analyze the resulting performance and closed-loop stability of the system under correlated attacks. We observe that, with full information of his follower, the operator is still able to maintain regional stability of the control system.**

I. Introduction

The recent convergence of sensing, wireless communication, and computing technologies has boosted the emergence of modern control systems (also termed cyber-physical systems) where information networks are tightly coupled to physical processes and human intervention. Engineering examples include sensor-actuator networks, autonomous vehicles, and transportation systems. Such sophisticated systems create a wealth of new opportunities at the expense of increased complexity and system vulnerability. In particular, malicious attacks in the cyber world are a current practice and a major concern for the deployment of cyber-physical systems. Thus, the ability to analyze their consequences becomes of prime importance in order to enhance resilience of these new-generation control systems.

In this paper, we consider a single-loop remotely-controlled system, where the plant, together with a sensor and an actuator, and the system operator are spatially distributed and connected via a communication network. In particular, state measurements are communicated from the sensor to the system operator through the network; then, the generated control policies are transmitted to the actuator through the same network. This model is an abstraction of a variety of existing cyber-physical systems, including supervisory control and data acquisition (SCADA) networks in critical infrastructures (e.g., power systems and water management systems) and remotely piloted unmanned aerial vehicles (UAVs). We consider a class of cyber attacks, produced by correlated jammers, where state measurements and control laws are intentionally tampered with. This extends the approach taken in the literature of networked control systems, where measurement and actuation errors are modeled as identically and independently distributed random variables. The previous model is reasonable if errors are induced by communication channel noises. However, this model fails to capture the features of human adversaries and the introduction of deceptive information by them. With this in mind, we model jammers as decision makers endowed with two important features. The first one is that the decisions of jammers are made in a real-time and feedback fashion, being highly correlated with the operator. The second one is that jammers are rational so that they attempt to destabilize the control system and/or degrade its performance while aiming to save their own attacking cost.

Literature review. The first set of references relevant to the topic and approaches of this work can be found in the literature of information-technology network security. Here, (non-cooperative) game theory [5], [9] has been widely used as a quantitative framework to model the interconnection between malicious attackers and system administrators. In this way, a variety of learning algorithms have been developed to predict the behavior of attackers and assess system jeopardy; see the (survey) references [1], [10], [19] and citations therein. These works do not consider the system-theoretic issues associated with dynamic systems to be controlled.

On the other hand, the problem of control and estimation over unreliable communication channels has received considerable attention over the last decade [11]. Key issues include quantization [14], packet dropout [3], [17], delay [7], and sampling [15]. However, these papers do not examine the potential consequences of intentional and rational attacks.

More recent efforts aim to address jointly the problem of control design and system security. The main approach consists of adding a detection mechanism to the control strategy to determine the presence of an intruder. For example, the papers [16], [18] determine conditions under which consensus multi-agent systems can detect misbehaving agents. A different, but related effort is [4], where the authors study ways in which a SCADA water management system can remain stable or not under a class of switching attacks.

Contributions. We consider two correlated attackers tampering with the wireless sensor and communication network of a remotely-operated system: a measurement jammer and a control jammer. The two jammers and the operator are rational decision makers and the coupled decision making process is novelly modeled as a two-level, constrained, receding-horizon and dynamic Stackelberg game. We propose a receding-horizon Stackelberg control law which allows the operator to maintain situational awareness. We quantitatively investigate two cases: in one, both types of jammers are

The authors are with Department of Mechanical and Aerospace Engineering, University of California, San Diego, 9500 Gilman Dr, La Jolla CA, 92093, {mizhu, soniamd}@ucsd.edu This work is supported by the NSF CAREER Award CMS-0643673 and NSF IIS-0712746.

978-1-4577-0079-8/11/$26.00 ©2011 AACC

present; in the other one, the control jammer is the only attacker. For the first case, we determine conditions for which the closed-loop system is regionally practically stable and derive an upper bound on the average infinite-horizon closed-loop system performance. For the second case, the results are refined to guarantee the closed-loop, regional exponential stability of the system, and we find a bound on the infinite-horizon closed-loop system performance. Due to the space limitation, the technical proofs are omitted and provided in the extended version [20] of this paper.

Notations. The set of all eigenvalues of matrix M, the spectrum of M, is denoted by $\sigma(M)$, and $\lambda_{\text{max}}(M)$ (resp. $\lambda_{\text{min}}(M)$) stands for the maximum (resp. minimum) eigenvalue of M. Consider the shorthands $\|x\|_M^2 := x^T M x$ for the norm weighted by the matrix M and $\langle x, y\rangle_M = x^T M y$ for the inner product weighted by the matrix M. Recall that $\lambda_{\text{min}}(M)\|x\|^2 \leq \|x\|_M^2 \leq \lambda_{\text{max}}(M)\|x\|^2$. Finally, $\mathbf{u}(k,\tau)$ is used to denote a sequence of control laws from k to $k+\tau$; i.e., $\mathbf{u}(k,\tau) := [u(k|k), u(k+1|k), \cdots, u(k+N-1|k)]$. For a given horizon $N > 0$, and when it is clear from the context, we will use $\mathbf{u}(k) \equiv \mathbf{u}(k, N)$. The notations of $\mathbf{u}_{\text{vir}}(k,\tau)$ and $\mathbf{u}_{\text{vir}}(k)$ are defined in an analogous way.

II. Problem formulation

A. Architecture of the controlled system

Consider the following discrete-time LTI system:

$$x(k+1) = Ax(k) + Bu(k), \tag{1}$$

where $x(k) \in X \subseteq \mathbb{R}^n$ is the system state, and $u(k) \in U \subseteq \mathbb{R}^m$ is the system input; which are to remain in some constraint sets X and U for each time $k \geq 0$. The matrices $A \in \mathbb{R}^{n\times n}$ and $B \in \mathbb{R}^{n\times m}$ represent the state and the input matrix, respectively. We assume that the pair (A, B) is stabilizable. The quantities $\|x(k)\|_P^2$ and $\|u(k)\|_Q^2$ are running state and input costs, respectively, for some P and Q positive-definite and symmetric matrices.

In the network, there are a measurement jammer and a control jammer. More precisely, the communication channel between the sensor and the operator involves the operator, the sensor, and the jammers, and it is modeled as:

$$x_c(k) = x(k) + x_a(k), \tag{2}$$

where $x(k)$ is the system state sent from the sensor, $x_a(k)$ is the measurement jammer's signal, and $x_c(k)$ is the corrupted measurement received by the operator and the control jammer at time $k \geq 0$. The attacking cost associated with the measurement jammer is modeled by $\|x_a(k)\|_{Q_{\text{msr}}}^2$, where $Q_{\text{msr}} = Q_{\text{msr}}^T > 0$. Similarly, the communication channel between the operator and the actuator, involving the operator, the actuator and the control jammer, is modeled as:

$$u_c(k) = u(k) + u_a(k), \tag{3}$$

where $u(k)$ is the control command sent from the operator, $u_a(k)$ is the control jammer's signal, and $u_c(k)$ is the corrupted control law received by the actuator at time k. The attacking cost of the control jammer is modeled by $\|u_a(k)\|_{Q_{\text{cnt}}}^2$ with $Q_{\text{cnt}} = Q_{\text{cnt}}^T > 0$. With the signals of the jammers, system (1) becomes:

$$\begin{aligned} x(k+1) &= Ax(k) + Bu_c(k) \\ &= Ax(k) + Bu(x_c(k)) + Bu_a(k). \end{aligned} \tag{4}$$

We model the process of sequential decision making on $x_a(k)$, $u(k)$ and $u_a(k)$ as a finite-horizon two-level Stackelberg (or leader-follower) game. More precisely, the measurement jammer first declares his decision $x_c(k)$ before the operator and control jammer choosing their own actions, and enforces $x_c(k)$ on the other two decision makers. In this way, the operator and the control jammer are *followers* of the measurement jammer, and they are only aware of $x_c(k)$ without knowing $x(k)$. After observing $x_c(k)$, the operator then announces his decision on $u(k)$ to the control jammer. As a result, besides acting as a follower of the measurement jammer, the operator functions as a leader to the control jammer. Once he knows $x_c(k)$ and $u(k)$, the control jammer responds to his leaders by taking the action $u_a(k)$.

B. Models of decision makers

We now proceed to describe how each player in the game makes his decision in more detail. It is worth mentioning that A, B, P and Q are common information for all decision makers. **The control jammer** is assumed to be rational and has two partly conflicting objectives: on the one hand, he aims to steer the system state as far away from the origin as possible; on the other hand, he would like to reduce his attacking cost $\|u_a(k)\|_{Q_{\text{cnt}}}^2$. This translates into the quadratic program parameterized by $(x_c(k), u(k)) \in \mathbb{R}^n \times \mathbb{R}^m$:

$$\begin{aligned} &\max_{u_a(k)\in\mathbb{R}^m} \|x(k+1|k)\|_P^2 - \|u_a(k)\|_{Q_{\text{cnt}}}^2, \\ &\text{s.t.} \quad x(k+1|k) = Ax_c(k) + Bu(k) + Bu_a(k), \end{aligned}$$

where $x(k+1|k)$ is the state at time $k+1$ predicted by the control jammer at time k based on $x_c(k)$ and $u(k)$. We refer to this program as $\text{QP}_{\text{cnt}}(x_c(k), u(k))$. The set of solutions to $\text{QP}_{\text{cnt}}(x_c(k), u(k))$ is denoted as $\text{OR}_{\text{cnt}}(x(k), u(k))$, where $\text{OR}_{\text{cnt}} : \mathbb{R}^n \times \mathbb{R}^m \to 2^{\mathbb{R}^m}$ is referred to as the optimal response map of the control jammer.

The operator is at the middle level of the Stackelberg game, acting as the leader of the control jammer and simultaneously as the follower of the measurement jammer. Then the operator knows the map QP_{cnt} and the state $x_c(k)$, but he is unaware of the strategy of the measurement jammer. We denote the control law of the operator as the set-valued map $\text{OR}_{\text{op}} : X \to 2^{\mathbb{R}^m}$, which will be defined later.

The measurement jammer is located at the high level of the hierarchy and thus has full information, including the uncorrupted state $x(k)$ and the decision maps of his followers; i.e., OR_{cnt} and OR_{op}. The measurement jammer is endowed with two partly conflicting objectives as well: he seeks to destabilize the system and increase actuation costs by manipulating the measurements while avoiding a high attacking cost $\|x_a(k)\|_{Q_{\text{msr}}}^2$, for some $Q_{\text{msr}} = Q_{\text{msr}}^T > 0$.

This can be modeled by the following quadratic program $\mathrm{QP}_{\text{msr}}(x(k))$ parameterized by $x(k) \in \mathbb{R}^n$:

$$\begin{aligned} \max_{x_a(k)\in\mathbb{R}^n} \; & \|u(k)\|_Q^2 + \|x(k+1)\|_P^2 - \|x_a(k)\|_{Q_{\text{msr}}}^2, \\ \text{s.t.} \quad & x(k+1) = Ax(k) + Bu(k) + Bu_a(k), \\ & x_a(k) \in \Omega_{\text{msr}}(x(k)), \end{aligned}$$

where $u(k) \in \mathrm{OR}_{\text{op}}(x(k) + x_a(k))$ and $u_a(k) \in \mathrm{OR}_{\text{cnt}}(x(k) + x_a(k), u(k))$. Here, $\Omega_{\text{msr}}(x(k))$ is the feasible solution set of the measurement jammer given $x(k)$ where the set-valued map $\Omega_{\text{msr}} : X \to 2^{\mathbb{R}^n}$ could depend upon OR_{op} and will be defined later. It is noticed that the measurement jammer can exactly determine $x(k+1)$ in $\mathrm{QP}_{\text{msr}}(x(k))$.

The above process to determine $x_a(k)$, $u(k)$ and $u_a(k)$ sequentially consists of a finite-horizon constrained Stackelberg game. That is, at any given time instant k, the measurement jammer adopts a Stackelberg equilibrium strategy as the leader of the operator and the control jammer, and the control jammer exploits the optimal response to its leaders' decisions. This procedure is repeated at the next time instant by shifting the horizon forward. We term the collection of these finite-horizon games over the infinite horizon as a two-level receding-horizon constrained dynamic Stackelberg game. The readers are referred to [5], and references therein, for additional information on Stackelberg games. The objective of this paper is to design the control law OR_{op} of the operator and characterize the class of correlated jamming attacks parameterized by Q_{msr} and Q_{cnt} under which the control law can maintain (practical) stability of system (4). We would like to mention that X and U are hard constraints for the operator, while the jammers have no incentive to enforce them. Thus, the operator has to maintain states and control laws in these regions through the devise of OR_{op}. We assume the following holds for the constraint sets:

Assumption 2.1 (Constraint set assumption): If only the control jammer is present, the set X (resp. U) is any convex set in $\mathbb{R}^n$ (resp. $\mathbb{R}^m$). Under both jammers, the constraint set has the form $X := \{x \in \mathbb{R}^n \mid x_{\min} \leq x \leq x_{\max}\}$, where $x_{\min} \leq x \leq x_{\max}$ (resp. $U := \{u \in \mathbb{R}^m \mid u_{\min} \leq u \leq u_{\max}\}$, where $u_{\min} \leq u \leq u_{\max}$) are vectors in $\mathbb{R}^n$ (resp. $\mathbb{R}^m$)[1].

Here we would like to make some remarks to justify our model. Dynamic non-cooperative games without constrained sets have been extensively studied; e.g., in [5] and references therein. These games have been used to study behavior of self-interested agents in economics and communication networks; see [2], [8]. Existing solutions involve solving a set of linear matrix equations and require some stabilizability and detectability properties of the limiting solutions of linear matrix equations. As pointed out in [5], solving the set of linear matrix equations and further satisfy the stabilizability and detectability properties is quite hard. Secondly, the presence of constraint sets hampers the use of the approaches in [5]. Thirdly, multiple levels introduce another challenge to find the solutions of dynamic games. Lastly, existing solutions to dynamic games require that decision makers are able to share their private information (e.g., payoffs or strategies) with opponents. Yet, this information exchange is not reasonable to expect in hostile environments. To overcome these challenges, our proposed model exploits a receding-horizon methodology to provide an approximation to the infinite-horizon dynamic Stackelberg game.

In the structure of the closed-loop control system, at each time instant, decision makers choose their actions *sequentially*. This motivates us to employ Stackelberg game to model this process. In an adversarial context, we argue that this is a more reasonable model than by Nash games where decisions are made *simultaneously*. Furthermore, the leader-follower framework allows us to capture possible information asymmetry between the control system operator and the jammers. This would facilitate the assessment of the *value of information* (equivalently, the price of the lack of information) in resilient control: how the decision makers play against opponents to maximize their own interests by means of manipulating the information they possess.

III. Receding-horizon Stackelberg control law

This section is devoted to the design of a receding-horizon Stackelberg control law. Fix a time horizon $N > 0$. Next, we introduce a **virtual control jammer**, and define his optimal response map $\mathrm{OR}_{\text{vir}}^N : X \times U^N \to 2^{\mathbb{R}^{m\times N}}$ as follows. Given $x_c(k) \in X$ and $\tilde{\mathbf{u}}(k) \in U^N$, we define $\tilde{\mathbf{u}}_{\text{vir}}(k)$ sequentially. Consider $x(k+\tau|k)$ and $\tilde{u}(k+\tau|k)$ for some $0 \leq \tau \leq N-1$, we define optimization problem $\mathrm{QP}_{\text{vir}}(x(k+\tau|k), \tilde{u}(k+\tau|k))$ for the virtual control jammer in the following form:

$$\begin{aligned} \max_{u_{\text{vir}}(k+\tau|k)\in\mathbb{R}^m} \; & \|x(k+\tau+1|k)\|_P^2 - \|u_{\text{vir}}(k+\tau|k)\|_{Q_{\text{cnt}}}^2, \\ \text{s.t.} \quad & x(k+\tau+1|k) = Ax(k+\tau|k) \\ & + B\tilde{u}(k+\tau|k) + Bu_{\text{vir}}(k+\tau|k). \end{aligned}$$

Let $\tilde{u}_{\text{vir}}(k+\tau|k)$ be a solution of $\mathrm{QP}_{\text{vir}}(x(k+\tau|k), \tilde{u}(k+\tau|k))$ and then we have $x(k+\tau+1|k) = Ax(k+\tau|k) + B\tilde{u}(k+\tau|k) + B\tilde{u}_{\text{vir}}(k+\tau|k)$. This process is repeated for all $0 \leq \tau \leq N$. The set of solutions $\tilde{\mathbf{u}}_{\text{vir}}(k) = [\tilde{u}_{\text{vir}}(k|k), \tilde{u}_{\text{vir}}(k+1|k), \cdots, \tilde{u}_{\text{vir}}(k+\tau|k)] \in \mathbb{R}^{m\times N}$ to the above N-horizon sequential optimization problem is denoted by $\mathrm{OR}_{\text{vir}}^N(x_c(k), \tilde{\mathbf{u}}(k))$.

With $\mathrm{OR}_{\text{vir}}^N$ defined above, we are now in a position to construct a N-horizon minimax problem (N-MINI, for short) parameterized by $x_c(k) \in \mathbb{R}^n$ for the operator:

$$\begin{aligned} & V_N(x_c(k)) := \min_{\mathbf{u}(k)\in\mathbb{R}^{m\times N}} \; \max_{\mathbf{u}_{\text{vir}}(k)\in\mathrm{OR}_{\text{vir}}^N(x_c(k),\mathbf{u}(k))} \\ & \sum_{\tau=0}^{N-1} \left(\|x(k+\tau|k)\|_P^2 + \|u(k+\tau|k)\|_Q^2\right) + \|x(k+N|k)\|_P^2 \\ & \text{s.t.} \quad x(k+\tau+1|k) = Ax(k+\tau|k) \\ & \quad + Bu(k+\tau|k) + Bu_{\text{vir}}(k+\tau|k), \\ & \quad x(k|k) = x_c(k), \quad x(k+\tau+1|k) \in X_0, \\ & \quad u(k+\tau|k) \in U, \quad 0 \leq \tau \leq N-1. \end{aligned}$$

In the N-MINI, the set $X_0 \subseteq X$ is some convex set and will be specified later. The set of solutions to the above minimax

[1] Inequalities are understood component-wise.

problem is denoted by $\mathrm{OR}_{\mathrm{op}}^N(x_c(k))$, where the set-valued map $\mathrm{OR}_{\mathrm{op}}^N : X \to 2^{U^N}$. The optimal response map of the operator $\mathrm{OR}_{\mathrm{op}} : X \to 2^U$ is defined in such a way that if $\mathbf{u}(k) \in \mathrm{OR}_{\mathrm{op}}^N(x_c(k))$ then $u(k|k) \in \mathrm{OR}_{\mathrm{op}}(x_c(k))$.

Remark 3.1: In the N-MINI parameterized by $x_c(k)$, the quantity $x(k+\tau|k)$ (resp. $u(k+\tau|k)$, $u_{\mathrm{vir}}(k+\tau|k)$) represents the future system state (resp. the input of the operator, the input of the virtual control jammer) at time $k+\tau$ predicted by the operator and the virtual control jammer at time k. This prediction starts from the corrupted state $x_c(k)$, and thus prediction errors on system states are propagated and amplified along the prediction horizon. •

We now formally state **the receding-horizon Stackelberg control law**, namely ψ_N, in the table. To do so, it is assumed that the operator has a choice on the running state matrix P, the input cost matrix Q, and the constraint set U.

Algorithm 1 The receding-horizon Stackelberg control law

```
Initialization: The operator executes the following steps:
    (I.1) Choose $P$ such that $Q_{\mathrm{cnt}} - B^T PB > 0$.
    (I.2) Choose $K$ such that $\sigma(\bar{A})$ is contained in the unit circle, where $\bar{A} := (I + \Lambda(Q_{\mathrm{cnt}}))(A + BK)$ and the linear operator $\Lambda : \mathbb{R}^{m\times m} \to \mathbb{R}^{n\times n}$ is defined as $\Lambda(Q_{\mathrm{cnt}}) := B(Q_{\mathrm{cnt}} - B^T PB)^{-1} B^T P$.
    (I.3) Choose any $\bar{Q} = \bar{Q}^T > 0$, solve the following Lyapunov equation to obtain its solution $\bar{P} = \bar{P}^T > 0$:
        $\bar{A}^T \bar{P} \bar{A} - \bar{P} = -\bar{Q}.$   (5)
    (I.4) If only the control jammer is present, choose the largest $c > 0$ such that the level set $X_0 := \{x \in \mathbb{R}^n \mid W(x) \le c\}$ is contained in $X$ where $W(x) := \|x\|_{\bar{P}}^2$. If both jammers are present, then choose $X_0 = X$. After that, choose $U$ such that $Kx \in U$ for all $x \in X_0$.
Iteration: At each time $k \ge 0$, the decision makers choose their own actions sequentially:
    The measurement jammer first corrupts the measurement $x(k)$ by adding the signal $x_a(k) \in \mathrm{OR}_{\mathrm{msr}}(x(k))$; i.e., $x_c(k) = x(k) + x_a(k)$.
    After receiving $x_c(k)$, the operator then chooses $u(k) = u(k|k) \in \mathrm{OR}_{\mathrm{op}}(x_c(k))$, and then sends $u(k)$ to the actuator through the communication channel.
    The control jammer corrupts $u(k)$ by adding its signal $u_a(k) \in \mathrm{OR}_{\mathrm{cnt}}(x_c(k), u(k))$; i.e., $u_c(k) = u(k) + u_a(k)$.
    The actuator receives and then implements the corrupted control law $u_c(k)$.
```

We conclude this section with some remarks. The N-MINI parameterized by $x_c(k)$ is equivalent to the following N-horizon quadratic program, namely N-QP, parameterized by $x_c(k) \in X$:

$$\begin{aligned} V_N(x_c(k)) = &\min_{\mathbf{u}(k)\in\mathbb{R}^{m\times N}} \sum_{\tau=0}^{N-1} \big(\|x(k+\tau|k)\|_P^2 \\ &+ \|u(k+\tau|k)\|_Q^2\big) + \|x(k+N|k)\|_P^2, \\ \text{s.t.}\quad & x(k+\tau+1|k) = (I + \Lambda(Q_{\mathrm{cnt}}))(Ax(k+\tau|k) \\ &+ Bu(k+\tau|k)),\ x(k|k) = x_c(k),\ x(k+\tau+1|k) \in X_0, \\ & u(k+\tau|k) \in U, \quad 0 \le \tau \le N-1, \end{aligned}$$

and then $\tilde{\mathbf{u}}_{\mathrm{vir}}(k)$ can be obtained through $\tilde{\mathbf{u}}_{\mathrm{vir}}(k) = \mathrm{OR}_{\mathrm{vir}}^N(x_c(k), \tilde{\mathbf{u}}(k))$. This equivalence allows the operator to find the solution to the N-MINI by solving the N-QP. The verification can be found in the extended version.

The operator employs a receding-horizon control methodology and its use is motivated by the advantages of receding-horizon control: suboptimal control and its unique ability to explicitly handle hard constraints. The paper [12] provides an excellent survey on recent advances in receding-horizon control. The control law for the operator is of mixed nature: on the one hand, it is an optimal plan at equilibrium with the leading Stackelberg strategy of the measurement jammer; on the other hand, the follower policy of the control jammer is at equilibrium with it. This control law takes advantage of the operator being the leader of the control jammer, and the information of the control jammer is utilized in the choices of the matrices of P, $\bar{A}$, $\bar{P}$, $\bar{Q}$, and constraint sets of X_0 and U. This allows the operator to maintain situational awareness. However, the operator does not have information on the cost of the measurement jammer, which could result in a greater damage to the system.

IV. Stability and performance analysis

We now proceed to analyze stability and infinite-horizon performance of system (4) under ψ_N. As before, we consider two cases depending on type of jammer present. We start by introducing some additional notation as follows: $\lambda := 1 - \lambda_{\max}(\bar{Q})/\lambda_{\max}(\bar{P})$ and

$$\begin{aligned} \alpha_N &:= \frac{\lambda_{\max}(K^T QK + \bar{A}^T P \bar{A})}{\lambda_{\min}(P)} \times \prod_{\kappa=0}^{N-1} \Big(1 - \frac{\lambda_{\min}(P)}{\phi_{\kappa+1}}\Big), \\ \phi_N &:= \frac{\lambda_{\max}(\bar{P})\lambda_{\max}(P + K^T QK)}{\lambda_{\min}(\bar{P})} \frac{1-\lambda^{N+1}}{1-\lambda}, \\ \phi_\infty &:= \frac{\lambda_{\max}(\bar{P})\lambda_{\max}(P + K^T QK)}{\lambda_{\min}(\bar{P})} \frac{1}{1-\lambda}. \end{aligned}$$

It follows from [13] that $\lambda \in (0,1)$, and clearly, $1 \le \phi_N \le \phi_\infty$ for any $N \in \mathbb{Z}_{>0}$. Observe that the following holds for any $\kappa \in \mathbb{Z}_{>0}$:

$$\frac{\lambda_{\min}(P)}{\phi_{\kappa+1}} \ge \frac{\lambda_{\min}(P)}{\lambda_{\max}(P + K^T QK)} \frac{\lambda_{\min}(\bar{P})}{\lambda_{\max}(\bar{P})}(1-\lambda) \in (0,1).$$

This ensures the monotonicity of α_N that $\alpha_N \searrow 0$ as $N \nearrow +\infty$. Let $\hat{c} > 0$ the largest positive constant such that the level set $\hat{X}_0 := \{x \in \mathbb{R}^n \mid W(x) \le \hat{c}\}$ is contained in X. Let $R \in (0, \frac{\hat{c}\lambda_{\min}(P)}{\phi_\infty \lambda_{\max}(\bar{P})})$ the largest constant such that $B_R := \{x \in \mathbb{R}^n \mid \|x\|^2 \le R\}$ is a subset of $\hat{X}_0$.

A. The presence of both jammers

We first examine the more general case where the measurement jammer is taken into account. It is worthy to recall that X and U are polyhedra as defined in Assumption 2.1. Notice that the following property holds:

$$\frac{\lambda_{\min}(P)}{\phi_N} = \frac{\lambda_{\min}(P)}{\lambda_{\max}(P + K^T QK)} \frac{\lambda_{\min}(\bar{P})}{\lambda_{\max}(\bar{P})} \frac{1-\lambda}{1-\lambda^{N+1}} < 1.$$

Recall $\alpha_N \searrow 0$ as $N \nearrow +\infty$. Then there is a smallest positive integer N^* such that $(1+\alpha_{N^*-1})(1-\frac{\lambda_{\min}(P)}{\phi_{N^*}}) < 1$. We then choose any $N \geq N^*$, and start our analysis by investigating the continuity and piecewise quadratic properties of V_N, and piecewise affinity of ψ_N.

Lemma 4.1: (Continuity and piecewise quadratic property of V_N and piecewise affinity of ψ_N) Let $\mathbf{u}(k)$ be the solution to the N-QP parameterized by $x_c(k)$. Then $V_N(x_c(k))$ is continuous and piecewise quadratic, and $u(k|k)$ is piecewise affine. That is, if $x_c(k)$ is in the critical region $CR_\ell := \{x \in \mathbb{R}^n \mid H_\ell x \leq \hat{H}_\ell\}$, then $V_N(x_c(k)) = \|x_c(k)\|^2_{M_\ell} + \langle R_\ell, x_c(k)\rangle + S_\ell$ and $u(k|k) = F_\ell x_c(k) + G_\ell$ where F_ℓ, G_ℓ, H_ℓ, $\hat{H}_\ell$, M_ℓ, R_ℓ and S_ℓ are matrices (or vectors, scalars) with appropriate dimensions.

Proof: This is a direct result of Corollary 1 and 2 in [6] by letting $C = I$ and $y_{\min} = -\infty$, $y_{\max} = +\infty$. ■

By [6], we know that the collection of critical regions CR_ℓ consists of a partition of X and the total number n_{cr} of critical regions is finite. For any $x \in X$, let $\ell_x \in \{1, \cdots, n_{\text{cr}}\}$ be the index such that $x \in CR_{\ell_x}$. Consider now the constants $\hat{\lambda} := \max_{\ell\in\{1,\cdots,n_{\text{cr}}\}} \lambda_{\max}(M_\ell)$ and $\hat{\beta} := \max_{\ell\in\{1,\cdots,n_{\text{cr}}\}} \|R_\ell\|$. For the partition, we choose the largest $\alpha > 0$ such that

$$(1 + \frac{\alpha}{\lambda_{\min}(P)} \sum_{\ell=1}^{n_{\text{cr}}} \lambda_{\max}(M_\ell))(1+\alpha_{N-1}) \times (1 - \frac{\lambda_{\min}(P)}{\phi_\infty})(1 + \frac{\alpha\hat{\lambda}}{\lambda_{\min}(P)}) < 1. \tag{6}$$

The existence of α can be verified by noting that $(1 + \alpha_{N^*-1})(1 - \frac{\lambda_{\min}(P)}{\phi_{N^*}}) < 1$ and $N \geq N^*$.

In the following, we enforce two restrictions on the strategies of the measurement jammer. These conditions are sufficient to guarantee system practical stability if the cost of the jammer is sufficiently high. First, $x_a(k)$ is to be linear in $x(k)$. Second, we require that the corrupted state $x_c(k)$ is in the same critical region as $x(k)$. This is formalized in the following assumption:

Assumption 4.1: In $\text{QP}_{\text{msr}}(x(k))$, the set-valued map Ω_{msr} is defined as $\Omega_{\text{msr}}(x(k)) = \{x_a \in \mathbb{R}^n \mid x_a = \alpha x(k), \quad \alpha \in \mathbb{R}\} \cap CR_{\ell_{x(k)}}$.

With the piecewise affine property of ψ_N and the restriction $x_a(k) \in CR_{\ell_{x(k)}}$, $\text{QP}_{\text{smr}}(x(k))$ is equivalent to the one restricted in critical region $\ell_{x(k)}$, which is given as follows:

$$\begin{aligned}
&\max_{\alpha_a(k)\in\mathbb{R}} \|F_{\ell_{x(k)}}(x(k) + x_a(k)) + G_{\ell_{x(k)}}\|^2_Q \\
&\quad + \|x(k+1)\|^2_P - \|x_a(k)\|^2_{Q_{\text{msr}}} \\
\text{s.t.}\quad & x(k+1) = (I + \Lambda(Q_{\text{cnt}})) \\
&\quad \times (Ax(k) + BF_{\ell_{x(k)}}(x(k) + x_a(k)) + BG_{\ell_{x(k)}}) \\
&\quad x_a(k) = \alpha_a(k)x(k), \\
&\quad H_{\ell_{x(k)}} x_a(k) \leq \hat{H}_{\ell_{x(k)}} - H_{\ell_{x(k)}} x(k).
\end{aligned}$$

The following assumption ensures that the quadratic program $\text{QP}_{\text{msr}}(x(k))$ is well defined:

Assumption 4.2: It holds that $Q_{\text{msr}} - \langle F_\ell, F_\ell\rangle_Q - \langle (I + \Lambda(Q_{\text{cnt}}))BF_\ell, (I + \Lambda(Q_{\text{cnt}}))BF_\ell\rangle_P > 0$ for all $\ell \in \{1, \cdots, n_{\text{cr}}\}$.

Roughly speaking, Assumption 4.2 requires that the cost of the measurement jammer is relatively high given the costs of his followers and the control law of the operator. Then, one can see that, when system state $x(k)$ is outside the unit circle, $\|x_a(k)\|$ is upper bounded by a linear function of $x(k)$; otherwise, $\|x_a(k)\|$ is uniformly bounded.

Lemma 4.2 (Boundedness of $x_a(k)$): If $\|x(k)\| \geq 1$, then $\|\alpha_a(k)\| \leq \eta$, for some positive η. Furthermore, if $\|x(k)\| \leq 1$, then $\|x_a(k)\| \leq \eta$.

The following lemma shows that $V_N(x_c)$ is bounded above by a scaled version of $V_N(x)$ added by a square function of $\|x_a\|$ where x_c is x perturbed by x_a.

Lemma 4.3: (Sensitivity analysis of the optimal value function V_N) Let $x, x_a, x_c \in \mathbb{R}^n$, with $x_c = x + x_a$. Then, we have $V_N(x_c) \leq \vartheta_a V_N(x) + \vartheta_b\|x_a\|^2 + \vartheta_c\|x_a\|$.

Before stating the main result of this section, we introduce several notations and an assumption. Denote constants Θ and Π as follows:

$$\begin{aligned}
\Theta :=\ & (\vartheta_a(1+\alpha_{N-1})(1 - \frac{\lambda_{\min}(P)}{\phi_N})(1 + \frac{\hat{\lambda}}{\alpha}) \\
& + \vartheta_b \lambda_{\max}(A^T(I + \Lambda(Q_{\text{cnt}}))^T(I + \Lambda(Q_{\text{cnt}}))A)) \frac{(\eta_a + \eta_b)^2}{\eta_c^2} \\
& + (\vartheta_a(1+\alpha_{N-1})(1 - \frac{\lambda_{\min}(P)}{\phi_N})\hat{\beta} \\
& + \vartheta_c\|(I + \Lambda(Q_{\text{cnt}}))A\|) \frac{\eta_a + \eta_b}{\eta_c}, \\
\Pi :=\ & \vartheta_a(1+\alpha_{N-1})(1 - \frac{\lambda_{\min}(P)}{\phi_N})(1 + \frac{\alpha\hat{\lambda}}{\lambda_{\min}(P)}) + \frac{\Theta}{\lambda_{\min}(P)}.
\end{aligned}$$

Choose $\epsilon \in (0, 1-(\vartheta_a(1+\alpha_{N-1})(1-\frac{\lambda_{\min}(P)}{\phi_N})(1+\frac{\alpha\hat{\lambda}}{\lambda_{\min}(P)})))$.

Assumption 4.3: It holds that $\Pi < 1 - \epsilon$, and there is $r > 0$ such that the following holds for some $\epsilon' \in (0, \epsilon)$:

$$\begin{aligned}
&(1 + \frac{(\eta_a + \eta_b)^2}{\eta_c^2})r \leq \frac{R}{2} - \frac{(\eta_a + \eta_b)^2}{\eta_c^2}, \\
&(1 + \frac{(\eta_a + \eta_b)^2}{\eta_c^2})\frac{(\phi_N r + \frac{\Theta}{\epsilon'})^2}{\lambda_{\min}(P)^2} \leq \frac{R}{2} - \frac{(\eta_a + \eta_b)^2}{\eta_c^2}.
\end{aligned}$$

Denote the ball $B_r := \{x \in \mathbb{R}^n \mid \|x\|^2 \leq r\}$. The following theorem is the main result of the section, and characterizes the practical stability of ψ_N with its average infinite-horizon performance under both jammers.

Theorem 4.1: (Regionally practical exponential stability and the average of the infinite-horizon performance) Consider the receding-horizon Stackelberg control law ψ_N in the presence of both jammers. If Assumptions 2.1, 4.1, 4.2 and 4.3 hold, then system (4) under ψ_N is practically exponentially stable in B_r with geometric convergence rate $1-\epsilon+\epsilon'$ and $\limsup_{k\to+\infty}\|x(k)\| \leq \sqrt{\frac{\Theta}{\lambda_{\text{min}}(P)\epsilon'}}$. Furthermore, the average of the infinite-horizon performance of ψ_N is estimated in the following way:

$$\limsup_{K\to+\infty}\frac{\sum_{k=0}^{K}(\|x(k)\|_P^2+\|u_c(k)\|_Q^2)}{K} \leq 2\gamma\phi_N(\frac{\eta_a+\eta_b}{\eta_c}$$
$$+\frac{\eta_a+\eta_b+\eta_c}{\eta_c}\frac{\Theta}{\epsilon'\lambda_{\text{min}}(P)})+\frac{\gamma\lambda_{\text{max}}(P)\Theta}{\epsilon'\lambda_{\text{min}}(P)}$$
$$+4|(Q_{\text{cnt}}-B^TPB)^{-1}B^TPA|^2\lambda_{\text{max}}(Q)\frac{(\eta_a+\eta_b)^2}{\eta_c^2}.$$

B. The presence of the control jammer

Here, we assume there is no measurement jammer in the network; i.e., $Q_{\text{msr}} = +\infty I$ and $x_a(k) = 0$. In this way, $x_c(k) = x(k)$ and $x(k+1|k) = x(k+1)$. Choose $c' > 0$ such that $X_{\text{int},N} := \{x \in \mathbb{R}^n \mid V_N(x) \leq c'\} \subseteq X_0$.

The following theorem characterizes regionally exponential stability and infinite-horizon performance of system (4) under ψ_N when the measurement jammer is absent.

Theorem 4.2: (Regionally exponential stability and infinite-horizon performance) Assume the measurement jammer is absent. Let N^* to be the smallest integer such that $(1+\alpha_{N^*-1})(1-\frac{\lambda_{\text{min}}(P)}{\phi_{N^*}}) < 1$. Then, if Assumption 2.1 holds, for any $N \geq N^*$, system (4) under ψ_N is exponentially stable in $X_{\text{int},N}$ and an estimate of the exponential convergence rate is $(1+\alpha_{N-1})(1-\frac{\lambda_{\text{min}}(P)}{\phi_N})$. Furthermore, the infinite-horizon performance of system (4) under ψ_N is bounded above by $\frac{\lambda_{\text{min}}(P)}{1-(1+\alpha_{N-1})(1-\frac{\lambda_{\text{min}}(P)}{\phi_N})}\|x(0)\|^2$.

Remark 4.1: Recall that α_N is strictly decreasing in N and ϕ_N is strictly increasing in N. Theorem 4.2 then reveals that, a larger horizon N in ϕ_N improves convergence rate and infinite-horizon performance of the closed-loop system. On the other hand, it follows from the monotonicity of V_N that $X_{\text{int},\infty} \subseteq X_{\text{int},N+1} \subseteq X_{\text{int},N}$. This means that the domain of attraction $X_{\text{int},N}$ shrinks as N increases. •

Remark 4.2: At each iteration, the measurement jammer, the operator and the control jammer face their corresponding optimization problems; i.e., $\text{QP}_{\text{smr}}(x(k))$, N-QP and $\text{QP}_{\text{cnt}}(x(k)+x_a(k), u(k))$ respectively. It should be noticed that these are all quadratic programs and there are a number of efficient algorithms (e.g., interior-point methods) to solve these problems. •

V. Conclusions

In this paper, we have studied a resilient control problem where a linear dynamic system is subject to cyber attacks launched by correlated jammers. We have proposed a novel leader-follower game formulation to model the interdependency between the operator and adversaries. We devised a receding-horizon Stackelberg control law to maintain situational awareness, and further analyzed closed-loop system stability and performance. Future work will address distributed versions of the proposed algorithm.

References

[1] T. Alpcan and T. Basar. *Network Security: A Decision And Game Theoretic Approach*. Cambridge University Press, 2011.

[2] E. Altman and T.Basar. Multi-user rate-based flow control. *IEEE Transactions on Communications*, 46(7):940–949, 1998.

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

[4] S. Amin, X. Litrico, S. Sastry, and A. M. Bayen. Stealthy deception attacks on water SCADA systems. In *Proceedings of the 13th ACM International Conference on Hybrid systems: Computation and Control*, pages 161–170, Stockholm, Sweden, 2010.

[5] T. Basar and G. Olsder. *Dynamic Noncooperative Game Theory*. SIAM Classics in Applied Mathematics, 1999.

[6] A. Bemporad, M. Morari, V. Dua, and E.N. Pistikopoulos. The explicit linear quadratic regulator for constrained systems. *Automatica*, 38:3–20, 2002.

[7] M.S. Branicky, S.M. Phillips, and W. Zhang. Stability of networked control systems: explicit analysis of delay. In *Proceedings of American Control Conference*, pages 2352–2357, Chicago, USA, 2000.

[8] E. Dockner, S. Jorgensen, N. V. Long, and G. Sorger. *Differential games in economics and management science*. Cambridge University Press, 2006.

[9] D. Fudenberg and J. Tirole. *Game theory*. The MIT press, 1991.

[10] A. Gupta, C. Langbort, and T. Basar. Optimal control in the presence of an intelligient jammer with limited actions. In *IEEE Conf. on Decision and Control*, pages 1096–1101, Atlanta, USA, December 2010.

[11] J. Hespanha, P. Naghshtabrizi, and Y. Xu. A survey of recent results in networked control systems. *Proceddings of IEEE Special Issue on Technology of Networked Control Systems*, 95(1):138–162, 2007.

[12] D. Q. Mayne, J. B. Rawlings, C. V. Rao, and P. O. M. Scokaert. Constrained model predictive control: stability and optimality. *Automatica*, 36:789–814, 2000.

[13] T. Mori, N. Fukuma, and M. Kuwahara. Upper and lower bounds for the solution to the discrete Lyapunov matrix equation. *International Journal of Control*, 36:889–892, 1982.

[14] G. N. Nair, R. J. Evans, I. M. Y. Mareels, and W. Moran. Topological feedback entropy and nonlinear stabilization. *IEEE Transactions on Automatic Control*, 49(9):1585–1597, 2004.

[15] D. Nesic and A. Teel. Input-output stability properties of networked control systems. *IEEE Transactions on Automatic Control*, 49(10):1650–1667, 2004.

[16] F. Pasqualetti, R. Carli, A. Bicchi, and F. Bullo. Identifying cyber attacks under local model information. In *IEEE Conf. on Decision and Control*, Atlanta, GA, USA, December 2010. To appear.

[17] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, and S. S. Sastry. Foundations of control and estimation over lossy networks. *Proceddings of IEEE Special Issue on Technology of Networked Control Systems*, 95(1):163–187, 2007.

[18] S. Sundaram and C. N. Hadjicostis. Distributed function calculation via linear iterations in the presence of malicious agents - parts I, II. In *American Control Conference*, pages 1350–1362, June 2008.

[19] G. Theodorakopoulos and J. S. Baras. Game theoretic modeling of malicious users in collaborative networks. *IEEE Journal on Selected Areas in Communications*, 7:1317–1327, 2008.

[20] M. Zhu and S. Martínez. Stackelberg game analysis of correlated attacks in cyber-physical systems. Extended version available at http://faemino.ucsd.edu/ soniamartinez/papers/data/mzsm.pdf, 2010.