Finite Energy and Bounded Actuator Attacks on Cyber-Physical Systems

Seddik M. Djouadi, Alexander M. Melin, Erik M. Ferragut, and Jason A. Laska, Jin Dong, Anis Drira

***Abstract*— As control system networks are being connected to enterprise level networks for remote monitoring, operation, and system-wide performance optimization, these same connections are providing vulnerabilities that can be exploited by malicious actors for attack, financial gain, and theft of intellectual property. Much effort in cyber-physical system (CPS) protection has focused on protecting the borders of the system through traditional information security techniques. Less effort has been applied to the protection of cyber-physical systems from intelligent attacks launched after an attacker has defeated the information security protections to gain access to the control system.**

In this paper, attacks on actuator signals are analyzed from a system theoretic context. The threat surface is classified into finite energy and bounded attacks. These two broad classes encompass a large range of potential attacks. The effect of theses attacks on a linear quadratic (LQ) control are analyzed, and the optimal actuator attacks for both finite and infinite horizon LQ control are derived, therefore the worst case attack signals are obtained. The closed-loop system under the optimal attack signals is given and a numerical example illustrating the effect of an optimal bounded attack is provided.

I. INTRODUCTION

The protection of industrial control systems (ICS) from malicious attacks is becoming an increasing concern. Supervisory control and data acquisition (SCADA) systems control many vital function including safety-critical system such as electric power distribution, oil and natural gas distribution, water and wastewater treatment, transportation systems, health-care devices, and weapon systems to name a few [1]. Traditionally, only safety-critical system have built in protections against attack, however recent cyber-attacks on control system, e.g. [2]–[11] have shown that many of these protections such as network airgaps are insufficient. Stuxnet in particular demonstrated the ease with which an airgap can be penetrated [9].

The many operational and business benefits to connecting SCADA and cyber-physical (CP) networks to enterprise networks and the increased utilization of wireless sensor and actuator networks [12] have introduced new vulnerabilities that can be exploited to attack control systems.

Information security methods for protecting network such an authentication and encryption do not appear to be sufficient for protecting CPSs [13]. Additionally, some information security techniques can reduce controller performance or render the control system unstable. Thus, in addition to information security techniques, attack detection and mitigation techniques need to be developed for the controller closed-loop dynamics.

Much research had been devoted to analyzing specific attacks on network sensor data. Denial of service and deception attacks on networked control systems are studied in [14] and a semidefinite programming countermeasure is proposed. False data injection attacks are shown in [15] and stealthy deception attacks are studied in [14], [16]. Replay attacks present difficulties in detection and their effects on control systems are studied in [17]. In [18] a resilient control problem where an attacker corrupts control packets is discussed and a receding-horizon control law is suggested for stabilization during an attack. Robust and resilient control techniques applied to CP systems have been reported in [19], [20]. The underlying physical dynamics are used for key establishment between the sensor and controller in [21].

In this paper, we analyze actuator attacks from a general systems theoretic perspective for a large class of potential attack signals. Sensor signal attacks are analyzed for observer-based controlled systems. In particular, the error signals between states of attack free systems and systems subject to these attacks are quantified. Optimal sensor signal attacks for the finite and infinite horizon linear quadratic (LQ) control in terms of maximizing the corresponding cost functions are computed. The closed-loop system under optimal signal attacks are provided.

II. ACTUATOR CYBER-ATTACKS

In this section, we analyze the effect of cyber-attacks on the actuators. We assume that the attacker actuator signals

S. Djouadi is an Associate Professor Currently with the Department of Electrical Engineering and Computer Science, Masdar Institute of Science and Technology, Masdar City, Abu Dhabi, UAE. On leave from the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996, djouadi@eecs.utk.edu

A. Melin is with the Sensors and Controls Research Group, Oak Ridge National Laboratory, Oak Ridge, TN 37831, melina@ornl.gov

E. Ferragut is with the Cyberspace Sciences and Information Intelligence Research Group, Oak Ridge National Laboratory, Oak Ridge, TN 37831, ferragutem@ornl.gov

J. Laska is with the Cyberspace Sciences and Information Intelligence Research Group, Oak Ridge National Laboratory, Oak Ridge, TN 37831, laskaja@ornl.gov

J. Dong is with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996, jdong@utk.edu

A. Drira is with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996, adrira@utk.edu

Research sponsored by the Laboratory Directed Research and Development Program of Oak Ridge National Laboratory (ORNL), managed by UT-Battelle, LLC for the U.S. Department of Energy under Contract No. DE-AC05-00OR22725.

with a time-varying signal $\Delta_u(t)$ that starts at $t = 0$. The system and controller based observer have the following form:

$$\begin{aligned} \dot{x}(t) &= Ax(t) + B(u_\alpha(t) + \Delta_u(t)) \\ y(t) &= Cx(t) \\ \dot{\hat{x}} &= A\hat{x} + B(u_\alpha(t) + \Delta_u(t)) + L(y(t) - C\hat{x}) \\ u_\alpha(t) &= -K\hat{x} + Gr(t) + \Delta_u(t) \end{aligned}$$

The error signal $err(t) = x(t) - \hat{x}(t)$, satisfies $\dot{err} = (A - LC)err(t)$ and therefore $err(t) \longrightarrow 0$ as $t \longrightarrow \infty$ independently of the actuator attack signal. DoS corresponds to the case where the attacker cancel out the control signal, i.e., $u_\alpha(t) = 0$, and will lead to destabilizing the system and the observer. To see this, from (1) by taking $u_\alpha(t) = 0$ we have:

$$\begin{pmatrix} \dot{x}(t) \\ \dot{err}(t) \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & A - LC \end{pmatrix} \begin{pmatrix} x(t) \\ err(t) \end{pmatrix} + \begin{pmatrix} B \\ 0 \end{pmatrix} \Delta_y(t) \tag{1}$$

showing that the system and observer are unstable, since L is always chosen such that $(A - LC)$ is Hurwitz, but then $-(A - LC)$ is not. It should be noted that canceling the control signal is not the only denial of service attack that cyber-physical systems are vulnerable to.

Two actuator attack signals classes will be considered in the following, finite energy signals, and bounded signals. Finite energy signals correspond to attacks such as individual packet loss or modification, finite time attacks, and impulse attacks. Bounded attack signals encompass a large class of potential long term attack scenarios. The denial of service attack consisting of canceling the control signal is a special case of these attack classes.

A. Finite Energy Attacks

The first scenario is to assume that the attacker can modify the actuator signal $u(t)$ with a finite energy signal in time, $\Delta u \in L^2([0, \infty))$ where $L^2([0, \infty))$ is the space of Lesbesgue measurable and square integrable functions

$$\|\Delta_u\|_2^2 := \int_0^\infty \|\Delta_u(t)\|^2 dt < \infty \tag{2}$$

where $\|\cdot\|$ is the Euclidean norm.

Assuming a deception attack of finite energy $\Delta_u(t) \in L^2[0, \infty)$, its Laplace transform $\Delta_u(s) \in H^2$. Taking the Laplace transform of (1) yields:

$$\begin{aligned} X(s) = &\ (sI - A + BK)^{-1}x(0) \\ &+ (sI - A + BK)^{-1}BKErr(s) \\ &+ (sI - A + BK)^{-1}BGR(s) \\ Err(s) = &\ (sI - A + LC)^{-1}err(0) \\ &- (sI - A + LC)^{-1}L\Delta_y(s) \end{aligned} \tag{3}$$

where $X(\cdot)$ and $Err(\cdot)$ are the Laplace Transforms of $x(t)$ and $err(t)$, respectively. Applying the final value theorem yields:

$$\lim_{t \longrightarrow \infty} x(t) = \lim_{s \longrightarrow 0} s(sI - A + BK)^{-1}BGR(s) \tag{4}$$

$$\lim_{t \longrightarrow \infty} err(t) = \lim_{s \longrightarrow 0} s\Big((sI - A + LC)^{-1}err(0)\Big) = 0 \tag{5}$$

Expression (4) shows that under a finite energy actuator deception attack, the steady state converges to the corresponding reference signal. This is expected since the finite energy assumption, $\Delta_u(t) \in L^2[0, \infty)$, implies that the time-varying bias signal satisfies $\Delta_u(t) \longrightarrow 0$ in steady state. (5) shows that the error signal converges to zero, in other words, the system maintains state awareness.

B. Bounded Attacks

For a persistent and bounded actuator attack, $\Delta_u(t) \in L^\infty[0, \infty)$,

$$\|\Delta_u\|_\infty = \operatorname{ess\,sup}_{t \in [0, \infty)} \|\Delta_u(t)\| \leq \beta, \ \exists\, \beta \geq 0 \tag{6}$$

and taking the reference signal $err(t) \equiv 0$, it follows from (1):

$$\begin{aligned} \lim_{t \longrightarrow \infty} \|x(t)\| \leq &\lim_{t \longrightarrow \infty} \Big\{ \|e^{(A-BK)t}e(0)\| \\ &+ \int_0^t \|e^{(A-BK)(t-\tau)}BKe(\tau)\| d\tau \\ &+ \int_0^t \|e^{(A-BK)(t-\tau)}\|\|B\|\|\Delta_u(\tau)\| d\tau \Big\} \\ &\leq -\frac{\beta c_1 \|B\|}{\tilde{\lambda}}, \ \exists\, c_1 \geq 0, \ \tilde{\lambda} < 0 \end{aligned} \tag{7}$$

III. Optimal Attacks on Finite Horizon Linear Quadratic (LQ) Control

We consider the plant described by the following state-space system:

$$\begin{aligned} \dot{x}(t) &= Ax(t) + B_2(t)u(t), \quad x(0) = x_0 \\ z(t) &= \begin{pmatrix} C_1\, x \\ u \end{pmatrix} \end{aligned} \tag{8}$$

The finite horizon linear quadratic (LQ) problem is concerned with minimizing the cost function:

$$J(u, x_0, h, Q) = \int_0^h z^T(\tau)z(\tau)d\tau + x^T(h)Qx(h) \tag{9}$$

where Q is a positive semi-definite matrix, $Q \geq 0$. The objective of the LQ controller is the minimization of the cost (9) over causal linear full-information controllers. From standard LQ theory the optimal controller is the state feedback [22]:

$$u = -B_2^T Px \tag{10}$$

where P is the solution of the Riccati equation:

$$-\dot{P} = PA + A^T P - PB_2B_2^T P + C_1^T C_1, \quad P(h) = Q \tag{11}$$

The matrix P is non negative semi-definite, $P \geq 0$ and is bounded above for any $\tau \leq h$ [22].
By completing the square the cost $J(u, x_0, h, Q)$ takes the form:

$$\begin{aligned} J(u, x_0, h, Q) = &\ x_0^T P(0)x_0 \\ &+ \int_0^h (u + B_2^T Px)^T(u + B_2^T Px)d\tau \end{aligned} \tag{12}$$

from where it can be seen that with no attack the optimal controller is given by (10), and the optimal cost:

$$J^\star(u, x_0, h, Q) = x_0^T P(0) x_0 \tag{13}$$

In the next section, the effect of actuator signal attacks on LQ control system is studied.

A. Optimal Actuator Attack

The LQ cost (9) at time t can be written as [23]:

$$\begin{aligned} &J(u, x_t, h, Q) - x^T(t)P(t)x(t) = \\ &\int_t^h \big[x^T C_1^T C_1 x + u^T u + \frac{d}{dt}(x^T P x)\big] d\tau, \quad P(h) = Q \\ &= \int_t^h \big[x^T C_1^T C_1 x + u^T u \\ &+ (Ax + B_2 u)^T P x + x^T P (Ax + B_2 u) + x^T \dot{P} x\big] d\tau \end{aligned} \tag{14}$$

An attack at the actuator takes the form:

$$u_\alpha(t) = u(t) + \Delta_u(t), \ t \geq 0 \tag{15}$$

and transforms the LQ cost function (14) into:

$$\begin{aligned} &J(u, x_t, h, Q) - x^T(t)P(t)x(t) = \\ &\int_t^h \big[x^T C_1^T C_1 x + u^T u + (Ax + B_2 u_\alpha)^T P x \\ &+ x^T P (Ax + B_2 u_\alpha) + x^T \dot{P} x\big] d\tau \\ &= \int_t^h \big[x^T C_1^T C_1 x + u^T u + (Ax + B_2 u)^T P x \\ &+ x^T P (Ax + B_2 u) + x^T \dot{P} x + 2 x^T P B_2 \Delta_u\big] d\tau \\ &= \int_t^h \big[(u + B_2^T P x)^T (u + B_2^T P x) \\ &+ 2 x^T P B_2 \Delta_u\big] d\tau \end{aligned} \tag{16}$$

The control $u(\cdot)$ objective is to minimize (16), while the attacker aims at maximizing it. Therefore, $u = -B_2^T P x$ and the optimal actuator attack is the solution to:

$$\begin{aligned} &\sup_{\Delta_u} J^\star(u, x_t, h, Q) - x^T(t)P(t)x(t) \\ &\qquad = 2 \sup_{\Delta_u} \int_t^h x^T P B_2 \Delta_u(\tau) d\tau \end{aligned} \tag{17}$$

As before we shall assume some constraints on the signal $\Delta_u(\cdot)$ otherwise the supremum in (22) would be infinite. That is, if the attacker has infinite energy or power then he can drive the cost to infinity. As discussed previously, more realistic attacks include finite energy and bounded signals. Let us first assume the former, i.e., $\Delta_u \in L^2([0, h), \mathbb{R}^m)$, with say $\|\Delta_u\|_2 \leq M$, for some constant $M > 0$. In this case, the RHS of (22) is the L^2-inner product of $B_2^T P x$ with Δ_u and satisfies the following by the Cauchy-Schwarz inequality:

$$\begin{aligned} &\sup_{\|\Delta_u\|_2 \leq M} \int_t^h x^T P B_2 \Delta_u(\tau) d\tau \\ &\leq \sqrt{\int_t^h \|B_2^T P x(\tau)\|^2 d\tau} \underbrace{\sqrt{\int_t^h \|\Delta_u(\tau)\|^2 d\tau}}_{\leq M} \\ &\leq M \sqrt{\int_t^h \|B_2^T P x(\tau)\|^2 d\tau} \end{aligned} \tag{18}$$

Equality in the Cauchy-Schwartz inequality (18) is achieved when Δ_u and $B_2^T P x$ are linearly dependent, i.e., there exits a scalar $\beta > 0$ such

$$\Delta_u(\tau) = \beta B_2^T P x(\tau), \ \ 0 \leq t \leq \tau < h \tag{19}$$

which gives the actuator signal attack that achieves the upper bound in (19). To compute β note that

$$\|\Delta_u\|_2 = \|\beta B_2^T P x\|_2 = M \implies \beta = \frac{M}{\|B_2^T P x\|_2} \tag{20}$$

Therefore, the optimal actuator signal attack is given by:

$$\Delta_u(\tau) = \frac{M}{\|B_2^T P x\|_2} \, B_2^T P x(\tau), \ \ 0 \leq t \leq \tau < h \tag{21}$$

The attack signal (21) yields the corresponding worst case cost function:

$$\begin{aligned} &\sup_{\Delta_u} J^\star(u, x_t, h, Q) - x^T(t)P(t)x(t) \\ &\qquad = 2 \int_t^h \frac{M}{\|B_2^T P x\|_2} \, x^T P B_2 B_2^T P x(\tau) d\tau \\ &\qquad = 2 \frac{M}{\|B_2^T P x\|_2} \|B_2^T P x\|_2^2 \\ &\qquad = 2M \|B_2^T P x\|_2 \end{aligned} \tag{22}$$

The closed-loop state-space system under the optimal actuator attack signal (21) takes the form:

$$\dot{x} = \big(A - B_2 B_2^T P + 2 \frac{M}{\|B_2^T P x\|_2} B_2 B_2^T P\big) x \tag{23}$$

Expression (23) shows that an optimal actuator attack can cancel out the optimal negative state feedback $u = -B_2^T P x$, and replace it with positive feedback completely destabilizing the closed-loop system. The solution to the state equation (23) can be written as:

$$\begin{aligned} x(t) &= \Phi(t, 0) x(0) \\ &+ 2M \underbrace{\int_0^t \Phi(t, \tau) B_2 \frac{B_2^T P(\tau) x(\tau)}{\|B_2^T P x\|_2} d\tau}_{\text{state response due to optimal L}^2 \text{ actuator attack}} \end{aligned} \tag{24}$$

where $\Phi(\cdot, \cdot)$ is the state transition matrix corresponding to $A - B_2 B_2^t P(\cdot)$.

Next, let us consider bounded signal actuator attacks, i.e. $\Delta_u \in L^\infty([0, h), \mathbb{R}^m$, with $\|\Delta_u\|_\infty \leq M$. In this case

$$\begin{aligned} &\sup_{\|\Delta_u\|_\infty \leq M} J^\star(u, x_t, h, Q) - x^T(t)P(t)x(t) \\ &\qquad = 2 \sup_{\|\Delta_u\|_\infty \leq M} \int_t^h x^T P B_2 \Delta_u(\tau) d\tau \end{aligned} \tag{25}$$

clearly, for all $\Delta_u \in L^\infty([0,h),\mathbb{R}^m$ the RHS of (25) satisfies the inequality:

$$\begin{aligned}\sup_{\|\Delta_u\|_\infty \le M} \int_t^h x^T P B_2 \Delta_u(\tau) d\tau \\ \le M \int_0^h \|B_2^T P x(\tau)\| d\tau\end{aligned} \tag{26}$$

The upper bound is achieved by choosing the actuator signal attack as:

$$\Delta_u(\tau) = M \frac{B_2^T P x(\tau)}{\|B_2^T P x(\tau)\|}, \tag{27}$$

on the set

$$E := \{\tau \in (0,h) : \ B_2^T P x(\tau) \neq 0\} \tag{28}$$

Note the actuator signal depend in a nonlinear fashion on the state vector $x(\cdot)$. As a result under (28) the closed-loop system becomes nonlinear and can be written as:

$$\dot{x}(\tau) = \begin{cases} (A - B_2 B_2^T P + M \frac{B_2 B_2^T P x(\tau)}{\|B_2^T P x(\tau)\|}) x(\tau), \ \tau \in E \\ A x(\tau), \text{ if } \ B_2^T P x(\tau) = 0, \ \tau \notin E) \end{cases} \tag{29}$$

The solution to (29) can be written as:

$$x(t) = \begin{cases} \Phi(t,0)x(0) + M \int_E \Phi(t,\tau) B_2 \frac{B_2^T P x(\tau)}{\|B_2^T P x(\tau)\|} d\tau \\ e^{At} x(0), \ \ t \notin E \end{cases} \tag{30}$$

In the next section, optimal actuator attacks for the infinite horizon LQ control are discussed.

IV. Optimal Actuator Attacks for Infinite Horizon LQ Control

The optimal actuator attacks in the infinite horizon case are similar to the finite horizon case. From (21) it is given by:

$$\Delta_u(\tau) = \frac{M}{\|B_2^T P x\|_2} B_2^T P x(\tau), \ \ 0 \le t \le \tau < \infty \tag{31}$$

for the finite energy case, and for bounded signal attacks by (28)

$$\Delta_u(\tau) = M \frac{B_2^T P x(\tau)}{\|B_2^T P x(\tau)\|}, \tag{32}$$

on the set

$$E := \{\tau \in (0,\infty) : \ B_2^T P x(\tau) \neq 0\} \tag{33}$$

The parallel closed-loop state equation is similar to the finite horizon case (23) with the state transition matrix $\Phi(\cdot,\cdot)$ in (24) given by:

$$\Phi(t,\tau) = \Phi(t-\tau) = e^{(A - B_2 B_2^T P)(t-\tau)}, \ t \ge \tau \tag{34}$$

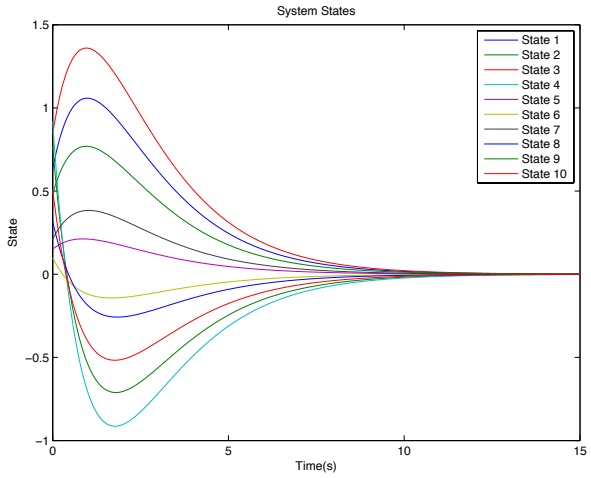

Fig. 1. All states with no attack infinite horizon

V. Numerical Example

This section provides a numerical experiment to demonstrate the effectiveness of the proposed attack strategies and validate the theoretical analysis. Considering the same power network model studied in [24], we illustrate the effect of the actuator attack on system states for both finite and infinite horizon cases. Assuming that the attacker has access to the system parameters such as the state matrices A, B and C, the optimal actuator attacks for the infinite horizon LQ problem and for the finite horizon are simulated.

To illustrate the finite energy actuator signal attack for infinite horizon using a power network system of five generators, therefore a total ten states the simulation results are shown by the following Figures: actuator signal with no attack in Figure 1, actuator signal with optimal attack in Figure 2, the difference between no attack and optimal attack signals in Figure 3. Now, to illustrate the finite energy actuator signal attack for finite horizon. The simulation results are shown by the following Figures: actuator signal with no attack in Figure 4, actuator signal with optimal attack in Figure 5, the difference between no attack and optimal attack signals in Figure 6.

Finally, the difference for the state signal with and without the undetectable attacks imply that the optimal actuator attack affect significantly the performance of the system.

VI. Conclusions

In this paper, a system theoretic analysis of the effect of finite energy and bounded attacks on linear systems with an LQ controller was presented. Specifically, the effects on the steady state response are derived. The optimal finite energy and bounded attacks for both the finite and infinite horizon LQ problem are developed my maximizing the corresponding LQ cost functions. The closed-loop systems under attack are given and a numerical simulation illustrates the effectiveness of the optimal attack. Future work will include analyzing the

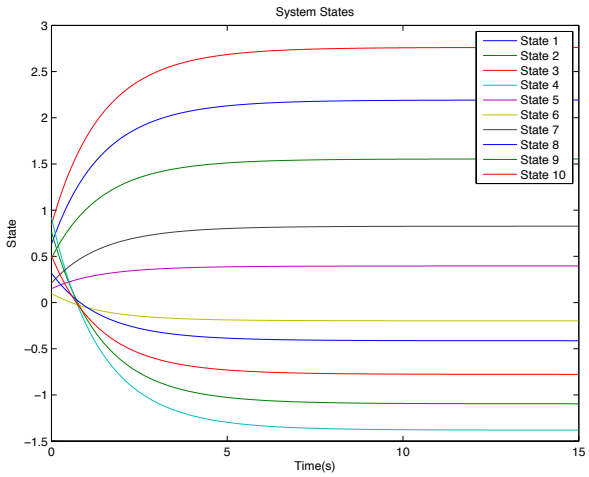

Fig. 2. All states with an optimal attack Case infinite horizon

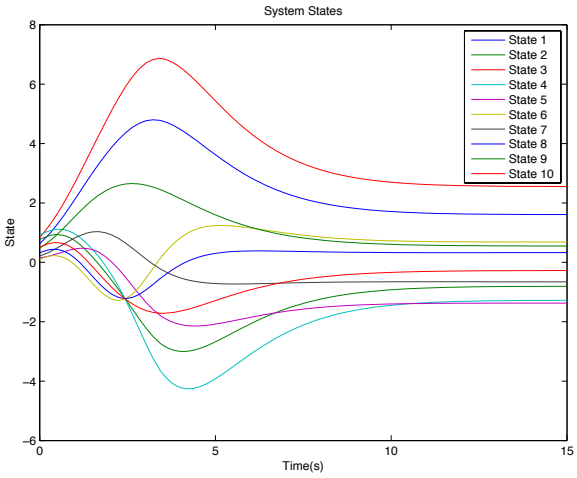

Fig. 5. All states with an optimal attack Case finite horizon

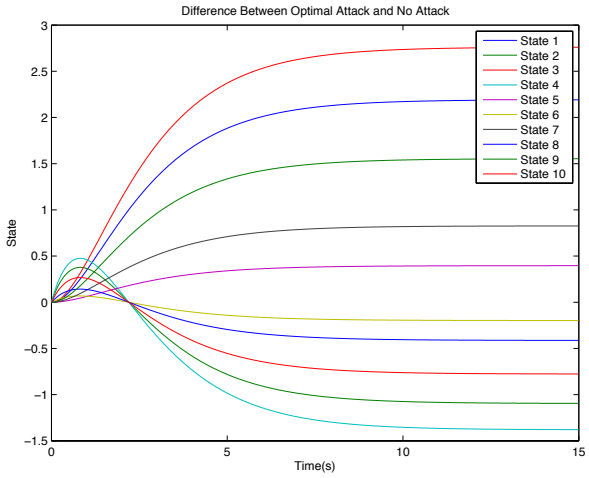

Fig. 3. The difference between no Attack and optimal attack infinite horizon

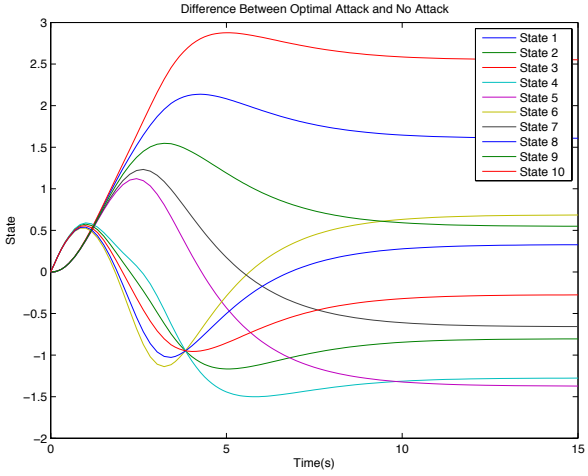

Fig. 6. The difference between no Attack and optimal attack finite horizon

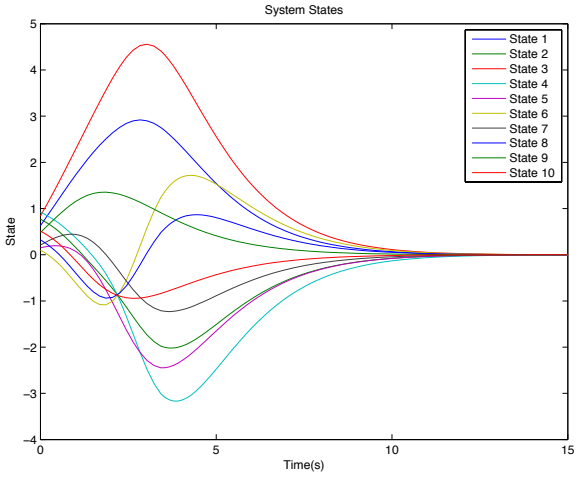

Fig. 4. All states with no attack finite horizon

effects of finite energy and bounded attacks on sensors and actuators for linear quadratic Gaussian control formulation and H^{∞} controller with external disturbances and noise.

REFERENCES

[1] A. A. Cardenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems," in *3rd USENIX workshop on Hot Topics in Security (HotSec '08), Associated with the 17th USENIX Security Symposium, San Jose, CA*, 2008.

[2] J. Slay and M. Miller, "Lessons learned from the maroochy water breach," *Critical Infrastructure Protection*, 2007.

[3] P. Quinn-Judge, "Cracks in the system," *TIME Magazine*, 2002.

[4] J. Leyden, "Teen derails tram after hacking train network," *The Register*, 2008.

[5] A. Greenberg, "Hackers cut cities' power." *Forbes*, 2008.

[6] T. Greene, "Experts hack power grid in no time," *NetworkWorld*, 2008.

[7] D. Halperin, T. Heydt-Benjamin, B. Ransford, S. Clark, B. Defend, W. Morgan, T. K. K. Fu, and W. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *IEEE Symposium on Security and Privacy*, 2008.

[8] G. I. Security, "Tva needs to address weaknesses in control systems and networks," Tech. Rep. GAO-08-526, Report to Congressional Requesters, Tech. Rep., 2008.

[9] N. Falliere, L. O. Murchu, and E. Chien, "W32.stuxnet.dossier," http://www.symantec.com/content/en/us/enterprise/media/security response/whitepapers/w32 stuxnet dossier.pdf, 2011.

[10] M. F. P. Services and M. Labs., "Global energy attacks: Night," http://www.mcafee.com/us/resources/whitepapers/wp-global-energy-cyberattacks-night-dragon.pdf, 2011.

[11] "Kaspersky lab and itu research reveals new advanced cyber threat," http://www.kaspersky.com/about/news/virus/2012/Kaspersky Lab and ITU Research Reveals New Advanced Cyber Threat, 2012.

[12] A. A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. A. Perrig, and S. Sastry, "Challenges for securing cyber physical systems," in *Workshop on Future Directions in Cyber-physical Systems Security, Newark, NJ*, 2009.

[13] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems part i: Models and fundamental limitations," *arXiv:1202.6144v2 [math.OC]*, 2012.

[14] S. Amin, A. Cardenas, and S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," *Hybrid Systems: Computation and Control*, 2009.

[15] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *ACM Conference on Computer*, 2009.

[16] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *IEEE Conference on Decision and Control, Atlanta, GA*, 2010.

[17] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Conference on Communications, Control and Computing, Monticello, IL*, 2010.

[18] M. Zhu and S. Martinez, "Stackelberg-game analysis of correlated attacks in cyber-physical systems," in *American Control Conference,San Francisco, CA*, 2011.

[19] Q. Zhu and T. Basar, "Robust and resilient control design for cyber-physical systems with an application to power systems," in *50th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC) Orlando, FL*, 2011.

[20] S. Zheng, T. Jiang, and J. Baras, "Robust state estimation under false data injection in distributed sensor networks," in *IEEE Globecom*, 2010.

[21] H. Li, L. Lai, S. Djouadi, , and X. Ma, "Key establishment via common state information in networked," in *Proceedings of the American Control Conference, San Francisco, CA*, 2011.

[22] K. Zhou, J. Doyle, and K. Glover, *Robust and Optimal Control*. Prentice Hall, 1995.

[23] M. Green and D. Limebeer, *Linear Robust Control*. Prentice Hall, 1995.

[24] S. M. Djouadi, A. M. Melin, E. M. Ferragut, J. A. Laska, and J. Dong, "Finite energy and bounded attacks on control system sensor signals," in *American Control Conference (ACC), 2014*. IEEE, 2014, pp. 1716–1722.

[25] F. Borrelli and T. Keviczky, "Distributed lqr design for identical dynamically decoupled systems," *IEEE Trans. Automatic Control*, 2008.