Risk-Sensitive Control Under Markov Modulated Denial-of-Service (DoS) Attack Strategies

Getachew K. Befekadu, *Member, IEEE*, Vijay Gupta, *Member, IEEE*, and Panos J. Antsaklis, *Fellow, IEEE*

***Abstract*—We consider 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 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 techniques. We also prove a separation principle under which a recursive optimal control policy together with a newly defined information-state constitutes an equivalent completely observable stochastic control problem. Remarkably, on the transformed measure space, the solution to the optimal control problem appears as if it depends only on the sample-path (or path-estimation) of the DoS attack sequences in the system.**

***Index Terms*—Denial-of-service, information-state, measure transformations, risk-sensitive control.**

I. Introduction

Recently, an increasing emphasis has been placed on addressing the problem of risk and vulnerability assessment to malicious cyber-attacks against critical infrastructure such as power grids and industrial control systems (e.g., see [1]–[5] and references therein). The issue of security in such critical sectors has now become as important as technical (and also practical) design problems. As these critical infrastructures become interconnected and more 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 cyber-attacks is a core area of current cyber-physical systems research. In particular, since such cyber-physical systems will couple control of critical infrastructure with communication networks, there is an urgent 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 on control systems, wireless sensor networks and IT infrastructure (e.g., see [6]–[11] and references therein).

By modeling the attacker as inducing network disruptions at every time step according to a Bernoulli process, Amin *et al.* [6] 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 strategies. Our choice of a risk-sensitive cost function is motivated by its use in robust control and dynamic games, where this criterion has proved to be an effective tool in mapping *a priori* knowledge of the system parameters to the cost functional (e.g., see [13]–[18] for details on this subject). We would also like to mention that the related problem of optimal control when control packets are being erased by a communication channel has been studied in networked control systems literature (e.g., see [19]–[23] and references therein).

Our main technical tool is a chain of measure transformations that allows us to consider the optimal control design problem merely on the sample-path (or path-estimation) 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 processes in the system (i.e., relative to the original (or reference) probability measure space on which all random variables were initially defined). In this equivalent probability measure space, the DoS attack sequences are independent over their observed values. Once this is accomplished, we introduce another (or different) probability measure transformation that separately characterizes the plant state and the observation variables of the discrete-time partially observed stochastic system. Specifically, this 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 valued processes in the system. This characterization allows us to define an equivalent information-state (and the corresponding adjoint measure valued process) for the partially observed stochastic system (e.g., see [17], [24], or [25] for additional discussions). Then, we can prove a separation principle that separates the optimal control problem from the estimation problem via this newly defined information-state. That is, the recursive optimal control policy together with the newly introduced 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. A preliminary version of this technical note was presented in [26].

The rest of the technical note 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 results—where an exact 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.For the sake of completeness, all proofs and a short description of Girsanov's theorem are included in a supplementary document.

II. Problem Formulation

In this section, we provide a framework for the problem of risk-sensitive stochastic control under a Markov modulated DoS attack model. We also describe the problem formulation and some of the

Manuscript received October 15, 2013; revised August 31, 2014 and February 26, 2015; accepted March 11, 2015. Date of publication March 27, 2015; date of current version December 1, 2015. This work was supported in part by the National Science Foundation under Grant CNS-1035655 and by the College of Engineering, University of Notre Dame. Recommended by Associate Editor C. M. Lagoa.

The authors are with the Department of Electrical Engineering, University of Notre Dame, Notre Dame, IN 46556 USA (e-mail: gbefekadu1@nd.edu; vgupta2@nd.edu; antsaklis.1@nd.edu).

Digital Object Identifier 10.1109/TAC.2015.2416926

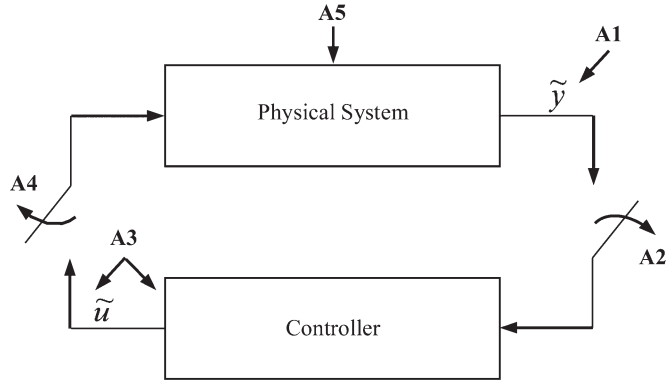

Fig. 1. Typical malicious cyber-attacks in control systems ([6]).

assumptions on the Markov modulated DoS attack model that are necessary for the development of our results.

A. The System Model

Let $(\Omega, \mathscr{F})$ be a measure space which is equipped with a global or full-information filtration $\{\mathscr{F}_k\}$, $k \in \mathbb{N}$, and let $\mathscr{P}(\Omega)$ be the set of probability measures on $(\Omega, \mathscr{F})$ satisfying the usual hypotheses (e.g., see [27]).[1] On this measure space, consider the following discrete-time partially observed stochastic system:

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

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 process (output) and $\gamma_{(Z_k)} \in \{0, 1\}$ is the DoS attack sequence that disrupts the control packets from reaching the actuator where Z_k is related to the internal state of the attacker.[2] Furthermore, we assume that 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 covariances Σ and Γ are assumed to be positive definite matrices. Fig. 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* attacks in the system. Other attack models such as integrity type attacks or direct physical attacks can also be considered. We remark that DoS attack is a common intrusion of cyber-physical systems (e.g., see [6], [7], or [28]).

In the following, we assume that $P \in \mathscr{P}(\Omega)$ and let $\mathscr{Y}_k \subset \mathscr{F}_k$ denote a complete filtration which is generated by $\{y_k\}_{k \in \mathbb{N}}$. We further assume that the DoS attack sequences follow a Markov process dynamics and are independent to the other random processes in the system. The admissible controls $\mathcal{U} \triangleq \mathcal{U}_{0,\, N} = \{u_k\}_{k=0}^{N-1}$ are $\mathbb{R}^m$-valued sequences and considered to be adapted process (or non-anticipating process that depends only on the observed output sequences and the sample-path of the DoS attack sequences).

Remark 1: We remark that an attacker, who may have (partial) knowledge about the system with possibly different time-scale compared to the system dynamics in (1), is probably difficult, but certainly an interesting problem.

In this technical note, we consider an exponential running cost with quadratic function of the form

$$J(u) = \left(\frac{1}{\theta}\right) \mathbb{E}\left[\exp\left\{ \left(\frac{\theta}{2}\right) \left\{ \sum_{k=0}^{N-1} \left(x_k^T M x_k + \gamma_{(Z_{k+1})} u_k^T S u_k \right) + x_N^T M_N x_N \right\}\right\}\right] \tag{2}$$

where $\theta > 0$ is the risk-sensitive parameter, $u_k \in \mathcal{U}_{0,N}$ is the admissible control sequences; while $\mathbb{E}[.]$ denotes the expectation with respect to a reference probability measure $P \in \mathscr{P}(\Omega)$. Moreover, M (and also M_N) and S are assumed to be positive semidefinite and positive definite matrices, respectively.

B. Markov Modulated DoS Attack Model

In the following, we describe the nature of the DoS attack sequences $\gamma_{(\cdot)}$ and discuss some of the associated assumptions necessary for the development of our main results. To this end, consider a process $\{Y_k\}_{k \in \mathbb{N}}$ 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 a known initial distribution, $\{F_k(.)\}_{k \in \mathbb{N}}$ is a bounded $\mathbb{R}^d$—valued measurable function and $\{W_k\}_{k \in \mathbb{N}}$ is a sequence of $\mathbb{R}^d$—valued independent random variables with density function $\{\psi_k(.)\}_{k \in \mathbb{N}}$.

Further, let $\{Z_k\}_{k \in \mathbb{N}}$ be a two-dimensional stochastic process with a finite state-space $\mathbb{S}$. Without loss of generality, we take the state-space to be the standard basis in $\mathbb{R}^2$, i.e., $\mathbb{S} \triangleq \{e_1, e_2\}$. Moreover, define the following nondecreasing family of σ sub-algebras $\mathscr{F}_0^{Z \vee Y} = \sigma\{Z_0, Y_0, Y_1\} \subset \mathscr{F}_0$ and $\mathscr{F}_k^{Z \vee Y} = \sigma\{Z_l, Y_{l+1}, l \leq k, k \geq 1\} \subset \mathscr{F}_k$ (and also augmented by a set $\mathscr{F}_k$ having P-measure zero). We assume that the process Z is a conditional Markov chain, i.e.,

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

where $\langle ., . \rangle$ is the standard inner product on $\mathbb{R}^2$ and $y \mapsto A(y) \triangleq [a_{ji}(y)] : \mathbb{R}^d \to \mathbb{R}^{2 \times 2}$ is an $\mathscr{F}_k^{Z \vee Y}$ measurable matrix function such that for all $y \in \mathbb{R}^d$ the following conditions are satisfied:

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

That is, the matrix function $A(y)$ is a Markov (or *row-stochastic*) matrix for all $y \in \mathbb{R}^d$.

The following lemma, which follows directly from equations (3), (4), and (5), will be stated without proof.

Lemma 1: The random process $\{Z_k\}_{k \in \mathbb{N}}$, which assumes value from the finite state-space $\mathbb{S}$, has the following representation:

$$Z_k = A\left(F_k(Y_{k-1})\right) Z_{k-1} + V_k \tag{6}$$

where the process $\{V_k\}_{k \in \mathbb{N}}$ is an $\mathscr{F}_k^{Z \vee Y}$—martingale increment, i.e., $E[V_k | \mathscr{F}_{k-1}^{Z \vee Y}] = 0$.

[1] Note that all random processes or random variables are defined on this measure space and they are also assumed to be progressively measurable. Thus, all results in this technical note are to be interpreted as *almost surely* (a.s.) with respect to a probability measure from the set $\mathscr{P}(\Omega)$.

[2] In Section II-A below, we provide the exact formulation of the Markov modulated DoS attack model [cf. (9) and (10)].

Next, we 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 measurable

$$\begin{aligned} N_k^r &= \sum_{l=1}^{k} \langle Z_l, e_r \rangle \\ &= \sum_{l=1}^{k} a_r(Z_{l-1}, Y_l) + M_k^r \\ &= \sum_{l=1}^{k} \sum_{i=1}^{2} a_{ri}(Y_l) \langle Z_{l-1}, e_r \rangle + M_k^r \end{aligned} \tag{7}$$

where $\{M_k^r\}$ is an $\mathscr{F}_k^{Z \vee Y}$—martingale increment.

Note that the Markov process $\{Y_k\}_{k \in \mathbb{N}}$ is not observed directly, but through another $\mathbb{R}^d$—valued random process $\{Q_{N_k^r}\}_{k \in \mathbb{N}}$ such that

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

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

Then, we construct a new random process using the following relation:

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

where $\{U_k^r\}$ is an $\mathscr{F}_k^{Z \vee Y}$—martingale increment and $\mathbf{1}_Q(Q_{N_k^r} \in dq)$ stands for an indicator function of the Borel set Q. Hence, the complete filtration generated by this observation process, i.e., $m_k^r(.)$, is given by

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

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

Finally, we can associate the evolution of the random process $\{Z_k\}_{k \in \mathbb{N}}$ to another $\{\gamma_{(Z_k)}\}_{k \in \mathbb{N}}$ process, where each $\gamma_{(Z_k)}$ is a binary random sequence (i.e., $\gamma_{(Z_k)} \in \{0, 1\}$ with $\gamma_{(Z_0)} = 0$).[3] Note that the distribution for this process depends on the state of the hidden Markov model, namely, the probability of its success changes with respect to the Markov process. Specifically, we exploit this property for our DoS attack model realization. Although, $\{\gamma_{(Z_k)}\}_{k \in \mathbb{N}}$ 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, i.e., $(\Omega, \mathscr{F}, P)$. Moreover, the discrete-time counting process N_k^r, which is given by (7), records a particular event that has been followed and its measured information equally serve for this process. Therefore, (9) and (10) effectively provide an observation model (i.e., path-estimation) for the Markov modulated random processes [cf. (12) below].

C. Problem Statement

The problem considered in this technical note is stated as follows:

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

$$\begin{aligned} V_0 &= \operatorname*{ess\,inf}_{u \in \mathcal{U}_{0,N-1}} J(u) \\ &= \operatorname*{ess\,inf}_{u \in \mathcal{U}_{0,N-1}} \left(\frac{1}{\theta}\right) \mathbb{E}\left[\exp\left\{\left(\frac{\theta}{2}\right)\left\{\sum_{k=0}^{N-1}\left(x_k^T M x_k \right.\right.\right.\right. \\ &\qquad \left.\left.\left.\left. + \gamma_{(Z_{k+1})} u_k^T S u_k\right) + x_N^N M_N x_N\right\}\right\}\right]. \end{aligned} \tag{11}$$

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 $\gamma_{(Z_k)}$ (see also the remark in footnote 3). In general, this attack model $\mathcal{A}_{\mathscr{M}(\gamma_{(Z.)})}$ will have the following sample-path sequence(s)

$$\mathcal{A}_{\mathscr{M}(\gamma_{(Z.)})} = \left\{\gamma_{(Z_0)}, \gamma_{(Z_1)}, \ldots, \gamma_{(Z_N)}\right\}. \tag{12}$$

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.[4] For a risk-neutral criterion, when θ is sufficiently close to zero, the risk-sensitive control problem reduces to an LQG control problem (e.g., see Bertsekas [14] for details).

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 sample-path (or path-estimation) of the DoS attack sequences 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 sample-path of the DoS attack 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

Let $\bar{P} \in \mathscr{P}(\Omega)$ and suppose the following random variables are given on measure space $(\Omega, \mathscr{F})$ under which the random variable Q is not affected by the random variables Y, Z, and m:

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

$$\bar{P}\left[Z_k = e_r \middle| \mathscr{F}_{k-1}^{Z \vee Y}\right] = \frac{1}{2}. \tag{13}$$

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

$$\bar{P}\left[Q_k \in dq \middle| Z_k = e_r, \mathscr{F}_{k-1}^{Z \vee Y}\right] = \varsigma(q) dq. \tag{14}$$

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

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

To recover the original probability measure $P \in \mathscr{P}(\Omega)$ under which the model is introduced, consider the following sequence:

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

[3] Notice that we can always achieve this via a sequence of bijective or one-to-one mapping functions. For instance, a bijective mapping $\gamma_{(Z_k)} = [0, 1] Z_k$ where $Z_k \in \mathbb{S}$ can generate a binary random sequence.

[4] Notice that if the parameter is $\theta < 0$ (resp. $\theta > 0$), then it will create a situation of *risk-seeking* (resp. *risk-averting*) on the part of the optimizer.

Using Girsanov's theorem [27], [29], we can set the Radon-Nikodym derivative as

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

where $\Gamma_{0,k} = \prod_{l=1}^{k} \gamma_l$, its restriction is 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 [29]. 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 measure valued processes) is given in the supplementary document.

B. Change of Measure for the Plant Dynamics Variables

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

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

Using this random variable, we can introduce a new equivalent measure transformation $\hat{P} \in \mathscr{P}(\Omega)$ as follows

$$d\hat{P} = \left[\Lambda_{0,k}^u\right]^{-1} d\bar{P}, \quad k = 0, 1, \ldots, N. \tag{19}$$

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 (e.g., see [24], [27], [29]). Further, if we combine the above change of measures, i.e., (17) and (19), then we have following:

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

Next, consider the following measure valued process for any admissible control u and DoS attack sequences in the system

$$\begin{aligned} \alpha_k^u(x,q)dxdq = &\hat{\mathbb{E}}\left[\Lambda_{0,k}^u \left[\Gamma_{0,k}^u\right]^{-1} \exp\left(\theta D_{0,k-1}^u\right) \mathbf{1}_A(x_k \in dx) \right. \\ &\left. \times \langle Z_k, e_r \rangle \mathbf{1}_Q \left(Q_{N_k^r} \in dq\right) | \mathscr{Y} \vee \mathscr{M} \right], k = 0, 1, \ldots, N \end{aligned} \tag{21}$$

where $\mathbf{1}_A(x_k \in dx)$ is the indicator function of the Borel set A, $D_{j,k}^u$ is the quadratic running function given by $D_{j,k}^u = (1/2)\sum_{l=j}^{k}(x_l^T M x_l + \gamma_{(Z_{l+1})} u_l^T S u_l)$ for $0 \leq j \leq k \leq N-1$. Note that the above expectation in the right-hand side is performed with respect to $\hat{P}$; and, moreover, the initial boundary condition for this measure valued process is given 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 $\alpha_k^u(x,q)$ satisfies the following forward recursion:

$$\begin{aligned} &\alpha_{k+1}^u(x,q)dxdq \\ &= \frac{1}{\phi(y_{k+1})} \int\limits_{\mathcal{B}(\mathbb{R}^d)} \int\limits_{\mathcal{B}(\mathbb{R}^n)} \sum_{r=1}^{2} \frac{\langle Z_{k+1}, e_r \rangle \varsigma(q)}{2a_r(Z_k, Y_{k+1})\lambda_{k+1}^r(Y_{k+1}, q)} \\ &\quad \times \exp\left(\theta D_{k,k}^u\right) \varphi\left(x - A\xi - \gamma_{(Z_{k+1})} Bu_k\right) \phi(y_{k+1} - C\xi) \\ &\quad \times \alpha_k^u(\xi, \tau) d\xi d\tau \end{aligned} \tag{22}$$

where $D_{k,k}^u = (1/2)(\xi^T M \xi + \gamma_{(Z_{k+1})} u_k^T S u_k)$.

For a finite-state Markov chain model of (3), the measure valued process $\alpha_k^u(x,q)$ (i.e., the information state for the discrete-time partially observed stochastic system in (1)) is determined by the following parameters $\Upsilon_k(u, Q_{N_k^r})$, $\Theta_k^{-1}(u)$ and $\mu_k(u)$ that involve coupled forward recursive relations (e.g., see [12]). With minor abuse of notation, we consider these parameters as an information-state for the system

$$\zeta_k^u(u,q) = \left(\Upsilon_k\left(u, Q_{N_k^r}\right), \Theta_k^{-1}(u), \mu_k(u)\right). \tag{23}$$

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

$$\begin{aligned} &\alpha_k^u(x,q) = \alpha_k^u\left(\zeta_k^u(u,q), x\right) \\ &= \Upsilon_k\left(u, Q_{N_k^r}\right) \exp\left\{-\frac{1}{2}\left(x - \mu_k(u)\right)^T \Theta_k^{-1}(u)(x - \mu_k(u))\right\}. \end{aligned} \tag{24}$$

C. Solution to Risk-Sensitive Control Problem Under a Markov Modulated DoS Attack Model

In the following, we further provide a solution for the optimal control policy in terms of finite-dimensional dynamics, i.e., a separated policy in terms of the equivalent information-state, using a dynamic programming technique.

For any admissible control sequences and sample-path of the DoS attacks, the expected total cost in (2) with respect to the equivalent probability measure transformation is given as follows:

$$\begin{aligned} J(u) = &\left(\frac{1}{\theta}\right)\mathbb{E}\left[\exp\left\{\left(\frac{\theta}{2}\right)\left\{\sum_{k=0}^{N-1}\left(x_k^T M x_k + \gamma_{(Z_{k+1})} u_k^T S u_k\right)\right.\right.\right. \\ &\left.\left.\left. + x_N^T M_N x_N\right\}\right\}\right] \\ = &\left(\frac{1}{\theta}\right)\hat{\mathbb{E}}\left[\Lambda_{0,N}^u \left[\Gamma_{0,N}^u\right]^{-1} \exp\left(\theta D_{0,N-1}^u\right)\right. \\ &\left. \times \exp\left\{\left(\frac{\theta}{2}\right) x_N^T M_N x_N\right\}\right] \\ = &\left(\frac{1}{\theta}\right)\hat{\mathbb{E}}\left[\hat{\mathbb{E}}\left[\Lambda_{0,N}^u \left[\Gamma_{0,N}^u\right]^{-1} \exp\left(\theta D_{0,N-1}^u\right)\right.\right. \\ &\left.\left. \times \exp\left\{\left(\frac{\theta}{2}\right) x_N^T M_N x_N\right\} | \mathscr{Y}_N \vee \mathscr{M}_N\right]\right] \\ = &\left(\frac{1}{\theta}\right)\hat{\mathbb{E}}\left[\int\limits_{\mathcal{B}(\mathbb{R}^d)} \int\limits_{\mathcal{B}(\mathbb{R}^n)} \exp\left\{\left(\frac{\theta}{2}\right) x^T M x\right\} \alpha_N(x,q) dx dq\right]. \end{aligned} \tag{25}$$

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

$$\begin{aligned} J(u) = &\left(\frac{1}{\theta}\right)\hat{\mathbb{E}}\left[\Lambda_{0,N}^u \left[\Gamma_{0,N}^u\right]^{-1} \exp\left(\theta D_{0,N-1}^u\right)\right. \\ &\left. \times \exp\left\{\left(\frac{\theta}{2}\right) x_N^T M_N x_N\right\}\right] \\ = &\left(\frac{1}{\theta}\right)\hat{\mathbb{E}}\left[\Lambda_{0,k}^u \left[\Gamma_{0,k}^u\right]^{-1} [\Lambda_{k+1,N}^u \left[\Gamma_{k+1,N}^u\right]^{-1}\right. \\ &\left. \times \exp\left(\theta D_{0,k-1}^u\right) \exp\left(\theta D_{k,N-1}^u\right) \exp\left\{\left(\frac{\theta}{2}\right) x_N^T M_N x_N\right\}\right] \\ = &\left(\frac{1}{\theta}\right)\hat{\mathbb{E}}\left[\Lambda_{0,k}^u \left[\Gamma_{0,k}^u\right]^{-1} \exp\left(\theta D_{0,k-1}^u\right)\right. \\ & \times \hat{\mathbb{E}}\left[\Lambda_{k+1,N}^u \left[\Gamma_{k+1,N}^u\right]^{-1} \exp\left(\theta D_{k,N-1}^u\right)\right. \\ &\left.\left. \times \exp\left\{\left(\frac{\theta}{2}\right) x_N^T M_N x_N\right\} | \sigma\{x_k\} \vee \sigma\left\{m_k^r\right\} \vee \mathscr{Y}_N \vee \mathscr{M}_N\right]\right] \end{aligned} \tag{26}$$

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

$$\eta_k^u(x_k,q) = \hat{\mathbb{E}}\Bigg[\Lambda_{k+1,N}^u\left[\Gamma_{k+1,N}^u\right]^{-1}\exp\left(\theta D_{k,N-1}^u\right)\exp\Bigg\{\left(\frac{\theta}{2}\right) \times x_N^T M_N x_N\Bigg\}|\sigma\{x_k\} \vee \sigma\{m_k^r\} \vee \mathscr{Y}_N \vee \mathscr{M}_N\Bigg]. \tag{27}$$

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

$$\begin{aligned} J(u) &= \left(\frac{1}{\theta}\right)\hat{\mathbb{E}}\left[\Lambda_{0,k}^u\left[\Gamma_{0,k}^u\right]^{-1}\exp\left(\theta D_{0,k-1}^u\right)\eta_k^u(x_k,q)\right] \\ &= \left(\frac{1}{\theta}\right)\hat{\mathbb{E}}\left[\hat{\mathbb{E}}\left[\Lambda_{0,k}^u\left[\Gamma_{0,k}^u\right]^{-1}\exp\left(\theta D_{0,k-1}^u\right)\eta_k^u(x_k,q)|\mathscr{Y}_N \vee \mathscr{M}_N\right]\right] \\ &= \left(\frac{1}{\theta}\right)\hat{\mathbb{E}}\left[\int\limits_{\mathcal{B}(\mathbb{R}^d)}\int\limits_{\mathcal{B}(\mathbb{R}^n)} \alpha_k^u(x,q)\eta_k^u(x,q)dxdq\right] \\ &= \left(\frac{1}{\theta}\right)\hat{\mathbb{E}}[\langle\alpha_k^u(x,q)\eta_k^u(x,q)\rangle] \end{aligned} \tag{28}$$

which is independent of k.

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

$$\eta_k^u(x_k,q) = \int\limits_{\mathcal{B}(\mathbb{R}^d)}\int\limits_{\mathcal{B}(\mathbb{R}^n)}\sum_{r=1}^{2}\frac{\langle Z_{k+1},e_r\rangle\varsigma(q)\phi(y_{k+1}-Cx_k)}{2a_r(Z_{k+1},Y_{k+1})\lambda_{k+1}^r(Y_{k+1},q)\phi(y_{k+1})} \times \varphi\left(x-Ax_k-\gamma_{(Z_{k+1})}Bu_k\right)\exp(\theta D_{k,k}^u)\eta_{k+1}^u(x,\tau)dxd\tau. \tag{29}$$

Moreover, the adjoint process η_k^u is given by the following equivalent relation [cf. (23) and (24)]:

$$\eta_k^u(x,q) = \tilde{\Upsilon}_k\left(u,Q_{N_k^r}\right)\exp\left\{-\frac{1}{2}\left(x-\tilde{\mu}_k(u)\right)^T\tilde{\Theta}_k^{-1}(u)(x-\tilde{\mu}_k(u))\right\} \tag{30}$$

where the finite-dimensional parameters $\tilde{\Upsilon}_k(u,Q_{N_k^r})$, $\tilde{\Theta}_k^{-1}(u)$ and $\tilde{\mu}_k(u)$ satisfy coupled backward, recursions. From (22) [and also equation (A.2) in the supplementary document], the information-state $\alpha_k^u(x,q)$ is determined by $\Upsilon_k(u,Q_{N_k^r})$, $\Theta_k^{-1}(u)$ and $\mu_k(u)$. Thus, based on the current value of ζ_k^u together with the new observation y_{k+1}, current control u_k and the sample-path of the DoS attack sequence $\gamma_{(Z_{k+1})}$, the next value for ζ_{k+1}^u can be determined by the following functional relation:

$$\zeta_{k+1}^u = \zeta_{k+1}^u\left(\zeta_k^u,u_k,y_{k+1},m_{k+1}^r\right). \tag{31}$$

Suppose at some intermediate time k, $0<k<N$, the information-state ζ_k^u is given by $\zeta=(\Upsilon(.),\Theta^{-1}(.),\mu(.))$, then from (28), the value function for the optimal control problem satisfies the following:

$$V(\zeta,k) = \operatorname*{ess\,inf}_{u\in\mathcal{U}_{k,N-1}}\hat{\mathbb{E}}\left[\langle\alpha_k^u,\eta_k^u\rangle\,|\alpha_k=\alpha_k(\zeta)\right]. \tag{32}$$

where $\mathcal{U}_{k,N-1}$ is the set of admissible control sequences in the interval $[k,N-1]$.

Theorem 3: The value function satisfies the following recursion with:

$$V(\zeta,k) = \operatorname*{ess\,inf}_{u\in\mathcal{U}_{k,k}}\hat{\mathbb{E}}\left[V\left(\zeta_{k+1}^u\left(\zeta,u,y_{k+1},m_{k+1}^r\right),k+1\right)\right] \tag{33}$$

with $V(\zeta,N)=\langle\alpha_N(\zeta),\eta_N(\zeta)\rangle$.

Finally, we remark that the optimal control sequences $u_k^*(\zeta_k)$ for each $k=0,1,\ldots,N-1$ of the dynamic programming problem are indeed the optimal control policies for the original problem stated in (11), i.e., $u^*\in\mathcal{U}_{0,N-1}$.

IV. Concluding Remarks

In this technical note, 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 an 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 constitute an equivalent fully observable stochastic control problem. Furthermore, 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, Cybern. A*, vol. 39, no. 5, pp. 1074–1085, 2009.

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

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

[4] A. Teixeira, G. Dan, H. Sandberg, and K. H. Johansson, "A cyber security study of a SCADA energy management system: Stealthy deception attacks on the state estimator," in *Proc. 18th IFAC World Congr.*, Milano, Italy, 2011, pp. 11271–11277.

[5] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inform. Syst. Secur.*, vol. 14, no. 1, pp. 13:1–13:33, 2011.

[6] 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*. Berlin/Heidelberg, Germany: Springer-Verlag, pp. 31–45, 22009.

[7] A. A. Cardenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems," in *Proc. 3rd USENIX Workshop on Hot Topics in Security (HotSec 08)*, 2008, pp. 1–6.

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

[9] 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.

[10] 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 Int. Conf. Systems Science*, 2010, pp. 1–10.

[11] S. Weinberger, "Computer security: Is this the start of cyberwarfare?" *Nature*, vol. 474, pp. 142–145, 2011.

[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 Conf.*, 2011, pp. 643–648.

[13] D. H. Jacobson, "Optimal stochastic linear systems with exponential performance criteria and their relation to deterministic differential games," *IEEE Trans. Autom. Control*, vol. AC-18, no. 2, pp. 124–131, Apr. 1973.

[14] D. P. Bertsekas, *Dynamic Programming and Stochastic Control*. New York, NY, USA: Academic Press, 1976.

[15] P. Whittle, "Risk-sensitive linear/quadratic/Gaussian control," *Adv. Appl. Probab.*, vol. 13, no. 4, pp. 764–777, 1981.

[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 Optimiz.*, vol. 23, pp. 599–613, 1985.

[17] M. R. James, J. Baras, and R. J. Elliott, "Risk-sensitive control and dynamic games for partially observed discrete-time nonlinear systems," *IEEE Trans. Autom. Control*, vol. 39, no. 4, pp. 780–792, Apr. 1994.

[18] I. I. Petersen, M. R. James, and P. Dupuis, "Optimal control of stochastic uncertain systems with relative entropy constraints," *IEEE Trans. Autom. Control*, vol. 45, no. 3, pp. 398–412, Mar. 2000.

[19] J. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proc. IEEE Special Issue on Techn. Netw. 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. Autom. Control*, vol. 50, no. 6, pp. 910–915, Jun. 2005.

[21] G. N. Nair, R. J. Evans, I. M. Y. Mareels, and W. Moran, "Topological feedback entropy and nonlinear stabilization," *IEEE Trans. Autom. Control*, vol. 49, no. 9, pp. 1585–1597, Sep. 2004.

[22] V. Gupta and N. Martins, "On stability in the presence of analog erasure channels between controller and actuator," *IEEE Trans. Autom. Control*, vol. 55, no. 1, pp. 175–179, Jan. 2010.

[23] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, and S. S. Sastry, "Foundations of control and estimation over lossy networks," *Proc. IEEE*, vol. 95, no. 1, pp. 163–187, Jan. 2007.

[24] G. B. Di Masi and W. J. Runggaldier, "On measure transformations for combined filtering and parameter estimation in discrete time," *Syst. Control Lett.*, vol. 2, no. 1, pp. 57–62, 1982.

[25] R. J. Elliott, L. Aggoun, and J. B. Moore, *Hidden Markov Models: Estimation and Control*. New York, NY, USA: Springer-Verlag, 1995.

[26] G. K. Befekadu, V. Gupta, and P. J. Antsaklis, "Risk-sensitive control under a Markov modulated denial-of-service attack model," in *Proc. 50th IEEE Dec. Contr. and Europ. Contr.*, Orlando, FL, USA, Dec. 2011, pp. 5714–5719.

[27] R. S. Liptser and A. N. Shiriyayev, *Statistics of Random Processes I: General Theory*, vol. 1. New York, NY, USA: Springer-Verlag, 1977.

[28] 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*. Boston, MA, USA: Springer, 2009, pp. 71–85.

[29] I. V. Girsanov, "On transforming a certain class of stochastic processes by absolutely continuous substitution of measures," *Theor. Probabil. Appl.*, vol. 5, no. 3, pp. 285–301, 1960.