On the Performance Analysis of Resilient Networked Control Systems Under Replay Attacks

Minghui Zhu and Sonia Martínez

***Abstract*—This technical note 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 deal with the replay attacks and analyze the resulting system performance degradation. A class of competitive (resp. cooperative) resource allocation problems for resilient networked control systems is also investigated.**

***Index Terms*— Networked control systems, resilient control.**

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 technical note 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 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 technical note is to design and analyze resilient controllers against replay attacks.

Literature Review: Recently, the cyber security of control systems has received increasing attention. The research effort has been devoted to studying two aspects: attack detection and attack-resilient control. Regarding attack detection, a particular class of cyber attacks, namely *false data injection*, against state estimation is studied in [26], [29], [30]. The paper [19] studies the detection of the *replay attacks*, which maliciously repeat transmitted data. In the context of multi-agent systems, the papers of [25], [28] determine conditions under which consensus multi-agent systems can detect misbehaving agents. As for attack-resilient control, the papers [2], [32], [33] 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], [9]. More specifically, the papers [1], [9] 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 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 [12]. Key issues include band-limited channels [15], [22], quantization [6], [21], packet dropout [10], [13], [27], delay [5] and sampling [23]. Receding-horizon networked control is studied in [7], [11], [24] for package dropouts and in [14], [16] for transmission delays. Package dropouts and DoS attacks (resp. transmission delays and replay attacks) cause similar affects to control systems. So the existing receding-horizon control approaches exhibit the robustness to certain classes of DoS and replay attacks under their respective assumptions. However, none of these papers characterizes the performance degradation of receding-horizon control induced by the communication unreliability.

Contributions: We study a variation of the receding-horizon control under the replay attacks. 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. By using such relation, we characterize a class of competitive (resp. cooperative) resource allocation problems for resilient networked control systems as convex games (resp. programs). The preliminary results are published in [33] where receding-horizon control is used to deal with a class of deception attacks. The complete version can be found in [36].

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 technical note, $u = Kx$ will be referred to as the auxiliary controller. We then impose the following condition on the constraint sets.

Manuscript received January 17, 2013; revised March 26, 2013; accepted July 12, 2013. Date of publication August 28, 2013; date of current version February 19, 2014. This work was supported by the AFOSR Grant 11RSL548. Recommended by Associate Editor L. Schenato.

M. Zhu is with the Department of Electrical Engineering, Pennsylvania State University, University Park, PA 16802 USA (e-mail: muz16@psu.edu).

S. Martínez is with the Department of Mechanical and Aerospace Engineering, University of California, San Diego, La Jolla CA 92093 USA (e-mail: soniamd@ucsd.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TAC.2013.2279896

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 in memory; i.e., $M^a(k+1) = \Upsilon$. In this case, $\vartheta(k) = 0$ and Υ 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 the adversary 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 [8], [18]. This class of attacks can be easily detected by attaching a time stamp to each control command. In the remainder of the technical note, we assume that the attacks can always be detected and focus on the design and analysis of resilient controllers against them.

C. Attack-Resilient Receding-Horizon Control Law

Here we propose **attack-resilient receding-horizon control law**, (for short, AR-RHC), a variation of the receding-horizon control in; e.g. [16], [17], to deal with the replay attacks. AR-RHC is formally stated in Algorithm 1. In particular, at each time instant, the plant stores the computed control sequence which will be used in response to replay attacks in the near future. The terminal state cost is chosen to coincide with the running state cost. This is instrumental for analyzing the Lyapunov function in terms of the computing horizon and further the performance degradation in Theorem 2.1.

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 $X_0 \triangleq \{x \in \mathbb{R}^n \mid \|x\|_{\bar{P}}^2 \leq c\} \subseteq X$.

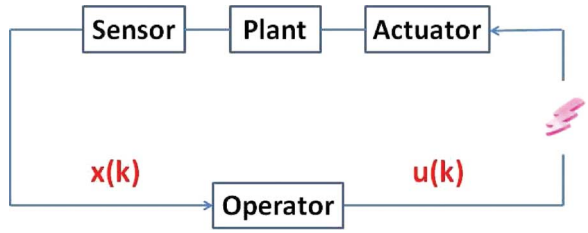

Fig. 1. Closed-loop system with attacks from the operator to the actuator.

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 $x(k) \in X$:

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

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 receives $\mathbf{u}(k)$, 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 $k = k+1$.

In what follows, we present the results characterizing the stability and infinite-horizon cost induced by AR-RHC. See Table I, for the main notations employed. Notice that the following property holds:

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

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

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

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

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

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 [20], 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
$W(x) \triangleq \|x\|_P^2$	matrix $\bar{P}$ is the solution to Lyapunov equation (2)
V_N	the optimal value function of N-QP

One can easily verify $\hat{N}^*(S) \le N^*(S)$. 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 2.1, 2.2 and 2.3 hold.

1) (**Exponential stability**) Suppose $N \ge \max\{N^*(S)+1, S+1\}$. 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 $V_{N-s(k-1)}(x(k)) \le \gamma_{N,S}^k V_N(x(0))$. In addition, the infinite-horizon cost of system (1) under AR-RHC is bounded above by $(1/(1-\gamma_{N,S}))V_N(x(0))$.
2) (**Asymptotic stability**) If $N \ge \max\{\hat{N}^*(S)+1, S+1\}$, then system (1) under AR-RHC is asymptotically stable when starting from X_0.

III. Discussion and Simulations

A. Extensions

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.

B. Explicit Upper Bounds on $N^*(S)$ and $\hat{N}^*(S)$

Consider $S \ge 2$ and let $\chi \triangleq (1-(\lambda_{\min}(P)/\phi_\infty))$ and $\psi \triangleq \lambda_{\max}(K^TQK+\bar{A}^TP\bar{A})/\lambda_{\min}(P)$. Note that

$$\begin{aligned}\gamma_{N,S} &\le \left(1-\frac{\lambda_{\min}(P)}{\phi_\infty}\right)(1+\alpha_{N-1})\prod_{\ell=N-S-1}^{N-1}(1+\alpha_\ell)\\ &\le \chi(1+\alpha_{N-S-1})^{S+2}\\ &\le \beta_{N,S}\\ &\triangleq \chi(1+\psi\chi^{N-S-1})^{S+2}. \end{aligned} \tag{3}$$

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

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

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

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

$$\begin{aligned}\hat{\gamma}_{N,S} &\le \left(1-\frac{\lambda_{\min}(P)}{\phi_\infty}\right)^2(1+\alpha_{N-1})(1+\alpha_{N-2})\\ &\quad\times\left(\max_{s\in\{1,\cdots,S\}}\prod_{\ell=2}^{s}\left(1-\frac{\lambda_{\min}(P)}{\phi_\infty}\right)(1+\alpha_{N-\ell-1})\right)\\ &\quad\times\prod_{\ell=N-S}^{N-1}(1+\alpha_\ell)\\ &\le \left(1-\frac{\lambda_{\min}(P)}{\phi_\infty}\right)^{S+1}(1+\alpha_{N-1})(1+\alpha_{N-2})\\ &\quad\times(1+\alpha_{N-S-1})^{S-1}\prod_{\ell=N-S}^{N-1}(1+\alpha_\ell)\\ &\le \left(1-\frac{\lambda_{\min}(P)}{\phi_\infty}\right)^{S+1}(1+\alpha_{N-S-1})^{2S+1}\\ &= \chi^{S+1}(1+\psi\chi^{N-S-1})^{2S+1}.\end{aligned}$$

So, an explicit upper bound on $\hat{N}^*(S)$ is $\Pi_A(S) \triangleq S+1+((\ln(\chi^{-((S+1)/(2S+1))}-1)-\ln\psi)/\ln\chi)$. 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. So exponential stability demands a much higher cost than asymptotic stability when S is large.

C. A Reverse Scenario

Reciprocally, for any horizon $N \ge 1$, there is a largest integer $S^*(N) \le N-1$ (resp. $\hat{S}^*(N) \le N-1$) such that for all $S \le S^*(N)$ (resp. $S \le \hat{S}^*(N)$), 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.

D. Optimal Resilience Management

The analysis of Theorem 2.1 quantifies the cost and constraints that allow the AR-RHC algorithm to work despite consecutive attacks under limited computation capabilities. These metrics can be used for optimal resilience management of a network as follows.

As [3], we consider a set of players $V \triangleq \{1, \cdots, N\}$ where the players share a communication network and each of them is associated with a decoupled dynamic system

$$x_i(k+1) = A_i x_i(k) + B_i u_i(k). \tag{4}$$

Each player i uses his own AR-RHC with horizon N_i. The notations in the previous sections can be defined analogously for each player and the notations of player i will be indexed by i.

By (3), we associate player i with the following cost function:

$$\mathcal{C}_i(M) = \left(1 + \psi_i \chi_i^{N_i - \mathcal{S}(\mathbf{1}^T M)}\right)^{\mathcal{S}(\mathbf{1}^T M)+1} + \frac{1}{2} a_i M_i^2 \tag{5}$$

where $M_i \in [M_{i,\min}, M_{i,\max}] \subset \mathbb{R}_{>0}$ is the security investment of player i, $a_i \in \mathbb{R}_{>0}$ is a weight on the security cost the and $\mathbf{1}$ is the vector with N ones. The non-negative real value $\mathcal{S}(\mathbf{1}^T M)$ represents the security level given the investment vector M of all players, where $\mathcal{S} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is convex, non-decreasing, and smooth. We assume that each player has a fixed computational power, and so N_i is fixed. The players need to make the investment such that

$$\mathcal{S}(\mathbf{1}^T M) \leq \min_{i \in V} S_i^*(N_i). \tag{6}$$

Remark 3.1: Note that S is an integer in (3). In (5) and (6), we use the real value of $\mathcal{S}(\mathbf{1}^T M)$ as an approximation. •

We now compute the first-order partial derivative of $\mathcal{C}_i$ as follows:

$$\frac{\partial \mathcal{C}_i}{\partial M_i} = a_i M_i - \ln\left(1 + \psi_i \chi_i^{N_i - \mathcal{S}(\mathbf{1}^T M)}\right) \times \left(1 + \psi_i \chi_i^{N_i - \mathcal{S}(\mathbf{1}^T M)}\right)^{\mathcal{S}(\mathbf{1}^T M)+1} (\ln \chi_i) \psi_i \chi_i^{N_i - \mathcal{S}_i(M)} \left(\frac{\partial \mathcal{S}}{\partial y}\right)^2$$

where we use the shorthand $y \triangleq \mathbf{1}^T M$. Recall that $\chi_i \in (0, 1]$ and $\mathcal{S}$ is non-decreasing and convex. We further derive the second-order partial derivative $\partial^2 \mathcal{C}_i / \partial M_i^2 \geq 0$ and $\mathcal{C}_i$ is convex in M_i. Analogously, one can show that $\mathcal{C}_i$ is convex in M.

1) Competitive Resource Allocation Scenario: Consider a *resilience management game*, where each player i minimizes his cost $\mathcal{C}_i(M)$, subject to the common constraint (6) and his private constraint $M_i \in [M_{i,\min}, M_{i,\max}] \subset \mathbb{R}_{>0}$. Since $\mathcal{C}_i$ and $\mathcal{S}$ are convex in M_i, then the game is a generalized convex game. The distributed algorithms in [31] can be directly utilized to numerically compute a Nash equilibrium of the resilience management game, and the algorithms in [31] are able to tolerate transmission delays and packet dropouts.

Remark 3.2: The paper [3] considers a set of identical and independent networked control systems and each of them aims to solve an infinite-horizon LQG problem. The authors study a different security game where the decisions of each player are binary, participating in the security investment or not. •

2) Cooperative Resource Allocation Scenario: Consider a *resilience management optimization problem*, where the players aim to collectively minimize $\sum_{i \in V} \mathcal{C}_i(M)$, subject to the global constraint (6) and the private constraint $M_i \in [M_{i,\min}, M_{i,\max}] \subset \mathbb{R}_{>0}$. Since $\mathcal{C}_i$ and $\mathcal{S}$ are convex, then the problem is a convex program. The distributed algorithms in [34] can be directly exploited to numerically compute a global minimizer of this problem, and the algorithms in [34] are robust to the dynamic changes of inter-player topologies.

E. Simulations

In this section, we provide a numerical example to illustrate the performance of our algorithm. The set of system parameters are given as follows:

$$A = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}, \quad B = \begin{bmatrix} 2 \\ 1 \end{bmatrix}, \quad K = [-3.25 \ \ -3]$$

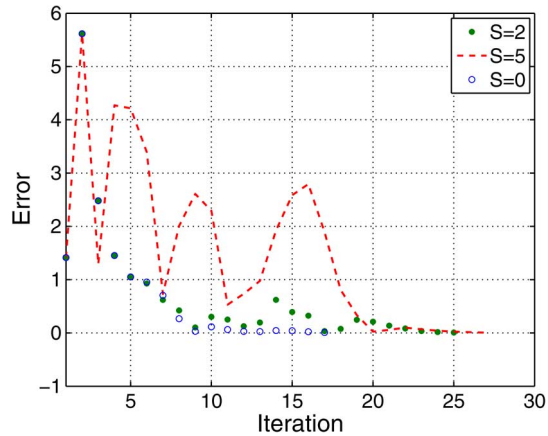

Fig. 2. Trajectories of $\|x(k)\|^2$ under the attack-resilient receding-horizon control algorithm for different values of S.

$$P = I, \quad Q = 1, \quad \bar{Q} = I,$$
$$\bar{P} = \begin{bmatrix} 25.6667 & 13.3333 \\ 13.3333 & 8.2963 \end{bmatrix}, \quad c = 100, \quad u_{\max} = 500.$$

Fig. 2 shows the temporal evolution of $\|x(k)\|^2$ under three attacking horizons $S = 0, 2, 5$. One can see that a larger S induces a longer time to converge, and larger oscillation before reaching the equilibrium. In our simulations, a smaller horizon $N = 15$ than the one determined theoretically is already sufficient to achieve system stabilization.

IV. Conclusions

In this technical note, 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. We have also studied a class of competitive (resp. cooperative) resource allocation problems for resilient networked control systems. Extensions to multi-agent systems will be considered in the future.

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*. Stockholm, Sweden: Springer, 2009, pp. 31–45.

[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*. Stockholm, Sweden: Springer, 2010, pp. 161–170.

[3] S. Amin, G. A. Schwartz, and S. S. Sastry, "Security of interdependent and identical networked control systems," *Automatica*, vol. 49, pp. 186–192, 2013.

[4] G. K. Befekadu, V. Gupta, and P. J. Antsaklis, "Risk-sensitive control under a class of denial-of-service attack models," in *Proc. American Control Conf.*, San Francisco, CA, Jun. 2011, pp. 643–648.

[5] M. S. Branicky, S. M. Phillips, and W. Zhang, "Stability of networked control systems: Explicit analysis of delay," in *Proc. American Control Conf.*, Chicago, IL, 2000, pp. 2352–2357.

[6] R. W. Brockett and D. Liberzon, "Quantized feedback stabilization of linear systems," *IEEE Trans. Autom. Control*, vol. 45, no. 7, pp. 1279–1289, Jul. 2000.

[7] B. Ding, "Stabilization of linear systems over networks with bounded packet loss and its use in model predictive control," *Automatica*, vol. 47, no. 9, pp. 2526–2533, Oct. 2011.

[8] N. Falliere, L. O. Murchu, and E. Chien, W32.Stuxnet Dossier Symantec Corporation, 2011.

[9] A. Gupta, C. Langbort, and T. Basar, "Optimal control in the presence of an intelligent jammer with limited actions," in *Proc. IEEE Int. Conf. Decision and Control*, Atlanta, GA, Dec. 2010, pp. 1096–1101.

[10] V. Gupta and N. Martins, "On stability in the presence of analog erasure channels between controller and actuator," *IEEE Trans. Autom. Control*, vol. 55, no. 1, pp. 175–179, Jan. 2010.
[11] V. Gupta, B. Sinopoli, S. Adlakha, and A. Goldsmith, "Receding horizon networked control," in *Proc. Allerton Conf. Communications, Control and Computing*, Urbana-Champaign, IL, Sep. 2006.
[12] J. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proc. IEEE Special Issue on Technology of Networked Control Systems*, vol. 95, no. 1, pp. 138–162, 2007.
[13] O. C. Imer, S. Yuksel, and T. Basar, "Optimal control of LTI systems over communication networks," *Automatica*, vol. 42, no. 9, pp. 1429–1440, 2006.
[14] K. Kobayashi and K. Hiraishi, "Self-triggered model predictive control with delay compensation for networked control systems," in *Acies*, 2012, pp. 3200–3205.
[15] D. Liberzon and J. P. Hespanha, "Stabilization of nonlinear systems with limited information feedback," *IEEE Trans. Autom. Control*, vol. 50, no. 6, pp. 910–915, Jun. 2005.
[16] 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," *Int. J. Control*, vol. 79, no. 4, pp. 288–297, Apr. 2006.
[17] D. Q. Mayne, J. B. Rawlings, C. V. Rao, and P. O. M. Scokaert, "Constrained model predictive control: Stability and optimality," *Automatica*, vol. 36, pp. 789–814, 2000.
[18] Y. Mo, T. Kim, K. Brancik, D. Dickinson, L. Heejo, A. Perrig, and B. Sinopoli, "Cyber-physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 195–209, p. 215, 2012.
[19] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Allerton Conf. on Communications, Control and Computing*, Urbana-Champaign, IL, Sep. 2009.
[20] T. Mori, N. Fukuma, and M. Kuwahara, "Upper and lower bounds for the solution to the discrete Lyapunov matrix equation," *Int. J. Control*, vol. 36, pp. 889–892, 1982.
[21] G. N. Nair, R. J. Evans, I. M. Y. Mareels, and W. Moran, "Topological feedback entropy and nonlinear stabilization," *IEEE Trans. Autom. Control*, vol. 49, no. 9, pp. 1585–1597, Sep. 2004.
[22] G. N. Nair, F. Fagnani, S. Zampieri, and R. J. Evans, "Feedback control under data rate constraints: An overview," *Proc. IEEE (Special Issue on Technology of Networked Control Systems)*, vol. 95, no. 1, pp. 108–137, 2007.
[23] D. Nesic and A. Teel, "Input-output stability properties of networked control systems," *IEEE Trans. Autom. Control*, vol. 49, no. 10, pp. 1650–1667, Oct. 2004.
[24] D. Mu noz de la Peña and P. D. Christofides, "Lyapunov-based model predictive control of nonlinear systems subject to data losses," *IEEE Trans. Autom. Control*, vol. 53, no. 9, pp. 2076–2089, Sep.. 2008.
[25] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," *IEEE Trans. Autom. Control*, vol. 57, no. 1, pp. 90–104, Jan. 2012.
[26] F. Pasqualetti, R. Carli, and F. Bullo, "A distributed method for state estimation and false data detection in power networks," in *Proc. IEEE Int. Conf. Smart Grid Communications*, Oct. 2011, pp. 469–474.
[27] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, and S. S. Sastry, "Foundations of control and estimation over lossy networks," *Proc. IEEE (Special Issue on Technology of Networked Control Systems)*, vol. 95, no. 1, pp. 163–187, 2007.
[28] S. Sundaram and C. N. Hadjicostis, "Distributed function calculation via linear iterative strategies in the presence of malicious agents," *IEEE Trans. Autom. Control*, vol. 56, no. 7, pp. 1731–1742, Jul. 2011.
[29] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *Proc. IEEE Int. Conf. Decision and Control*, Atlanta, GA, Dec. 2010, pp. 5991–5998.
[30] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Proc. IEEE Int. Conf. on Smart Grid Communications*, Gaithersburg, MD, Oct. 2010, pp. 226–231.
[31] M. Zhu and E. Frazzoli, "On distributed equilibrium seeking for generalized convex games," in *Proc. IEEE Int. Conf. Decision and Control*, Maui, HI, Dec. 2012.
[32] M. Zhu and S. Martínez, "Attack-resilient distributed formation control via online adaptation," in *IEEE Int. Conf. on Decision and Control*, Orlando, FL, Dec. 2011, pp. 6624–6629.
[33] M. Zhu and S. Martínez, "Stackelberg game analysis of correlated attacks in cyber-physical system," in *Proc. American Control Conf.*, Jun. 2011, pp. 4063–4068.
[34] M. Zhu and S. Martínez, "On distributed convex optimization under inequality and equality constraints via primal-dual subgradient methods," *IEEE Trans. Autom. Control*, vol. 57, no. 1, pp. 151–164, Jan. 2012.
[35] M. Zhu and S. Martínez, "On distributed resilient consensus against replay attacks in adversarial networks," in *Proc. American Control Conf.*, Montreal, QC, Canada, Jun. 2012, pp. 3553–3558.
[36] M. Zhu and S. Martínez, "On the performance analysis of resilient networked control systems under replay attack," 2013. [Online]. Available: http://arxiv.org/abs/1307.2790

Adaptive Failure Compensation Control for Uncertain Systems With Stochastic Actuator Failures

Huijin Fan, Bing Liu, Yindong Shen, and Wei Wang

***Abstract*—In this technical note, an adaptive failure compensation problem has been studied for a class of nonlinear uncertain systems subject to stochastic actuator failures and unknown parameters. The stochastic functions related to Markovian variables have been introduced to denote the failure scaling factors for each actuators which is much more practical and challenging. Firstly, by taking into account of the Markovian variables existing in the system, some preliminary knowledges have been established. Then, by employing backstepping strategy, an adaptive failure compensation control scheme has been proposed, which ensures the boundedness in probability of all the closed-loop signals in the presence of stochastic actuator failures. A simulation example is presented to show the effectiveness of the proposed scheme.**

***Index Terms*—Adaptive control, backstepping, failure compensation, Markovian variables, stochastic actuator failures.**

I. Introduction

Actuator failure is usually encountered in practical systems [1]–[4], i.e., flight control systems, networked control systems and so on. Such unexpected actuator failure may degrade the system performance, render the instability of the closed-loop system, or even worse, lead to catastrophic accidents. To increase system reliability and security, it is significantly important to design failure compensation scheme, which compensates the actuator failure and maintains the performance of the closed-loop system. Different actuator failure compensation approaches have been proposed in literatures; see, for example, multiple-mode designs [5], fault detection and diagnosis-based designs [6], eigenstructure assignment [7], sliding mode control-based scheme [8] and adaptive methods [9]–[13]. Among which, adaptive-based failure

Manuscript received August 31, 2012; revised March 07, 2013 and July 23, 2013; accepted October 15, 2013. Date of publication October 24, 2013; date of current version February 19, 2014. This work was supported by the National Natural Science Foundation of China under Grants 61174079, 61034006, 61203081, and 61203068. Recommended by Associate Editor P. Shi.

H. Fan is with the Key Laboratory of Image Processing and Intelligent Control, School of Automation, Huazhong University of Science and Technology, Wuhan 430074, China (e-mail: ehjfan@mail.hust.edu.cn).

B. Liu and Y. Shen are with the Key Laboratory of Image Processing and Intelligent Control, School of Automation, Huazhong University of Science and Technology, Wuhan 430074, China (e-mail: lbhust621@126.com; yindong@mail.hust.edu.cn).

W. Wang is with Department of Automation, Tsinghua University, Beijing 100084, China (e-mail: wwang28@tsinghua.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TAC.2013.2287115