On resilient networked control systems against replay attacks

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 commands are transmitted over a communication network and could be corrupted by adversaries. In particular, we consider the replay attackers who maliciously repeat the messages sent from the operator to the actuator. We propose a variation of the receding-horizon control law to play against the replay attackers, and analyze the resulting system stability and performance degradation under the attacks.

I. Introduction

The recent advances of information technologies have boosted the emergence of networked control systems where information networks are tightly coupled to physical processes and human intervention. 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 networked control systems. Thus, the ability to analyze their consequences becomes of prime importance in order to enhance the resilience of these new-generation control systems.

This paper considers a single-loop remotely-controlled system, in which 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 commands are

M. Zhu is with the Laboratory for Information and Decision Systems, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge MA, 02139, (mhzhu@mit.edu). S. Martínez is with the Department of Mechanical and Aerospace Engineering, University of California, San Diego, 9500 Gilman Dr, La Jolla CA, 92093, (soniamd@ucsd.edu).

transmitted to the actuator through the same network. This model is an abstraction of a variety of existing networked control 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). The objective of the paper is to design and analyze resilient controllers against the replay and denial-of-service attacks.

Literature review. Recently, it has been receiving increasing attention to address jointly the problem of control design and system security. The first set of papers are concerned with attack detection. For example, the papers of [27], [30] determine conditions under which consensus multi-agent systems can detect misbehaving agents. A particular class of cyber attacks, namely *false data injection*, against state estimation has been attracting considerable attention recently; an incomplete reference list includes [28], [31], [32]. The paper [21] studies the detection of the *replay attacks*, which maliciously repeat transmitted data. The second set of papers focus on the analysis of the consequences caused by subclasses of cyber attacks and system resilience against such attacks. The papers [2], [33], [34] are devoted to studying *deception attacks*, where attackers intentionally modify measurements and control commands. *Denial-of-service* (DoS) attacks destroy the data availability in control systems and are tackled in recent papers [1], [3], [4], [11]. More specifically, the papers [1], [11] formulate finite-horizon LQG control problems as dynamic zero-sum games between the controller and the jammer. In [3], the authors investigate the security independency in infinite-horizon LQG against DoS attacks, and fully characterize the equilibrium of the induced game. In [5], [6], the authors exploit pursuit-evasion games to compute optimal evasion strategies for mobile agents when facing jamming attacks. In our paper [35], a distributed receding-horizon control law is proposed to ensure that vehicles reach the desired formation despite the DoS and replay attacks.

The problems of control and estimation over unreliable communication channels have received considerable attention over the last decade [14]. Key issues include band-limited channels [17], [24], quantization [8], [23], packet dropout [12], [15], [29], delay [7] and sampling [25]. Receding-horizon networked control is studied in [9], [13], [26] for package dropouts and in [16], [18] for transmission delays. However, none of these papers characterizes the performance degradation of receding-horizon control induced by the communication unreliability.

Contributions. We propose a variation of the receding-horizon control to play against the replay attackers. A set of sufficient conditions are provided to ensure asymptotical and exponential stability. More importantly, we derive a simple and explicit relation between the infinite-horizon cost and the computing and attacking horizons. The preliminary results are published in [34] where receding-horizon control is used to play against a class of deception attacks. The technical relations between this paper and [34] will be explained at the very beginning of Section III.

II. Attack-resilient receding-horizon control

A. Description of the controlled system

Consider the following discrete-time, linear time-invariant dynamic system:

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

where $x(k) \in \mathbb{R}^n$ is the system state, and $u(k) \in \mathbb{R}^m$ is the system input at 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. States and inputs of system (1) are constrained to be in some sets; i.e., $x(k) \in X$ and $u(k) \in U$, for all $k \geq 0$, where $0 \in X \subseteq \mathbb{R}^n$ and $0 \in U \subseteq \mathbb{R}^m$. 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. We assume the following holds for the system:

Assumption 2.1: (Stabilizability) The pair (A, B) is stabilizable. •

This assumption ensures the existence of K such that the spectrum $\sigma(\bar{A})$ is strictly inside the unit circle where $\bar{A} \triangleq A + BK$. In the remainder of the paper, $u = Kx$ will be referred to as the auxiliary controller. We then impose the following condition on the constraint sets.

Assumption 2.2: (Constraint sets) The sets X and U are convex and $Kx \in U$ for $x \in X$.•

B. The closed-loop system with the replay attacker

System (1) together with the sensor and the actuator are spatially separated from the operator. These entities are connected through communication channels. In the network, there is a replay attacker who maliciously repeats the messages delivered from the operator to the actuator. In particular, the adversary is associated with a memory whose state is denoted by $M^a(k)$. If a replay attack is launched at time k, the adversary executes the following: (i) erases the data sent from the operator; (ii) sends previous data stored in her memory, $M^a(k)$, to the actuator; (iii) maintains the state of the memory; i.e., $M^a(k+1) = M^a(k)$. In this case, we use $\vartheta(k) = 1$ to indicate the occurrence of a replay attack. If the attacker keeps idle at time k, then data is intercepted, say Υ, sent from the operator to plant, and stored it in memory; i.e., $M^a(k+1) = \Upsilon$. In this case, $\vartheta(k) = 0$ and u is successfully received by the actuator. Without loss of any generality, we assume that $\vartheta(-1) = \vartheta(0) = 0$.

We now define the variable $s(k)$ with initial state $s(0) = s(-1) = 0$ to indicate the consecutive number of the replay attacks. If $\vartheta(k) = 1$, then $s(k) = s(k-1) + 1$; otherwise, $s(k) = 0$. So, the quantity $s(k)$ represents the number of consecutive attacks up to time k.

A replay attack requires spending certain amount of energy. We assume that the energy of the adversary is limited, and adversary i is only able to launch at most $S \geq 1$ consecutive attacks. This assumption is formalized as follows:

Assumption 2.3: (Maximum number of consecutive attacks) There is an integer $S \geq 1$ such that $\max_{k\geq 0} s(k) \leq S$. •

Replay attacks have been successfully used by the virus attack of Stuxnet [10], [20]. This class of attacks can be easily detected by attaching a time stamp to each control command. This is formally stated as follows:

Assumption 2.4: (Attack detection) Each transmitted message is attached a time stamp. The plant and actuator can recognize the occurrence of replay attacks by checking the time stamps.

C. Attack-resilient receding-horizon control law

Here we propose a variation of the receding-horizon control in; e.g. [19], [18], to play against the replay attacks. Our **attack-resilient receding-horizon control law**, (for short, AR-RHC) is stated in Algorithm 1. In particular, the terminal state cost is chosen to coincide with the running state cost. This is instrumental for the analysis of stability and performance degradation in Theorem 2.1.

D. Stability and performance analysis

In this section, we present the results characterizing the stability and infinite-horizon cost induced by AR-RHC. See Table I, for the main notations employed, and Section III for the complete proof.

Notice that the following property holds:

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

Algorithm 1 The attack-resilient receding-horizon control law

---

Initialization: The following steps are first performed by the operator:

1: Choose K so that $\sigma(\bar{A})$ is strictly inside the unit circle.

2: Choose $\bar{Q} = \bar{Q}^T > 0$ and obtain $\bar{P}$ by solving the following Lyapunov equation:

$$\bar{A}^T \bar{P} \bar{A} - \bar{P} = -\bar{Q}. \tag{2}$$

3: Choose a constant $c > 0$ such that $X_0 \triangleq \{x \in \mathbb{R}^n \mid \|x\|^2_{\bar{P}} \leq c\} \subseteq X$.

Iteration: At each $k \geq 0$, the operator, actuator and sensor execute the following steps:

1: The operator solves the following N-horizon quadratic program, namely N-QP, parameterized by $x(k) \in X$:

$$\min_{\mathbf{u}(k)\in\mathbb{R}^{m\times N}} \sum_{\tau=0}^{N-1} \left(\|x(k+\tau|k)\|^2_P + \|u(k+\tau|k)\|^2_Q\right) + \|x(k+N|k)\|^2_P,$$

$$\text{s.t.} \quad x(k+\tau+1|k) = Ax(k+\tau|k) + Bu(k+\tau|k),$$

$$x(k|k) = x(k), \quad x(k+\tau+1|k) \in X_0, \quad u(k+\tau|k) \in U, \quad 0 \leq \tau \leq N-1,$$

obtains the solution $\mathbf{u}(k) \triangleq [u(k|k), \cdots, u(k+N-1|k)]$, and sends it to the actuator.

2: If $s(k) = 0$, the actuator sets $M^p(k+1) = \mathbf{u}(k)$, implements $u(k|k)$, and the sensor sends $x(k+1)$ to the operator. If $s(k) \geq 1$, the actuator implements $u(k|k-s(k))$ in $M^p(k)$, sets $M^p(k+1) = M^p(k)$, and the sensor sends $x(k+1)$ to the operator.

3: Repeat for $k = k+1$.

---

where λ and ϕ_N are defined in Table I. On the other hand, for α_N in Table I, $\alpha_N \searrow 0$ as $N \nearrow +\infty$, and ϕ_N is strictly increasing in N and upper bounded by ϕ_∞. Then, given any integer $S \geq 1$, there is a smallest integer $N^*(S) \geq S$ such that for all $N \geq N^*(S)$, it holds that:

$$\gamma_{N,S} \triangleq (1 - \frac{\lambda_{\min}(P)}{\phi_\infty}) \max\{(1+\alpha_{N-S-1}), (1+\alpha_{N-1}) \prod_{\ell=N-S}^{N-1} (1+\alpha_\ell)\} < 1.$$

Analogously, given any integer $S \geq 1$, there is a smallest integer $\hat{N}^*(S) \geq S$ such that for all

TABLE I

MAIN NOTATIONS USED IN THE FOLLOWING SECTIONS

$\lambda_{\max}(R)$ (resp. $\lambda_{\min}(R)$)	the maximum (resp. minimum) eigenvalue of matrix R
$\lambda \triangleq 1 - \frac{\lambda_{\max}(\bar{Q})}{\lambda_{\min}(\bar{P})}$	positive constant, $\lambda \in (0,1)$, see [22], defined with $\bar{Q}$, $\bar{P}$ introduced in AR-RHC
$\phi_N \triangleq \frac{\lambda_{\max}(\bar{P})\lambda_{\max}(P+K^TQK)}{\lambda_{\min}(\bar{P})}\frac{(1-\lambda^{N+1})}{1-\lambda}$	positive constant defined for all $N > 0$, with $\bar{Q}$, $\bar{P}$, and K introduced in AR-RHC
$\phi_\infty \triangleq \frac{\lambda_{\max}(\bar{P})\lambda_{\max}(P+K^TQK)}{\lambda_{\min}(\bar{P})(1-\lambda)}$	positive constant defined with $\bar{Q}$, $\bar{P}$, and K introduced in AR-RHC
$\alpha_N \triangleq \frac{\lambda_{\max}(K^TQK+\bar{A}^TP\bar{A})}{\lambda_{\min}(P)} \times \prod_{\kappa=0}^{N-1}(1-\frac{\lambda_{\min}(P)}{\phi_{\kappa+1}})$	positive constant defined for all $N > 0$, with $\bar{A}$ and K introduced in AR-RHC, and λ introduced here
$\rho_N \triangleq (1+\alpha_{N-1})(1-\frac{\lambda_{\min}(P)}{\phi_N})$	a discount factor
$W(x) \triangleq \Vert x\Vert^2_{\bar{P}}$	matrix $\bar{P}$ is the solution to Lyapunov equation (2)
V_N	the optimal value function of N-QP

$N \geq \hat{N}^*(S)$, it holds that

$$\hat{\gamma}_{N,S} \triangleq (1-\frac{\lambda_{\min}(P)}{\phi_\infty})^2(1+\alpha_{N-1})(1+\alpha_{N-2}) \times \Big(\max_{s\in\{1,\cdots,S\}}\prod_{\ell=2}^{s}(1-\frac{\lambda_{\min}(P)}{\phi_\infty})(1+\alpha_{N-\ell-1})\Big)\prod_{\ell=N-S}^{N-1}(1+\alpha_\ell) < 1.$$

One can easily verify $\hat{N}^*(S) \leq N^*(S)$. The following theorem characterizes the stability and infinite-horizon cost of system (1) under AR-RHC where $V_\ell(x)$ represents the value of the ℓ-QP parameterized by $x \in X$.

Theorem 2.1: (Stability and infinite-horizon cost) Let Assumptions 2.4, 2.1, 2.2 and 2.3 hold.

1) **(Exponential stability)** Suppose $N \geq \max\{N^*(S)+1, S+1\}$. Then system (1) under AR-RHC is exponentially stable when starting from X_0 with a rate of $\gamma_{N,S}$ in the sense that $V_{N-s(k-1)}(x(k)) \leq \gamma^k_{N,S}V_N(x(0))$. In addition, the infinite-horizon cost of system (1) under AR-RHC is bounded above by $\frac{1}{1-\gamma_{N,S}}V_N(x(0))$.
2) **(Asymptotic stability)** If $N \geq \max\{\hat{N}^*(S)+1, S+1\}$, then system (1) under AR-RHC is asymptotically stable when starting from X_0.

Remark 2.1: AR-RHC with Theorem 2.1 can be readily extended to several scenarios, including DoS attacks, measurement attacks and the combinations of such attacks. If the adversary launches a DoS attack on control commands, the actuator receives nothing and then performs Step 3 in AR-RHC. The adversary may produce the replay attacks on the measurements sent from the sensor to the operator. If this happens, then the operator does not send anything to the actuator and the actuator performs Step 3 in AR-RHC. •

III. Analysis

The proofs of Theorem 2.1 are collected in this section. In particular, the proofs for the intermediate lemmas are based on the corresponding results in our previous paper [34] on deception attacks. The proofs for the main theorem are new and not included in [34]. In the proof of Theorem 2.1, we choose $V_{N-s(k-1)}(x(k))$ as a Lyapunov function candidate. To analyze its convergence, we first establish several instrumental properties of V_N, including the monotonicity, diminishing rations with respect to N and decreasing property.

Recall the definitions of λ, α_N, ϕ_N, and ϕ_∞ summarized in Table I. It follows from [22] that $\lambda \in (0,1)$, and clearly, $1 \leq \phi_N \leq \phi_\infty$ for any $N \in \mathbb{Z}_{>0}$. Observe that the following holds for any $\kappa \in \mathbb{Z}_{>0}$:

$$\frac{\lambda_{\min}(P)}{\phi_{\kappa+1}} = \frac{\lambda_{\min}(P)}{\lambda_{\max}(P+K^TQK)}\frac{\lambda_{\min}(\bar{P})}{\lambda_{\max}(\bar{P})}\frac{1-\lambda}{1-\lambda^{\kappa+2}} \geq \frac{\lambda_{\min}(P)}{\lambda_{\max}(P+K^TQK)}\frac{\lambda_{\min}(\bar{P})}{\lambda_{\max}(\bar{P})}(1-\lambda) \in (0,1).$$

This ensures the monotonicity of α_N and, moreover, that $\alpha_N \searrow 0$ as $N \nearrow +\infty$.

We show the forward invariance property of system (1) in X_0 under Kx.

Lemma 3.1 (Forward invariance in X_0): The set X_0 is forward invariant for system (1) under the auxiliary controller Kx with the control constraint U; i.e., for any $x \in X_0$, it holds that $u = Kx \in U$ and $\bar{A}x \in X_0$.

Proof: The differences of W along the trajectories of the dynamics (1) under $u(k) = Kx(k)$, $x(k) = x$ can be characterized by:

$$W(x(k+1)) - W(x) = \|\bar{A}x(k+1)\|^2_{\bar{P}} - \|x(k)\|^2_{\bar{P}} = -\|x\|^2_{\bar{Q}} \leq -\lambda_{\min}(\bar{Q})\|x\|^2, \tag{3}$$

where $W(x)$, $\bar{A}$, $\bar{P}$ and $\bar{Q}$ are given in Table I, and in the second equality we apply the Lyapunov equation (2). Since $\bar{Q} > 0$, then $W(x(k+1)) \leq W(x)$. Since $x \in X_0$, so is $x(k+1)$. Since $X_0 \subseteq X$, we know that $u(k) \in U$ by Assumption 2.2. The forward invariance property of X_0 for system (1) follows. ■

On the other hand, one can see that the N-QP parameterized by $x \in X_0$ has at least one solution generated by the auxiliary controller.

Lemma 3.2 (Feasibility of the N-QP): For any $x \in X_0$, consider system (1) with $x(k|k) = x$ and $u(k+\tau|k) = Kx(k+\tau|k)$, for $0 \le \tau \le N-1$. Then, $\mathbf{u}(k)$ is a feasible solution to the N-QP parameterized by $x(k) \in X_0$.

Proof: It is a direct result of Lemma 3.1 and Assumption 2.2. ■

The following lemma demonstrates that V_N is bounded above and below by two quadratic functions, respectively.

Lemma 3.3: (Positive-definite and decrescent properties of V_N) The function V_N is quadratically bounded above and below as $\lambda_{\min}(P)\|x\|^2 \le V_N(x) \le \phi_N \|x\|^2$ for any $x \in X_0$.

Proof: Consider any $x \in X_0$. It is easy to see that $V_N(x) \ge \lambda_{\min}(P)\|x\|^2$, and thus positive definiteness of V_N follows. We now proceed to show that V_N is decrescent. In order to simplify the notations in the proof, we will drop the dependency on time k in what follows. Toward this end, we let $\{x(\tau)\}_{\tau \ge 0}$ be the solution produced by the system $x(\tau+1) = \bar{A}x(\tau)$, that is, the closed-loop system solution of the dynamics (1) under the auxiliary controller Kx, with initial state $x(0) = x \in X_0$. We denote $x(\tau|0) \equiv x(\tau)$ and $u(\tau|0) \equiv u(\tau)$. Recall the estimate (3):

$$W(x(\tau+1)) \le W(x(\tau)) - \lambda_{\min}(\bar{Q})\|x(\tau)\|^2 \le W(x(\tau)) - \frac{\lambda_{\max}(\bar{Q})}{\lambda_{\max}(\bar{P})} W(x(\tau)), \tag{4}$$

where we use the property that $\lambda_{\min}(\bar{P})\|x\|^2 \le W(x) \le \lambda_{\max}(\bar{P})\|x\|^2$. It follows from Lemma 3.2 that the sequence of control commands $u(\tau) = Kx(\tau)$ for $0 \le \tau \le N-1$ consists of a feasible solution to the N-QP parameterized by $x \in X_0$. Then we achieve the following on $V_N(x)$:

$$\begin{aligned} V_N(x) &\le \sum_{\tau=0}^{N-1} \left(\|x(\tau)\|_P^2 + \|Kx(\tau)\|_Q^2 \right) + \|x(N)\|_P^2 \\ &\le \sum_{\tau=0}^{N-1} \lambda_{\max}(P + K^T Q K)\|x(\tau)\|^2 + \lambda_{\max}(P)\|x(N)\|^2 \\ &\le \frac{\lambda_{\max}(P + K^T Q K)}{\lambda_{\min}(\bar{P})} \sum_{\tau=0}^{N-1} W(x(\tau)) + \frac{\lambda_{\max}(P)}{\lambda_{\min}(\bar{P})} W(x(N)). \end{aligned} \tag{5}$$

Substituting inequality (4) into (5), we obtain the following estimates on $V_N(x)$:

$$\begin{aligned} V_N(x) &\le \frac{\lambda_{\max}(P + K^T Q K)}{\lambda_{\min}(\bar{P})} W(x) \sum_{\tau=0}^{N-1} \lambda^\tau + \frac{\lambda_{\max}(P)}{\lambda_{\min}(\bar{P})} W(x)\lambda^N \\ &\le \frac{\lambda_{\max}(\bar{P})\lambda_{\max}(P + K^T Q K)}{\lambda_{\min}(\bar{P})} \frac{1 - \lambda^{N+1}}{1 - \lambda} \|x\|^2. \end{aligned}$$

where we use the fact $\lambda = 1 - \frac{\lambda_{\max}(\bar{Q})}{\lambda_{\max}(\bar{P})} \in (0,1)$ in [22]. The decrescent property of V_N immediately follows from the above relations. ■

Next, one can show that for any $x \in X_0$, $V_N(x)$ does not decrease as N increases.

Lemma 3.4 (Monotonicity of V_N): The optimal value function V_N is monotonic in N; i.e., for any $x \in X_0$, $V_{N'}(x) \leq V_N(x)$ for $N' < N$.

Proof: Consider $N' < N$, and denote by J_N and $J_{N'}$ the objective functions of the N-QP and the N'-QP, respectively. Let $\mathbf{u}_N$ be a solution to the N-QP parameterized by x, with $\mathbf{u}_N = [u(0), \ldots, u(N-1)]$, and let $\mathbf{u}_{N'}$, with $\mathbf{u}_{N'} = [u(0), \ldots, u(N'-1)]$, be a solution to the N'-QP parameterized by $x \in X_0$. We construct $\tilde{\mathbf{u}}_{N'} \in U^{N'}$, a truncated version of $\mathbf{u}_N$, in such a way that $\tilde{u}(k) = u(k)$ for $0 \leq k \leq N'-1$. Since $\mathbf{u}_N$ is a solution to the N-QP parameterized by x, then one can show that $\tilde{\mathbf{u}}_{N'}$ is a feasible solution to the N'-QP parameterized by x. This renders the following upper bound on $V_{N'}(x)$:

$$V_{N'}(x) = J_{N'}(x, \mathbf{u}_{N'}) \leq J_{N'}(x, \tilde{\mathbf{u}}_{N'}). \tag{6}$$

Denote by $\mathbf{x}_N \triangleq [x(0), \cdots, x(N)]$ the corresponding trajectory to $\mathbf{u}_N$ with initial state $x(0) = x$ and by $\tilde{\mathbf{x}}_{N'} \triangleq [\tilde{x}(0), \cdots, \tilde{x}_{N'}]$ the corresponding trajectory generated by the sequence of $\tilde{\mathbf{u}}_{N'}$ with the initial state $\tilde{x}(0) = x$. Since $\tilde{\mathbf{u}}_{N'}$ is a truncated version of $\mathbf{u}_N$, we have that $\tilde{x}(k) = x(k)$ for $0 \leq k \leq N'$. Denote further $\tilde{\mathbf{u}}_{N'} \triangleq [\tilde{u}(0), \cdots, \tilde{u}(N'-1)]$. Then we have

$$J_{N'}(x, \tilde{\mathbf{u}}_{N'}) = \sum_{k=1}^{N'} \left(\|\tilde{x}(k)\|_P^2 + \|\tilde{u}(k)\|_Q^2 \right) + \|\tilde{x}(N')\|_P^2$$

$$= \sum_{k=1}^{N'} \left(\|x(k)\|_P^2 + \|u(k)\|_Q^2 \right) + \|x(N')\|_P^2 \leq \sum_{k=1}^{N} \left(\|x(k)\|_P^2 + \|u(k)\|_Q^2 \right) + \|x(N)\|_P^2 = V_N(x).$$

The combination of (6) and the above relation establishes that $V_{N'}(x) \leq V_N(x)$ for $x \in X_0$. ■

The following lemma formalizes that for any $x \in X_0$, the difference between $V_{N+1}(x)$ and $V_N(x)$ decreases as N increases by noting that $V_N(x) \leq V_{N+1}(x)$ and α_N is strictly decreasing in N, where V_{N+1} and V_N are the optimal value functions for the $(N+1)$-QP and the N-QP, respectively. This property is referred to as the property of diminishing ratios of V_N in N by noting that $\alpha_N \searrow 0$ as $N \nearrow +\infty$.

Lemma 3.5: (The diminishing ratios of V_N in N) The optimal value function V_N is diminishingly increasing in N in such a fashion that $\frac{V_{N+1}(x) - V_N(x)}{V_N(x)} \leq \alpha_N$ for any $x \in X_0$.

Proof: Let $\mathbf{u}_N$, with $\mathbf{u}_N = [u(0), \ldots, u(N-1)]$, be a solution to the N-QP parameterized by $x \in X_0$. Let $\mathbf{x}_N = [x(0), \ldots, x(N)]$, $x(0) = x$, be the corresponding trajectory. Notice that $x(k) \in X_0$ for $0 \leq k \leq N$. We construct an extended version $\tilde{\mathbf{u}}_{N+1} \in U^{N+1}$ of $\mathbf{u}_N$ as $\tilde{\mathbf{u}}_{N+1} = [u(0), \ldots, u(N-1), Kx(N)]$. Since $x(N) \in X_0$, then $\tilde{x}(N+1) := \bar{A}x(N) \in X_0$ by Lemma 3.1, implying that $\tilde{\mathbf{u}}_{N+1}$ consists of a feasible solution to the $(N+1)$-QP parameterized by x. Then we establish the following upper bounds on $V_{N+1}(x)$:

$$V_{N+1}(x) \leq J_{N+1}(x, \tilde{\mathbf{u}}_{N+1}) = J_N(x, \mathbf{u}_N) + \|Kx(N)\|_Q^2 + \|\tilde{x}(N+1)\|_P^2 \leq V_N(x) + \varsigma\|x(N)\|^2, \tag{7}$$

where $\varsigma := \lambda_{\max}(K^T QK + \bar{A}^T P\bar{A})$. We now turn our attention to find a relation between $\|x(N)\|^2$ and $V_N(x)$. To achieve this, we will show the following holds for $\ell \in \{0, \cdots, N\}$ by induction:

$$V_\ell(x(N-\ell)) \leq \prod_{\kappa=\ell}^{N-1}(1 - \frac{\lambda_{\min}(P)}{\phi_{\kappa+1}})V_N(x). \tag{8}$$

It follows from Bellman's principle of optimality that

$$V_N(x) = \|x(0)\|_P^2 + \|u(0)\|_Q^2 + V_{N-1}(x(1)).$$

We can further see that $V_N(x) - V_{N-1}(x(1))$ is lower bounded in the following way:

$$V_N(x) - V_{N-1}(x(1)) \geq \lambda_{\min}(P)\|x\|^2 \geq \frac{\lambda_{\min}(P)}{\phi_N}V_N(x), \tag{9}$$

where we use the decrescent property in Lemma 3.3 in the last inequality. Rearrange terms in (9) and it renders that (8) holds for $\ell = N-1$.

Assume that (8) holds for some $\ell + 1 \in \{1, \cdots, N-1\}$; i.e., the following holds:

$$V_{\ell+1}(x(N-\ell-1)) \leq \prod_{\kappa=\ell+1}^{N-1}(1 - \frac{\lambda_{\min}(P)}{\phi_{\kappa+1}})V_N(x). \tag{10}$$

Similar to (9), it follows from Bellman's principle of optimality and Lemma 3.3 that

$$V_{\ell+1}(x(N-\ell-1)) - V_\ell(x(N-\ell)) \geq \lambda_{\min}(P)\|x(N-\ell-1)\|^2 \geq \frac{\lambda_{\min}(P)}{\phi_{\ell+1}}V_{\ell+1}(x(N-\ell-1)). \tag{11}$$

Combining (10) and (11) renders that

$$V_\ell(x(N-\ell)) \leq (1 - \frac{\lambda_{\min}(P)}{\phi_{\ell+1}})V_{\ell+1}(x(N-\ell-1)) \leq \prod_{\kappa=\ell}^{N-1}(1 - \frac{\lambda_{\min}(P)}{\phi_{\kappa+1}})V_N(x).$$

This implies (8) holds for ℓ. By induction, we conclude that (8) holds for $\ell \in \{0, \cdots, N\}$. Let $\ell = 0$ in (8), and we have that $V_0(x(N)) \leq \prod_{\kappa=0}^{N-1}(1 - \frac{\lambda_{\min}(P)}{\phi_{\kappa+1}})V_N(x)$, implying that $\|x(N)\|^2 \leq$

$\frac{1}{\lambda_{\min}(P)}\prod_{\kappa=0}^{N-1}(1-\frac{\lambda_{\min}(P)}{\phi_{\kappa+1}})V_N(x)$ by Lemma 3.3. By combining this relation with (7), we obtain the desired relation between V_{N+1} and V_N. ■

A relation between $V_N(x(k+1|k))$ and $V_N(x(k))$ for $x(k)\in X_0$, and $x(k+1|k)$ generated through the N-QP, is found next.

Lemma 3.6 (Decreasing property of V_N in X_0): With $x(k+1|k)$ generated through the N-QP starting from $x(k)$, the following decreasing property holds for any $x(k)\in X_0$:

$$V_N(x(k+1|k)) \leq \rho_N V_N(x(k)).$$

Proof: With Lemma 3.3 and 3.5, we reach the following relation between $V_N(x(k+1|k))$ and $V_N(x(k))$ for any $x(k)\in X_0$:

$$\begin{aligned}&V_N(x(k+1|k)) \leq (1+\alpha_{N-1})V_{N-1}(x(1)) \leq (1+\alpha_{N-1})(V_N(x(k)) - \|x(k)\|_P^2)\\ &\leq (1+\alpha_{N-1})(V_N(x(k)) - \lambda_{\min}(P)\|x(k)\|^2) \leq (1+\alpha_{N-1})(1-\frac{\lambda_{\min}(P)}{\phi_N})V_N(x(k)),\end{aligned}$$

where Lemma 3.5 and Lemma 3.3 are used in the first and last inequalities, respectively, by noting that $x(k+1|k)$ and $x(k)$ in X_0. ■

Proof of Theorem 2.1:

Proof: **[Part 1: Exponential stability]** Let us consider the first part of $N\geq\max\{N^*(S)+1, S+1\}$. Recall that $x(0)\in X_0$ and the state constraint X_0 is enforced in the N-QP. Repeatedly apply Lemma 3.2 and we have that $x(k)\in X_0$ for all $k\geq 0$. We now distinguish four cases:

Case 1: $\vartheta(k)=1$ and $\vartheta(k-1)=0$. For this case, $s(k)=1$, $s(k-1)=0$, and we have

$$\begin{aligned}&V_{N-s(k)}(x(k+1)) = V_{N-1}(x(k+1)) \leq \rho_{N-1}V_{N-1}(x(k))\\ &\leq \rho_{N-1}V_N(x(k)) = \rho_{N-1}V_{N-s(k-1)}(x(k)),\end{aligned}$$

where the first inequality uses Lemma 3.6 and the principle of optimality, and the second one exploits Lemma 3.4.

Case 2: $\vartheta(k)=\vartheta(k-1)=0$. Here, $s(k)=s(k-1)=0$. By Lemma 3.6, we have

$$V_{N-s(k)}(x(k+1)) = V_N(x(k+1)) \leq \rho_N V_N(x(k)) = \rho_N V_{N-s(k-1)}(x(k)).$$

Case 3: $\vartheta(k)=\vartheta(k-1)=1$. Note that $s(k)=s(k-1)+1$, and then

$$V_{N-s(k)}(x(k+1)) \leq \rho_{N-s(k)}V_{N-s(k)}(x(k)) \leq \rho_{N-s(k)}V_{N-s(k-1)}(x(k)),$$

where the first inequality utilizes Lemmas 3.6 and the principle of optimality, and the second one exploits Lemma 3.4.

Case 4: $\vartheta(k) = 0$ and $\vartheta(k-1) = 1$. For this case, we have $s(k) = 0$, $s(k-1) \geq 1$ and thus

$$V_{N-s(k)}(x(k+1)) = V_N(x(k+1)) \leq \rho_N V_N(x(k)) \leq \rho_N \prod_{\ell=N-s(k-1)}^{N-1} (1+\alpha_\ell) V_{N-s(k-1)}(x(k)),$$

where the last inequality repeatedly applies Lemma 3.5.

Combine the above four cases, and it renders the following:

$$\begin{aligned} V_{N-s(k)}(x(k+1)) &\leq \max\{\max_{s\in\{1,\cdots,S\}}\{\rho_{N-s}\}, \rho_N \max_{s=1,\cdots,S}\{\prod_{\ell=N-s}^{N-1}(1+\alpha_\ell)\}\} V_{N-s(k-1)}(x(k)) \\ &\leq \gamma_{N,S} V_{N-s(k-1)}(x(k)). \end{aligned} \tag{12}$$

Since $0 < \gamma_{N,S} < 1$, $\{V_{N-s(k-1)}(x(k))\}$ exponentially diminishes, and the following holds:

$$V_{N-s(k-1)}(x(k)) \leq \gamma_{N,S}^k V_N(x(0)). \tag{13}$$

Recall $N \geq S+1$. It follows from (13) that the infinite-horizon cost is characterized as follows:

$$\sum_{k=0}^{+\infty} (\|x(k)\|_P^2 + \|u(k)\|_Q^2) \leq \sum_{k=0}^{+\infty} V_{N-s(k-1)}(x(k)) \leq \sum_{k=0}^{+\infty} \gamma_{N,S}^k V_N(x(0)) = \frac{1}{1-\gamma_{N,S}} V_N(x(0)).$$

We then have finished the proofs for the first part.

[Part 2: Asymptotic stability] We now proceed to show the second part of $N \geq \max\{\hat{N}^*(S)+1, S+1\}$. Towards this end, we partition the time horizon $\{0, 1, \cdots\}$ into a sequence of subsets $\{C_1, A_1, C_2, A_2, \cdots\}$ where $C_i = \{c_i^L, \cdots, c_i^U\}$ and $A_i = \{a_i^L, \cdots, a_i^U\}$ with for $k \in C_i$, then $\vartheta(k) = 0$; and $k \in A_i$, then $\vartheta(k) = 1$. Note that $c_0^L = 0$ and $a_i^L = c_i^U + 1$.

Case 1: $k \in C_i \setminus \{c_i^L\}$. Note that $s(k) = s(k-1) = 0$ for all $k \in C_i \setminus \{c_i^L\}$. By Lemma 3.6, we have

$$V_{N-s(k)}(x(k+1)) \leq \rho_N V_{N-s(k-1)}(x(k)), \quad \forall k \in C_i \setminus \{c_i^L\}.$$

Case 2: $k = a_i^L$. Note that $\vartheta(a_i^L) = 1$ and $\vartheta(a_i^L - 1) = 0$. By Case 1 in Part 1, we have

$$V_{N-s(a_i^L)}(x(a_i^L+1)) \leq \rho_{N-1} V_{N-s(a_i^L-1)}(x(a_i^L)).$$

Case 3: $k = A_i \setminus \{a_i^L\}$. Recall that $\vartheta(k) = 1$ for $k \in A_i$. By repeating the result of Case 3 in Part 1, we have

$$V_{N-s(k)}(x(k+1)) \leq \prod_{\ell=2}^{k-a_i^L} \rho_{N-\ell} V_{N-s(a_i^L)}(x(a_i^L+1)), \quad \forall k \in A_i \setminus \{a_i^L\}.$$

Case 4: $k = c_{i+1}^L = a_i^U + 1$. Note that $\vartheta(c_{i+1}^L) = 0$ and $\vartheta(c_{i+1}^L - 1) = 1$. By Case 4 in Part 1, it holds that

$$V_{N-s(c_{i+1}^L)}(x(c_{i+1}^L + 1)) \leq \rho_N \prod_{\ell=N-s(c_{i+1}^L-1)}^{N-1} (1+\alpha_\ell) V_{N-s(c_{i+1}^L-1)}(x(c_{i+1}^L)).$$

The combination of the above four relations renders the following:

$$\begin{aligned}
V_{N-s(c_{i+1}^L)}(x(c_{i+1}^L + 1)) &\leq \rho_N \prod_{\ell=N-s(c_{i+1}^L-1)}^{N-1} (1+\alpha_\ell) V_{N-s(c_{i+1}^L-1)}(x(c_{i+1}^L)) \\
&= \rho_N \prod_{\ell=N-s(c_{i+1}^L-1)}^{N-1} (1+\alpha_\ell) V_{N-s(c_{i+1}^L-1)}(x(a_i^U + 1)) \\
&\leq \rho_N \prod_{\ell=2}^{a_i^U - a_i^L} \rho_{N-\ell} \prod_{\ell=N-s(c_{i+1}^L-1)}^{N-1} (1+\alpha_\ell) V_{N-s(c_{i+1}^L-1)}(x(a_i^L + 1)) \\
&\leq \rho_N \rho_{N-1} \prod_{\ell=2}^{a_i^U - a_i^L} \rho_{N-\ell} \prod_{\ell=N-s(c_{i+1}^L-1)}^{N-1} (1+\alpha_\ell) V_{N-s(c_{i+1}^L-1)}(x(a_i^L)) \\
&= \rho_N \rho_{N-1} \prod_{\ell=2}^{a_i^U - a_i^L} \rho_{N-\ell} \prod_{\ell=N-s(c_{i+1}^L-1)}^{N-1} (1+\alpha_\ell) V_{N-s(c_{i+1}^L-1)}(x(c_i^U + 1)) \\
&\leq \hat{\gamma}_{N,S} V_{N-s(c_{i+1}^L-1)}(x(c_i^L)),
\end{aligned}$$

where the four inequalities sequentially apply Cases 4 to 1. Since $\hat{\gamma}_{N,S} \in (0,1)$, the subsequence $\{V_{N-s(c_{i+1}^L-1)}(x(c_{i+1}^L))\}$ exponentially decreases.

By the above four cases, it is not difficult to verify that the following holds for all $k \in A_i \cup C_i \setminus \{c_i^L\}$:

$$V_{N-s(k-1)}(x(k)) \leq \max\{\rho_{N-1}, 1\} \rho_N \max_{s\in\{2,\cdots,S\}} \prod_{\ell=2}^{s} \rho_{N-\ell} \prod_{\ell=N-s(c_{i+1}^L-1)}^{N-1} (1+\alpha_\ell) V_{N-s(c_{i+1}^L-1)}(x(c_i^L)).$$

Hence, the whole sequence $\{V_{N-s(k-1)}(x(k))\}$ diminishes. It establishes the asymptotical stability.

■

IV. Discussion

A. Explicit upper bounds on $N^*(S)$ and $\hat{N}^*(S)$

Consider $S \geq 2$ and let $\chi \triangleq (1 - \frac{\lambda_{\min}(P)}{\phi_\infty})$ and $\psi \triangleq \frac{\lambda_{\max}(K^T QK + \bar{A}^T P \bar{A})}{\lambda_{\min}(P)}$. Note that

$$\gamma_{N,S} \leq (1 - \frac{\lambda_{\min}(P)}{\phi_\infty})(1 + \alpha_{N-1}) \prod_{\ell=N-S-1}^{N-1} (1 + \alpha_\ell)$$
$$\leq \chi(1 + \alpha_{N-S-1})^{S+2} \leq \beta_{N,S} \triangleq \chi(1 + \psi\chi^{N-S-1})^{S+2}. \quad (14)$$

So it suffices to find N such that $\beta_{N,S} < 1$. The relation $\beta_{N,S} < 1$ is equivalent to the following:

$$N - S - 1 > \frac{\ln\left(\frac{1}{\psi}(\chi^{-\frac{1}{S+2}} - 1)\right)}{\ln \chi} = \frac{\ln(\chi^{-\frac{1}{S+2}} - 1) - \ln \psi}{\ln \chi}.$$

Hence, an explicit upper bound on $N^*(S)$ is $\Pi_E(S) \triangleq S + 1 + \frac{\ln(\chi^{-\frac{1}{S+2}} - 1) - \ln \psi}{\ln \chi}$.

We now move to find an explicit upper bound on $\hat{N}^*(S)$. Note that

$$\hat{\gamma}_{N,S} \leq (1 - \frac{\lambda_{\min}(P)}{\phi_\infty})^2(1 + \alpha_{N-1})(1 + \alpha_{N-2})\big(\max_{s\in\{1,\cdots,S\}} \prod_{\ell=2}^{s}(1 - \frac{\lambda_{\min}(P)}{\phi_\infty})(1 + \alpha_{N-\ell-1})\big) \prod_{\ell=N-S}^{N-1} (1 + \alpha_\ell)$$
$$\leq (1 - \frac{\lambda_{\min}(P)}{\phi_\infty})^{S+1}(1 + \alpha_{N-1})(1 + \alpha_{N-2})(1 + \alpha_{N-S-1})^{S-1} \prod_{\ell=N-S}^{N-1} (1 + \alpha_\ell)$$
$$\leq (1 - \frac{\lambda_{\min}(P)}{\phi_\infty})^{S+1}(1 + \alpha_{N-S-1})^{2S+1} = \chi^{S+1}(1 + \psi\chi^{N-S-1})^{2S+1}.$$

So, an explicit upper bound on $\hat{N}^*(S)$ is $\Pi_A(S) \triangleq S + 1 + \frac{\ln(\chi^{-\frac{S+1}{2S+1}} - 1) - \ln \psi}{\ln \chi}$. This pair of upper bounds clearly demonstrate that a higher computational complexity; i.e., a larger N, is caused by a larger S, indicating that the adversary is less energy constrained. On the other hand, the second term in $\Pi_A(S)$ approaches a constant as S goes to infinity. So $\Pi_A(S)$ can be upper bounded by an affine function. However, the second term in $\Pi_E(S)$ dominates when S is large. That is, exponential stability demands a much higher cost than asymptotic stability when S is large.

B. A reverse scenario

Reciprocally, for any horizon $N \geq 1$, there is a largest integer $S^*(N) \leq N - 1$ (resp. $\hat{S}^*(N) \leq N - 1$) such that for all $S \leq S^*(N)$ (resp. $S \leq \hat{S}^*(N)$), it holds that $\gamma_{N,S} < 1$ (resp. $\hat{\gamma}_{N,S} < 1$). Theorem 2.1 still applies to this reverse scenario and characterizes the "security level" or "amount of resilience" that the proposed receding-horizon control algorithm possesses.

V. CONCLUSIONS

In this paper, we have studied a resilient control problem where a linear dynamic system is subject to the replay and DoS attacks. We have proposed a variation of the receding-horizon control law for the operator and analyzed system stability and performance degradation.

REFERENCES

[1] 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.

[2] S. Amin, X. Litrico, S.S. Sastry, and A.M. Bayen. Stealthy deception attacks on water SCADA systems. In *Hybrid systems: Computation and Control*, pages 161–170, Stockholm, Sweden, 2010.

[3] S. Amin, G.A. Schwartz, and S.S. Sastry. Security of interdependent and identical networked control systems. *Automatica*, July 2010. submitted.

[4] G.K. Befekadu, V. Gupta, and P.J. Antsaklis. Risk-sensitive control under a class of denial-of-service attack models. In *American Control Conference*, pages 643–648, San Francisco, USA, June 2011.

[5] S. Bhattacharya and T. Basar. Game-theoretic analysis of an aerial jamming attack on a UAV communication network. In *American Control Conference*, pages 818–823, Baltimore, USA, June 2010.

[6] S. Bhattacharya and T. Basar. Graph-theoretic approach for connectivity maintenance in mobile networks in the presence of a jammer. In *IEEE Int. Conf. on Decision and Control*, pages 3560–3565, Atlanta, USA, December 2010.

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

[8] R. W. Brockett and D. Liberzon. Quantized feedback stabilization of linear systems. *IEEE Transactions on Automatic Control*, 45(7):1279–1289, 2000.

[9] B. Ding. Stabilization of linear systems over networks with bounded packet loss and its use in model predictive control. *Automatica*, 47(9):2526–2533, October 2011.

[10] N. Falliere, L.O. Murchu, and E. Chien. W32.stuxnet dossier. *Symantec Corporation*, 2011.

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

[12] V. Gupta and N. Martins. On stability in the presence of analog erasure channels between controller and actuator. *IEEE Transactions on Automatic Control*, 55(1):175–179, 2010.

[13] V. Gupta, B. Sinopoli, S. Adlakha, and A. Goldsmith. Receding horizon networked control. In *Allerton Conf. on Communications, Control and Computing*, Illinois, USA, September 2006.

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

[15] O.C. Imer, S. Yuksel, and T. Basar. Optimal control of LTI systems over communication networks. *Automatica*, 42(9):1429–1440, 2006.

[16] K. Kobayashi and K. Hiraishi. Self-triggered model predictive control with delay compensation for networked control systems. In *acies*, pages 3200–3205, 2012.

[17] D. Liberzon and J.P. Hespanha. Stabilization of nonlinear systems with limited information feedback. *IEEE Transactions on Automatic Control*, 50(6):910–915, 2005.

[18] G.P. Liu, J.X. Mu, D. Rees, and S.C. Chai. Design and stability analysis of networked control systems with random communication time delay using the modified MPC. *International Journal of Control*, 79(4):288–297, April 2006.

[19] 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.

[20] Y. Mo, T. Kim, K. Brancik, D. Dickinson, L. Heejo, A. Perrig, and B. Sinopoli. Cyber-physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(195-209):215, 2012.

[21] Y. Mo and B. Sinopoli. Secure control against replay attacks. In *Allerton Conf. on Communications, Control and Computing*, Illinois, USA, September 2009.

[22] 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.

[23] 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.

[24] G.N. Nair, F. Fagnani, S. Zampieri, and R.J. Evans. Feedback control under data rate constraints: an overview. *Proceddings of IEEE Special Issue on Technology of Networked Control Systems*, 95(1):108–137, 2007.

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

[26] D. Mu noz de la Peña and P.D. Christofides. Lyapunov-based model predictive control of nonlinear systems subject to data losses. *IEEE Transactions on Automatic Control*, 53(9):2076–2089, October 2008.

[27] F. Pasqualetti, A. Bicchi, and F. Bullo. Consensus computation in unreliable networks: A system theoretic approach. *IEEE Transactions on Automatic Control*, February 2010. To appear.

[28] F. Pasqualetti, R. Carli, and F. Bullo. A distributed method for state estimation and false data detection in power networks. In *IEEE Int. Conf. on Smart Grid Communications*, pages 469–474, October 2011.

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

[30] S. Sundaram and C.N. Hadjicostis. Distributed function calculation via linear iterative strategies in the presence of malicious agents. *IEEE Transactions on Automatic Control*, 56(7):1731–1742, 2011.

[31] A. Teixeira, S. Amin, H. Sandberg, K.H. Johansson, and S.S. Sastry. Cyber security analysis of state estimators in electric power systems. In *IEEE Int. Conf. on Decision and Control*, pages 5991–5998, Atlanta, USA, December 2010.

[32] L. Xie, Y. Mo, and B. Sinopoli. False data injection attacks in electricity markets. In *IEEE Int. Conf. on Smart Grid Communications*, pages 226–231, Gaithersburg, USA, October 2010.

[33] M. Zhu and S. Martínez. Attack-resilient distributed formation control via online adaptation. In *IEEE Int. Conf. on Decision and Control*, pages 6624–6629, Orlando, FL, USA, December 2011.

[34] M. Zhu and S. Martínez. Stackelberg game analysis of correlated attacks in cyber-physical system. In *American Control Conference*, pages 4063–4068, June 2011.

[35] M. Zhu and S. Martínez. On distributed resilient consensus against replay attacks in adversarial networks. In *American Control Conference*, pages 3553 – 3558, Montreal, Canada, June 2012.