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

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

Getachew K Befekadu, Vijay Gupta and Panos J Antsaklis

Abstract— **In this paper, we consider the problem of risk-sensitive control under a class of Denial-of-Service (DoS) attack strategies and derive a solution for the optimal control policy when the attacker jams randomly the control packets in the system. For a discrete-time partially observed stochastic system with an exponential running cost, we provide a solution in terms of finite-dimensional dynamics of the system via a measure transformation approach and dynamic programming. We use the risk-sensitive criterion rather than quadratic cost to directly highlight one's belief about system uncertainties back to the cost functional. Moreover, on the transformed measure space, the solution to the optimal control problem appears as if it depends on the average path of the DoS attacks in the system.**

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 electric power grids, industrial control systems and banking/finance sectors (e.g., 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, 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 challenging and important area of research. 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 on control systems, wireless sensor networks and IT infrastructures (e.g., see references [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 models, 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 attack strategies are more sophisticated, including the case of Markov modulated DoS attack model. 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]-[18], 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 were originally 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 allows us to define an equivalent information state (and also the corresponding adjoint measure process) for the partially observed stochastic system that simplifies the optimal control problem as a separated policy problem in terms of this information state [16], [19] and [20]. Moreover, the use of this measure transformation provides a formula that establishes a separation principle for the partially observed stochastic system, i.e., the recursive optimal control policy together with the newly defined information state essentially constitutes an equivalent fully observable stochastic control problem.

This paper is organized as follows. In Section II, we introduce some preliminary concepts and formulate the risk-sensitive control problem under a class of DoS attack models. Section III presents the main result. The solution of the optimal control problem is formally stated 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 sake of completeness.

This work was supported in part by the National Science Foundation under Grants No. CCF-0819865 and CNS-1035655; GKB acknowledges support from the Moreau Fellowship of the University of Notre Dame.

G. K. Befekadu is with the Department of Electrical Engineering, University of Notre Dame, Notre Dame, IN, 46556. gbefekadu1@nd.edu

V. Gupta is with the Department of Electrical Engineering, University of Notre Dame, Notre Dame, IN, 46556. vgupta2@nd.edu

P. J. Antsaklis is with the Department of Electrical Engineering, University of Notre Dame, Notre Dame, IN, 46556. antsaklis.1@nd.edu

II. PROBLEM FORMULATION

A. Process Model and Cost Function

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

$$\begin{aligned} x_{k+1} &= Ax_k + \beta_{k+1}Bu_k + \nu_{k+1} \\ y_{k+1} &= Cx_k + \ w_{k+1} \\ & k = 0, 1, \ldots, T-1 \end{aligned} \tag{1}$$

where $x_k \in \mathbb{R}^n$ is the state of the system, $u_k \in \mathbb{R}^m$ is the control input, $y_k \in \mathbb{R}^p$ is the observation output, $\beta_k \in \{0, 1\}$ is the DoS attack sequence that disrupts the control packets from reaching the actuator. We assume the process noise ν_k and measurement noise w_k are 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 assumed to be positive definite. Denial of service is a popular attack model for cyber-physical systems (e.g., see references [7], [9], [21]). Fig. 1 shows other malicious cyber attacks in a control system: $A1$ and $A3$ represent integrity or deception type attacks, $A2$ and $A4$ are DoS type attacks, and $A5$ is a direct physical attack in the system.

Let $\mathcal{Y}_k$ denote the complete filtration generated by $\{y_1, y_2, \ldots, y_k\}$, while $\mathcal{B}_k = \{\beta_0, \beta_1, \ldots, \beta_k\}$ denotes the corresponding DoS attack sequences which are assumed to be independent to the other random variables in the system. Moreover, the admissible controls $\{u_0, u_1, \ldots, u_{T-1}\}$ are $\mathbb{R}^m$ - valued sequences and considered to be adapted process (i.e., non-anticipating processes that depend on the output sequences and DoS attacks path). 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

$$\begin{aligned} J(u) =& (1/\theta)E\left[exp\left\{ (\theta/2)\left\{ \sum_{k=0}^{T-1} (x_k'Mx_k \right.\right.\right. \\ & \left.\left.\left. + \beta_{k+1}u_k'Nu_k) + x_T'M_Tx_T \right\}\right\}\right] \end{aligned} \tag{2}$$

where $\theta > 0$ is the risk-sensitive parameter, $u \in \mathcal{U}_{0,T}$ is an admissible control sequence, while $E[.]$ denotes the expectation with respect to the 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 class of DoS attack models, i.e.,

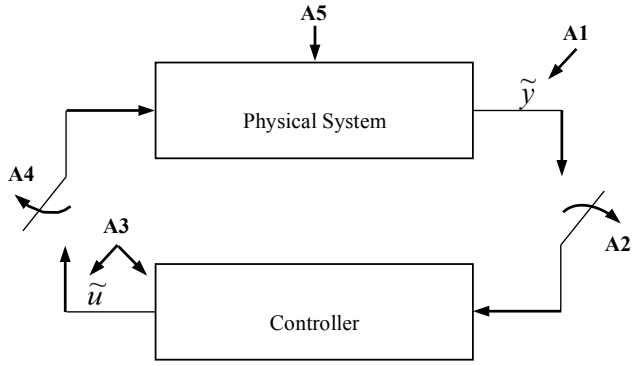

Fig. 1. Typical malicious cyber attacks in control systems

$$\begin{aligned} F_0 &= \inf_{u \in \mathcal{U}_{0,T-1}} J(u) \\ &= \inf_{u \in \mathcal{U}_{0,T-1}} (1/\theta)E\left[exp\left\{ (\theta/2)\left\{ \sum_{k=0}^{T-1} (x_k'Mx_k \right.\right.\right. \\ & \left.\left.\left. + \beta_{k+1}u_k'Nu_k) + x_T'M_Tx_T \right\}\right\}\right] \end{aligned} \tag{3}$$

Here we consider the class of DoS attack models as Bernoulli packet drops due to network jams induced by the attacker at each time k with success probability β_k. In general, this attack model $\mathcal{A}_{Ber(\beta)}$ will have the following attack sequences or path

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

We remark that the exponential running cost function weighted by a risk-sensitive parameter θ highlights the belief of the designer about system uncertainty 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 a linear quadratic Gaussian (LQG) control problem. A similar idea is followed by Amin et al. [7] using the LQG control problem formulation under a class of DoS attack models, but in a different context. Schenato et al. [22] have also considered the LQG control problem in the context of network reliability for Bernoulli type packet drops and their effect on the performance of the control system.

III. CHANGE OF MEASURE AND SOLUTION TO RISK-SENSITIVE CONTROL PROBLEM UNDER A DoS ATTACK MODEL

In this section, we use a measure transformation technique to derive the optimal control policy for the risk-sensitive control problem under a class of DoS attack models. The key idea is to introduce measure transformation technique under which the observation and state variables become independent along the anticipated DoS attack sequences or path in the system. This allows us to obtain recursive formulas for the equivalent information state and the associated adjoint process based on the observation history, the current control

input and the anticipated DoS attack sequences or path. Using this fact, we further derive a formula that establishes the separation principle for the partially observed stochastic system.

A. Change of Measure and Finite-Dimensional Information State

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

$$\Lambda^u_{0,0} = 1$$
$$\Lambda^u_{1,k} = \prod_{l=1}^{k} \frac{\varphi(x_l - Ax_{l-1} - \beta_l Bu_{l-1})\phi(y_l - Cx_{l-1})}{\varphi(x_l)\phi(y_l)} \quad k = 1, 2, \ldots, T \tag{5}$$

Using this random variable, we can introduce another equivalent measure transformation $\bar{P}$ as follows

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

Under this measure transformation $\bar{P}$, the state x_k and the observation y_k will become normal densities and independent to each other. Moreover, the restriction of the Radon-Nikodym derivative implies the measure $[\Lambda^u_{0,k}]^{-1}$ is a martingale process with respect to the complete filtration (e.g., see references [19], [23], [24]). This fact is also a direct application of Girsanov's theorem [24]. 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.

Consider the following measure process for any admissible control u and DoS attack sequences in the system

$$\alpha^u_k(x)dx = \bar{E}\left[\ \Lambda^u_{0,k} exp(\theta D^u_{0,k-1}) I_A(x_k \in dx) \ \middle|\ \mathcal{Y}_k \vee \mathcal{B}_k\ \right] \quad k = 0, 1, \ldots, T \tag{7}$$

where $I_A(x_k \in dx)$ is the indicator function for the Borel set A, $D^u_{j,k}$ is the quadratic running function given by $D^u_{j,k} = (1/2)\sum_{l=j}^{k}\left(x_l' M x_l + \beta_{l+1} u_l' N u_l\right)$ for $0 \le j \le k \le T-1$. Moreover, the initial boundary condition for this measure valued process is specified by $\alpha^u_0(x_0) = \varphi(x_0)$.

Then, we obtain the following theorem.

Theorem 1: The measure valued process $\alpha^u_k(x)$ satisfies the following forward recursion

$$\alpha^u_{k+1}(x)dx = \frac{1}{\phi(y_{k+1})}\int_{B(\mathbb{R}^n)} exp(\theta D^u_{k,k})\varphi(x - A\xi - \beta_{k+1}Bu_k) \times \phi(y_{k+1} - C\xi)\alpha^u_k(\xi)d\xi \tag{8}$$

where $D^u_{k,k} = (1/2)(\xi' M \xi + \beta_{k+1} u_k' N u_k)$.

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

$$\begin{aligned}
&\int_{B(\mathbb{R}^n)} f(z)\alpha^u_{k+1}(z)dz \\
&= \bar{E}\left[\ f(x_{k+1})\Lambda^u_{0,k+1} exp(\theta D^u_{0,k}) \ \middle|\ \mathcal{Y}_{k+1} \vee \mathcal{B}_{k+1}\ \right] \\
&= \bar{E}\left[\ f(Ax_k + \beta_{k+1}Bu_k + \nu_{k+1})\Lambda^u_{0,k} exp(\theta D^u_{0,k-1}) \right. \\
&\quad \times \frac{\varphi(x_{k+1} - Ax_k - \beta_{k+1}Bu_k)\phi(y_{k+1} - Cx_k)}{\varphi(x_{k+1})\phi(y_{k+1})} \\
&\quad \left. \times exp(\theta D^u_{k,k}) \ \middle|\ \mathcal{Y}_{k+1} \vee \mathcal{B}_{k+1}\ \right] \\
&= \frac{1}{\phi(y_{k+1})}\bar{E}\left[\ \int_{B(\mathbb{R}^n)} f(Ax_k + \beta_{k+1}Bu_k + \nu)\Lambda^u_{0,k} exp(\theta D^u_{0,k-1}) \right. \\
&\quad \left. \times \varphi(\nu)d\nu\phi(y_{k+1} - Cx_k) exp(\theta D^u_{k,k}) \ \middle|\ \mathcal{Y}_{k+1} \vee \mathcal{B}_{k+1}\ \right] \\
&= \frac{1}{\phi(y_{k+1})}\int_{B(\mathbb{R}^n)}\int_{B(\mathbb{R}^n)} f(A\xi + \beta_{k+1}Bu_k + \nu) exp(\theta D^u_{k,k}) \\
&\quad \times \varphi(\nu)\phi(y_{k+1} - C\xi)\alpha^u_k(\xi)d\xi d\nu
\end{aligned} \tag{9}$$

With change of variable $z = A\xi + \beta_{k+1}Bu_k + \nu$, we have

$$\int_{B(\mathbb{R}^n)} f(z)\alpha^u_{k+1}(z)dz = \frac{1}{\phi(y_{k+1})}\int_{B(\mathbb{R}^n)}\int_{B(\mathbb{R}^n)} f(z) exp(\theta D^u_{k,k}) \times \varphi(z - A\xi - \beta_{k+1}Bu_k)\phi(y_{k+1} - C\xi)\alpha^u_k(\xi)d\xi dz \tag{10}$$

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

Due to the linearity of the system (about the average/anticipated DoS attack path), the measure valued process $\alpha^u_k(x)$ has a normal density and is given by

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

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

$$R_{k+1}^{-1}(u) = 2\theta M + C'\Gamma^{-1}C + \Sigma^{-1}\left\{I - Ar^{-1}(u)A'\Sigma^{-1}\right\} \tag{12}$$

$$\mu_{k+1}(u) = R_{k+1}^{-1}(u)\left\{\ C'\Gamma^{-1}y_{k+1} + \Sigma^{-1}Ar^{-1}(u)R_k^{-1}(u)\mu_k(u) + \left(\ I + \Sigma^{-1}Ar^{-1}(u)A'\ \right)\Sigma^{-1}B\ \right\} \tag{13}$$

$$Z_{k+1}(u) = Z_k(u)(2\pi)^{-n/2}|\Sigma|^{-n/2} exp\left\{\ -\tfrac{1}{2}\left(\ z(u) - (\ R_{k+1}^{-1}(u)\mu_{k+1}(u)\ )'\ R_{k+1}^{-1}(u)\mu_{k+1}(u)\ \right)\right\} \tag{14}$$

where

$$r(u) = A'\Sigma^{-1}A + R_k^{-1}(u)$$

and

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

Therefore, the measure valued process $\alpha^u_k(x)$ (i.e., the information state for this partially observed stochastic system)

is determined by the following parameters $Z_k(u)$, $R_k^{-1}(u)$ and $\mu_k(u)$ that involve coupled forward recursive relations.

With minor abuse of notation, we consider these parameters as an new information state variables for the system

$$\zeta_k^u(u) = (\, Z_k(u), R_k^{-1}(u), \mu_k(u)\,) \tag{15}$$

Furthermore, we can rewrite the measured process $\alpha_k^u(x)$ as follows

$$\begin{aligned}\alpha_k^u(x) &= \alpha_k^u\,(\,\zeta_k^u(u), x\,)\\ &= Z_k(u) exp\,\{\,-\tfrac{1}{2}\,(\,x-\mu_k(u)\,)'\,R_k^{-1}(u)\,(\,x-\mu_k(u)\,)\}\end{aligned} \tag{16}$$

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

B. Solution to Risk-Sensitive Control Problem Under a Class of DoS Attack Models

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 the equivalent probability measure transformation is given as follows

$$\begin{aligned}J(u) &= (1/\theta)E\Big[\, exp\Big\{\,(\theta/2)\Big\{\sum_{k=0}^{T-1}(\,x_k'Mx_k\\ &\qquad +\beta_{k+1}u_k'Nu_k\,) + x_T'M_Tx_T\,\Big\}\Big\}\Big]\\ &= (1/\theta)\bar{E}\Big[\,\Lambda_{0,T}^u exp\Big\{\,(\theta/2)\Big\{\sum_{k=0}^{T-1}(x_k'Mx_k\\ &\qquad +\beta_{k+1}u_k'Nu_k) + x_T'M_Tx_T\,\Big\}\Big\}\Big]\\ &= (1/\theta)\bar{E}\Big[\,\Lambda_{0,T}^u exp(\theta D_{0,T-1}^u) exp\{(\theta/2)x_T'M_Tx_T\}\,\Big]\\ &= (1/\theta)\bar{E}\Big[\,\bar{E}\Big[\,\Lambda_{0,T}^u exp(\theta D_{0,T-1}^u)\\ &\qquad \times exp\{(\theta/2)x_T'M_Tx_T\}\,\Big|\,\mathcal{Y}_T\vee\mathcal{B}_T\,\Big]\Big]\\ &= (1/\theta)\bar{E}\Big[\int_{B(\mathbb{R}^n)} exp\{(\theta/2)x'M_Tx\}\alpha_T(x)dx\Big]\end{aligned} \tag{17}$$

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

$$\begin{aligned}J(u) &= (1/\theta)\bar{E}\Big[\,\Lambda_{0,T}^u exp(\theta D_{0,T-1}^u) exp\{(\theta/2)x_T'M_Tx_T\}\,\Big]\\ &= (1/\theta)\bar{E}\Big[\,\Lambda_{0,k}^u\Lambda_{k+1,T}^u exp(\theta D_{0,k-1}^u) exp(\theta D_{k,T-1}^u)\\ &\qquad \times exp\{(\theta/2)x_T'M_Tx_T\}\,\Big]\\ &= (1/\theta)\bar{E}\Big[\,\Lambda_{0,k}^u exp(\theta D_{0,k-1}^u)\bar{E}\Big[\,\Lambda_{k+1,T}^u\ exp(\theta D_{k,T-1}^u)\\ &\qquad \times exp\{(\theta/2)x_T'M_Tx_T\}\,\Big|\,\sigma\{x_k\}\vee\mathcal{Y}_T\vee\mathcal{B}_T\,\Big]\Big]\end{aligned} \tag{18}$$

where the inner expectation involves only conditioning on $\sigma\{x_k\}$ due to the Markov property of x_k. Define a new adjoint process

$$\begin{aligned}\eta_k^u(x_k) = \bar{E}\Big[\,&\Lambda_{k+1,T-1}^u exp(\theta D_{k+1,T-1}^u)\Lambda_{T,T}^u\\ &exp\,\{\,(\theta/2)x_T'M_Tx_T\,\}\Big|\,\sigma\{x_k\}\vee\mathcal{Y}_T\vee\mathcal{B}_T\,\Big]\end{aligned} \tag{19}$$

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

$$\begin{aligned}J(u) &= (1/\theta)\bar{E}\Big[\,\Lambda_{0,k}^u exp(\theta D_{0,k-1}^u)\eta_k^u(x_k)\,\Big]\\ &= (1/\theta)\bar{E}\Big[\,\bar{E}\Big[\,\Lambda_{0,k}^u exp(\theta D_{0,k-1}^u)\eta_k^u(x_k)\,\Big|\,\mathcal{Y}_T\vee\mathcal{B}_T\,\Big]\Big]\\ &= (1/\theta)\hat{E}\Big[\int_{B(\mathbb{R}^n)}\alpha_k^u(x)\eta_k^u(x)dx\,\Big]\\ &= (1/\theta)\hat{E}\,[\,\langle\alpha_k^u(x),\eta_k^u(x)\rangle\,]\end{aligned} \tag{20}$$

which is independent of k.

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

$$\begin{aligned}\eta_k^u(x_k) = \int_{B(\mathbb{R}^n)}&\frac{\phi(y_{k+1}-Cx_k)}{\phi(y_{k+1})}\varphi(x-Ax_k-\beta_{k+1}Bu_k)\\ &\times exp(\theta D_{k,k}^u)\eta_{k+1}^u(x)dx\end{aligned} \tag{21}$$

Proof: From (19), $\eta_k^u(x)$ is given by

$$\begin{aligned}\eta_k^u(x_k) &= \bar{E}\Big[\,\Lambda_{k+1,T}^u exp(\theta D_{k,T-1}^u) exp\{(\theta/2)x_T'M_Tx_T\}\\ &\qquad \Big|\,\sigma\{x_k\}\vee\mathcal{Y}_T\vee\mathcal{M}_T\,\Big]\\ &= \bar{E}\Big[\,\bar{E}\Big[\,\Lambda_{k+2,T}^u\frac{\varphi(x_{k+1}-Ax_k-\beta_{k+1}Bu_k)\phi(y_{k+1}-Cx_k)}{\varphi(x_{k+1})\phi(y_{k+1})}\\ &\qquad \times exp(\theta D_{k,k}^u) exp(\theta D_{k+1,T-1}^u) exp\{(\theta/2)x_T'M_Tx_T\}\\ &\qquad \Big|\,\sigma\{x_k,x_{k+1}\}\vee\mathcal{Y}_T\vee\mathcal{M}_T\,\Big]\Big|\,\sigma\{x_k\}\vee\mathcal{Y}_T\vee\mathcal{M}_T\,\Big]\\ &= \bar{E}\Big[\,\frac{\varphi(x_{k+1}-Ax_k-\beta_{k+1}Bu_k)\phi(y_{k+1}-Cx_k)}{\varphi(x_{k+1})\phi(y_{k+1})}\\ &\qquad \times exp(\theta D_{k,k}^u)\eta_{k+1}^u(x_{k+1})\,\Big|\,\sigma\{x_k\}\vee\mathcal{Y}_T\vee\mathcal{M}_T\,\Big]\end{aligned} \tag{22}$$

Using the independent property under $\bar{P}$, integrating the last equation of (22) with respect to x_{k+1} gives equation (21) of Theorem 2. □

Moreover, the adjoint process η_k^u is given by the following equivalent relation (c.f. equation (11))

$$\eta_k^u(x) = \tilde{Z}_k(u)\ exp\,\{\,-\tfrac{1}{2}\,(\,x-\gamma_k(u)\,)'\,S_k^{-1}(u)\,(\,x-\gamma_k(u)\,)\} \tag{23}$$

where the finite-dimensional parameters $\tilde{Z}_k(u)$, $S_k^{-1}(u)$ and $\gamma_k(u)$ satisfy coupled backward recursions. The boundary condition for the adjoint process is given by

$$\eta_T^u(x_T) = \Lambda_{T,T}^u exp\,\{\,(\theta/2)x_T'M_Tx_T\,\} \tag{24}$$

From equations (8) and (11), 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 recursions. Thus, based on the current value of ζ_k^u together with the new observation y_{k+1}, the current control u_k

and the anticipated attack sequence β_{k+1}, the next value for ζ^u_{k+1} can be determined by the following functional relation

$$\zeta^u_{k+1} = \zeta^u_{k+1}\ (\ \zeta^u_k, u_k, y_{k+1}, \beta_{k+1}\ ) \tag{25}$$

Suppose at some intermediate time k, $0 < k < T$, the information state ζ^u_k is given by $\zeta = (Z(u), R^{-1}(u), \mu(u))$, then from equation (20), the value function for the optimal control problem satisfies the following

$$F(\zeta, k) = \inf_{u \in \mathcal{U}_{k,T-1}} \bar{E}\left[\ \langle \alpha^u_k, \eta^u_k \rangle \ \middle|\ \alpha_k = \alpha_k(\zeta)\ \right] \tag{26}$$

Theorem 3: The value function satisfies the following recursion

$$F(\zeta, k) = \inf_{u \in \mathcal{U}_{k,k}} \bar{E}\left[\ F\ (\ \zeta^u_{k+1}\ (\ \zeta, u, y_{k+1}, \beta_{k+1}\ ), k+1\ )\right] \tag{27}$$

with $F(\zeta, T) = \langle \alpha_T(\zeta), exp\ \{\ (\theta/2)\zeta M_T \zeta\ \}\rangle$.

Proof: Consider equation (26)

$$F(\zeta, k) = \inf_{u \in \mathcal{U}_{k,T-1}} \bar{E}\left[\ \langle \alpha^u_k(\zeta), \eta^u_k \rangle \ \middle|\ \zeta_k = \zeta\ \right]$$

Note that the adjoint process η_k is determined from η_{k+1} via the backward recursion of (21), i.e., for the adjoint process, we can specify a functional recursion equation in the form of $\eta_k = \eta^u_k(\eta^u_{k+1})$. Thus, the value function satisfies

$$\begin{aligned}
F(\zeta, k) &= \inf_{u \in \mathcal{U}_{k,k}} \inf_{v \in \mathcal{U}_{k+1,T-1}} \bar{E}\ \left[\ \langle \alpha^u_k(\zeta), \eta^u_k(\eta^u_{k+1}) \rangle \ \middle|\ \zeta_k = \zeta\ \right] \\
&= \inf_{u \in \mathcal{U}_{k,k}} \inf_{v \in \mathcal{U}_{k+1,T-1}} \bar{E}\left[\ \bar{E}\left[\ \langle \alpha^u_{k+1}(\zeta_{k+1}), \eta^u_{k+1} \rangle \right.\right. \\
&\qquad \left.\left. \ \middle|\ \mathcal{Y}_{k+1} \vee \sigma\{\beta_{k+1}\}, \zeta_k = \zeta\ \right] \middle|\ \zeta_k = \zeta\ \right] \\
&= \inf_{u \in \mathcal{U}_{k,k}} \bar{E}\left[\ \inf_{v \in \mathcal{U}_{k+1,T-1}} \bar{E}\ \left[\ \langle \alpha^u_{k+1}(\zeta_{k+1}), \eta^u_{k+1} \rangle \right.\right. \\
&\qquad \left.\left. \ \middle|\ \mathcal{Y}_{k+1} \vee \sigma\{\beta_{k+1}\}, \zeta_k = \zeta\ \right] \middle|\ \zeta_k = \zeta\ \right] \\
&= \inf_{u \in \mathcal{U}_{k,k}} \bar{E}\left[\ F\ (\ \zeta^u_{k+1}\ (\ \zeta, u, y_{k+1}, \beta_{k+1}\ ), k+1\ )\right]
\end{aligned} \tag{28}$$

□

Due to the lattice property of the control sequences, we interchanged the order of conditional expectation and minimization operations in the last equation of (28). Moreover, the optimal control sequences $u^*_k(\zeta_k)$ 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 models when the attacker strategy is to disrupt the network or jam the control packets from reaching the actuator. Using measure transformation technique and dynamic programming, we derived a recursive optimal control policy in terms of the finite-dimensional dynamics of the system, i.e., the recursive optimal control policy together with the newly defined information state essentially constitutes an equivalent fully observable stochastic control problem. Moreover, the solution to the optimal control problem appeared as if it depends on the average sequences or path of the DoS attack in the system.

APPENDIX

The following theorem is the discrete-time version of Girsanov's theorem [24].

Theorem 4: Let the process z_k on the probability space $(\Omega, \mathcal{F}, P)$ admits the following representation

$$z_k = f_k + H_k \zeta_k, \quad k = 0, 1, \ldots, T \tag{29}$$

where ζ_k is a Gaussian white process with respect to the family of σ sub-algebra $\mathcal{F}_k \subset \mathcal{F}$ and H_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 $\bar{P}$ with the Radon-Nikodym derivative as

$$d\bar{P} = \prod_{k=0}^{T} exp\ (\ \psi'_k \zeta_k - \tfrac{1}{2}|\psi_k|^2\ )\ dP \tag{30}$$

On this new probability space $(\Omega, \mathcal{F}, \bar{P})$, the process $\bar{\zeta}_k = \zeta_k - \psi_k$ will then become a Gaussian white process.

Moreover, the process z_k admits the following representation

$$z_k = \bar{f}_k + H_k \bar{\zeta}_k, \quad k = 0, 1, \ldots, T \tag{31}$$

where $\bar{f}_k = f_k + H_k \psi_k$.

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

$$\bar{E}\left[I_A(\zeta_k) | \mathcal{F}_{k-1}\right] \quad = E\left[exp\ (\ \psi'_k \zeta_k - \tfrac{1}{2}|\psi_k|^2\ )\ I_A(\zeta_k)\ \middle|\ \mathcal{F}_{k-1}\right] \tag{32}$$

□

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-CIGR 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. 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] I. I. Petersen, M. R. James and P. Dupuis, "Optimal control of stochastic uncertain systems with relative entropy constraints," *IEEE Trans. Automat. Contr.*, vol. 45, no. 3, pp. 398-412, 2000.

[18] P. Whittle, "Risk-sensitive linear/quadratic/Gaussian control," *Adv. Appl. Probab.*, vol. 13, pp. 764-777, 1981.

[19] 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.

[20] R. J. Elliott, L. Aggoun and J. B. Moore, *Hidden Markov models: estimation and control*, Springer-Verlag, New York, 1995.

[21] 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] R. S. Liptser and A. N. Shiriyaev, *Statistics of random processes*, Springer-Verlag, New York, 1977.

[24] 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.