2011 50th IEEE Conference on Decision and Control and
European Control Conference (CDC-ECC)
Orlando, FL, USA, December 12-15, 2011

Risk-Sensitive Control Under a Markov Modulated Denial-of-Service Attack Model

Getachew K. Befekadu, Vijay Gupta and Panos J. Antsaklis

Abstract— **This paper considers the problem of risk-sensitive stochastic control under a Markov modulated Denial-of-Service (DoS) attack strategy in which the attacker, using a hidden Markov process model, stochastically jams 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 the finite-dimensional dynamics of the system through a chain of measure transformation technique which surprisingly satisfies a separation principle, i.e., the recursive optimal control policy together with a suitably defined information state constitutes an equivalent fully observable stochastic control problem. 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

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 and industrial control systems (e.g., see references [1]-[4]). 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 malicious cyber attacks will gain even more importance. A systematic study of design approaches that provide provable security against 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., see references [5]-[11]).

By modeling the attacker as inducing network disruptions at every time step according to a Bernoulli process, Amin *et al.* [5] considered the LQG control problem and Befekadu *et al.* [12] 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 an optimal risk-sensitive control policy under this class of attack strategy. Our choice of a risk-sensitive cost function is motivated by its use in 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 [13]-[18]. 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., see references [19]-[25]).

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 equivalent 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 were originally defined). In this equivalent 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 as 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 further allows us to define an equivalent information state (and the corresponding adjoint measure process) for the partially observed stochastic system [16], [26], [27]. We can then prove a separation principle that separates the optimal control problem from the estimation problem via this newly defined information state, i.e., the recursive optimal control policy together with the newly defined information state constitute an equivalent fully observable stochastic control problem. It may be noted that such a separation principle is not a priori obvious given the risk-sensitive cost function and the hidden Markov model based attacker model.

This paper is organized as follows. In Section II, we introduce some preliminary concepts and formulate the risk-sensitive control problem under a Markov modulated DoS attack model. Section III presents the main result. Solution for 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.

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.

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

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

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

978-1-61284-801-3/11/$26.00 ©2011 IEEE

II. PROBLEM FORMULATION

A. Process Model and Cost Function

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

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

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, $\chi(Z_k) \in \{0, 1\}$ 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 II-B below. We assume the process noise ν_k and measurement noise w_k are mutually 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 [5], [6], [28]). Other attack models such as integrity (or deception) type attacks or direct physical attacks can also be considered.

Let $\mathcal{Y}_k$ denote the complete filtration generated by $\{y_1, y_2, \dots, y_k\}$. We further assume that the anticipated DoS attack sequences follow a Markov process dynamics and are independent to the other random variables in the system. Moreover, the admissible controls $u = \{u_0, u_1, \dots, u_{T-1}\}$ are $\mathbb{R}^m$ - valued sequences and considered to be adapted process (or non-anticipating process that depends on the output sequences and DoS attack path). The set of all admissible control sequences on the interval $k, k+1, \dots, l$ is denoted by $\mathcal{U}_{k,l}$. We consider an exponential running cost with quadratic function for the risk-sensitive control problem

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

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

B. Markov Modulated DoS Attack Model

Consider a process $\{Y_k\}_{k \in N}$ which is an $\mathbb{R}^d$ - 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, $\{F_k(.)\}_{k \in N}$ is a bounded $\mathbb{R}^d$ - valued measurable function and $\{W_k\}_{k \in N}$ is a sequence of $\mathbb{R}^d$ - 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 $\mathbb{R}^2$, 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.,

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

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

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

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

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

where the $\{M_k^r\}$ is an $\mathcal{F}_k$ - martingale increment.

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

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

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

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

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

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

Let us associate the evolution of the random process $\{Z_k\}_{k \in N}$ to another $\{\chi(Z_k)\}_{k \in N}$ process, where each

$\chi(Z_k)$ 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.

C. 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.,

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

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

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

We remark that the exponential running cost function weighted by a risk-sensitive parameter θ highlights designers 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.

III. MAIN RESULTS

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 mutually 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 dynamic programming.

A. 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:

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

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

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

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

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

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

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

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

Using Girsanov's theorem [26], [29], [30], we can set the Radon-Nikodym derivative as

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

where $\Gamma_{0,k} = \prod_{l=1}^{k}\gamma_l$, 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 [30].

B. Change of Measure for the Plant Dynamics Variables

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

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

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

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

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 $[\Lambda^u_{0,k}]^{-1}$ is a martingale process with respect to the complete filtration (e.g. see references [26], [29], [30]). Next let us combine the above change of measures, i.e., equations (17) and (19), as follows

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

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

$$\begin{aligned} \alpha^u_k(x,q)dxdq = \hat{\mathbb{E}}\Bigg[& \Lambda^u_{0,k}[\Gamma^u_{0,k}]^{-1} exp(\theta D^u_{0,k-1}) \\ & \times\ I_A(x_k \in dx)\langle Z_k, e_r\rangle I_Q(Q_{N^r_k} \in dq) \,\Bigg|\, \mathcal{Y} \vee \mathcal{M} \Bigg], \\ & k = 0, 1, \dots, T \end{aligned} \tag{21}$$

where $I_A(x_k \in dx)$ is the indicator function of the Borel set A, $D^u_{j,k}$ is the quadratic running function given by $D^u_{j,k} = (1/2)\sum_{l=j}^{k}(x'_l M x_l + \chi(Z_{l+1})u'_l N u_l)$ for $0 \le j \le k \le T-\ 1$. Moreover, the initial boundary condition for this measure valued process is specified by $\alpha^u_0(x_0, q_0) = \varphi(x_0)\varsigma(q_0)$.

Then, we obtain the following theorem.

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

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

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

$$\begin{aligned} &\int_{\mathcal{B}(\mathbb{R}^d)}\int_{B(\mathbb{R}^n)} f(\rho)g(\tau)\alpha^u_{k+1}(\rho,\tau)d\rho d\tau \\ &= \hat{\mathbb{E}}\Bigg[f(x_{k+1})g(Q_{N^r_{k+1}})\Lambda^u_{0,k+1}[\Gamma^u_{0,k+1}]^{-1} exp(\theta D^u_{0,k}) \\ &\qquad \Bigg|\, \mathcal{Y} \vee \mathcal{M} \Bigg] \\ &= \hat{\mathbb{E}}\Bigg[\int_{\mathcal{B}(\mathbb{R}^d)}\int_{\mathcal{B}(\mathbb{R}^n)} f(Ax_k + \chi(Z_{k+1})Bu_k + \nu) \\ &\sum_{r=1}^{2}\left\{ \frac{\langle Z_{k+1}, e_r\rangle}{2\lambda^r_{k+1}(Y_{k+1}, Q_{N^r_{k+1}})}\frac{\varsigma(Q_{N^r_{k+1}})}{a_r(Z_{k+1}, Y_{k+1})}\right\}\Lambda^u_{0,k} \\ &\times [\Gamma^u_{0,k}]^{-1} exp(\theta D^u_{0,k-1})\varphi(\nu)d\nu\varsigma(\lambda)d\lambda\phi(y_{k+1} - Cx_k) \\ &\qquad \times g(Q_{N^r_{k+1}}) exp(\theta D^u_{k,k}) \,\Bigg|\, \mathcal{Y} \vee \mathcal{M} \Bigg] \end{aligned}$$

$$\begin{aligned} &= \int_{\mathcal{B}(\mathbb{R}^d)}\int_{\mathcal{B}(\mathbb{R}^n)}\int_{\mathcal{B}(\mathbb{R}^d)}\int_{\mathcal{B}(\mathbb{R}^n)} \frac{\phi(y_{k+1} - C\xi)}{\phi(y_{k+1})} exp(\theta D^u_{k,k}) \\ &\times \sum_{r=1}^{2}\frac{\langle Z_{k+1}, e_r\rangle}{2a_r(Z_{k+1}, Y_{k+1})}\frac{\varsigma(\tau)}{\lambda^r_{k+1}(Y_{k+1}, \tau)} g(\tau)\varphi(\nu)\varsigma(\lambda) \\ &\qquad \times f(A\xi + \chi(Z_{k+1})Bu_k + \nu)\alpha^u_k(\xi,\tau)d\nu d\lambda d\xi d\tau \end{aligned} \tag{23}$$

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

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

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

For a finite-state Markov chain 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 [12]. With minor abuse of notation, we consider these parameters as an information state for the system

$$\zeta^u_k(u,q) = (\ Z_k(u, Q_{N^r_k}), R^{-1}_k(u), \mu_k(u)\ ) \tag{25}$$

Furthermore, we can rewrite the measured process $\alpha^u_k(x,q)$ as follows

$$\begin{aligned} &\alpha^u_k(x,q) = \alpha^u_k\ (\ \zeta^u_k(u,q), x\ ) \\ &= Z_k(u, Q_{N^r_k}) exp\{-\frac{1}{2}(x - \mu_k(u))' R^{-1}_k(u)(x - \mu_k(u))\} \end{aligned} \tag{26}$$

C. 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

$$\begin{aligned} J(u) &= (1/\theta)\,\mathbb{E}\Bigg[exp\Bigg\{ (\theta/2)\Bigg\{ \sum_{k=0}^{T-1}(x'_k M x_k \\ &\qquad +\ \chi(Z_{k+1})u'_k N u_k) + x'_T M_T x_T \Bigg\}\Bigg\}\Bigg] \\ &= (1/\theta)\,\hat{\mathbb{E}}\Bigg[\hat{\mathbb{E}}\Bigg[\Lambda^u_{0,T}[\Gamma^u_{0,T}]^{-1} exp(\theta D^u_{0,T-1}) \\ &\qquad \times exp\{(\theta/2)x'_T M_T x_T\} \,\Bigg|\, \mathcal{Y}_T \vee \mathcal{M}_T \Bigg]\Bigg] \end{aligned}$$

$$= (1/\theta)\,\hat{\mathbb{E}}\left[\int_{B(\mathbb{R}^d)}\int_{B(\mathbb{R}^n)} exp\{(\theta/2)x'Mx\}\alpha_T(x,q)dxdq\right] \tag{27}$$

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

$$\begin{aligned} J(u) &= (1/\theta)\,\hat{\mathbb{E}}\Big[\ \Lambda^u_{0,T}[\Gamma^u_{0,T}]^{-1}exp(\theta D^u_{0,T-1})exp\{(\theta/2) \\ &\qquad \times\ x'_T M_T x_T\}\ \Big] \\ &= (1/\theta)\,\hat{\mathbb{E}}\Big[\ \Lambda^u_{0,k}[\Gamma^u_{0,k}]^{-1}[\Lambda^u_{k+1,T}[\Gamma^u_{k+1,T}]^{-1}exp(\theta D^u_{0,k-1}) \\ &\qquad \times\ exp(\theta D^u_{k,T-1})exp\{(\theta/2)x'_T M_T x_T\}\ \Big] \\ &= (1/\theta)\,\hat{\mathbb{E}}\Big[\ \Lambda^u_{0,k}[\Gamma^u_{0,k}]^{-1}exp(\theta D^u_{0,k-1})\,\hat{\mathbb{E}}\Big[\ \Lambda^u_{k+1,T} \\ &\qquad \times\ [\Gamma^u_{k+1,T}]^{-1}exp(\theta D^u_{k,T-1})exp\{(\theta/2)x'_T M_T x_T\} \\ &\qquad \Big|\ \sigma\{x_k\}\vee\sigma\{m^r_k\}\vee\mathcal{Y}_T\vee\mathcal{M}_T\ \Big]\Big] \end{aligned} \tag{28}$$

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

$$\begin{aligned} \eta^u_k(x_k,q) &= \hat{\mathbb{E}}\Big[\ \Lambda^u_{k+1,T}[\Gamma^u_{k+1,T}]^{-1}exp(\theta D^u_{k,T-1}) \\ &\quad \times\ exp\{(\theta/2)x'_T M_T x_T\}\ \Big|\ \sigma\{x_k\}\vee\sigma\{m^r_k\}\vee\mathcal{Y}_T\vee\mathcal{M}_T\ \Big] \end{aligned} \tag{29}$$

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

$$\begin{aligned} J(u) &= (1/\theta)\,\hat{\mathbb{E}}\Big[\ \Lambda^u_{0,k}[\Gamma^u_{0,k}]^{-1}exp(\theta D^u_{0,k-1})\eta^u_k(x_k,q)\ \Big] \\ &= (1/\theta)\,\hat{\mathbb{E}}\Big[\ \hat{\mathbb{E}}\Big[\ \Lambda^u_{0,k}[\Gamma^u_{0,k}]^{-1}exp(\theta D^u_{0,k-1}) \\ &\qquad \times\eta^u_k(x_k,q)\ \Big|\ \mathcal{Y}_T\vee\mathcal{M}_T\ \Big]\Big] \\ &= (1/\theta)\,\hat{\mathbb{E}}\left[\int_{\mathcal{B}(\mathbb{R}^d)}\int_{\mathcal{B}(\mathbb{R}^n)}\alpha^u_k(x,q)\eta^u_k(x,q)dxdq\right] \\ &= (1/\theta)\,\hat{\mathbb{E}}\Big[\ \langle\alpha^u_k(x,q)\eta^u_k(x,q)\rangle\ \Big] \end{aligned} \tag{30}$$

which is independent of k.

Theorem 2: The adjoint process $\eta^u_k(x,q)$ satisfies the following backward recursion

$$\begin{aligned} \eta^u_k(x_k,q) &= \int_{\mathcal{B}(\mathbb{R}^d)}\int_{\mathcal{B}(\mathbb{R}^n)}\varphi(x - Ax_k - \chi(Z_{k+1})Bu_k) \\ &\quad \times\sum_{r=1}^{2}\frac{\langle Z_{k+1},e_r\rangle\varsigma(q)\phi(y_{k+1}-Cx_k)}{2a_r(Z_{k+1},Y_{k+1})\lambda^r_{k+1}(Y_{k+1},q)\phi(y_{k+1})} \\ &\qquad \times exp(\theta D^u_{k,k})\eta^u_{k+1}(x,\tau)dxd\tau \end{aligned} \tag{31}$$

Proof: From (29), $\eta^u_k(x,q)$ is given by

$$\begin{aligned} \eta^u_k(x_k,q) &= \hat{\mathbb{E}}\Big[\ \Lambda^u_{k+1,T}[\Gamma^u_{k+1,T}]^{-1}exp(\theta D^u_{k,T-1}) \\ &\quad \times exp\{(\theta/2)x'_T M_T x_T\}\ \Big|\ \sigma\{x_k\}\vee\sigma\{m^r_k\}\vee\mathcal{Y}_T\vee\mathcal{M}_T\ \Big] \\ &= \hat{\mathbb{E}}\Big[\sum_{r=1}^{2}\frac{\langle Z_{k+1},e_r\rangle\varsigma(Q_{N^r_{k+1}})}{2a_r(Z_{k+1},Y_{k+1})\lambda^r_{k+1}(Y_{k+1},Q_{N^r_{k+1}})}exp(\theta D^u_{k,k}) \\ &\quad \times\ \frac{\varphi(x_{k+1}-Ax_k-\chi(Z_{k+1})Bu_k)}{\varphi(x_{k+1})}\frac{\phi(y_{k+1}-Cx_k)}{\phi(y_{k+1})} \\ &\quad \times\ \eta^u_{k+1}(x_{k+1},Q_{N^r_{k+1}})\ \Big|\ \sigma\{x_k\}\vee\sigma\{m^r_k\}\vee\mathcal{Y}_T\vee\mathcal{M}_T\ \Big] \end{aligned} \tag{32}$$

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

$$\eta^u_T(x_T,Q_{N_T}) = \Lambda^u_{T,T}[\Gamma^u_{T,T}]^{-1}exp\{(\theta/2)x'_T M_T x_T\}\varsigma(Q_{N_T}) \tag{33}$$

■

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

$$\begin{aligned} \eta^u_k(x,q) &= \tilde{Z}_k(u,Q_{N^r_k}) \\ &\times exp\Big\{-\frac{1}{2}\,\big(\,x-\tilde{\mu}_k(u)\,\big)'\,\tilde{R}^{-1}_k(u)\,\big(\,x-\tilde{\mu}_k(u)\,\big)\Big\} \end{aligned} \tag{34}$$

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

$$\zeta^u_{k+1} = \zeta^u_{k+1}\,\big(\,\zeta^u_k,u_k,y_{k+1},m^r_{k+1}\,\big) \tag{35}$$

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

$$F(\zeta,k) = \inf_{u\in\mathcal{U}_{k,T-1}}\hat{\mathbb{E}}\Big[\ \langle\alpha^u_k,\eta^u_k\rangle\ \Big|\ \alpha_k = \alpha_k(\zeta)\ \Big] \tag{36}$$

Theorem 3: The value function satisfies the following recursion with

$$F(\zeta,k) = \inf_{u\in\mathcal{U}_{k,k}}\hat{\mathbb{E}}\Big[\ F\ \big(\ \zeta^u_{k+1}(\zeta,u,y_{k+1},m^r_{k+1}),k+1\ \big)\Big] \tag{37}$$

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

Proof: Consider equation (36)

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

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 the following

$$\begin{aligned} &F(\zeta, k) \\ &= \inf_{u \in \mathcal{U}_{k,k}} \inf_{\upsilon \in \mathcal{U}_{k+1,T-1}} \hat{\mathbb{E}} \left[\langle \alpha_k^u(\zeta), \eta_k^u(\eta_{k+1}^u) \rangle \,\middle|\, \zeta_k = \zeta \right] \\ &= \inf_{u \in \mathcal{U}_{k,k}} \inf_{\upsilon \in \mathcal{U}_{k+1,T-1}} \hat{\mathbb{E}} \Bigg[\hat{\mathbb{E}} \Bigg[\langle \alpha_{k+1}^u(\zeta_{k+1}), \eta_{k+1}^u \rangle \\ &\qquad \Bigg| \mathcal{Y}_{k+1} \vee \sigma\{m_{k+1}^r\}, \zeta_k = \zeta \Bigg] \Bigg| \zeta_k = \zeta \Bigg] \\ &= \inf_{u \in \mathcal{U}_{k,k}} \hat{\mathbb{E}} \Bigg[\inf_{\upsilon \in \mathcal{U}_{k+1,T-1}} \hat{\mathbb{E}} \Bigg[\langle \alpha_{k+1}^u(\zeta_{k+1}), \eta_{k+1}^u \rangle \\ &\qquad \Bigg| \mathcal{Y}_{k+1} \vee \sigma\{m_{k+1}^r\}, \zeta_k = \zeta \Bigg] \Bigg| \zeta_k = \zeta \Bigg] \\ &= \inf_{u \in \mathcal{U}_{k,k}} \hat{\mathbb{E}} \left[F\left(\zeta_{k+1}^u(\zeta, u, y_{k+1}, m_{k+1}^r), k+1 \right) \right] \end{aligned} \tag{38}$$

■

Due to the lattice property of the control sequences, we interchanged the order of conditional expectation and minimization operations in the last equation of (38). 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., $u^* \in \mathcal{U}_{0,T-1}$.

IV. 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., the recursive optimal control policy together with the newly defined information state constitutes an equivalent completely 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.

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] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] G. K. Befekadu, V. Gupta and P. J. Antsaklis, "Risk-sensitive control under a class of Denial-of-Service attack models," in *Proc. American Control Conference*, 2011, pp. 643–648.

[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] 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.

[20] 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.

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

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

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

[28] 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.

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

[30] 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.