RISK-SENSITIVE CONTROL UNDER A MARKOV MODULATED DENIAL-OF-SERVICE ATTACK MODEL

Technical Report of the ISIS Group
University of Notre Dame
ISIS-2010-004
November, 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 MARKOV MODULATED DENIAL-OF-SERVICE ATTACK MODEL

GETACHEW K. BEFEKADU, VIJAY GUPTA AND PANOS J. ANTSAKLIS

Abstract. This paper discusses the problem of risk-sensitive stochastic control under a Denial-of-Service (DoS) attack strategy in which the attacker stochastically jams the control packets. We model the attacker using a hidden Markov process and the plant as a discrete-time partially observed system with an exponential running cost function, where the latter is used to emphasize directly the designer's belief about system uncertainty back to the cost function. Through a chain of measure transformation techniques and dynamic programming, we derive the optimal control policy in terms of the original system matrices which surprisingly satisfies a separation principle, i.e., constitutes implicitly an equivalent fully observable stochastic control problem via the newly defined information state. Moreover, on the transformed measure space, the solution for the optimal control problem appears as if it depends on the average of anticipated DoS attack sequences in the system.

1. Introduction

Recently, increasing effort has been placed in addressing the problem of risk and vulnerability assessment to malicious attacks against 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 dynamics, distributed structure with a continued deployment of new IT technology, solutions that ensure security against malicious cyber attacks will gain even more importance. A systematic study of design approaches that provide provable security against faults and malicious attacks is a core area of research. In particular, since such cyber-physical systems will couple control of critical infrastructure with communication networks, there is a need to study the impact of cyber attacks in control systems. Accordingly, there have appeared many recent works that consider security requirements, attacks, and vulnerabilities in control systems, wireless sensor networks and IT infrastructures (e.g., [7]-[14]).

By modeling the attacker as inducing a network disruption at every time step according to a Bernoulli process, Amin *et al.* [7] considered the LQG control problem and Befekadu *et al.* [15] considered the risk-sensitive control problem. In this work, we extend the attacker model from a memoryless Bernoulli process to one that follows a hidden Markov model and derive the optimal risk-sensitive control policy. Our choice of a risk-sensitive cost function is motivated by its use in

University of Notre Dame, ISIS Laboratory, ISIS Technical Report # ISIS-2010-004, October, 2010.

G. K. Befekadu is with the Department of Electrical Engineering, University of Notre Dame, USA.
E-mail: gbefekadu1@nd.edu.

V. Gupta is with the Department of Electrical Engineering, University of Notre Dame, USA.
E-mail: vgupta2@nd.edu.

P. J. Antsaklis is with the Department of Electrical Engineering, University of Notre Dame, USA.
E-mail: antsaklis.1@nd.edu.

robust control and dynamic games, where this criterion has proven an effective tool in mapping a priori knowledge of the system parameters to the cost functional [16]-[20]. We would also like to mention that the problem of optimal control when control packets are being erased has been studied in networked control systems literature (e.g., [21]-[27]).

Our main technical tool is a chain of probability measure transformations that allow us to consider the optimal control design problem merely on the average path followed by the attacker. Initially, we introduce a new probability measure that characterizes the nature of DoS attack sequences relative to all existing random variables (i.e., relative to the original probability space on which all random variables originally defined). In this new probability measure space, the DoS attack sequences show independent character over their observed values. Once this is accomplished, we introduce another probability measure transformation that characterizes separately the plant state and observation variables of the partially observed stochastic system. Specifically, the latter measure transformation is derived in such a way to make the plant state and observation sequences independent while the other variables remained unaffected under it. Finally, we combine these measure transformations to obtain a system characterization in which the DoS attack sequences are independent over their observed values; while the plant observation sequences are mutually independent to the other measure variables in the system. This final step will allow us to define an equivalent information state (together with the corresponding adjoint measure process) for the partially observed stochastic system [19], [28], [29]. We can then prove a separation principle that implicitly separates the optimal control problem from the estimation problem via this information state, and effectively the optimal control problem constitutes fully-observable system. It may be noted that such a separation principle is not a priori obvious given the risk-sensitive cost function and the hidden Markov process based attacker model.

This paper is organized as follows. In Section 2, we define our notation and formulate the main problem for risk-sensitive control problem under a Markov modulated DoS attack model. Section 3 presents the main results. Solution for the optimal control problem is formally stated and the associated recursive solution for the optimal cost value is derived. Finally, Section 4 provides concluding remarks. A short description of Girsanov's theorem is also included in the Appendix for the sake of completeness.

2. Problem Formulation

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

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

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, $\chi(Z_k) \in \{0, 1\}$ is the DoS attack sequence that disrupts the control packets from reaching the actuator while Z_k is related to the internal state of the attacker which is discussed in Section 2.2. We assume the process noise ν_k and measurement noise 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 assumed to be positive definite. Denial of service is a popular attack model for cyber-physical systems (see references [7], [8], [30]). Other attack models such as integrity (or deception) type attacks or direct physical attacks can also be considered. Figure 1 shows typical malicious cyber

attacks in control systems: $A1$ 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 $\{y_1, y_2, \ldots, y_k\}$. We assume that the anticipated DoS attack sequences follow a Markov process model and are independent to the other random 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 adapted process (or non-anticipating process). 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

$$J(u) = (1/\theta)E\left[exp\left\{ (\theta/2)\left\{ \sum_{k=0}^{T-1}(x_k' M x_k + \chi(Z_{k+1})u_k' N u_k) + x_T' M x_T \right\}\right\}\right] \tag{2}$$

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

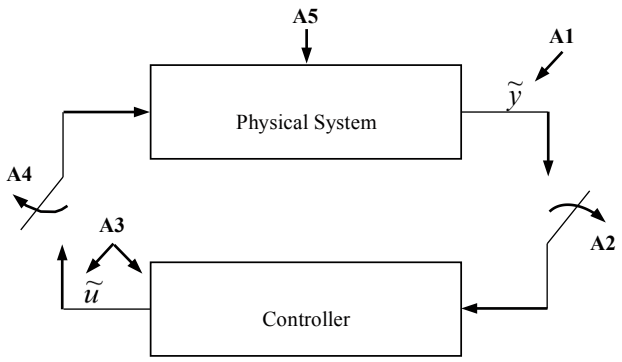

FIGURE 1. *Typical malicious cyber attacks in control systems*

2.2. **Markov Modulated DoS Attack Model.** Consider a process $\{\mathcal{Y}_k\}_{k\in N}$ which is an $\mathcal{R}^d$ - valued Markov process with dynamics

$$Y_k = F_k(Y_{k-1}) + W_k \tag{3}$$

where Y_0 is assumed to have known initial distribution or constant value, $\{F_k(.)\}_{k\in N}$ is a bounded $\mathcal{R}^d$ - valued measurable function and $\{W_k\}_{k\in N}$ is a sequence of $\mathcal{R}^d$ - valued independent random variables with density function $\{\psi_k(.)\}_{k\in N}$.

Let $\{Z_k\}_{k\in N}$ be a two-dimensional stochastic process with finite state-space. Without loss of generality, we take the state-space to be the set of a standard basis in $\mathcal{R}^2$, i.e., $S = \{e_1, e_2\}$, where the vector e_i has one in the i-th position and zero elsewhere for $i = 1, 2$. Moreover, define the complete filtration $\mathcal{F}_0 = \sigma\{Z_0, Y_0, Y_1\}$ and $\mathcal{F}_k = \sigma\{Z_l, Y_{l+1}, l \le k, k \ge 1\}$. We assume that the process Z is a conditional Markov chain, i.e.,

$$\begin{aligned} P[Z_k = e_j|\mathcal{F}_{k-1}] &= P[Z_k = e_j|Z_{k-1}, Y_k] \\ &= a_j(Z_{k-1}, Y_k) = \sum_{i=1}^{2} a_{ji}(Y_k)\langle Z_{k-1}, e_j\rangle \end{aligned} \tag{4}$$

where $\langle .,. \rangle$ is the inner product and $A(y) = [a_{ji}(y)]$ is a 2×2 matrix function defined on $\mathcal{R}^d$ such that for all $y \in \mathcal{R}^d$ the following conditions are satisfied

$$\begin{aligned} 0 <& a_{ji} < 1 \\ \sum_{i=1}^{2} a_{ji}(y) &= 1, \quad i,j = 1,2 \end{aligned} \tag{5}$$

From equations (3), (4) and (5), we note that the process $\{Z_k\}_{k \in N}$ has the following representation

$$Z_k = F_k(Y_k) Z_{k-1} + V_k \tag{6}$$

where the process $\{V_k\}_{k \in N}$ is an $\mathcal{F}_k$ - martingale increment, i.e., $E[V_k | \mathcal{F}_{k-1}] = 0$.

Define a discrete-time counting process N_k^r that counts the number of times the process Z has been in state r up to time k

$$\begin{aligned} N_k^r &= \sum_{l=1}^{k} \langle Z_l, e_r \rangle \\ &= \sum_{l=1}^{k} a_r(Z_{l-1}, Y_l) + M_k^r \end{aligned} \tag{7}$$

where the process $\{M_k^r\}$ is an $\mathcal{F}_k$ - martingale increment, i.e., $E[M_k^r | \mathcal{F}_{k-1}] = 0$.

In the following, we assume that the Markov signal $\{Y_k\}_{k \in N}$ is not directly observed, but through another $\mathcal{R}^d$ - valued random process $\{Q_{N_k^r}\}_{k \in N}$ such that

$$P\left[Q_{N_k^r} \in dq, Z_k = e_r | \mathcal{F}_{k-1}\right] = a_r(Z_{k-1}, Y_k) \lambda_k^r(Y_k, q) dq \tag{8}$$

where $\lambda_k^r(Y_k, .)$ is a probability density function defined on $\mathcal{R}^d$ for every $q \in \mathcal{R}^d$.

Thus, we can associate another random variable using the following representation

$$\begin{aligned} m_k^r(dq) &= \langle Z_k, e_r \rangle I_Q(Q_{N_k^r} \in dq) \\ &= a_r(Z_{k-1}, Y_k) \lambda_k^r(Y_k, q) dq + U_k^r \end{aligned} \tag{9}$$

where $\{U_k^r\}$ is an $\mathcal{F}_k$ - martingale increment and $I_Q(.)$ stands for an indicator function.

Therefore, the complete filtration generated by this observation process is given by

$$\mathcal{M}_k = \sigma\left\{m_l^r(\mathcal{E}), l \leq k, r = 1,2 \text{ and } \mathcal{E} \in \mathrm{B}(\mathcal{R}^{\mathrm{d}})\right\} \tag{10}$$

where $\mathcal{E}$ is a Borel set of $B(\mathcal{R}^d)$.

Let us associate the evolution of the random process $\{Z_k\}_{k \in N}$ to another $\{\chi(Z_k)\}_{k \in N}$ process, where $\chi(Z_k)$ is binary random variable (i.e., $\chi(Z_k) \in \{0,1\}$ with $\chi(Z_0) = 0$). We can achieve this via a sequence of bijective/one-to-one mapping functions (e.g., $\chi(Z_k) = [0,1] Z_k$ as a bijective mapping). Note that the distribution for this process depends on the state of the hidden Markov process, namely, the probability of its success changes with respect to the Markov process. We specifically exploit this property for our DoS attack model realization. Although, $\{\chi(Z_k)\}_{k \in N}$ is a sequence of identically distributed binary random variables, they are not necessarily ordinary Bernoulli processes since they are not independent in the original probability measure space. Moreover, the discrete-time counting process, which is given by (7), records a particular event that has been followed and its measured-information equally serve for this process. Therefore, equations (9) and (10) provide effectively the observation model for our modulated Markov random sequences.

2.3. **Problem Statement.** The problem considered in this paper is stated as follows.

Find an optimal control policy for the finite-horizon risk-sensitive control problem under a Markov modulated DoS attack model, i.e.,

$$\begin{aligned} F_0 &= \inf_{u\in\mathcal{U}_{0,T-1}} J(u) \\ &= \inf_{u\in\mathcal{U}_{0,T-1}} (1/\theta)E\left[exp\left\{ (\theta/2)\left\{ \sum_{k=0}^{T-1}(x_k'Mx_k \ + \chi(Z_{k+1})u_k'Nu_k) + x_T'Mx_T \right\}\right\}\right] \end{aligned} \tag{11}$$

Here we consider the DoS attack sequences as a Markov modulated packet drops due to network jams induced by the attacker at each time k with success probability $\chi(Z_k)$. In general, this attack model $\mathcal{A}_{\mathcal{M}(\chi(Z_k)}$ will have the following attack path

$$\mathcal{A}_{\mathcal{M}(\chi(Z_k)} = \{\chi(Z_0), \chi(Z_1), \ldots, \chi(Z_T)\} \tag{12}$$

We remark that the exponential running cost function weighted by a risk-sensitive parameter θ highlights designer's belief 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 an LQG control problem.

3. Change of Measure and Solution to Risk-Sensitive Control Problem under a Markov Modulated DoS Attack Model

In this section, we explicitly use the measure transformation technique to derive the optimal control policy for the risk-sensitive control problem under a Markov modulated DoS attack model. 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 associated adjoint process based on the observation history, the current control input and the anticipated DoS attack path or sequences. 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) via the dynamic programming.

3.1. **Change of Measure for the DoS Attack Model.** Suppose the following random variables are given on a new probability space $(\Omega, \mathcal{F}, \bar{P})$ under which the random variable Q is not affected by the random variables Y, Z and m:

- $\{Z_k\}_{k\in N}$ is a sequence of *i.i.d.* random variable uniformly distributed on the set $S = \{e_1, e_2\}$, i.e.,

$$\bar{P}[Z_k = e_r|\mathcal{F}_{k-1}] = 1/2 \tag{13}$$

- $\{Q_k\}_{k\in N}$ is a sequence of *i.i.d.* random variable with probability density function $\varsigma(.)$ on $\mathcal{R}^d$ such that

$$\bar{P}[Q_k \in dq|Z_k = e_r, \mathcal{F}_{k-1}] = \varsigma(q)dq \tag{14}$$

- $\{m_k^r\}_{k\in N}, r = 1, 2$ are random measures on $(\mathcal{R}^d, B(\mathcal{R}^d))$ with $\bar{P}$ and their representations are

$$\begin{aligned} m_k^r(dq) &= \langle Z_k, e_r\rangle I_Q(Q_{N_k^r} \in dq) \\ &= (1/2)\varsigma(q)dq + \bar{U}_k^r \end{aligned} \tag{15}$$

where the process $\bar{U}_k^r$ is an $\mathcal{F}_k$ - martingale increment, i.e., $E[\bar{U}_k^r|\mathcal{F}_{k-1}] = 0$.

To recover the original probability measure P under which the model is introduced (i.e., all variables defined), consider the following sequence

$$\begin{aligned} &\gamma_0 = 1 \\ &\gamma_k = \prod_{r=1}^{2} \left[\frac{2a_r(Z_{k-1}, Y_k)\lambda_k^r(Y_k, Q_{N_k^r})}{\varsigma(Q_{N_k^r})} \right]^{\langle Z_k, e_r \rangle}, \quad k = 1, 2, \ldots T \end{aligned} \tag{16}$$

Using Girsanov's theorem (see e.g., [29, 31, 32]), we can set the Radon-Nikodym derivative as

$$dP = \Gamma_{0,k} d\bar{P}, \ k = 0, 1, \ldots, T \tag{17}$$

where $\Gamma_{0,k} = \prod_{l=0}^{k} \gamma_l$, its restriction implicitly known to the complete filtration that is generated by the processes Y, Z and Q. This fact is a direct application of Girsanov's theorem [32]. For the sake of completeness, a short description of this theorem including the measure transformation (i.e., the construction of this change of measure for the discrete-time process) is given in the Appendix.

3.2. **Change of Measure for the Plant's Dynamic Variables.** For any admissible control sequences $u \in \mathcal{U}_{0,T-1}$, consider the following random variable

$$\begin{aligned} &\Lambda_{0,0}^u = 1 \\ &\Lambda_{1,k}^u = \prod_{l=1}^{k} \frac{\varphi(x_l - Ax_{l-1} - \chi(Z_l)Bu_{l-1})\phi(y_l - Cx_{l-1})}{\varphi(x_l)\phi(y_l)}, \quad k = 1, 2, \ldots, T \end{aligned} \tag{18}$$

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

$$d\hat{P} = [\Lambda_{0,k}^u]^{-1} d\bar{P}, \ k = 0, 1, \ldots, T \tag{19}$$

Under this measure transformation $\hat{P}$, 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 $[\Lambda_{0,k}^u]^{-1}$ is a martingale process with respect to the complete filtration (see [29], [31], [32]).

Next let us combine the above change of measures, i.e., equations (17) and (19), as follows

$$\begin{aligned} d\hat{P} &= [\Lambda_{0,k}^u]^{-1} d\bar{P}, \\ &= [\Lambda_{0,k}^u]^{-1} \Gamma_{0,k} dP, \quad k = 0, 1, \ldots, T \end{aligned} \tag{20}$$

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

$$\begin{aligned} \alpha_k^u(x, q)dxdq = \hat{E} \left[\Lambda_{0,k}^u [\Gamma_{0,k}^u]^{-1} exp(\theta D_{0,k-1}^u) I_A(x_k \in dx) \langle Z_k, e_r \rangle I_Q(Q_{N_k^r} \in dq) \,\middle|\, \mathcal{Y} \vee \mathcal{M} \right], \\ k = 0, 1, \ldots, T \end{aligned} \tag{21}$$

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 $D_{j,k}^u = (1/2) \sum_{l=j}^{k} \{x_l' M x_l + \chi(Z_{l+1}) u_l' N u_l\}$ for $0 \leq j \leq k \leq T-1$. Moreover, the initial boundary condition for this measure valued process is specified by $\alpha_0^u(x_0, q_0) = \varphi(x_0)\varsigma(q_0)$.

Then, we obtain the following theorem.

Theorem 1. *The measure valued process $\alpha^u_k(x,q)$ satisfies the following forward recursion*

$$\alpha^u_{k+1}(x,q) = \frac{1}{\phi(y_{k+1})}\int_{B(\mathcal{R}^d)}\int_{B(\mathcal{R}^n)}\sum_{r=1}^{2}\frac{\langle Z_{k+1},e_r\rangle\varsigma(q)}{2a_r(Z_k,Y_{k+1})\lambda^r_{k+1}(Y_{k+1},q)}$$
$$\times exp(\theta D^u_{k,k})\varphi(x-A\xi-\chi(Z_{k+1})Bu_k)\phi(y_{k+1}-C\xi)\alpha^u_k(\xi,\tau)d\xi d\tau \tag{22}$$

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

Proof: For any Borel test functions $f(x)$ and $g(x)$, consider the following

$$\int_{B(\mathcal{R}^d)}\int_{B(\mathcal{R}^n)} f(\rho)g(\tau)\alpha^u_{k+1}(\rho,\tau)d\rho d\tau = \hat{E}\Big[\, f(x_{k+1})g(Q_{N^r_{k+1}})\Lambda^u_{0,k+1}[\Gamma^u_{0,k+1}]^{-1}$$
$$\times exp(\theta D^u_{0,k})\,\Big|\,\mathcal{Y}\vee\mathcal{M}\,\Big]$$
$$= \hat{E}\Big[\, f(Ax_k+\chi(Z_{k+1})Bu_k+\nu_{k+1})g(Q_{N^r_{k+1}})\Lambda^u_{0,k}[\Gamma^u_{0,k}]^{-1}exp(\theta D^u_{0,k-1})$$
$$\times\frac{\varphi(x_{k+1}-Ax_k-\chi(Z_{k+1})Bu_k)\phi(y_{k+1}-Cx_k)}{\varphi(x_{k+1})\phi(y_{k+1})}$$
$$\times\Big[\frac{\varsigma(Q_{N^r_{k+1}})}{2a_r(Z_k,Y_{k+1})\lambda^r_{k+1}(Y_{k+1},Q_{N^r_{k+1}})}\Big]^{\langle Z_{k+1},e_r\rangle} exp(\theta D^u_{k,k})\,\Big|\,\mathcal{Y}\vee\mathcal{M}\,\Big]$$
$$= \hat{E}\Big[\int_{B(\mathcal{R}^d)}\int_{B(\mathcal{R}^n)}\sum_{r=1}^{2}\frac{\langle Z_{k+1},e_r\rangle\varsigma(Q_{N^r_{k+1}})}{2a_r(Z_k,Y_{k+1})\lambda^r_{k+1}(Y_{k+1},Q_{N^r_{k+1}})}$$
$$\times f(Ax_k+\chi(Z_{k+1})Bu_k+\nu)g(Q_{N^r_{k+1}})\Lambda^u_{0,k}[\Gamma^u_{0,k}]^{-1}$$
$$\times exp(\theta D^u_{0,k-1})\;\varphi(\nu)\varsigma(\lambda)d\nu d\lambda\phi(y_{k+1}-Cx_k)exp(\theta D^u_{k,k})\,\Big|\,\mathcal{Y}\vee\mathcal{M}\,\Big]$$
$$= \int_{B(\mathcal{R}^d)}\int_{B(\mathcal{R}^n)}\int_{B(\mathcal{R}^d)}\int_{B(\mathcal{R}^n)}\frac{1}{\phi(y_{k+1})}\sum_{r=1}^{2}\frac{\langle Z_{k+1},e_r\rangle}{2a_r(Z_k,Y_{k+1})}\;\frac{\varsigma(\tau)}{\lambda^r_{k+1}(Y_{k+1},\tau)}$$
$$\times f(A\xi+\chi(Z_{k+1})Bu_k+\nu)g(\tau)\varphi(\nu)\varsigma(\lambda)\phi(y_{k+1}-C\xi)$$
$$\times exp(\theta D^u_{k,k})\alpha^u_k(\xi,\tau)d\nu d\lambda d\xi d\tau \tag{23}$$

With change of variable $\rho = A\xi+\chi(Z_{k+1})Bu_k+\nu$, we have

$$\int_{B(\mathcal{R}^d)}\int_{B(\mathcal{R}^n)} f(\rho)g(\tau)\alpha^u_{k+1}(\rho,\tau)d\rho d\tau$$
$$= \int_{B(\mathcal{R}^d)}\int_{B(\mathcal{R}^n)}\int_{B(\mathcal{R}^d)}\int_{B(\mathcal{R}^n)}\frac{1}{\phi(y_{k+1})}\sum_{r}^{2}\frac{\langle Z_{k+1},e_r\rangle}{2a_r(Z_k,Y_{k+1})}\;\frac{\varsigma(\tau)}{\lambda^r_{k+1}(Y_{k+1},\tau)}$$
$$\times f(\rho)g(\tau)exp(\theta D^u_{k,k})\varphi(\rho-A\xi-\chi(Z_{k+1})Bu_k)\varsigma(\lambda)\phi(y_{k+1}-C\xi)\alpha^u_k(\xi,\tau)d\xi d\lambda d\rho d\tau \tag{24}$$

The above holds for all Borel test functions, thus we have equation (22). □

For a finite-state Markov process model of (3), the measure valued process $\alpha^u_k(x,q)$ (i.e., the information state for this partially observed stochastic system) is determined by the following parameters $Z_k(u,Q_{N^r_k})$, $R^{-1}_k(u)$ and $\mu_k(u)$ that involve coupled forward, recursive relations [15].

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

$$\zeta_k^u(u,q) = \big(Z_k(u, Q_{N_k^r}), R_k^{-1}(u), \mu_k(u)\big) \tag{25}$$

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

$$\begin{aligned} \alpha_k^u(x,q) &= \alpha_k^u\left(\zeta_k^u(u,q), x\right) \\ &= Z_k(u, Q_{N_k^r}) exp\left\{(-1/2)(x-\mu_k(u))' R_k^{-1}(u)(x-\mu_k(u))\right\} \end{aligned} \tag{26}$$

3.3. **Solution to Risk-Sensitive Control Problem under a Markov Modulated 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 the equivalent probability measure transformation is given as follows

$$\begin{aligned} J(u) &= (1/\theta) E\left[exp\left\{ (\theta/2)\left\{ \sum_{k=0}^{T-1} (x_k' M x_k + \chi(Z_{k+1}) u_k' N u_k) + x_T' M x_T \right\}\right\}\right] \\ &= (1/\theta)\hat{E}\left[\Lambda_{0,T}^u [\Gamma_{0,T}^u]^{-1} \; exp\left\{ (\theta/2)\left\{ \sum_{k=0}^{T-1} (x_k' M x_k + \chi(Z_{k+1}) u_k' N u_k) + x_T' M x_T \right\}\right\}\right] \\ &= (1/\theta)\hat{E}\left[\Lambda_{0,T}^u [\Gamma_{0,T}^u]^{-1} exp(\theta D_{0,T-1}^u) exp\{(\theta/2) x_T' M x_T\} \right] \\ &= (1/\theta)\hat{E}\left[\hat{E}\left[\Lambda_{0,T}^u [\Gamma_{0,T}^u]^{-1} \; exp(\theta D_{0,T-1}^u) exp\{(\theta/2) x_T' M x_T\} \;\middle|\; \mathcal{Y}_T \vee \mathcal{M}_T \right] \right] \\ &= (1/\theta)\hat{E}\left[\int_{B(\mathcal{R}^d)} \int_{B(\mathcal{R}^n)} exp\{(\theta/2) x' M x\} \alpha_T(x,q) dx dq \right] \end{aligned} \tag{27}$$

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

$$\begin{aligned} J(u) &= (1/\theta)\hat{E}\left[\Lambda_{0,T}^u [\Gamma_{0,T}^u]^{-1} exp(\theta D_{0,T-1}^u) exp\{(\theta/2) x_T' M x_T\} \right] \\ &= (1/\theta)\hat{E}\left[\Lambda_{0,k}^u [\Gamma_{0,k}^u]^{-1} [\Lambda_{k+1,T}^u [\Gamma_{k+1,T}^u]^{-1} \; exp(\theta D_{0,k-1}^u) exp(\theta D_{k,T-1}^u) \right. \\ &\qquad \left. \times exp\{(\theta/2) x_T' M x_T\} \right] \\ &= (1/\theta)\hat{E}\left[\Lambda_{0,k}^u [\Gamma_{0,k}^u]^{-1} exp(\theta D_{0,k-1}^u) \hat{E}\left[\Lambda_{k+1,T}^u [\Gamma_{k+1,T}^u]^{-1} \; exp(\theta D_{k,T-1}^u) \right. \right. \\ &\qquad \left. \left. \times exp\{(\theta/2) x_T' M x_T\} \;\middle|\; \sigma\{x_k\} \vee \sigma\{m_k^r\} \vee \mathcal{Y}_T \vee \mathcal{M}_T \right] \right] \end{aligned} \tag{28}$$

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

$$\begin{aligned}\eta_k^u(x_k,q) = \hat{E}\Big[\ & \Lambda_{k+1,T}^u[\Gamma_{k+1,T}^u]^{-1} exp(\theta D_{k,T-1}^u) \\ & \times exp\{(\theta/2)x_T' M x_T\} \ \Big|\ \sigma\{x_k\} \vee \sigma\{m_k^r\} \vee \mathcal{Y}_T \vee \mathcal{M}_T \Big] \end{aligned} \tag{29}$$

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

$$\begin{aligned} J(u) &= (1/\theta)\hat{E}\Big[\ \Lambda_{0,k}^u[\Gamma_{0,k}^u]^{-1} exp(\theta D_{0,k-1}^u)\eta_k^u(x_k,q)\ \Big] \\ &= (1/\theta)\hat{E}\Big[\ \bar{E}\Big[\ \Lambda_{0,k}^u[\Gamma_{0,k}^u]^{-1} exp(\theta D_{0,k-1}^u)\eta_k^u(x_k,q)\ \Big|\ \mathcal{Y}_T \vee \mathcal{M}_T\ \Big]\Big] \\ &= (1/\theta)\hat{E}\left[\int_{B(\mathcal{R}^d)}\int_{B(\mathcal{R}^n)} \alpha_k^u(x,q)\eta_k^u(x,q)dxdq\right] \\ &= (1/\theta)\hat{E}\Big[\ \langle \alpha_k^u(x,q),\ \eta_k^u(x,q)\rangle\ \Big] \end{aligned} \tag{30}$$

which is independent of k.

Theorem 2. *The adjoint process $\eta_k^u(x,q)$ satisfies the following backward recursion*

$$\begin{aligned}\eta_k^u(x_k,q) = \int_{B(\mathcal{R}^d)}\int_{B(\mathcal{R}^n)} & \sum_{r=1}^{2} \frac{\langle Z_{k+1}, e_r\rangle \varsigma(q)\phi(y_{k+1} - Cx_k)}{2a_r(Z_k, Y_{k+1})\lambda_{k+1}^r(Y_{k+1},q)\phi(y_{k+1})} \\ & \times \varphi(x - Ax_k - \chi(Z_{k+1})Bu_k) exp(\theta D_{k,k}^u)\eta_{k+1}^u(x,\tau)dxd\tau \end{aligned} \tag{31}$$

Proof: From (29), $\eta_k^u(x,q)$ is given by

$$\begin{aligned}\eta_k^u(x_k,q) &= \hat{E}\Big[\ \Lambda_{k+1,T}^u[\Gamma_{k+1,T}^u]^{-1} exp(\theta D_{k,T-1}^u) exp\{(\theta/2)x_T' M x_T\}\ \Big|\ \sigma\{x_k\} \vee \sigma\{m_k^r\} \vee \mathcal{Y}_T \vee \mathcal{M}_T\ \Big] \\ &= \hat{E}\Big[\ \hat{E}\Big[\ \sum_{r=1}^{2} \frac{\langle Z_{k+1}, e_r\rangle \varsigma(Q_{N_{k+1}^r})}{2a_r(Z_k, Y_{k+1})\lambda_{k+1}^r(Y_{k+1}, Q_{N_{k+1}^r})} \Lambda_{k+2,T}^u[\Gamma_{k+2,T}^u]^{-1} \\ &\quad \times \frac{\varphi(x_{k+1} - Ax_k - \chi(Z_{k+1})Bu_k)\phi(y_{k+1} - Cx_k)}{\varphi(x_{k+1})\phi(y_{k+1})} exp(\theta D_{k,k}^u) exp(\theta D_{k+1,T-1}^u) \\ &\quad \times exp\{(\theta/2)x_T' M x_T\}\ \Big|\ \sigma\{x_k, x_{k+1}\} \vee \mathcal{Y}_T \vee \mathcal{M}_T\ \Big]\ \Big|\ \sigma\{x_k\} \vee \sigma\{m_k^r\} \vee \mathcal{Y}_T \vee \mathcal{M}_T\ \Big] \\ &= \hat{E}\Big[\ \sum_{r=1}^{2} \frac{\langle Z_{k+1}, e_r\rangle \varsigma(Q_{N_{k+1}^r})}{2a_r(Z_k, Y_{k+1})\lambda_{k+1}^r(Y_{k+1}, Q_{N_{k+1}^r})}\ \frac{\varphi(x_{k+1} - Ax_k - \chi(Z_{k+1})Bu_k)}{\varphi(x_{k+1})\phi(y_{k+1})} \\ &\quad \times \phi(y_{k+1} - Cx_k) exp(\theta D_{k,k}^u)\eta_{k+1}^u(x_{k+1}, Q_{N_{k+1}^r})\ \Big|\ \sigma\{x_k\} \vee \sigma\{m_k^r\} \vee \mathcal{Y}_T \vee \mathcal{M}_T\ \Big] \end{aligned} \tag{32}$$

Using the independent property under $\hat{P}$, performing the expectation operation in the last equation gives equation (31). Moreover, the boundary condition for the adjoint process is given by

$$\eta_T^u(x_T, Q_{N_T}) = \Lambda_{T,T}^u[\Gamma_{T,T}^u]^{-1} exp\{(\theta/2)x_T' M_T x_T\}\varsigma(Q_{N_T})$$

□

Moreover, the adjoint process η_k^u is given by the following equivalent relation (c.f. equations (25) and (26))

$$\eta_k^u(x,q) = \tilde{Z}_k(u, Q_{N_k^r}) exp\left\{(-1/2)(x-\tilde{\mu}_k(u))' \tilde{R}_k^{-1}(u)(x-\tilde{\mu}_k(u))\right\} \tag{33}$$

where the finite-dimensional parameters $\tilde{Z}_k(u, Q_{N_k^r})$, $\tilde{R}_k^{-1}(u)$ and $\tilde{\mu}_k(u)$ satisfy coupled backward, recursions (see [15]). From equations (22) and (24), the information state $\alpha_k^u(x,q)$ is determined by $Z_k(u, Q_{N_k^r})$, $R_k^{-1}(u)$ and $\mu_k(u)$ that involve forward recursions. Thus, based on the current value of ζ_k^u together with the new observation y_{k+1}, current control u_k and the anticipated attack sequence $\chi(Z_{k+1})$ (or $Q_{N_{k+1}^r}$ - the number of attack sequences) the next value can be determined by the following functional relation

$$\zeta_{k+1}^u = \zeta_{k+1}^u(\zeta_k^u, u_k, y_{k+1}, m_{k+1}^r) \tag{34}$$

Suppose at some intermediate time k, $0 < k < T$, the information state ζ_k^u is given by $\zeta = (Z, R^{-1}, \mu)$, then from equation (30), the value function for the optimal control problem satisfies the following

$$F(\zeta, k) = \inf_{u \in \mathcal{U}_{k,T-1}} \hat{E}\left[\langle \alpha_k^u, \eta_k^u \rangle \,\middle|\, \alpha_k = \alpha_k(\zeta) \right] \tag{35}$$

Theorem 3. *The value function, via Dynamic programming formulation, satisfies the following recursion*

$$F(\zeta, k) = \inf_{u \in \mathcal{U}_{k,k}} \hat{E}\left[F(\zeta_{k+1}^u(\zeta, u, y_{k+1}, m_{k+1}^r), k+1) \right] \tag{36}$$

with $F(\zeta, T) = \langle \alpha_T(\zeta), \eta_T(\zeta) \rangle$.

Proof: Consider equation (35)

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

Note that the adjoint process η_k is determined from η_{k+1} via the backward recursion of (31), i.e., for the adjoint process, we can specify a functional recursion equation in the form of $\eta_k = \eta_k^u(\eta_{k+1}^u)$. Thus, the value function satisfies

$$\begin{aligned}
F(\zeta, k) &= \inf_{u \in \mathcal{U}_{k,k}} \inf_{v \in \mathcal{U}_{k+1,T-1}} \hat{E}\left[\langle \alpha_k^u(\zeta), \eta_k^u(\eta_{k+1}^u \rangle \,\middle|\, \zeta_k = \zeta \right] \\
&= \inf_{u \in \mathcal{U}_{k,k}} \inf_{v \in \mathcal{U}_{k+1,T-1}} \hat{E}\left[\hat{E}\left[\langle \alpha_{k+1}^u(\zeta_{k+1}), \eta_{k+1}^u \rangle \,\middle|\, \mathcal{Y}_{k+1} \vee \sigma\{m_{k+1}^r\}, \zeta_k = \zeta \right] \middle| \, \zeta_k = \zeta \right] \\
&= \inf_{u \in \mathcal{U}_{k,k}} \hat{E}\left[\inf_{v \in \mathcal{U}_{k+1,T-1}} \hat{E}\left[\langle \alpha_{k+1}^u(\zeta_{k+1}), \eta_{k+1}^u \rangle \,\middle|\, \mathcal{Y}_{k+1} \vee \sigma\{m_{k+1}^r\}, \zeta_k = \zeta \right] \middle| \, \zeta_k = \zeta \right] \\
&= \inf_{u \in \mathcal{U}_{k,k}} \hat{E}\left[F(\zeta_{k+1}^u(\zeta, u, y_{k+1}, m_{k+1}^r), k+1) \right] \qquad (37)
\end{aligned}$$

□

Due to the lattice property of the control sequences, we interchanged the order of conditional expectation and minimization operations in the last equation of (37). 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 (11), i.e., $u^* \in \mathcal{U}_{0,T-1}$.

4. Conclusion

In this paper we considered a finite-horizon risk-sensitive control problem under a Markov modulated DoS attack model when the attacker strategy is to disrupt the network or jam the control packets from reaching the actuator. Using a chain of measure transformation techniques and dynamic programming, we derived a recursive optimal control policy in terms of the finite-dimensional dynamics of the system that satisfies a separation principle, i.e., constitutes an equivalent fully observable stochastic control problem via the newly defined information state. Moreover, the solution to the optimal control problem appeared as if it depends on the average of anticipated DoS attack sequences in the system

Appendix A

The following theorem is the discrete-time version of Girsanov's theorem [32].

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

$$z_k = f_k + H_k \zeta_k, \quad k = 0, 1, \ldots, T \tag{38}$$

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. Introduce a new probability measure $\bar{P}$ with the Radon-Nikodym derivative

$$d\bar{P} = \prod_{k=0}^{T} exp(\psi_k' \zeta_k - \frac{1}{2}|\psi_k|^2) dP \tag{39}$$

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

$$z_k = \bar{f}_k + H_k \bar{\zeta}_k, \quad k = 0, 1, \ldots, T \tag{40}$$

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

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

$$\bar{E}\left[I_A(\zeta_k) | \mathcal{F}_{k-1}\right] = E\left[exp(\psi_k' \zeta_k - \frac{1}{2}|\psi_k|^2) I_A(\zeta_k) \,\middle|\, \mathcal{F}_{k-1}\right] \tag{41}$$

□

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. 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] P. M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros and G. Andersson, "Cyber attack in a two-area power system: Impact identification using reachability," in *Proc. American Control Conference*, 2010, pp. 962-967.
[12] 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.
[13] 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.
[14] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya and Q. Wu, "A Survey of game theory as applied to network security," *in Proc. 43rd Hawaii Inter. Conf. Syst. Scie.*, 2010, pp. 1-10.
[15] G. K. Befekadu, V. Gupta and P. J. Antsaklis, "Risk-sensitive control under a class of Denial-of-Service attack models," University of Notre Dame, ISIS Laboratory, *Technical Report*, ISIS-2010-003, 2010. Available: http://www.nd.edu/ isis/techreports/isis-2010-003.pdf
[16] 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.
[17] 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.
[18] 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.
[19] 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.
[20] P. Whittle, "Risk-sensitive linear/quadratic/Gaussian control," *Adv. Appl. Probab.*, vol. 13, pp. 764-777, 1981.
[21] J. Hespanha, P. Naghshtabrizi, and Y. Xu "A survey of recent results in networked control systems," in *Proc. IEEE Special Issue on Techn. Netwo. Cont. Syst.*, vol. 95, no. 1, pp. 138-162, 2007.
[22] D. Liberzon and J. P. Hespanha, "Stabilization of nonlinear systems with limited information feedback," *IEEE Trans. Auto. Contr.*, vol. 50, no. 6, pp. 910-915, 2005.
[23] R. W. Brockett and D. Liberzon, "Quantized feedback stabilization of linear systems," *IEEE Trans. Auto. Contr.*, vol. 45, no. 7, pp.1279-1289, 2000.
[24] G. N. Nair, R. J. Evans, I. M. Y. Mareels, and W. Moran, "Topological feedback entropy and nonlinear stabilization," *IEEE Trans. Auto. Contr.*, vol. 49, no. 9, pp. 1585-1597, 2004.
[25] V. Gupta, and N. Martins, "On stability in the presence of analog erasure channels between controller and actuator," *IEEE Trans. Auto. Contr.*, vol. 55, no. 1, pp. 175-179, 2010.
[26] M.S. Branicky, S.M. Phillips, and W. Zhang, "Stability of networked control systems: Explicit analysis of delay," in *Proc. American Control Conference*, 2000, pp. 2352-2357.
[27] 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.
[28] 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.
[29] R. J. Elliott, L. Aggoun, and J. B. Moore, *Hidden Markov models: estimation and control*, Springer-Verlag, New York, 1995.
[30] 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.
[31] R. S. Liptser, and A. N. Shiriyaev, *Statistics of random processes*, Springer-Verlag, New York, 1977.
[32] 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.