Effects of Jamming Attacks on a Control System with Energy Harvesting

Steffi Knorn and André Teixeira

***Abstract*—We consider the problem of control and remote state estimation with battery constraints and energy harvesting at the sensor (transmitter) under DoS/jamming attacks. We derive the optimal non-causal energy allocation policy that depends on current properties of the channel and on future energy usage. The performance of this policy is analyzed under jamming attacks on the wireless channel, in which the assumed and the true channel gains differ, and we show that the resulting control cost is not monotonic with respect to the assumed channel gain used in the transmission policy. Additionally, we show that, in case there exists a stabilizing policy, then the optimal causal policy ensures stability of the estimation process. The results were illustrated for non-causal and causal energy allocation policies under different jamming attacks.**

***Index Terms*—energy harvesting, energy allocation, optimal control, cybersecurity, jamming attack**

I. Introduction

NETWORKED control systems have vast and promising applications, such as distributed sensing and control based on Internet-of-Things devices, and flexible and scalable process control through wireless communication networks [1]. The development of low-energy embedded sensors with higher computation and communication capabilities, and the creation of efficient and reliable communication protocols, are the main driving forces behind these applications. Nonetheless, the full benefits of such technologies may be hindered by issues underlying the use of digital connected devices and communication networks, such as malicious cyber-attacks.

Cybersecurity has become an increasingly important aspect of control systems in recent years, driven by the pervasive use of information and communication technologies, as well as by the steadily increasing number of newly discovered vulnerabilities and reported cyber-attacks [2]. See the overview in [3], [4]. Rational adversaries are highlighted as one of the key items in security for control systems, where adversaries may exploit existing vulnerabilities and limitations in the modern closed-loop systems. For instance, targeting battery-powered wireless devices with jamming attacks to deplete their batteries [5].

Denial-of-Service (DoS) attacks affecting the availability of data have been recently addressed from different angles. In DoS attacks, the adversary aims at dropping transmitted data packets, or jamming the wireless communication medium [6], so that the performance of the closed-loop system is deteriorated [7], [8], possibly resulting in instability.

S. Knorn and A. Teixeira are with the Department of Engineering Sciences, Uppsala University, Sweden; Email: {steffi.knorn;andre.teixeira}@angstrom.uu.se. This work was supported in part by the Swedish Research Council (grant 2018-04396).

DoS attacks have recently been addressed in the literature, both with the purpose of analyzing such attacks, as well as to mitigate their impact. For instance, in [9], [10] the authors formulate the DoS attacks using zero-sum dynamic games, where the optimal attack strategy aims at maximizing the impact on control performance. Similarly, [6] considers a state estimation problem under DoS attacks, using game-theory to derive the optimal attack strategy that most degrades estimation performance. Approaches to mitigate the impact of DoS attacks have also been proposed, including game theoretic schemes [6], [9], [10], optimal control [7] and event-triggered control [8], [11], [12].

Common to most of this work is the assumption that the transmitter and receiver have no energy constraints. In contrast, the adversary is often assumed to be constrained in the amount of packets it can block [9], or in the available energy to jam the communication channel. Transmission and jamming power constraints are also considered in the remote estimation problem in [6], but battery dynamics and capacity constraints were neglected.

In contrast, we consider a remote state estimation scenario with energy harvesting at the battery-powered sensor (transmitter) in a closed control loop. This paper is an initial study of the problem of remote state estimation with energy harvesting and battery constraints in a closed control loop under DoS attacks, and focuses on its structural properties.

As a first step, we derive the optimal non-causal energy allocation policy that depends on properties of the channel and on future energy usage. The performance of this policy is analyzed under jamming attacks on the wireless channel, in which the assumed channel gain (used in the policy) differs from the true channel gain (due to the DoS attack). In particular, we show that the resulting control cost is not monotonic with respect to the assumed channel gain. Additionally, we establish that, in case there exists a stabilizing policy, then the optimal causal policy stabilizes the estimation process.

Sec. II describes the nominal wireless control system. The optimal energy allocation policy in the absence of attack is described in Sec. III. Sec. IV analyzes how the optimal policy performs under attack. Numerical examples are presented in Sec. V. The paper concludes in Sec. VI.

II. System Model

A scheme of the system model can be found in Figure 1. A detailed description of the components is given below.

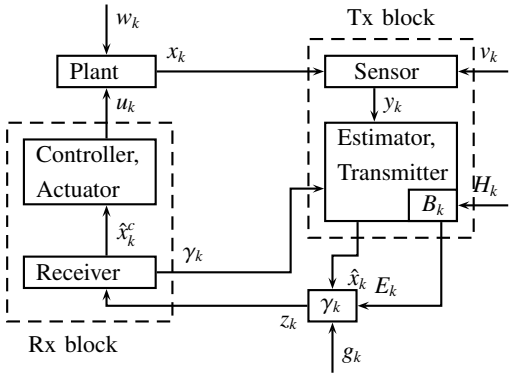

Figure 1: Scheme of system model

A. Plant Model

The plant is modeled as a linear system with state $x_k \in \mathbb{R}^n$, process noise $w_k \in \mathbb{R}^n$, and a control input $u_k \in \mathbb{R}^p$: $x_{k+1} = Ax_k + Bu_k + w_k$ with initial state x_0. The process noise is assumed to be i.i.d. Gaussian noise with zero mean and covariance matrix $M = \mathbb{E}\{w_k w_k^{\mathrm{T}}\} \geq 0$. A, B are matrices of appropriate dimensions. Similar to [13], we assume that (A, B) and $(A, M^{\frac{1}{2}})$ are controllable.

B. Sensor

The sensor produces a noisy measurement of the state given by $y_k = Cx_k + v_k$ where (A,C) is assumed to be observable, $y_k \in \mathbb{R}^q$, and $v_k \in \mathbb{R}^q$ is assumed to be i.i.d. Gaussian noise (independent of x_0 and w_k) with zero mean and covariance matrix $N = \mathbb{E}\{v_k v_k^{\mathrm{T}}\} > 0$.

C. State Estimator at the Transmitter

We assume a smart sensor with computational capability to estimate the current state, and that the sensor/transmitter forwards a state estimate to the controller. The sensor measurements are used at the transmitter to estimate the current state x_k based on the information set $\mathcal{I}_k = \{\hat{x}_0, y_l, \gamma_{l-1} : 1 \leq l \leq k\}$, where γ_l denotes the packet loss process in the sensor-receiver communication link, which is made available to the transmitter through the channel feedback acknowledgment, as discussed in detail in Sec. II-E below. Since the transmitter knows the exact packet loss sequence and the control law, it can reconstruct the Kalman filter at the receiver, and the exact control input applied to the plant, which is calculated by the receiver based on its state estimate.

We assume that the Kalman filter at the transmitter has been running for a long time before $k = 0$ such that the Kalman filter at the transmitter has reached a steady state with the error covariance matrix given by P_∞.

D. Energy Harvester and Battery Dynamics

The transmitter has a rechargeable battery or (super) capacitor equipped with an energy harvester, that can gather energy from the environment. The unpredictable energy available to be harvested at k, denoted H_k, is described as a stationary first-order homogeneous finite-state Markov process, [14]. We assume that the energy for sensing and computational purposes at the transmitter are negligible compared to the transmission energy. The stored energy in the battery at k, B_k, evolves according to

$$B_{k+1} = \min\{B_k - E_k + H_k; \quad \bar{B}\} \tag{1}$$

with $0 \leq B_1 \leq \bar{B}$ and where $\bar{B}$ is the battery capacity, and E_k is the energy used for transmission at k.

E. Communication Channel

A wireless communication channel is used to transmit the state estimate $\hat{x}_k$ to the controller/actuator, referred to as Rx block. The channel is a packet dropping link such that the estimate is either exactly received (for $\gamma_k = 1$) or completely lost due to corrupted data or substantial delay (for $\gamma_k = 0$), where γ_k is the Bernoulli random variable modelling the packet loss process. The received signal is $z_k = \gamma_k \hat{x}_k$. Based on wireless communication principles [15], we suppose that the channel is affected by independent additive white Gaussian noise (AWGN) with energy n_0, in which case the probability of successful transmitting a packet depends on the signal-to-noise ratio (SNR) of the channel. Denoting E_k as the energy for transmitting the packet at time k over the channel, and $g = \frac{1}{n_0}$ as the channel gain, the SNR is given by gE_k and the probability of successfully transmitting the packet is

$$\mathbb{P}(\gamma_k = 1 | E_k) := h(gE_k) \tag{2}$$

where the function $h : [0,\infty] \to [0,1]$ is monotonically increasing and continuous. The function h relates to how the SNR affects the packet-error rate, which depends on the modulation of the channel, see [15] for further details.

We assume that the channel gain g is constant. In practice, there might be several reasons to make such assumption. First, listening to a pilot signal in order to estimate the channel gain consumes significant amounts of energy, which might instead be used for data transmission. Further, in known environments and maybe even connections with line of sight, channel gains might not vary significantly and can be simplified as being constant over time. This also simplifies the analysis and computation, which might be another significant advantage in practice. Note that this is assumption is similar to assuming a constant packet drop probability, which is common in the literature, see for instance [13].

Based on the channel harvested energy H_k, and the current battery level B_k, the transmitter finds an optimal energy allocation policy $\{E_k\}$ in order to minimise a suitable finite horizon control cost. The details of this optimal energy allocation scheme will be provided in the next section.

After receiving z_k over the lossy communication channel, the receiver sends an ACK/NACK packet, i.e. γ_k, to the transmitter over a perfect feedback channel.

F. Estimator/Controller and Actuator in the Receiver block

The controller in the receiver block has access to the information set $\mathcal{I}_k^c := \{\hat{x}_0^c, z_l, \gamma_l : 1 \leq l \leq k\}$. As the estimates from the transmitter Kalman filter are dropped with probability $1 - h(gE_k)$, the current state estimate is not always available at the Rx block. Hence, the state estimate at the Rx block, $\hat{x}_{k|k}^c = E[x_k | \mathcal{I}_k^c]$, is given by

$$\hat{x}_k^c := \hat{x}_{k|k}^c = \gamma_k \hat{x}_k + (1 - \gamma_k)\left(A\hat{x}_{k-1}^c + Bu_{k-1}\right). \tag{3}$$

The estimation error covariance matrix at the Rx block is

$$\begin{aligned} P_k^{\mathrm{c}} :=& \mathbb{E}\left\{(x_k - \hat{x}_k^{\mathrm{c}})(x_k - \hat{x}_k^{\mathrm{c}})^{\mathrm{T}} | \mathcal{I}_k^{\mathrm{c}}\right\} \\ =& \gamma_k P_\infty + (1-\gamma_k)\left(AP_{k-1}^{\mathrm{c}}A^{\mathrm{T}} + M\right). \end{aligned} \tag{4}$$

We assume that the Rx block uses as initial state distribution $P_0^{\mathrm{c}} := P_\infty$. Since it is assumed that the Tx block receives the ACK/NACK packet without fault, a copy of P_k^{c} can be kept at the Tx block.

The task of the controller is to design an optimal control sequence $\{u_k\}$ based on the information pattern $\mathcal{I}_k^{\mathrm{c}}$ such that a suitable average control cost is minimised. It is assumed that the link between the Rx block and the plant is lossless, such that the correct control signal u_k is applied to the plant. This is a reasonable assumption in case the actuator is directly connected or located very close to the plant.

G. Optimisation Problem and Separation Principle

We seek to find the optimal transmission energy allocation policy E^{K^*} and the optimal control policy u^{K^*}, that jointly minimise the finite horizon LQG control cost

$$J(u^K, E^K, x_0, P_\infty) = \mathbb{E}\left\{x_{K+1}^{\mathrm{T}} Q x_{K+1} + \sum_{k=1}^{K}\left(x_k^{\mathrm{T}} Q x_k + u_k^{\mathrm{T}} S u_k\right)\right\}$$

where $u^K = \{u_1, \ldots, u_K\}$, $E^K = \{E_1, \ldots, E_K\}$, and the cost depend on the mean and the variance of the initial state.

Similar to the case in [16], it can be shown that a separation principle holds: Note that the control input u_k is perfectly known at the transmitter due to receiving perfect acknowledgments. Thus, the estimation error is independent of the control input (see also [13]) and the separation principle holds in this case. Hence, the tasks of obtaining the optimal Kalman filtered state estimate $\hat{x}_k, \hat{x}_k^{\mathrm{c}}$, calculating the optimal control input u_k^* at the controller, and computing the optimal energy allocation E_k^* at the transmitter can be done separately. Therefore, implementing the Kalman filters as discussed above is optimal. Further, the optimal control policy is an LQG controller as in [16]. The optimization problem for finding the optimal transmission energy allocation is described below. Note that we will consider both the nominal case and the system under DoS/jamming attack, which reduces the channel gain. Hence, in contrast to [16], which analyzed the effect of perfect vs imperfect acknowledgements but accurate knowledge of the channel gain, this paper considers the impact of jamming attacks on a system with perfect acknowledgements and using the optimal (for the nominal case) energy allocation policy.

III. Energy Allocation Policy

In this section, we characterize the optimal causal policy, and look further into the optimal non-causal policy to derive structural results used to analyze the effects of jamming attacks in the following section.

A. Optimal Solution for Causal Information and Limited Battery Capacity

Since the separation principle holds, the optimal energy allocation policy at the transmitter can be obtained by solving

$$\min_{0\le E_k\le B_k \forall k} \sum_{k=1}^{K} \tilde{J}_k(H_k, B_k, P_{k-1}^{\mathrm{c}}, E_k), \tag{5}$$

where $\tilde{J}_k(H_k,B_k,P_{k-1}^{\mathrm{c}},E_k) := \mathbb{E}\left\{tr(P_k^{\mathrm{c}}) \,|\, H_k,B_k,P_{k-1}^{\mathrm{c}}, E_k\right\}$. In the remainder of the paper, we omit the argument of $\tilde{J}_k$ when there is no ambiguity. Indeed, (5) is a stochastic control problem with the state process $(H_k,B_k,P_{k-1}^{\mathrm{c}})$ and the control action E_k. In practice, only causal information about the harvested energy and battery level is available. Hence, the future unpredictable energy harvesting information is not a priori known. In this case, the solution to the stochastic control problem (5) is given as follows:

Theorem 1: Let the initial condition be $\mathcal{I}_1 = \{H_1, B_1, P_0^{\mathrm{c}} = P_\infty\}$. Then the value of the finite-time horizon minimisation problem (5) with causal information is given by $V_1(H_1,B_1,P_0^{\mathrm{c}})$, which can be computed recursively from the backward Bellman dynamic programming equation

$$\begin{aligned} V_k(H_k,B_k,P_{k-1}^{\mathrm{c}}) = & \min_{0\le E_k\le B_k} \Big\{\tilde{J}_k(H_k,B_k,P_{k-1}^{\mathrm{c}},E_k) \\ & + \mathbb{E}\left\{V_{k+1}(H_{k+1},B_{k+1},P_k^{\mathrm{c}}) \middle| E_k,H_k,B_k,P_{k-1}^{\mathrm{c}}\right\}\Big\} \end{aligned} \tag{6}$$

with the battery dynamic equation (1) and the terminal condition $V_K(H_K,B_K,P_{K-1}^{\mathrm{c}}) = \mathbb{E}\left\{tr(P_K^{\mathrm{c}})|B_K\right\}$, where all remaining energy is used up for transmission in the final time K.

Proof: The proof follows from the optimality equations for finite-time horizon stochastic control problems, [17]. ■

The optimal energy allocation policy can be calculated for all possible combinations of H_k, B_k, and P_{k-1}^{c}, and for all k and stored in a look-up table. Then, when implementing the policy, the optimal value of E_k is simple taken from the table. However, the optimal solution is based on the assumption that the channel gain is indeed the known value g, which may be untrue on the case of jamming attacks. Analyzing the influence of the jamming attack onto the optimal solution for causal information is difficult since no closed form solution exists. Hence, instead we will analyze the optimal solution for the unrealistic case of non-causal state information and unlimited battery capacity, for which an explicit solution exists. Of course, the influence onto the performance under the optimal policy for the causal information case with limited battery capacity will be different. However, analyzing the case below offers structural insights into the problem and is an important benchmark for the optimal solution under realistic conditions.

B. Lagrangian Formulation for Non-causal Information and Unlimited Battery Capacity

Using (2), the properties of the trace and the expected value, the function $\tilde{J}_k(H_k,B_k,P_{k-1}^{\mathrm{c}},E_k)$ can be rewritten as

$$\begin{aligned} \tilde{J}_k =& \mathbb{E}\left\{\left(\gamma_k tr(P_\infty) + (1-\gamma_k) tr\left(AP_{k-1}^{\mathrm{c}}A^{\mathrm{T}} + M\right)\right) | E_k\right\} \\ =& h(gE_k) tr(P_\infty) + (1 - h(gE_k)) tr\left(AP_{k-1}^{\mathrm{c}}A^{\mathrm{T}} + M\right). \end{aligned}$$

Hence, the Lagrangian formulation for this problem, given the Lagrange multipliers $\lambda_k \ge 0$, $k = 1, 2, \ldots, K$ is [17],

$$\mathcal{L}(E,\lambda) = \sum_{k=1}^{K}\left[\lambda_k\left(\sum_{l=1}^{k} E_l - \sum_{l=1}^{k-1} H_l - B_1\right) + \tilde{J}_k\right]. \tag{7}$$

E_k^o, and λ_k^o are primal and dual optimal solutions to (7) if and only if they satisfy the Karush-Kuhn-Tucker (KKT) optimality conditions for $k = 1, 2, \ldots, K$ i. e.,

$$E_k \geq 0, \quad \lambda_k \geq 0, \quad \sum_{l=1}^{k} E_l - \sum_{l=1}^{k-1} H_l - B_1 \leq 0, \tag{8}$$

$$\lambda_k \left(\sum_{l=1}^{k} E_l - \sum_{l=1}^{k-1} H_l - B_1 \right) = 0, \tag{9}$$

$$\frac{\partial \mathcal{L}}{\partial E_k}\bigg|_{E_k = E_k^o} \begin{cases} \geq 0 & \text{for } E_k^o = 0 \\ = 0 & \text{for } 0 < E_k^o < B_k \\ \leq 0 & \text{for } E_k^o = B_k \end{cases} \tag{10}$$

The Lagrangian multipliers λ_k are introduced as penalty terms to ensure that energy causality is respected, that is, to ensure that not more energy is used for data transfer than is available in the battery at the same time step, see (8). The KKT condition (9) ensures that the optimal solution of the Lagrangian is identical to the solution of the original optimisation problem (5) with energy causality constraints. The last KKT condition (10) follows from the fact that the Lagrangian function $\mathcal{L}$ is convex due to the convexity of the objective function and the linearity of the constraints.

C. Optimal Solution for Non-Causal Information and Unlimited Battery Capacity

Based on the Lagrangian formulation in (7), the KKT conditions (8)-(10) and an additional assumption on the function h in (2), the optimal solution for the non-causal case with unlimited battery capacity can be obtained:

Theorem 2: Suppose that the Tx-block has a battery of unlimited capacity and access to non-causal information on the harvested energy for all time steps. Further, assume that the first derivative of h in (2) exists and is invertible for non-negative arguments. Then, the optimal transmission energy allocation at time k is given by

$$E_k^o = \begin{cases} 0 & \text{if } \Phi_k \leq 0 \\ \Phi_k & \text{if } 0 < \Phi_k < B_k^* \\ B_k^* & \text{if } \Phi_k \geq B_k^* \end{cases} \tag{11}$$

with the largest possible energy for data transmission at k being $B_k^* = B_1 + \sum_{l=1}^{k-1} H_l - \sum_{l=1}^{k-1} E_l$ and

$$\Phi_k = \xi \left(\frac{\Lambda_k}{tr\left(\Delta P_k\right) g} \right) \Bigg| g \tag{12}$$

where $\Delta P_k := A P_{k-1}^{\mathrm{c}} A^{\mathrm{T}} + M - P_\infty$, $\Lambda_k := \sum_{l=k}^{K} \lambda_l$ and ξ is the inverse function of $\frac{dh(x)}{dx}$.

Proof: The KKT condition (10) for $E_k^o > 0$ yields

$$\frac{\partial \mathcal{L}}{\partial E_k}\bigg|_{E_k = E_k^o} = - g \left. \frac{dh(x)}{dx} \right|_{x = g E_k^o} tr\left(\Delta P_k\right) + \Lambda_k = 0. \tag{13}$$

Solving for E_k^o leads to (12). Whenever Φ_k is within the achievable boundaries of 0 and the battery level B_k^* we have $E_k^o = \Phi_k$. Otherwise Φ_k will be saturated below at 0 and above at B_k^* to ensure the KKT conditions are satisfied. ■

Remark 1: Note that h is a non-decreasing function, which reaches 1 asymptotically as its argument tends towards infinity. Assuming that its first derivative is invertible for non-negative arguments, the derivative is a non-negative, decreasing function. The same is also true for its inverse ξ.

Remark 2: Due to (8), Λ_k is non-increasing in k. Hence, for constant P_{k-1}^{c}, the argument of ξ in (12) will be non-decreasing in k. Since ξ is a decreasing function, the optimal transmission energy for constant P_{k-1}^{c} is also non-decreasing in k such that there exists a tendency to use more energy at later time steps k. This is similar to the directional or staircase water filling algorithm shown to be the optimal energy allocation policy for a similar problem in [18], [19].

A more in depth analysis of the optimal solution, for the case with non-causal information and unlimited battery capacity, can be found in the following subsection.

IV. Optimal Policy under Jamming Attack

This section more closely examines the effects of jamming attacks on the control cost and stability of the control system, given that the optimal energy allocation policy is used with an assumed nominal (but possibly incorrect) channel gain g.

A. Channel model under jamming attack

As detailed in Sec. II-E, we consider a AWGN wireless channel. The effect of a jammer on the communication channel is the same as that of an interference source. Therefore, the channel under a jamming attack is modeled in terms of the signal-to-interference-plus-noise ratio (SINR) of the channel. Denoting $g_{\text{true}} = \frac{1}{E_{\text{jam}} + n_0}$ as the channel gain under the interference of a jamming attack with energy E_{jam}, the SINR is given by $g_{\text{true}} E_k$ and the probability of successfully transmitting the packet is $\mathbb{P}(\gamma_k = 1 | E_k) := h(g_{\text{true}} E_k)$. Similarly as the interference-free case, the function h relates to the SINR and the modulation of the channel, see [15] for further details.

B. Analysis of the Optimal Solution with Non-Causal Information under Jamming Attack

It is an interesting question how the optimal policy, which was derived for assuming non-causal information, unlimited battery capacity and an assumed, nominal channel gain g, will perform under a jamming attack, where the unknown true channel gain $g_{\text{true}} < g$.

For this, we will make two simplifying assumptions:

- A1 The probability function h in (2) is of the form $h(gE_k) = 1 - \mathrm{e}^{-gE_k/\tau}$, such that $\xi(y) = -\tau \ln(\tau y)$.
- A2 The saturation in (11) is ignored such that $E_k^o = \Phi_k$ as given in (12).

Then, the following result can be shown.

Lemma 1: Consider policy (12) and Assumptions A1 and A2 above hold. Then, the expected increase of the accumulated error covariance in (5) for time k is given by

$$\tilde{J}_k = tr(P_\infty) + tr(\Delta P_k) \left(\frac{\tau \Lambda_k}{tr(\Delta P_k) g} \right)^{g_{\text{true}}/g} \tag{14}$$

Proof: Using the definition of $\tilde{J}_k$ and applying A1 and A2 yield the result. ■

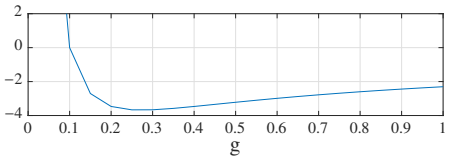

Figure 2: Illustration of factor $\frac{1}{g}\left(\log\left(\frac{\tau\Lambda_k}{tr(\Delta P_k)}\right)-\log(g)\right)$ in (15) for $\frac{\tau\Lambda_k}{tr(\Delta P_k)}=0.1$ as a function of g.

Remark 3: In the worst case $g_{\text{true}}=0$ such that $\tilde{J}_k=tr(P_\infty)+tr(\Delta P_k)=tr(AP^{\text{c}}_{k-1}A^{\text{T}}+M)$, capturing the fact that the packet will be lost with probability 1, such that the state estimate must be achieved by a simple prediction step given the last available state estimate.

Remark 4: For arbitrary values of g_{true} the difference between the actual expected increase in the accumulated error covariance measure, $\tilde{J}_k$, and the best possible situation, $tr(P_\infty)$, is given by $\tilde{J}_k-tr(P_\infty)=tr(\Delta P_k)\left(\frac{\tau\Lambda_k}{tr(\Delta P_k)g}\right)^{g_{\text{true}}/g}$ which yields in logarithmic scale

$$\log\left(\tilde{J}_k-tr(P_\infty)\right)=\log(tr(\Delta P_k))+\frac{g_{\text{true}}}{g}\left(\log\left(\frac{\tau\Lambda_k}{tr(\Delta P_k)}\right)-\log(g)\right). \tag{15}$$

Note that the factor $\frac{1}{g}\left(\log\left(\frac{\tau\Lambda_k}{tr(\Delta P_k)}\right)-\log(g)\right)$ is not monotonic in g and might even change sign. See Figure 2.

The results in this subsection were derived with several simplifying assumptions, including non-causal information, unlimited battery capacity, ignoring the saturation of E^o_k in (11) and assuming a specific function for h in (2). Hence, we cannot conclude that the derived results hold true for realistic and more general model cases. However, they show that the effects of jamming attacks leading to a mismatch between the assumed nominal g and the true g_{true} are far from trivial. Nonetheless, we will show that even in case of jamming attacks, stability might be guaranteed in some cases.

C. Stability Analysis for the Optimal Solution with Causal Information under Jamming Attack

Consider again the case that the communication system is suffering a jamming attack such that the actual channel gain g_{true} is lower than the assumed, nominal channel gain g.

It is straightforward to show that in general the energy allocation policy (11) will not be optimal in case the true channel gain is not the same as the assumed channel gain, i.e., $g_{\text{true}}\neq g$. As time K grows without bound, hence the system might become unstable in case too many packets are lost between the transmitter and the receiver. However, we will show below that as long as there exists a policy that given enough harvested energy stabilises the plant, then using the policy (11) despite $g_{\text{true}}\neq g$ will also stabilise the system.

As a first step, we show that there exists a policy to ensure that the error covariance matrix is bounded in case the harvested energy is sufficient under the greedy policy, for which $E_k=B_k,\forall k$.

Theorem 3: Assume the error covariance matrix at the controller P^{c}_k in (4). If there exists a $\psi\in[0,1)$ such that

$$\sup_H\int_{H_{k-1}}\left(1-h\left(g_{\text{true}}\min\left\{H_{k-1},\bar{B}\right\}\right)\right)\times\mathbb{P}\left(H_k|H_{k-2}=H\right)dH_{k-1}\leq\frac{\psi}{\|A\|^2}, \tag{16}$$

then there exists a policy $\{E_k\}$ such that for some scalars $\alpha,\beta>0$ the norm of P^{c}_k satisfies

$$\mathbb{E}\left\{\left\|P^{\text{c}}_k\right\|\right\}\leq\alpha\psi^k+\beta\text{ for all }k\geq 1. \tag{17}$$

Proof: The proof is based on [20, Thm 1] showing that for constant channel gain g_{true} a sufficient condition for exponential stability in the sense of (17) is $\sup_H\mathbb{P}\left(\gamma_k=0|H_{k-1}=H\right)\leq\frac{\psi}{\|A\|^2}$ for some $\psi\in[0,1)$. The exponential stability condition yields (16) with $\min\left\{H_{k-1},\bar{B}\right\}=E_k$ for some $\psi\in[0,1)$. Assume all the harvested energy at each time step is used for data transmission. Then, $E_1=B_1$ and $E_k=\min\{H_{k-1};\bar{B}\}$ for $k>1$. Then (16) is a sufficient condition to guarantee (17). ■

The theorem above shows that in case the probability of loosing a packet when using the greedy policy is small enough, then there exists an energy allocation policy, which guarantees that $\mathbb{E}(tr(P^{\text{c}}_k))$ is bounded according to (17). So, if we can show that the optimal policy designed for the nominal case with g, given the actual channel gain g_{true} performs better than or converges to the greedy policy, i.e., towards $E_k=B_k,\forall k$, then using the optimal policy designed for g stabilises the system under a jamming attack with $g_{\text{true}}<g$.

Theorem 4: Consider the error covariance matrix at the controller P^{c}_k in (4) and there exists a $\psi\in[0,1)$ such that (16) for g_{true}. Then, using the energy allocation policy (11) derived for $g>g_{\text{true}}$ guarantees that there exists some scalars $\alpha,\beta>0$ such that (17) holds true.

Proof: The proof follows by contradiction. Consider that the error covariance matrix grows without bound. Hence, the trace in the denominator of the argument of ξ in (12) tends towards zero. Since ξ is a non-negative, decreasing function, see Remark 1, Φ_k grows without bound and the transmission energy will converge to the available energy in the battery. In case this policy is continued due to large values of Φ_k, this corresponds to the greedy policy in which all available energy is immediately used for transmission. However, it was shown in Theorem 3 that, under the greedy policy and gain g_{true}, condition (16) guarantees (17). ■

V. Numerical Example

A scalar system with parameters $A=1.1$, $B=1$, $C=1$, $M=1$ and $N=1$ is considered. It is assumed that the sensor uses a binary phase shift keying (BPSK) transmission scheme, [15], with $b=4$ bits per packet. Hence, $\mathbb{P}\{\gamma_k=1|g_k,E_k\}=h(g_kE_k)=\left(\int_{-\infty}^{\sqrt{g_kE_k}}\frac{1}{\sqrt{2\pi}}e^{-t^2/2}dt\right)^b$. The battery capacity is set to 5mW and the harvested energy is chosen randomly using an exponential distribution with $\mu_H=1mW$.

Four scenarios have been simulated. In the first two scenarios, the optimal solutions are obtained. In the first case, we consider non-causal information for the harvested energy.

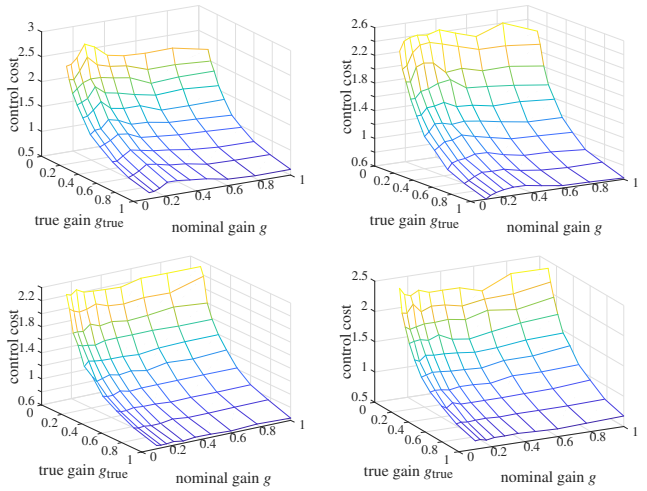

Figure 3: Control cost for Scenario 1 (non-causal inf., optimal sol; top. left), Scenario 2 (causal inf., optimal sol.; top right), Scenario 3 (causal inf., greedy policy; bottom left), Scenario 4 (causal inf., inverted channel policy; bottom right)

The second scenario only uses causal information of the harvested energy and dynamic programming is used to solve the Bellman optimality equation. Scenarios 3 and 4 consider two heuristic policies. In scenario 3 the greedy policy is used, in which $E_k = B_k, \forall k$. The second heuristic policy, shown in scenario 4, is the "inverted channel policy": Denote the required transmission energy such that the expected drop-out probability of the communication channel with channel gain g is equal to a desired probability $\bar{\gamma}$, by $E_{\bar{\gamma}}(\bar{\gamma},g)$. Then, $E_k = \min\{B_k, E_{\bar{\gamma}}(\bar{\gamma},g)\}$. The control cost for all scenarios for $K = 25$ (averaged over 10000 runs) is shown in Fig. 3.

The control cost increases for all scenarios as the true channel gain decreases. Consider specially the case where the nominal channel gain g decreases, due to the transmitter's belief of being under an increasingly harsh jamming attack, whereas the true channel gain remains constant. For both optimal solutions (Scenarios 1 and 2) the control cost increases as the nominal channel gain decreases until $g = 0.2$ and then decreases again for g between 0.1 and 0.2. This lack of monotonicity can be explained by the structure of the optimal solution, see Sec. IV-B. Further, due to the mismatch between g and g_{true}, the optimal solution (derived for g) performs noticeably worse than the heuristics.

VI. Conclusions

In this paper, we have considered a closed-loop with a remote state estimation scenario with battery constraints and energy harvesting at the transmitter under DoS/jamming attacks. Supported by the separation principle for the nominal case without attacks, an optimal causal energy allocation policy was characterized as a dynamic programming problem. To shed light onto the effects of jamming attacks, the non-causal case was analyzed, where the optimal non-causal energy allocation policy was derived and parameterized by the future battery usage and the current channel properties. Analyzing this optimal non-causal policy under jamming attacks, in which the assumed and the true channel gains differ, we observed that the resulting control cost is not monotonic on the assumed channel gain used in the transmission policy. Despite this result, we have shown that, in case there exists a stabilizing policy, then the optimal causal policy ensures stability of the estimation process. The results were illustrated for non-causal and causal energy allocation policies under different jamming attacks.

References

[1] J. Åkerberg, M. Gidlund, and M. Björkman, "Future research challenges in wireless sensor and actuator networks targeting industrial automation," in *9th IEEE International Conference on Industrial Informatics*, jul 2011.

[2] T. Micro, "Unseen threats, imminent losses 2018 midyear security roundup," 2018. [Online]. Available: https://documents.trendmicro.com/assets/rpt/rpt-2018-Midyear-Security-Roundup-unseen-threats-imminent-losses.pdf

[3] A. A. Cárdenas, S. Amin, and S. S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *First International Workshop on Cyber-Physical Systems*, jun 2008.

[4] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, no. 1, pp. 135–148, 2015.

[5] C. Pielli, F. Chiariotti, N. Laurenti, A. Zanella, and M. Zorzi, "A game-theoretic analysis of energy-depleting jamming attacks," in *2017 International Conference on Computing, Networking and Communications (ICNC)*, Jan 2017, pp. 100–104.

[6] K. Ding, X. Ren, D. E. Quevedo, S. Dey, and L. Shi, "Dos attacks on remote state estimation with asymmetric information," *IEEE Transactions on Control of Network Systems*, 2018.

[7] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *International Workshop on Hybrid Systems: Computation and Control*. Springer, 2009, pp. 31–45.

[8] C. De Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Trans. Automatic Control*, vol. 60, 2015.

[9] A. Gupta, C. Langbort, and T. Başar, "Dynamic games with asymmetric information and resource constrained players with applications to security of cyberphysical systems," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 71–81, 2017.

[10] V. Ugrinovskii and C. Langbort, "Controller–jammer game models of denial of service in control systems operating over packet-dropping links," *Automatica*, vol. 84, pp. 128–141, 2017.

[11] A. Cetinkaya, H. Ishii, and T. Hayakawa, "Networked control under random and malicious packet losses," *IEEE Transactions on Automatic Control*, vol. 62, no. 5, pp. 2434–2449, 2017.

[12] D. Senejohnny, P. Tesi, and C. De Persis, "A jamming-resilient algorithm for self-triggered network coordination," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 3, pp. 981–990, 2018.

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

[14] C. K. Ho, P. D. Khoa, and P. C. Ming, "Markovian models for harvested energy in wireless communications," in *IEEE International Conference on Communication Systems (ICCS)*, 2010, pp. 311–315.

[15] J. Proakis, *Digital Communications*, 4th ed. New York: McGraw-Hill, 2001.

[16] S. Knorn and S. Dey, "Optimal sensor transmission energy allocation for linear control over a packet dropping link with energy harvesting," in *IEEE Conference on Decision and Control (CDC)*, 2015.

[17] D. P. Bertsekas, *Dynamic Programming and Optimal Control*, 3rd ed. Athena Scientific, 1995, vol. 1.

[18] C. K. Ho and R. Zhang, "Optimal energy allocation for wireless communications with energy harvesting constraints," *IEEE Transactions on Signal Processing*, vol. 60, no. 9, pp. 4808–4818, September 2012.

[19] O. Ozel, J. Yang, and S. Ulukus, "Optimal transmission schemes for parallel and fading gaussian broadcast channels with an energy harvesting rechargeable transmitter," *Computer Communications*, vol. 36, no. 12, pp. 1360–1372, 2013.

[20] D. E. Quevedo, A. Ahlén, and K. H. Johansson, "State estimation over sensor networks with correlated wireless fading channels," *IEEE Trans. Automatic Control*, vol. 58, no. 3, pp. 581–593, March 2013.