Deception Attack Detection using Reduced Watermarking

Arunava Naha[1], André Teixeira[1], Anders Ahlén[1] and Subhrakanti Dey[2]

***Abstract*— The addition of physical watermarking to the control input is a well-adopted technique to detect the data deception attacks on the cyber-physical systems. However, the addition of the watermarking increases the control cost. On the other hand, the attack might be a rare event. In this paper, we propose to reduce the control cost when the system is not under attack by adding the watermarking as and when needed depending on a posterior probability of attack. We first formulate a stochastic optimal control problem, and then solve it using dynamic programming by keeping a balance between the detection delay, false alarm rate (FAR), and the reduction in control cost. We numerically find two thresholds from the value iterations, Th_e and Th_d, Th_d is greater than Th_e, for the posterior probability of attack p_k. If p_k is greater than or equal to Th_e, then the watermarking signal is added for the $(k+1)$-th instant of time. On the other hand, if p_k greater than or equal to Th_d, then we declare that the system is under attack. We have provided simulation results to illustrate our approach. For the example system model considered in this paper, we have achieved a considerable reduction in the control cost during the normal operation compared to the case where watermarking is always present without sacrificing much in the detection delay.**

I. Introduction

Large cyber-physical systems (CPS) employing networked controls are getting deployed for various safety-critical applications, such as intelligent transportation, smart grids, manufacturing industries, etc. [1]. However, the use of commodity software and off-the-shelf components for networking and computation make the CPS vulnerable to the attacks [2]. Before we go for large scale implementations of the CPS for various safety-critical applications, such vulnerabilities must be addressed. Several effective protection schemes, such as cryptography, firewall, digital watermarking, etc. are in place to protect the cyber layer of the CPS. However, such protection schemes may not be adequate to protect the physical layer of the CPS against the data deception attacks and denial of service (DoS) attacks. There are multiple incidents in the past where the attacker successfully caused damage to the CPS despite the presence of various protection schemes for the cyber layer [2]. Stuxnet attack is probably the most famous one [3]. In the data deception attack, the attacker replaces the true observations and/or the actual control inputs with fake data and/or harmful exogenous inputs. In one form of data deception attacks, the attacker records the true observations and replays it back at some later point in time. Such attacks are called replay attacks, and the Stuxnet attack was an incident of a replay attack. In the DoS, the attacker overpowers the wireless communication channel so that the required information could not be transmitted. Attacks on the physical layer can cause monetary loss as well as it can pose serious threats to human safety. Therefore, it is of immense importance to detect the attack on the CPS as soon as possible to reduce the amount of damage.

In this paper, we have studied the problem of data deception attacks where the attacker replaces the true observations either with the fake data generated from a separate stochastic process or with the previous recordings of the true observations. A well-adopted technique to detect such data deception attacks on the networked control systems (NCS) is to add the watermarking signals to the control inputs. The watermarking signals may be generated randomly from some Gaussian distributions [4] or hidden Markov models (HMM) [2]. Attacks are generally detected by different statistical tests on the innovation signal [2] or the observations [5]. Such methods are studied intensively in the literature [2], [5]. However, the addition of the watermarking increases control cost. In [2], the authors provide an analytical expression for the increase in the linear quadratic Gaussian (LQG) control cost if the watermarking is added to the control inputs for every time instants during the normal operation of the system.

Since the attack on the system can be considered to be a rare event, the addition of the watermarking to the system operating under the normal conditions for a long time will increase the total control cost significantly. There are few approaches found in the literature that address the problem of increased control cost due to the added watermarking. In one approach, the authors add periodic watermarking to reduce the control cost and keep a balance between the improvement in terms of the control cost and the increase in the detection delay [6]. In another approach, the researchers add or multiply the watermarking signals to the observations before the transmission. At the receiver end, the watermarking signals are filtered out before feeding the observations to the controller. Therefore, the control cost does not increase. In [7], each output is modulated by a watermarking signal before the transmission. In [8], authors use pairs of filters to add and remove sinusoidal watermarking signals, whereas, in [9], random noise watermarking signals are used. However, if the attacker can hijack the sensor node and replaces the true observations before the addition of the watermarking, then such methods may not be able to detect the attacks.

In this paper, we have devised an adaptive technique for

*This work is supported by The Swedish Research Council (VR) under grants 2017-04053 and 2018-04396, and by the Swedish Foundation for Strategic Research.

[1]Arunava Naha, André Teixeira, and Anders Ahlén are with the Department of Electrical Engineering, Uppsala University, 751 03 Uppsala, Sweden arunava.naha@angstrom.uu.se, andre.teixeira@angstrom.uu.se, and Anders.Ahlen@angstrom.uu.se

[2]Subhrakanti Dey is with the Department of Electronic Engineering, Hamilton Institute, National University of Ireland, Maynooth, Ireland. He is also with the Department of Electrical Engineering, Uppsala University, 751 03 Uppsala, Sweden Subhra.Dey@signal.uu.se

adding watermarking to reduce the control cost during the normal operation of the system. The proposed watermarking scheme is formulated as an optimal stochastic control problem inspired by the method of reducing the sampled data required to detect a change in a process [10]. In [10], a Bayesian sequential detection technique is applied, which is asymptotically optimal under certain conditions [11]. One of the conditions is that the prior distribution of the change point should obey either of the following two conditions, see (1) and (2). In our study, we assume the attack start point Γ to be a random variable (RV) having a geometric distribution with parameter ρ, which is similar to several other literature [10], [12]. A geometric prior distribution of the attack start point meets the condition given in (1).

$$\lim_{k\to\infty} \frac{\log \mathrm{P}\{\Gamma \geq k+1\}}{k} = -c,\ c>0, \tag{1}$$

$$\lim_{k\to\infty} \frac{\log \mathrm{P}\{\Gamma \geq k+1\}}{k} = 0, \tag{2}$$

At every time step k, we need to make two decisions, 1) whether to add the watermarking for the $k{+}1$-th time instant, 2) whether to accept that the attack is present in the system. We have used dynamic programming to find the optimal policy that will minimize the average detection delay (ADD) subject to some constraints on the false alarm rate (FAR) and the average number of times the watermarking (ANW) is added. By solving the optimization problem using dynamic programming, we find two thresholds Th_e and Th_a for the posterior probability of attack p_k. If for the k-th instant, the posterior probability $p_k \geq Th_e$, then the watermarking signal is added to the $k+1$-th instant control input u_{k+1}. On the other hand, if $p_k \geq Th_d$, then it is decided that the attack is present in the system, *i.e.*, $k \geq \Gamma$. We have illustrated the proposed technique by numerical results from the simulation of a single-input-single-output (SISO) system under attack and no-attack conditions.

This paper is organized as follows. Section II provides the system model under normal and attack conditions. Section III explains the problem formulation and the proposed solution in detail. Section IV discusses the numerical results, and Section V concludes the paper.

II. System Model

The system model during normal operations and the model with the data deception attack are discussed in this section.

A. System model during normal operation

A schematic diagram of the NCS, considered in this paper, during the normal operation is shown in Fig. 1. The state

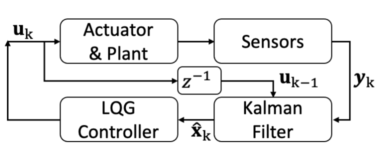


Fig. 1: Schematic diagram of the system during normal operation.

update and the measurement equations of the linear and time-invariant SISO system are given as

$$x_k = Ax_{k-1} + Bu_{k-1} + w_{k-1},\ \text{and} \tag{3}$$

$$y_k = Cx_k + v_k, \tag{4}$$

where x_k and u_k are the state and input variables at the k-th instant. y_k is the observation at the k-th instant. The process noise w_k and the observation noise v_k are assumed to be independent and identically distributed (iid) zero-mean Gaussian processes with variances Q and R respectively. w_k and v_k are uncorrelated with each other, and both are uncorrelated to the initial state x_0. All the quantities in (3) and (4) are real and scalar. We also assume that the system was started a long time ago and currently is at a steady-state. The Kalman filter is used to estimate the state as follows,

$$\hat{x}_{k|k-1} = A\hat{x}_{k-1|k-1} + Bu_{k-1} \tag{5}$$

$$\hat{x}_{k|k} = \hat{x}_{k|k-1} + K\gamma_k, \tag{6}$$

where $\hat{x}_{k|k-1} = E\left[x_k|\xi_{k-1}\right]$ and $\hat{x}_{k|k} = E\left[x_k|\xi_k\right]$ are the Kalman predicted and filtered states respectively. $E[\cdot]$ denotes the expectation operator and ξ_k is the set of all input and output data up to the k-th instant of time. γ_k is the innovation signal given as

$$\gamma_k = y_k - C\hat{x}_{k|k-1}. \tag{7}$$

The steady-state Kalman gain K is as follows,

$$K = CP\left(C^2P + R\right)^{-1}. \tag{8}$$

Here, $P = E\left[\left(x_k - \hat{x}_{k|k-1}\right)^2\right]$, which can be obtained from the solution to the following algebraic Riccati equation,

$$P = A^2P + Q - A^2C^2P^2\left(C^2P + R\right)^{-1}. \tag{9}$$

The optimal control signal u_k^* is derived by minimizing the following infinite horizon LQG cost,

$$J_{lqg} = \lim_{T\to\infty} E\left[\frac{1}{2T+1}\sum_{k=-T}^{T}\left(Wx_k^2 + Uu_k^2\right)\right], \tag{10}$$

where W and U are the two positive weights. The LQG control policy gives a fixed-gain linear control signal as

$$u_k^* = L\hat{x}_{k|k}, \tag{11}$$

$$\text{and } L = -ABS\left(B^2S + U\right)). \tag{12}$$

Here, S is the solution to the following algebraic Riccati equation,

$$S = A^2S + W - A^2B^2S^2\left(B^2S + U\right)^{-1}. \tag{13}$$

B. Attack Model

We assume that the attacker has access to the sensor nodes and can replace the true observations with fake data. We also assume that the attacker has complete knowledge about the system parameters, *i.e.*, A, B, C, Q, and R, and the control policy, *i.e.*, L. However, the attacker can not alter the control signal. The attacker replaces the true observations y_k by the fake data z_k from $k \geq \Gamma$. The fake observation data z_k is assumed to be generated from a general stationary stochastic process as

$$z_k = \alpha z_{k-1} + w_{a,k-1}, \tag{14}$$

where α is the attacker's system parameter and $w_{a,k}$ is the iid noise. $w_{a,k} \sim \mathcal{N}(0, Q_a)$. Such an attack model can also be used for sequential replay attack detections after a few modifications as studied in [13]. The following statistics can be derived from (14).

$$E\left[z_k^2\right] = \sigma_z^2 = \frac{Q_a}{1-\alpha}, \text{ and} \tag{15}$$

$$E\left[z_k z_{k-k_0}\right] = \alpha^{k_0}\sigma_z^2, \ [\alpha < 1]. \tag{16}$$

The attacker's system parameters σ_z^2 and α can be estimated online from the received observations, which will operate in parallel with the attack detection algorithm. During the attack, the Kalman predicted and filtered states are denoted as $\hat{x}^F_{k|k-1}$ and $\hat{x}^F_{k|k}$, respectively, which are derived from (5) and (6), but the innovation signal $\widetilde{\gamma}_k$ during the attack takes the following form,

$$\widetilde{\gamma}_k = z_k - C\hat{x}^F_{k|k-1}. \tag{17}$$

We assume that the defender will know the estimated values of σ_z^2 and α.

A schematic diagram of the system under the data deception attack is shown in Fig. 2.

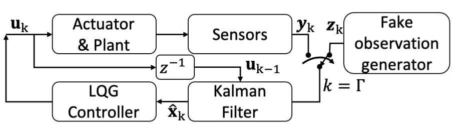


Fig. 2: Schematic diagram of the system under attack.

The attack start point $k = \Gamma$ is assumed to be a RV with a geometric distribution of parameter ρ, where $0 < \rho < 1$. Therefore, the probability $\Pi_k = \mathrm{P}\{\Gamma = k\}$ will be [10]

$$\begin{aligned}\Pi_k = P\{\Gamma = k\} &= \Pi_0 \mathbb{1}_{\{k=0\}} \\ &+ (1-\Pi_0)\,\rho\,(1-\rho)^{k-1}\,\mathbb{1}_{\{k\geq 1\}}.\end{aligned} \tag{18}$$

Here, $\Pi_0 = \mathrm{P}\{\Gamma \leq 0\}$, *i.e.*, Π_0 is the probability of the attack happening before the start of the observation time $k = 0$. $\mathbb{1}_{\{condition\}}$ is the indicator function, $\mathbb{1}_{\{condition\}} = 1$ if the condition is satisfied, otherwise, $\mathbb{1}_{\{condition\}} = 0$. In general, $0 \leq \Pi_0 < 1$. However, for our problem formulation we have taken $\Pi_0 = 0$. The defender does not know the exact value of the attack start point Γ, but he knows about the prior distribution of Γ and the geometric distribution parameter ρ.

III. Defence Mechanism

In this section, we discuss the proposed defence mechanism against the data deception attack by adaptively adding watermarking to the control input.

A. Watermarking the Inputs

For attack detection, we perform hypothesis testing to decide from the following two hypotheses.

H_0: No attack present.

H_1: Attack present in the system.

We add iid zero-mean Gaussian noise watermarking signal e_k with variance σ_e^2 to the optimal LQG control input u_k^* to authenticate the observations. The addition of watermarking increases the attack detectability [2], at the same time, it also increases the control cost. If watermarking is added to the input signal for every k-th instant of time, then the increase in the LQG control cost, ΔLQG, during the normal system operation becomes [4]

$$\Delta LQG = \left(U + B^2\left(W + L^2U\right)\left[1-(A+BL)^2\right]^{-1}\right)\sigma_e^2. \tag{19}$$

ΔLQG is the time average of the increase in the control cost. Since an attack is a rare event, the system is expected to run normally for a long time. Therefore, the increase in the total control cost becomes significant over time. Hence, we propose an adaptive technique for the addition of watermarking to reduce the average number of times we add the watermarking, *i.e.*, ANW, to the control input. The reduction in the watermarking will reduce the control cost compared to the case where watermarking is present all the time. We decide to add the watermarking or to declare an attack is present in the system based on the posterior probability p_k defined as follows,

$$p_k \triangleq \mathrm{P}\{\Gamma \leq k | \mathcal{I}_k\}. \tag{20}$$

$\mathcal{I}_k$ is the set of all available information up to the k-th instant of time. Therefore, we need two decision variables, s_k and d_k as follows,

$$s_k = \begin{cases} 0, & \text{no watermarking for } (k+1)\text{-th time instant} \\ 1, & \text{add watermarking for } (k+1)\text{-th time instant.} \end{cases} \tag{21}$$

$$d_k = \begin{cases} 0, & \text{Hypothesis } H_0 \text{ selected} \\ 1, & \text{Hypothesis } H_1 \text{ selected.} \end{cases} \tag{22}$$

A schematic diagram of the system with the need-based watermarking is shown in Fig. 3. The input signal under the proposed defence mechanism takes the following form,

$$u_k = u_k^* + s_{k-1}e_k. \tag{23}$$

Detection of attacks without the watermarking is a limiting case for the proposed scheme, where $\sigma_e^2 = 0$. However, such a choice will result in a large detection delay.

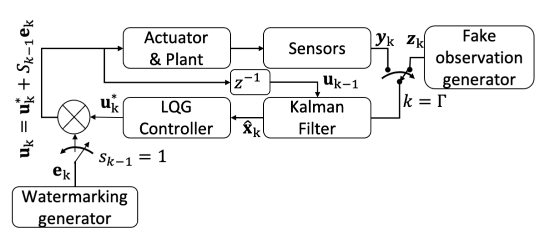


Fig. 3: Schematic diagram of the system with need-based watermarking.

B. Selection of test data

The innovation signals before and after the attack, γ_k and $\widetilde{\gamma}_k$, for the watermarked input, take the following forms [4],

$$\gamma_k = CA\left(x_{k-1} - \hat{x}_{k-1|k-1}\right) + Cw_{k-1} + v_k, \tag{24}$$

$$\widetilde{\gamma}_k = z_k - C\left(A + BL\right)\hat{x}^F_{k-1|k-1} - CBe_{k-1}. \tag{25}$$

Therefore, the innovation signal γ_k before the attack is uncorrelated to the watermarking signal e_{k-1}, and on the contrary, the innovation signal $\widetilde{\gamma}_k$ after the attack is correlated with the watermarking signal e_{k-1}. Such property motivates the use of the innovation signal as the test data for attack detections. If the watermarking is added to the input, then we use the joint distributions of the innovation signal and the watermarking signal, because it increases the Kullback-Leibler divergence (KLD) between the two distributions before and after the attack as discussed by [4]. Distributions of the innovation signals, *i.e.*, γ_k and $\widetilde{\gamma}_k$, and the joint distributions of the innovation and the watermarking before and after the attack are all zero-mean Gaussian distributions. The required variances are given as follows, [4],

$$\mathrm{E}\left[\gamma_k^2\right] = \sigma_\gamma^2 = C^2P + R, \tag{26}$$

$$\mathrm{E}\left[\widetilde{\gamma}_k^2\right] = \sigma_{\widetilde{\gamma}}^2 = \left[\left(1 - \frac{\alpha CK\left(A + BL\right)}{1 - \alpha\mathcal{A}}\right)^2 + \frac{\left(1-\alpha^2\right)C^2K^2\left(A+BL\right)^2}{\left(1-\mathcal{A}^2\right)\left(1-\alpha\mathcal{A}\right)^2}\right]\sigma_z^2 + \frac{B^2C^2}{1-\mathcal{A}^2}\sigma_e^2, \tag{27}$$

$$\mathrm{E}\left[\gamma_{e,k}\gamma_{e,k}^T\right] = \begin{bmatrix}\sigma_\gamma^2 & 0\\ 0 & \sigma_e^2\end{bmatrix}, \tag{28}$$

$$\mathrm{E}\left[\widetilde{\gamma}_{e,k}\widetilde{\gamma}_{e,k}^T\right] = \begin{bmatrix}\sigma_{\widetilde{\gamma}}^2 & -BC\sigma_e^2\\ -BC\sigma_e^2 & \sigma_e^2\end{bmatrix}, \tag{29}$$

where $\mathcal{A} = \left(1 - CK\right)\left(A + BL\right)$, $\gamma_{e,k} = \begin{bmatrix}\gamma_k & e_{k-1}\end{bmatrix}^T$, and $\widetilde{\gamma}_{e,k} = \begin{bmatrix}\widetilde{\gamma}_k & e_{k-1}\end{bmatrix}^T$.

C. Problem Formulation

Our objective is to find the optimal policy for the decision variables, s_k and d_k, so that it minimizes the ADD for the fixed thresholds on FAR and ANW. We define ADD, FAR, and ANW as in [10],

$$ADD = \mathrm{E}_1\left[\tau - \Gamma | \tau \geq \Gamma\right], \tag{30}$$

$$FAR = \mathrm{P}_0\left\{\tau < \Gamma\right\}, \tag{31}$$

$$ANW = \mathrm{E}_0\left[N_e\right]. \tag{32}$$

Here, $\mathrm{E}_0[\cdot]$ and $\mathrm{E}_1[\cdot]$ represent the expectation with respect to the before and after attack distributions P_0 and P_1, respectively. τ is the time when the attack is detected by the algorithm. N_e is the number of times the watermarking is added before the attack start point. After the attack start point, our primary objective is to detect the attack as soon as possible to reduce the amount of damage to the CPS, and we are not concerned about the increase in the control cost. Now, the optimization problem can be formulated as

$$\begin{aligned}&\min_{u_d}\ ADD\\ &\text{s.t. } FAR \leq FAR_{th}\\ &ANW \leq ANW_{th},\end{aligned} \tag{33}$$

where FAR_{th} and ANW_{th} are the thresholds for FAR and ANW respectively. u_d represents the policy for the decision variables s_k and d_k. The control space of the stochastic optimization problem under study is finite, and we have discretized the state-space into a finite set. From the accessibility hypothesis as defined in [14], the constrained optimization problem of (33) can be converted into an unconstrained Lagrangian form as follows [10], [14],

$$J^* = \min_{u_d}\ ADD + \lambda_f FAR + \lambda_e ANW, \tag{34}$$

where $\lambda_f > 0$ and $\lambda_e > 0$ are the Lagrangian multipliers. Now, the system can be in one of the following three stages at any k-th instant of time, see (35).

$$\theta_k = \begin{cases}0 & \text{No attack,}\\ 1 & \text{System under attack,}\\ T_e & \text{Termination stage, attack detected.}\end{cases} \tag{35}$$

ADD, FAR and ANW can be expressed in terms of the state variable θ_k and control variables s_k and d_k as follows [15].

$$ADD = \mathrm{E}\left[\mathbb{1}_{\{\theta_k=1\}}\mathbb{1}_{\{d_k=0\}}\right], \tag{36}$$

$$FAR = \mathrm{E}\left[\mathbb{1}_{\{\theta_k=0\}}\mathbb{1}_{\{d_k=1\}}\right], \text{ and} \tag{37}$$

$$ANW = \mathrm{E}\left[\mathbb{1}_{\{\theta_k=0\}}\mathbb{1}_{\{d_k=0\}}\mathbb{1}_{\{s_k=1\}}\right]. \tag{38}$$

Using (36)-(38) in (34), we can represent the cost function as the following summation.

$$J^* = \min_{u_d}\ \mathrm{E}\left[\sum_{k=0}^{\tau} g_k\left(\theta_k, s_k, d_k\right)\right]. \tag{39}$$

Here $g_k(\cdot)$ is the per stage cost which is given as follows,

$$\begin{aligned}g_k\left(\theta_k, s_k, d_k\right) = \mathbb{1}_{\{\theta_k \neq T_e\}}\big[&\mathbb{1}_{\{\theta_k=1\}}\mathbb{1}_{\{d_k=0\}}\\ &+\lambda_f\mathbb{1}_{\{\theta_k=0\}}\mathbb{1}_{\{d_k=1\}} + \lambda_e\mathbb{1}_{\{\theta_k=0\}}\mathbb{1}_{\{s_k=1\}}\mathbb{1}_{\{d_k=0\}}\big].\end{aligned} \tag{40}$$

The probability p_k from (20) can also be written as

$$p_k = \mathrm{P}\left(\theta_k = 1 | \mathcal{I}_k\right). \tag{41}$$

Therefore, the expected value of the per stage cost function $g_k(\cdot)$ can be expressed using (41) as

$$\begin{aligned}&\mathrm{E}\left[g_k\left(\theta_k, s_k, d_k\right)\right] = g_{E,k}\left(p_k, u_{d,k}\right) = p\mathbb{1}_{\{d_k=0\}} +\\ &\lambda_f\left(1-p\right)\mathbb{1}_{\{d_k=1\}} + \lambda_e\left(1-p\right)\mathbb{1}_{\{s_k=1\}}\mathbb{1}_{\{d_k=0\}}.\end{aligned} \tag{42}$$

D. Finding the optimal policy

The optimization problem of (39) is solved by applying the dynamic programming approach as in [16] using the sufficient statistics p_k. p_k can be updated using the following lemma.

Lemma 1: The posterior probability of the attack p_k follows the following update rule,

$$p_{k+1} = \begin{cases}\frac{T_m\mathrm{L}(\bar{\gamma}_{k+1})}{T_m\mathrm{L}(\bar{\gamma}_{k+1})+1-T_m} & \text{if } s_k = 0\\ \frac{T_m\mathrm{L}(\bar{\gamma}_{k+1}, e_k)}{T_m\mathrm{L}(\bar{\gamma}_{k+1}, e_k)+1-T_m} & \text{if } s_k = 1\end{cases} \tag{43}$$

where $T_m = p_k + (1 - p_k)\,\rho$. $\mathrm{L}(\bar{\gamma}_{k+1})$ and $\mathrm{L}(\bar{\gamma}_{k+1}, e_k)$ are the likelihood ratios as given below,

$$\mathrm{L}(\bar{\gamma}_{k+1}) = \frac{\widetilde{f}(\bar{\gamma}_{k+1})}{f(\bar{\gamma}_{k+1})} \tag{44}$$

$$\mathrm{L}(\bar{\gamma}_{k+1}, e_k) = \frac{\widetilde{f}(\bar{\gamma}_{k+1}, e_k)}{f(\bar{\gamma}_{k+1}, e_k)} \tag{45}$$

where $\bar{\gamma}_k = \gamma_k$ if $k < \Gamma$, and $\bar{\gamma}_k = \widetilde{\gamma}_k$ if $k \geq \Gamma$. $f(\cdot)$ and $\widetilde{f}(\cdot)$ denote the likelihoods before and after the attack respectively.

Proof 1: Using the Baye's rule the recursion of p_k can be proved directly [10].

The value iteration in [16] is used to solve the optimization problem (39)) in the following steps.

Step-1: Discretize $0 \leq p_k \leq 1$ into 50 discrete levels and denote them as i. Therefore, $i \in \{1, 2, \cdots, 50\}$.

Step-2: Simulate the system model as given in Section II with and without the watermarking for several test runs.

1) Attack start point Γ selected from a geometric distribution with parameter ρ.
2) Likelihood ratios are evaluated using the distributions given in (26) to (29).
3) Evaluate and store p_k for all k using (43). We assume $p_0 = 0$.
4) Convert the real valued p_k into the discrete level as defined in Step-1.
5) Two state transition matrices $\mathbf{P}_{ne}$ and $\mathbf{P}_e$ are estimated for the systems without and with the watermarking, respectively. The maximum likelihood estimation technique is used for the 50×50 state transition matrix evaluation.

Step-3: Run the following value iteration, see (46), several times till it converges for each grid point of the search space bounded by $0 \leq \lambda_f \leq 1000$ and $0 \leq \lambda_e \leq 1$.

$$\mathrm{T}^{k+1}\mathbf{J} = \min_{u_{d,k}} \Big[\mathbf{g}(u_{d,k}) + \mathbf{P}_{ne}\left[\mathrm{T}^k\mathbf{J}\right] \mathbb{1}_{\{d_k=0\}} \mathbb{1}_{\{s_k=0\}} + \mathbf{P}_e\left[\mathrm{T}^k\mathbf{J}\right] \mathbb{1}_{\{d_k=0\}} \mathbb{1}_{\{s_k=1\}} \Big] \tag{46}$$

Here, T represents the transformation operator. $\mathbf{J}$ and $\mathbf{g}(u_{d,k})$ are given as

$$\mathbf{J} = \begin{bmatrix} J(1) & \cdots & J(50) \end{bmatrix}^T, \tag{47}$$

$$\mathbf{g}(u_{d,k}) = \begin{bmatrix} g_{E,k}(1, u_{d,k}) & \cdots & g_{E,k}(50, u_{d,k}) \end{bmatrix}^T. \tag{48}$$

$J(i)$ represents the cost function value when the initial state is i. $g_{E,k}(i, u_{d,k})$ is derived from (42) by replacing the discrete state i with a corresponding real value of p_k. The decision variable $u_{d,k}$ has three discrete level to choose from, as given in Table I.

TABLE I: Decision variables

$u_{d,k}$	d_k	s_k
1	0	0
2	0	1
3	1	0

Therefore, after completing the Step-3, we get the optimum policy for each combination of λ_f and λ_e from the search grid. $\mathbf{U}_d$, a $50 \times N_u$ matrix, stores all the optimal policies u_d^*. Therefore, each column of $\mathbf{U}_d$ holds the optimal policy u_d^* for a particular pair of λ_f and λ_e from the search grid of total N_u points.

Step-4: For each combination of λ_f and λ_e from the search grid, we run the model simulation several times. We decide about the addition of the watermarking and the presence of an attack based on the value of p_k and $u_{d,k}^*$ from $\mathbf{U}_d$. We then evaluate the ADD, FAR, and ANW numerically from a large number of trials and select the λ_f and λ_e values matching the requirements.

Remark 1: Depending on the selected parameters, there could also be a three-threshold policy. Two thresholds, say Th_e and Th_{e2}, for the selection of s_k, and one threshold, Th_d, for the selection of d_k. However, for most of the practical cases [10], and also for the test case considered in this paper, $Th_{e2} \geq Th_d$, which makes the third threshold unnecessary.

IV. Numerical Results

We have considered a SISO system for the numerical simulations. The system is open-loop unstable. All the parameters needed for the simulation are as follows, $A = 1.1$, $B = C = R = Q = W = 1$, $U = 0.4$, $\sigma_z^2 = 5$, $\alpha = 0.5$, and $\rho = 0.01$.

Figure 4 shows the optimal decision variable u_d^* with respect to different values of p for three different values of λ_e, while λ_f is kept fixed. We can observe two distinct thresholds, Th_e and Th_d, which decide the addition of the watermarking and the presence of an attack, respectively. With the increase in λ_e, the threshold Th_e also charges to a higher value. Higher Th_e reduces the amount of the watermarking added, but at the same time, it increases the ADD as shown later.

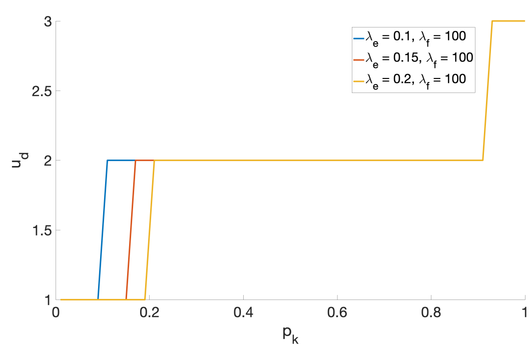


Fig. 4: Optimal policy for different λ_e but fixed λ_f.

Figure 5 shows the optimal decision variable u_d^* with respect to different values of p for three different values of λ_f, while λ_e is kept fixed. Comparing the plots, we can comment that λ_f controls the threshold Th_d, which decides whether the attack is present in the system or not. Higher λ_f increases Th_d, which in turn reduces the FAR, but increases ADD as shown later. It is also observed from Figure 4 and Figure 5 that λ_e does not have effect on Th_d and at the same time λ_f does not effect Th_e.

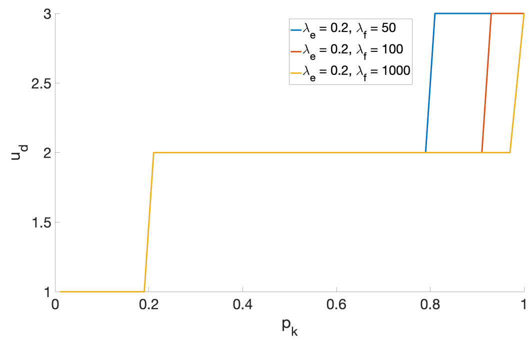
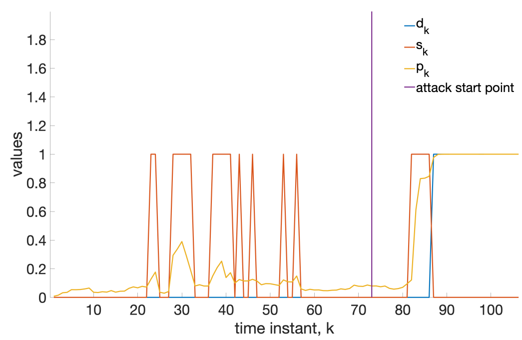
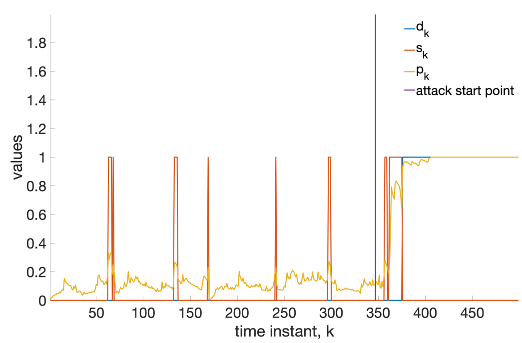


Fig. 5: Optimal policy for different λ_f but fixed λ_e.

Figure 6 shows two trial runs for two different values of λ_e, while λ_f is kept fixed. We have plotted p_k, s_k, d_k, and the actual attack point with respect to the time index k. Figure 7 shows the similar plots for two different values of λ_f, while λ_e is kept fixed. We can observe that the number of times the watermarking has been added before the attack point reduces with the increase in λ_e and Th_e.



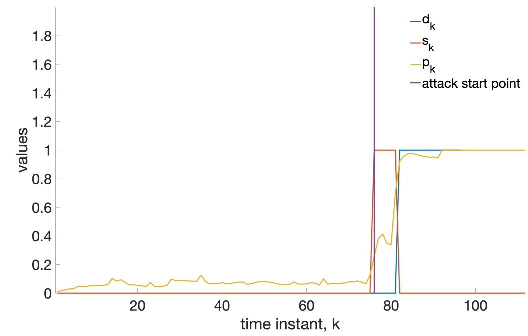
(a)



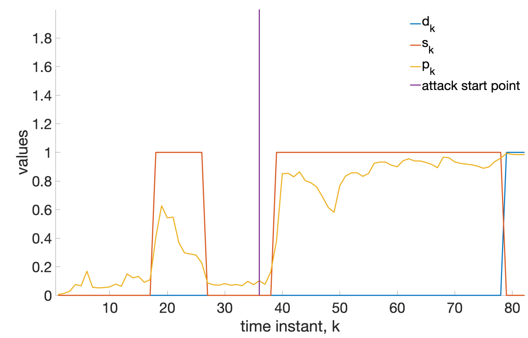
(b)

Fig. 6: p_k, s_k, d_k, and the actual attack point vs k, when a) $\lambda_e = 0.1$ and $\lambda_f = 100$, and b) $\lambda_e = 0.2$ and $\lambda_f = 100$.

Figure 8 plots ADD and FAR vs. σ_e^2 for the proposed method, and ADD and FAR vs. σ_e^2 when the watermarking is added all the time for two different values of λ_e, while λ_f is kept fixed. Figure 9 shows the similar plots for two different values of λ_f, while λ_e is kept fixed. We observe the increase in ADD for the proposed method for the same FAR, but the increase is not much. For the Fig. 8.a the increase is only 12.2% at $\sigma_e^2 = 0.99$. The increase in λ_f and Th_d reduces FAR but it also increases ADD, see Fig. 9.

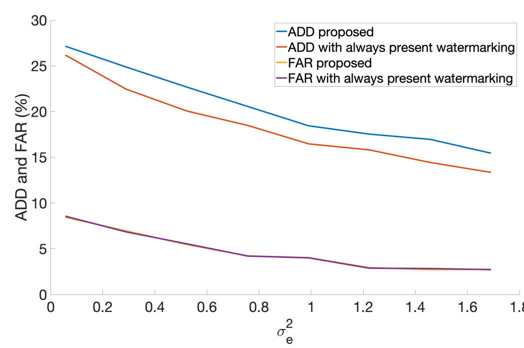


(a)

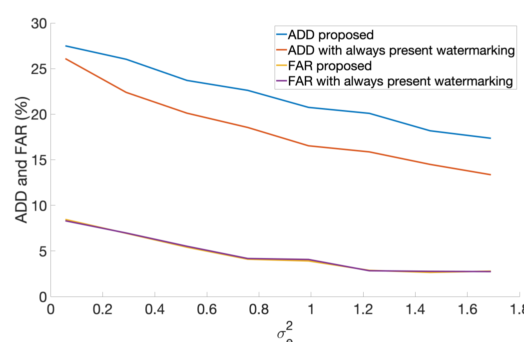


(b)

Fig. 7: p_k, s_k, d_k, and the actual attack point vs k, when a) $\lambda_f = 50$ and $\lambda_e = 0.2$, and b) $\lambda_f = 1000$ and $\lambda_e = 0.2$.



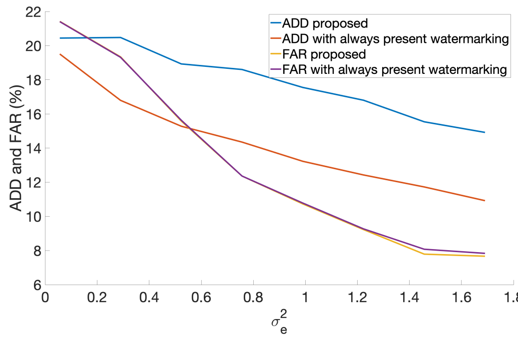
(a)



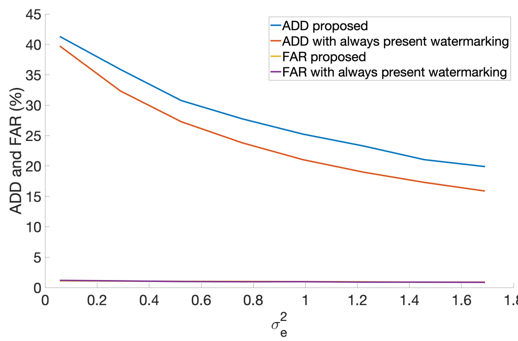
(b)

Fig. 8: ADD and FAR (%) vs σ_e^2, when a) $\lambda_e = 0.1$ and $\lambda_f = 100$, and b) $\lambda_e = 0.2$ and $\lambda_f = 100$.

Figure 10 plots ΔLQG vs. σ_e^2 for the proposed method and ΔLQG vs. σ_e^2 when the watermarking is added all the time for two different values of λ_e, while λ_f is kept fixed. We can certainly observe that we achieve a huge benefit in



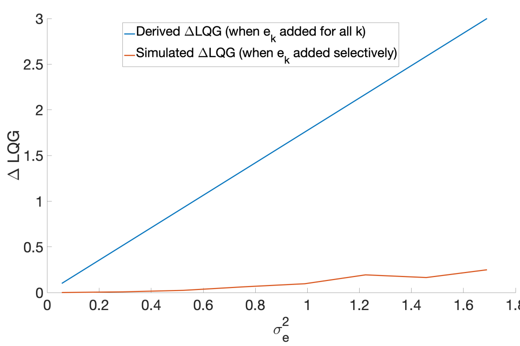
(a)



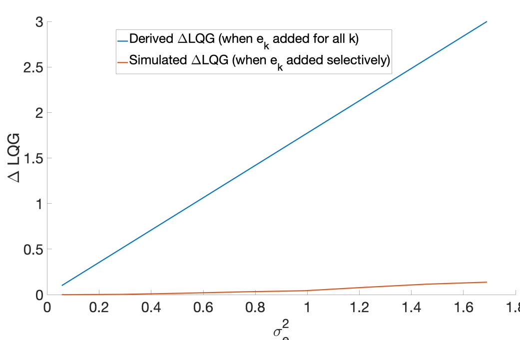
(b)

Fig. 9: ADD and FAR (%) vs σ_e^2, when a) $\lambda_f = 50$ and $\lambda_e = 0.2$, and b) $\lambda_f = 1000$ and $\lambda_e = 0.2$.

terms of the control cost. For the Fig. 10.a the decrease in ΔLQG is 94.5% at $\sigma_e^2 = 0.99$. The increase in λ_e reduces the ΔLQG further but at the cost of increased ADD.



(a)



(b)

Fig. 10: ADD and FAR (%) vs σ_e^2, when a) $\lambda_e = 0.1$ and $\lambda_f = 100$, and b) $\lambda_e = 0.2$ and $\lambda_f = 100$.

V. Conclusion

The proposed method reduces the ΔLQG to a significant amount at the expense of only a small increase in the ADD. We solve the optimization problem of minimizing the ADD for the fixed thresholds on the FAR and ANW using the value iteration. The dynamic programming solution of the optimization problem provides two thresholds on the posterior probability of attack. The numerical results from the simulation of a SISO system illustrate the proposed method in details. We also provide useful insights regarding the choice of the Lagrangian multiplier values. As the future scope, the proposed method can be extended for the more general case of multi-input-multi-output (MIMO) systems. Furthermore, the analytical expressions of the ADD, FAR, and ΔLQG for the two threshold policy can be derived.

References

[1] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, "Cyber-physical systems and their security issues," *Comput. Ind.*, vol. 100, no. July 2017, pp. 212–223, 2018. [Online]. Available: https://doi.org/10.1016/j.compind.2018.04.017

[2] Y. Mo, S. Weerakkody, and B. Sinopoli, "Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs," *IEEE Control Syst.*, vol. 35, no. 1, pp. 93–109, jan 2015.

[3] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Secur. Priv.*, vol. 9, no. 3, pp. 49–51, 2011.

[4] S. Salimi, S. Dey, and A. Ahlen, "Sequential Detection of Deception Attacks in Networked Control Systems with Watermarking," pp. 883–890, 2019.

[5] B. Satchidanandan and P. R. Kumar, "Dynamic Watermarking: Active Defense of Networked Cyber–Physical Systems," *Proc. IEEE*, vol. 105, no. 2, pp. 219–240, feb 2017.

[6] C. Fang, Y. Qi, P. Cheng, and W. X. Zheng, "Optimal periodic watermarking schedule for replay attack detection in cyber–physical systems," *Automatica*, vol. 112, p. 108698, 2020.

[7] C. Trapiello, D. Rotondo, H. Sanchez, and V. Puig, "Detection of replay attacks in CPSs using observer-based signature compensation," *2019 6th Int. Conf. Control. Decis. Inf. Technol. CoDIT 2019*, pp. 1–6, 2019.

[8] R. M. Ferrari and A. M. Teixeira, "Detection and Isolation of Replay Attacks through Sensor Watermarking," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 7363–7368, 2017.

[9] D. Ye, T. Y. Zhang, and G. Guo, "Stochastic coding detection scheme in cyber-physical systems against replay attack," *Inf. Sci. (Ny).*, vol. 481, no. 61773097, pp. 432–444, 2019. [Online]. Available: https://doi.org/10.1016/j.ins.2018.12.091

[10] T. Banerjee and V. V. Veeravalli, "Data-Efficient Quickest Change Detection with On-Off Observation Control," *Seq. Anal.*, vol. 31, no. 1, pp. 40–77, 2012.

[11] A. G. Tartakovsky and V. V. Veeravalli, "General asymptotic Bayesian theory of quickest change detection," *Theory of Probability and its Applications*, vol. 49, no. 3, pp. 458–497, 2005.

[12] K. Premkumar and A. Kumar, "Optimal sleep-wake scheduling for quickest intrusion detection using sensor networks," in *Proc. - IEEE INFOCOM*, no. ii, 2008, pp. 2074–2082.

[13] A. Naha, A. Teixeira, A. Ahlen, and S. Dey, "Sequential detection of replay attacks," *arXiv preprint arXiv:2012.10748*, 2020.

[14] F. J. Beutler and K. W. Ross, "Optimal policies for controlled markov chains with a constraint," *Journal of mathematical analysis and applications*, vol. 112, no. 1, pp. 236–252, 1985.

[15] T. Banerjee and V. V. Veeravalli, "Data-Efficient Minimax Quickest Change Detection in a Decentralized System," *Seq. Anal.*, vol. 34, no. 2, pp. 148–170, 2015.

[16] D. P. Bertsekas, *Dynamic programming and optimal control*. Athena scientific Belmont, MA, 1995, vol. 1, no. 2.