Risk-Sensitive Control under a Class of Denial-of-Service Attack Models

Technical Report of the ISIS Group
University of Notre Dame
ISIS-2010-003
September, 2010

Getachew K. Befekadu, Vijay Gupta and Panos J. Antsaklis
Department of Electrical Engineering
University of Notre Dame
Notre Dame, IN 46556

Interdisciplinary Studies in Intelligent Systems

Risk-Sensitive Control under a Class of Denial-of-Service Attack Models

Getachew K. Befekadu, Vijay Gupta and Panos J. Antsaklis
Department of Electrical Engineering
University of Notre Dame
Notre Dame, IN 46556
e-mail: gbefekadu1@nd.edu, vgupta2@nd.edu, antsaklis.1@nd.edu

Abstract

In this paper, we examine the problem of risk-sensitive control under a class of Denial-of-Service (DoS) attack model and derive a solution for the optimal control policy when attacker jams randomly the control packets in the system. For a discrete-time partially observed stochastic system with exponential running cost, we provide an exact solution in terms of finite-dimensional dynamics of the system via a measure transformation approach. We use the risk-sensitive criterion rather than quadratic cost to directly highlight one's belief about system uncertainties back to the cost functional. Our results show that the optimal control problem can be considered with respect to the average path of the DoS attack model.

I. INTRODUCTION

Over the past few years, increasing effort has been placed in addressing the problem of risk/vulnerability assessment of malicious attacks against today's critical infrastructure such as power grids, industrial control systems and banking/finance sectors (see references [1]–[6]). The issue of security in such critical sectors has now become as important as technical design. As these critical infrastructures become more interconnected and complex in terms of either the dynamics or the distributed structure, solutions that ensure security against such attacks will gain importance to an even greater extent. A systematic study of design tools that provide provable security against faults and malicious attacks is a core, although challenging, problem. Control theoretic tools are likely to play an important role in developing such tools. To mention a few, there are some interesting works involving security requirements, attacks and vulnerabilities in control systems, wireless sensor networks and IT infrastructures (e.g., [7]–[12]).

In this paper, we consider a finite horizon control of a discrete-time plant in which the controller communicates the control sequences to the actuator over a communication network. We consider a Denial-of-Service (DoS) attacker that aims to disrupt the network or jam the control packets from reaching the actuator. In our setting, we consider a class of DoS attack model, where the success of denying service, i.e., jamming the control packets from reaching the actuator, follows according to independent Bernoulli processes [7], [8]. In general, DoS attack models, unlike assumed stochastic uncertainty models in the system, change their targets or strategies in response to the protective measures that the decision makers usually take against them, so the risks and the consequence of risks are constantly changing. We are currently working on extending the results of this paper to the case when the DoS attacks are more sophisticated, including the case of Markov modulated DoS attack models. However to fully develop the measure transformation based approach for risk sensitive control in this context, here we concentrate on the case when the DoS attacks are modeled as a Bernoulli process.

By gaining motivation from robust control and dynamic games, where such uncertainty about the parameters has been fruitfully considered by adopting a risk sensitive stochastic control function [13]–[17], we adopt the same framework in a different context. Our main technical tool is a measure transformation, which allows us to derive the optimal control policy for this particular problem. To this end, we use two different probability measures, i.e., the original reference probability measure and another new equivalent probability measure (via change of measure transformation), on which all process variables including the DoS attack sequences defined. With the new measure transformation, the DoS attack sequences appeared to remain always independent over their range values; while the plant observation sequences show independent characteristic to the other measure variables in the system. This further allows us to define an equivalent information state (together with the

corresponding adjoint measure process) for a partially observed stochastic system, which simplifies the optimal control problem as a separated policy problem in terms of this information state. Moreover, the use of this measure transformation provides an implicit formula that essentially combines estimation and control as a single problem for the partially observed stochastic system [16], [18], [19].

This paper is organized as follows. In Section II, we introduce some preliminary concepts including the main problem formulation for risk-sensitive control problem under a class of DoS attack model. Section III presents the main results. Solution for the optimal control problem is stated formally and the associated recursive solution for the optimal cost value is derived. Finally, Section IV provides concluding remarks. A short description of Girsanov's theorem is also included in the Appendix for the convenience of readers.

II. PRELIMINARIES AND PROBLEM STATEMENT

A. Preliminaries

Consider a probability space $(\Omega, \mathcal{F}, P)$ equipped with a complete filtration $\{\mathcal{F}_k\}$, $k \in N$. Unless otherwise stated, all the random variables initially defined on this reference probability measure. Consider the following discrete-time partially observed stochastic system

$$\begin{aligned} x_{k+1} &= A x_k + \beta_{k+1} B u_k + v_{k+1} \\ y_{k+1} &= C x_k + w_{k+1}, \quad k = 0,1,\ldots,T-1 \end{aligned} \tag{1}$$

where $x_k \in \mathcal{R}^n$ is the state of the system, $u_k \in \mathcal{R}^m$ is the control input, $y_k \in \mathcal{R}^p$ is the observation output; and $\beta_k \in \{0,1\}$ is the DoS attack sequences that disrupt the control packets from reaching the actuator. Fig 1 shows typical malicious cyber attacks in control systems: A1 and A3 are integrity or deception type attacks, A2 and A4 are DoS type attacks, and A5 is a direct physical attack in the system (see references [7], [8], [21]).

We assume that the processes υ_k and w_k are jointly independent with normal densities $\varphi \sim \mathcal{N}(0, \Sigma)$ and $\phi \sim \mathcal{N}(0, \Gamma)$, respectively; and the covariance matrices Σ and Γ are also assumed positive definite.

Let $\mathcal{Y}_k$ denoted the complete filtration generated by $\{y_1, y_2, \ldots, y_k\}$; while $\mathcal{B}_k$ be the corresponding anticipated DoS attack sequences (or path) and assumed to be independent to the other measure variables in the system. Moreover, the admissible controls $u = \{u_0, u_1, \ldots, u_{T-1}\}$ are $\mathcal{R}^m$ - valued sequences and considered to be $\{\mathcal{Y}_k \vee \mathcal{B}_k\}$ adapted processes. The set of all admissible control sequences on the interval $k, k+1, \ldots, l$ is denoted by $\mathcal{U}_{k,l}$.

We consider an exponential running cost with quadratic function for the risk-sensitive control problem

$$\begin{aligned} J(u) = \theta E\Big[\exp(\theta/2)\Big\{\textstyle\sum_{k=0}^{T-1}(x_k' M x_k + \beta_{k+1} u_k' N u_k) \\ + x_T' M_T x_T\Big\}\Big] \end{aligned} \tag{2}$$

where $\theta > 0$ is the risk-sensitive parameter, $u \in \mathcal{U}_{0,T-1}$ is the admissible control sequences; while $E[.]$ denotes the expectation with respect to the original reference probability measure P.

B. Problem Statement

The problem considered in this paper is stated as follows.

Problem: Find an optimal control policy for the finite-horizon risk-sensitive control problem under a given class of DoS attack model, i.e.,

$$\begin{aligned} F_0 &= \inf_{u \in \mathcal{U}_{0,T-1}} J(u) \\ &= \inf_{u \in \mathcal{U}_{0,T-1}} \theta E\Big[\exp(\theta/2)\Big\{\textstyle\sum_{k=0}^{T-1}(x_k' M x_k + \beta_{k+1} u_k' N u_k) \\ &\qquad + x_T' M_T x_T\Big\}\Big] \end{aligned} \tag{3}$$

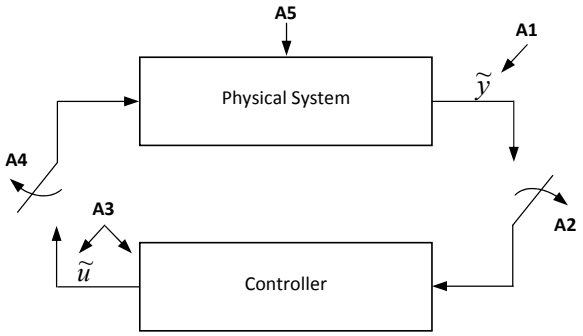

Fig. 1 Typical malicious cyber attacks in control systems.

Here we consider the class of DoS attack model as a Bernoulli packet drop model, in which at each time k, the attacker jams a control packet according to independent Bernoulli random trials with success probability β_k. In general, this attack model $\mathcal{A}_{Ber(\beta)}$ will have the following anticipated attack strategy

$$\mathcal{A}_{Ber(\beta)} = \Big\{ \mathcal{B}_k = \{\beta_0, \beta_1, \ldots, \beta_T\} \,\Big|\, P(\beta_k = 1) = \overline{\beta}, \quad k = 0, 1, \ldots, T \Big\} \tag{4}$$

We remark that the exponential running cost function weighted by a risk-sensitive parameter θ highlights one's belief about system uncertainties back to the scale of cost functional. For a risk-neutral criterion, when θ is sufficiently close to zero, the risk-sensitive control problem reduces to an LQG control problem. We pointed out that a similar idea is followed by Amin *et al.* [7] using LQG control problem under a class of DoS attack model, but in a different context. Schenato *et al.* [22] have also done a similar work in the context of network reliability and its effect on the performance of the control system.

III. Change of Measure and Solution to Risk-Sensitive Control Problem under a Class of DoS Attack Models

In this section, we explicitly use the measure transformation technique to derive the optimal control policy for the risk-sensitive control problem under a class of DoS attack model. The key idea is to introduce a new measure transformation (which is equivalent to the original probability measure) under which the observation and state variables become independent along the anticipated DoS attack path in the system. This allows us to obtain algebraic recursive formulas for the equivalent information state and associated adjoint process based on the observation history, the current control input and the anticipated average path of the DoS attacks. Using this fact, we further derive an implicit formula for optimal control policy (i.e., separated policy which essentially combines estimation and control as a single problem) in terms of the original system matrices via the dynamic programming.

A. Change of measure and finite-dimensional information state

For any admissible control sequences $u \in \mathcal{U}_{0,T-1}$, consider the following random variable

$$\begin{aligned} \Lambda^u_{1,k} &= \prod_{l=1}^{k} \frac{\varphi(x_l - A x_{l-1} - \beta_l B u_{l-1}) \phi(y_l - C x_{l-1})}{\varphi(x_l)\phi(y_l)} \\ \Lambda^u_{0,0} &= 1, \qquad\qquad k = 1, 2, \ldots, T \end{aligned} \tag{5}$$

Using this random variable, we can introduce an equivalent measure transformation $\overline{P}$ (where the restriction of the Radon-Nikodym derivative implies the measure $[\Lambda^u_{0,k}]^{-1}$ is an $\mathcal{F}_k$ - martingale process [19], [20], [23]) as follows

$$d\overline{P} = [\Lambda^u_{0,k}]^{-1} dP, \quad k = 0, 1, \ldots, T \tag{6}$$

Under this measure transformation $\overline{P}$, the state x_k and the observation y_k will become normal densities and

independent to each other on the anticipated path of the DoS attacks in the system. This fact is a direct application of Girsanov's theorem [23]. For the convenience of readers, a short description of this theorem including the measure transformation (i.e., the construction of this change of measure for the discrete-time measure processes) is given in the Appendix.

Moreover, consider the following measure for any admissible control u and anticipated DoS attack sequences or path in the system

$$\alpha_k^u(x)dx = \overline{E}\left[\Lambda_{0,k}^u \exp(\theta D_{0,k-1}^u) I_A(x_k \in dx) \,\middle|\, \mathcal{Y}_k \vee \mathcal{B}_k\right] \qquad k = 0, 1, \ldots, T \tag{7}$$

where $I_A(x_k \in dx)$ is the indicator function of the Borel set A, $D_{j,k}^u$ is the quadratic running function given by $D_{j,k}^u = (1/2)\left\{\sum_{l=j}^k x_l' M x_l + \beta_{l+1} u_l' N u_l\right\}$ for $0 \le j \le k < T-1$. Moreover, the initial boundary condition for this measure valued process is specified by $\alpha_0(x_0) = \varphi(x_0)$.

Then, we obtain the following theorem.

Theorem 1: (forward recursive formula for $\alpha_k^u(x)$). The measure valued process $\alpha_k^u(x)$ satisfies the following forward recursion

$$\alpha_{k+1}^u(x) = \frac{1}{\phi_{k+1}(y_{k+1})} \int_{B(\mathcal{R}^n)} \exp(\theta D_{k,k}^u)\, \varphi(x - A\xi - \beta_{k+1} B u_k) \times \phi(y_{k+1} - C\xi) \alpha_k^u(\xi)\, d\xi \tag{8}$$

where $D_{k,k}^u$ is given by $1/2\{\xi' M \xi + \beta_{k+1} u_k' N u_k\}$.

Proof: For any Borel test function $f(x)$, consider the following

$$\begin{aligned}
&\overline{E}\left[f(x_{k+1}) \Lambda_{0,k+1}^u \exp(\theta D_{0,k}^u) \,\middle|\, \mathcal{Y}_{k+1} \vee \mathcal{B}_{k+1}\right] \\
&\qquad = \int_{B(\mathcal{R}^n)} f(z)\, \alpha_{k+1}^u(z)\, dz \\
&= \overline{E}\Big[f(Ax_k + \beta_{k+1} B u_k) \Lambda_{0,k}^u \exp(\theta D_{0,k-1}^u) \\
&\qquad \times \frac{\varphi(x_{k+1} - Ax_k - \beta_{k+1} B u_k)\, \phi(y_{k+1} - Cx_k)}{\varphi(x_{k+1})\, \phi(y_{k+1})} \\
&\qquad \times \exp(\theta D_{k,k}^u) \,\Big|\, \mathcal{Y}_{k+1} \vee \mathcal{B}_{k+1}\Big] \\
&= \frac{1}{\phi(y_{k+1})} \overline{E}\Big[\int_{B(\mathcal{R}^n)} f(Ax_k + \beta_{k+1} B u_k + \upsilon) \Lambda_{0,k}^u \exp(\theta D_{0,k-1}^u) \\
&\qquad \times \varphi(\upsilon)\, d\upsilon\, \phi(y_{k+1} - Cx_k) \exp(\theta D_{k,k}^u) \,\Big|\, \mathcal{Y}_{k+1} \vee \mathcal{B}_{k+1}\Big] \\
&= \frac{1}{\phi(y_{k+1})} \int_{B(\mathcal{R}^n)} \int_{B(\mathcal{R}^n)} f(A\xi + \beta_{k+1} B u_k + \upsilon) \exp(\theta D_{k,k}^u) \\
&\qquad \times \varphi(\upsilon)\, \phi(y_{k+1} - C\xi)\, \alpha_k^u(\xi)\, d\xi\, d\upsilon
\end{aligned} \tag{9}$$

With change of variable $z = A\xi + \beta_{k+1} B u_k + \upsilon$, we have

$$\begin{aligned}
&\int_{B(\mathcal{R}^n)} f(z)\, \alpha_{k+1}^u(z)\, dz \\
&= \frac{1}{\phi(y_{k+1})} \int_{B(\mathcal{R}^n)} \int_{B(\mathcal{R}^n)} f(z) \exp(\theta D_{k,k}^u) \\
&\qquad \times \varphi(z - A\xi - \beta_{k+1} B u_k)\, \phi(y_{k+1} - C\xi) \alpha_k^u(\xi)\, d\xi\, dz
\end{aligned} \tag{10}$$

The above holds for all Borel test functions, thus we have equation (8). □

Due to the linearity of the system (together with the anticipated average path of the DoS attacks) the measure valued process α_k^u has a normal density and is given by

$$\alpha_k^u(x) = Z_k(u)\exp(-1/2)(x-\mu_k(u))' R_k^{-1}(u)(x-\mu_k(u)) \tag{11}$$

Moreover, $Z_k(u)$, $R_k^{-1}(u)$ and $\mu_k(u)$ are given by the following coupled forward, algebraic recursive equations.

$$\begin{aligned} R_{k+1}^{-1}(u) &= \ 2\theta M + C'\Gamma^{-1}C + \Sigma^{-1}\{I - Ar^{-1}(u)A'\Sigma^{-1}\} \\ \mu_{k+1}(u) &= R_{k+1}^{-1}(u)\{C'\Gamma^{-1}y_{k+1} + \Sigma^{-1}Ar^{-1}(u)R_k^{-1}(u)\mu_k(u) \\ &\quad + (I + \Sigma^{-1}Ar^{-1}(u)A')\Sigma^{-1}B\} \\ Z_{k+1}(u) &= Z_k(u)(2\pi)^{-n/2}|\Sigma|^{-1/2}\exp(-1/2)\{\bar{z}(u) \\ &\quad - (R_{k+1}^{-1}(u)\mu_{k+1}(u))'(R_{k+1}^{-1}(u)\mu_{k+1}(u))\} \end{aligned} \tag{12}$$

where

$$\begin{aligned} r(u) &= A'\Sigma^{-1}A + R_k^{-1}(u) \\ z(u) &= -2\theta\beta_{k+1}u_k'Nu_k + B'\Sigma^{-1}\{I - Ar^{-1}(u)A'\Sigma^{-1}\}B \\ &\quad + R_k^{-1}(u)\mu_k(u)\{R_k^{-1}(u)\mu_k(u) - r^{-1}(u)R_k^{-1}(u)\mu_k(u)\} \\ &\quad - 2B'\Sigma^{-1}Ar^{-1}(u)R_k^{-1}(u)\mu_k(u), \end{aligned}$$

and

$$\begin{aligned} \bar{z}(u) &= E_\beta[z(u)] \\ &= -2\theta(1-\bar{\beta})u_k'Nu_k + B'\Sigma^{-1}\{I - Ar^{-1}(u)A'\Sigma^{-1}\}B \\ &\quad + R_k^{-1}(u)\mu_k(u)\{R_k^{-1}(u)\mu_k(u) - r^{-1}(u)R_k^{-1}(u)\mu_k(u)\} \\ &\quad - 2B'\Sigma^{-1}Ar^{-1}(u)R_k^{-1}(u)\mu_k(u) \end{aligned}$$

Therefore, the measure valued process $\alpha_k^u(x)$ (i.e., the information state for this partially observed stochastic system) is determined by these finite-dimensional parameters $Z_k(u)$, $R_k^{-1}(u)$ and $\mu_k(u)$ that involve coupled forward, algebraic recursive relations.

With minor abuse of notation, we consider these parameters as a new state variable of the system

$$\xi_k^u(u) = (Z_k(u), R_k^{-1}(u), \mu_k(u)) \tag{13}$$

Furthermore, we can rewrite this equivalent information state $\alpha_k^u(x)$ as follows

$$\begin{aligned} \alpha_k^u(x) &= \alpha_k^u(\xi_k^u, x) \\ &= Z_k(u)\exp(-1/2)(x-\mu_k(u))' R_k^{-1}(u)(x-\mu_k(u)) \end{aligned} \tag{14}$$

Remark 1: Note that these parameters are determined on the average path of the DoS attack model since the value for $\bar{z}(u)$ computed as an expected value with respect to anticipated DoS attacks.

B. Solution to risk-sensitive control problem under a class of DoS attack model

In the following, we provide an exact solution for the optimal control policy in terms of finite-dimensional dynamics, i.e., separated policy in terms of the equivalent information state, using dynamic programming technique. For any admissible control and anticipated DoS attack sequences, the expected total cost of (2) with respect to equivalent probability measure transformation is given as follows

$$
\begin{aligned}
J(u) &= \theta E\left[\exp(\theta/2)\left\{\textstyle\sum_{k=1}^{T-1}(x_k' M x_k + \beta_{k+1} u_k' N u_k) + x_T' M_T x_T\right\}\right] \\
&= \theta \overline{E}\left[\Lambda_{0,T}^u \exp(\theta/2)\left\{\textstyle\sum_{k=1}^{T-1}(x_k' M x_k + \beta_{k+1} u_k' N u_k) + x_T' M_T x_T\right\}\right] \\
&= \theta \overline{E}\left[\Lambda_{0,T}^u \exp(\theta D_{0,T-1}^u) \times \exp\{(\theta/2) x_T' M_T x_T\}\right] \\
&= \theta \overline{E}\left[\overline{E}\left[\Lambda_{0,T}^u \exp(\theta D_{0,T-1}^u) \times \exp\{(\theta/2) x_T' M_T x_T\} \,\middle|\, \mathcal{Y}_T \vee \mathcal{B}_T\right]\right] \\
&= \theta \overline{E}\left[\int_{B(\mathcal{R}^n)} \exp\{(\theta/2) x' M_T x\} \alpha_T(x)\, dx\right]
\end{aligned}
\tag{15}
$$

For any k, $0<k<T$, the expected total cost can be expressed in terms of this equivalent information state as

$$
\begin{aligned}
J(u) &= \theta \overline{E}\left[\Lambda_{0,T}^u \exp(\theta D_{0,T-1}^u) \times \exp\{(\theta/2) x_T' M_T x_T\}\right] \\
&= \theta \overline{E}\left[\Lambda_{0,k}^u \Lambda_{k+1,T}^u \exp(\theta D_{0,k}^u) \exp(\theta D_{k+1,T-1}^u) \times \exp\{(\theta/2) x_T' M_T x_T\}\right] \\
&= \theta \overline{E}\left[\Lambda_{0,k}^u \exp(\theta D_{0,k}^u) \overline{E}[\Lambda_{k+1,T}^u \exp(\theta D_{k+1,T-1}^u) \times \exp\{(\theta/2) x_T' M_T x_T\} \,\middle|\, \sigma\{x_k\} \vee \mathcal{Y}_T \vee \mathcal{B}_T\right]\right]
\end{aligned}
\tag{16}
$$

where the inner expectation of the last equation in (16) involves conditioning on $\sigma\{x_k\}$ due to the Markov property of x. Define a new adjoint process

$$
\begin{aligned}
\eta_k^u(x_k) = \overline{E}\Big[&\Lambda_{k+1,T-1}^u \exp(\theta D_{k+1,T-1}^u) \\
&\times \Lambda_{T,T}^u \exp\{(\theta/2) x_T' M_T x_T\} \,\big|\, \sigma\{x_k\} \vee \mathcal{Y}_T \vee \mathcal{B}_T\Big]
\end{aligned}
\tag{17}
$$

With this, the expected total cost can be further rewritten as

$$
\begin{aligned}
J(u) &= \theta \overline{E}\left[\Lambda_{0,k}^u \exp(\theta D_{0,k}^u) \eta_k^u(x_k)\right] \\
&= \theta \overline{E}\left[\overline{E}\left[\Lambda_{0,k}^u \exp(\theta D_{0,k}^u) \eta_k^u(x_k) \,\middle|\, \mathcal{Y}_T \vee \mathcal{B}_T\right]\right] \\
&= \theta \overline{E}\left[\int_{B(\mathcal{R}^n)} \alpha_k^u(x) \eta_k^u(x)\, dx\right] \\
&= \theta \overline{E}\left[\left\langle \alpha_k^u(x),\, \eta_k^u(x) \right\rangle\right]
\end{aligned}
\tag{18}
$$

which is independent of k.

Theorem 2: (backward recursive formula for $\eta_k^u(x)$). The adjoint process $\eta_k^u(x)$ satisfies the following backward recursion

$$
\begin{aligned}
\eta_k^u(x_k) = \int_{B(\mathcal{R}^n)} &\frac{\phi(y_{k+1} - C x_k)}{\phi(y_{k+1})} \varphi(x - A x_k - \beta_{k+1} G u_k) \\
&\times \exp(\theta D_{k,k}^u) \eta_{k+1}^u(x)\, dx
\end{aligned}
\tag{19}
$$

where $D_{k,k}^u$ is given by $1/2\{x' M x + \beta_{k+1} u_k' N u_k\}$.

Proof: From (17), $\eta_k^u(x_k)$ is given by

$$
\begin{aligned}
\eta_k^u(x_k) &= \overline{E}\Big[\Lambda_{k+1,T}^u \exp(\theta D_{k+1,T-1}^u) \\
&\quad \times \exp\{(\theta/2)x_T' M_T x_T\} \,\Big|\, \sigma\{x_k\} \vee \mathcal{Y}_T \vee \mathcal{B}_T\Big] \\
&= \overline{E}\Big[\ \overline{E}\Big[\ \frac{\varphi(x_{k+1} - Ax_k - \beta_{k+1}Bu_k)\,\phi(y_{k+1} - Cx_k)}{\varphi(x_{k+1})\,\phi(y_{k+1})} \\
&\quad \times \exp\{(\theta/2)(x_k' M x_k + \beta_{k+1} u_k' N u_k)\} \\
&\quad \times \Lambda_{k+2,T}^u \exp(\theta D_{k+2,T-1}^u) \exp\{(\theta/2)x_T' M_T x_T\} \\
&\quad \times |\, \sigma\{x_k, x_{k+1}\} \vee \mathcal{Y}_T \vee \mathcal{B}_T\Big] \,\Big|\, \sigma\{x_k\} \vee \mathcal{Y}_T \vee \mathcal{B}_T\Big] \\
&= \overline{E}\Big[\ \frac{\varphi(x_{k+1} - Ax_k - \beta_{k+1}Bu_k)\,\phi(y_{k+1} - Cx_k)}{\varphi(x_{k+1})\,\phi(y_{k+1})} \\
&\quad \times \exp\{(\theta/2)(x_k' M x_k + \beta_{k+1} u_k' N u_k)\} \\
&\quad \times \eta_{k+1}^u(x_{k+1}) \,\Big|\, \sigma\{x_k\} \vee \mathcal{Y}_T \vee \mathcal{B}_T\Big]
\end{aligned}
\tag{20}
$$

Using the independent property under $\overline{P}$, integrating the last equation in (20) with respect to the density of x_{k+1} gives equation (19) in the above theorem. □

Remark 2: The boundary condition for the adjoint process is given by $\eta_T(x_T) = \Lambda_{T,T}^u \exp\{(\theta/2)x_T' M_T x_T\}$.

Moreover, the adjoint process η_k^u has a normal density (c.f. equation (11)) and given by

$$
\eta_k^u(x) = \widetilde{Z}_k(u) \exp(-1/2)(x - \gamma_k(u))' S_k^{-1}(u)(x - \gamma_k(u)) \tag{21}
$$

where the finite-dimensional parameters $\widetilde{Z}_k$, $S_k^{-1}(u)$ and $\gamma_k(u)$ satisfy coupled backward, algebraic recursions.

From equations (8) and (12), the information state $\alpha_k^u(x)$ is determined by $Z_k(u)$, $R_k^{-1}(u)$ and $\mu_k(u)$ that involve only algebraic recursive equations. Thus, based on the current value of ξ_k^u together with the new observation y_{k+1}, current control u_k and anticipated attack β_{k+1}, the next value can be determined by the following functional recursion

$$
\xi_{k+1}^u = \xi_{k+1}^u(\xi_k^u, u_k, y_{k+1}, \beta_{k+1}) \tag{22}
$$

Suppose at some intermediate time $k,\ 0 < k < T$, the information state ξ_k^u is given by $\xi = (Z, R^{-1}, \mu)$, then, from equation (18), the value function for the optimal control problem satisfies the following

$$
F(\xi,\ k) = \inf_{u \in \mathcal{U}_{k,T-1}} \overline{E}\Big[\big\langle \alpha_k^u\ ,\ \eta_k^u \big\rangle \,\Big|\, \alpha_k = \alpha_k(\xi)\Big] \tag{23}
$$

Theorem 3: (dynamic programming formulation). The value function satisfies the following recursive equation

$$
F(\xi,\ k) = \inf_{u \in \mathcal{U}_{k,k}} \overline{E}\big[F(\xi_{k+1}(\xi, u, y_{k+1}, \beta_{k+1}),\ k+1)\big] \tag{24}
$$

with $F(\xi, T) = \big\langle \alpha_T(\xi), \exp\{(\theta/2)\xi' M_T\, \xi\}\big\rangle$.

Proof: Consider equation (23)

$$
F(\xi,\ k) = \inf_{u \in \mathcal{U}_{k,T-1}} \overline{E}\Big[\big\langle \alpha_k^u(\xi)\ ,\ \eta_k^u \big\rangle \,\Big|\, \xi_k = \xi\Big]
$$

Note that the adjoint process η_k is determined from η_{k+1} via the backward recursion of (19), which means we

can specify a functional recursion form $\eta_k = \eta_k^u(\eta_{k+1}^v)$ for this adjoint process. Thus, the value function satisfies

$$\begin{aligned} F(\xi,k) &= \inf_{u\in\mathcal{U}_{k,k}} \inf_{v\in\mathcal{U}_{k+1,T-1}} \overline{E}\Big[\big\langle \alpha_k^u(\xi), \eta_k^u(\eta_{k+1}^v)\big\rangle \,\Big|\, \xi_k = \xi\Big] \\ &= \inf_{u\in\mathcal{U}_{k,k}} \inf_{v\in\mathcal{U}_{k+1,T-1}} \overline{E}\Big[\overline{E}\Big[\big\langle \alpha_{k+1}^u(\xi_{k+1}^u), \eta_{k+1}^v\big\rangle \\ &\qquad \Big| \mathcal{Y}_{k+1} \vee \sigma\{\beta_{k+1}\}, \xi_k = \xi\Big]\Big| \xi_k = \xi\Big] \\ &= \inf_{u\in\mathcal{U}_{k,k}} \overline{E}\Big[\inf_{v\in\mathcal{U}_{k+1,T-1}} \overline{E}\Big[\big\langle \alpha_{k+1}^u(\xi_{k+1}^u), \eta_{k+1}^v\big\rangle \\ &\qquad \Big| \mathcal{Y}_{k+1} \vee \sigma\{\beta_{k+1}\}, \xi_k = \xi\Big]\Big| \xi_k = \xi\Big] \\ &= \inf_{u\in\mathcal{U}_{k,k}} \overline{E}\Big[F(\xi_{k+1}^u(\xi,u,y_{k+1},\beta_{k+1}), k+1)\Big] \end{aligned} \tag{25}$$

□

Due to the lattice property of the control sequences, we interchanged the order of conditional expectation and minimization operations in the last equation of (25). Moreover, the optimal control sequences $u_k^*(\xi_k)$ for each $k = 0,1,\ldots, T-1$ of the dynamic programming problem are indeed the optimal control policies for the original problem stated in (3), i.e., $u^* \in \mathcal{U}_{0,T-1}$.

IV. Conclusion

In this paper we considered a finite-horizon risk-sensitive control problem under a class of DoS attack model when the attacker strategy is to disrupt the network or jam the control packets from reaching the actuator. Using, risk-sensitive criterion, we derived recursive optimal control policy in terms of finite-dimensional dynamics via measure transformation technique, while highlighting one's belief about the system uncertainties into the cost functional. Our results show the optimal control problem will have an implicit formula (that essentially combines estimation and control as a single problem) in terms of the original system matrices and the average path of the DoS attack sequences.

References

[1] E. Bompard, G Ciwei, R. Napoli, A. Russo, M. Masera, and A. Stefanini, "Risk assessment of malicious attacks against power systems," *IEEE Trans. Syst., Man, Cyber.*, *Part A*, vol. 39, no. 5, pp.1074-1085, 2009.

[2] E. Byres and J. Lowe, "The myths and facts behind cyber security risks for industrial control systems," in *Proc. of VDE Congress*, Berlin, Germany, 2004.

[3] G. Ericsson, "Toward a framework for managing information security for an electric power utility-CIGRÉ experiences," *IEEE Trans. Power Del.*, vol. 22, no. 3, pp. 1461-1469, 2007.

[4] T. Moore, D. Pym, C. Ioannidis, R. Anderson and S. Fuloria, "Security economics and critical national infrastructure," in *Economics of Information Security and Privacy,* Springer, pp. 55-66, 2010.

[5] J. Perkel, "Cybersecurity: how safe are your data?" *Nature* 464, pp.1260-1261, 2010.

[6] A. Pinar, J. Meza, V. Donde, and B. Lesieutre, "Optimization strategies for the vulnerability analysis of the power grid," *SIAM J. Optim*., vol. 20, no. 4, pp. 1786-1810, 2010.

[7] S. Amin, A. A. Cardenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Hybrid Systems: Computation and Control*, Springer-Verlag, Berlin/Heidelberg, pp. 31-45, 2009.

[8] 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), 2008.

[9] V.M. Igure and R. D. Williams, "Taxonomies of attacks and vulnerabilities in computer systems," *IEEE Commun. Surv. Tutor.,* vol. 10, no. 1, pp. 6-19, 2008.

[10] U. Lindqvist and E. Jonsson, "How to systematically classify computer security intrusions," in *Proc. 1997 IEEE Symposium on Security and Privacy*, May 1997, pp. 154-163.

[11] K. C. Nguyen, T. Alpcan and T. Basar, "A decentralized Bayesian attack detection algorithm for network security," in *Proc. of 23rd Intl. Information Security Conf*, Milan, Italy, September 2008, pp. 413-428.

[12] D. R. Raymond and S. F. Midkiff, "Denial-of-Service in wireless sensor networks: attacks and defenses," *IEEE Perv. Comput.*, vol. 7, no. 1, pp. 74-81, 2008.

[13] A. Bensoussan and J.H. van Schuppen, "Optimal control of partially observable stochastic systems with an exponential-of-integral performance index," *SIAM J. Control Optim*., vol. 23, no. 4, pp. 599-613, 1985.

[14] D. H. Jacobson, "Optimal stochastic linear systems with exponential performance criteria and their relation to deterministic differential games," *IEEE Trans. Automat. Contr.*, vol. 18, no. 2, pp. 124-131, 1973.

[15] M. R. James, "Asymptotic analysis of nonlinear stochastic risk-sensitive control and differential games," *Math. Contr. Sig. Syst.*, vol. 5, no. 4, pp. 401-417, 1992.

[16] M. R. James, J. Baras and R.J. Elliott, "Risk sensitive control and dynamic games for partially observed discrete-time nonlinear systems," *IEEE Trans. Automat. Contr.,* vol. 39, no. 4, pp. 780-792, 1994.
[17] P. Whittle, "Risk-sensitive linear/quadratic/Gaussian control," *Adv. Appl. Probab*. vol. 13, pp. 764-777, 1981.
[18] G. B. Di Masi and W.J. Runggaldier, "On measure transformations for combined filtering and parameter estimation in discrete time," *Syst. Contr. Lett.*, vol. 2, no. 1, pp. 57-62, 1982.
[19] R. J. Elliott, L. Aggoun and J. B. Moore, *Hidden Markov models: estimation and control*, Springer-Verlag, New York, 1995.
[20] R. S. Liptser and A. N. Shiriyaev, *Statistics of random processes*, Springer-Verlag, New York, 1977.
[21] M. Papa, S. Shenoi, T. Fleury, H. Khurana and V. Welch, "Towards a taxonomy of attacks against energy control systems," in *Critical Infrastructure Protection II*, Springer, Boston, pp. 71-85, 2009.
[22] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, and S. S. Sastry, "Foundations of control and estimation over lossy networks," in *Proc. IEEE*, vol. 95, no. 1, 2007, pp. 163-187.
[23] I. V. Girsanov, "On transforming a certain class of stochastic processes by absolutely continuous substitution of measures," *Theo. Probab. Appl.*, vol. 5, pp. 285-301, 1960.

APPENDIX

The following theorem is the discrete-time version of Girsanov's theorem [23].

Theorem A: Assume the process z_k on the probability space $\{\Omega, \mathcal{F}, P\}$ admit the following representation

$$z_k = f_k + F_k \zeta_k, \quad k = 0,1, \ldots, T \tag{26}$$

where ζ_k is a Gaussian white process with respect to the family of σ sub-algebra $\mathcal{F}_k \subset \mathcal{F}$; and F_k is a matrix sequence with an appropriate dimension. Let ψ_k be another $\mathcal{F}$ predictable process with the same dimension as ζ_k. Next introduce a new probability measure $\overline{P}$ as follows:

$$d\overline{P} = \prod_{k=0}^{T} \exp(\psi_k' \zeta_k - 1/2 |\psi_k|^2)\, dP \tag{27}$$

On this new probability space $\{\Omega, \mathcal{F}, \overline{P}\}$, the process $\overline{\zeta}_k = \zeta_k - \psi_k$ will become a Gaussian white process; moreover, the process z_k admits the following representation $z_k = \bar{f}_k + F_k \overline{\zeta}_k$ where $\bar{f}_k = f_k + F_k \psi_k$.

Proof: The proof follows from the fact that for all Borel sets A, the following identity holds true

$$\overline{E}\left[I_A(\zeta_k) \middle| \mathcal{F}_{k-1} \right] = E\left[\exp(\psi_k' \zeta_k - 1/2 |\psi_k|^2)\, I_A(\zeta_k) \middle| \mathcal{F}_{k-1} \right] \tag{28}$$

□