2018 Indian Control Conference (ICC)
January 4-6, 2018. IIT Kanpur, India

Observability-based Secure State Encryption Design For Cyberphysical Systems

Yimeng Dong[1] and Nikhil Chopra[2]

Abstract— **While the area of cryptography has progressed considerably over the last few decades, its applications to networked dynamical systems are only being considered recently. In this paper, we view the encryption problem for cyberphysical systems through the lens of modern control theory. Specifically, an encryption-like algorithm is proposed for a general nonlinear dynamical system by exploiting the observability property of dynamical systems. The proposed encryption design is applied to augment the security of a recently developed signal authentication mechanism in networked multi-agent systems. The effectiveness of proposed method is studied through numerical simulations.**

I. INTRODUCTIONS

Cyber-Physical System(s) (CPS) are engineered systems that tightly integrates computation and communication with monitoring and controlling of entities in the physical world. With the development of real-time computation and communication technology, CPS such as medical devices, networked vehicles, smart buildings, smart grids, etc. are increasingly becoming widespread. A good overview on CPS research can be found in [1].

Due to the open nature of communication networks, CPS are vulnerable to cyber attacks. Recently, the importance of guaranteeing CPS security is being increasingly realized [2]. The failure of CPS can potentially damage the associated physical system. Examples of cyber attacks on CPS include stuxnet malware sabotaging Iran's nuclear infrastructure [3], water SCADA system attack [4], etc. Various cyber attacks include the denial-of-service (DoS) attack [5], the replay attack [6], the data integrity attack [7], and the eavesdropping attack [8]. On the other hand, various defensive strategies have been proposed to address the security issues like quantitative risk management approach, game theoretical methods, control theory, physical authentication by watermarked control input (see [9]).

For a CPS, disclosure of its system state can be catastrophic to the associated physical system or human users. In [10], [11], it was demonstrated that an attacker can design a malignant content modification attack based on knowledge of the system state, leading to overall system instability. In healthcare systems [12], the system state information may contain significant private knowledge of users and the disclosure of system state may violate privacy laws. In the traditional information security field, the standard methodology to handle information disclosure issue is through encryption and authentication. For instance, [13] proposes an architecture called Onion Routing, which can limit the networks vulnerability to traffic analysis. In contrast to information systems, CPS involve the physical systems as well. Hence, it is preferable to utilize physics of these system to develop approaches that can preserve state secrecy.

Assuming that the attacker has knowledge of the system dynamics/output, deducing the system state from the output is related to the system observability problem. Hence, if the system can be rendered unobservable or hard to observe, then the disclosure of system state information can be prevented. In this paper, CPS with nonlinear dynamics are considered, and a nonlinear observability criterion is exploited to preserve secrecy of the system state.

Currently, there are mainly three main criterions to characterize observability of nonlinear systems. The first is the geometric observability rank condition [14], [15], which provides a sufficient condition for determining local observability at a certain point in the state space. The second is the algebraic condition based on the distinguishability of system's initial states. The necessary and sufficient conditions for nonlinear system observability are derived based on the concept of ideals and affine varieties [16], [17]. The third is the numerical method based on the observability grammian. Instead of ascertaining whether the system is observable or not, it characterizes the degree of observability. [18] proposed a measure for nonlinear system observability called unobservability index where it is claimed that a larger unobservability index indicates smaller observability degree. In [19], [20], an optimization problem was formulated to characterize the observability degree, which coincides with the unobservability index in [18]. [21] adopted this approach to find the optimal sensor locations in a data assimilation application.

In this paper, **first**, we consider a CPS with nonlinear dynamics and design a secure state encryption coefficient. By treating the coefficient as an additional state, an augmented state system is obtained whose output is a function of the original system state and encryption coefficient. We then propose to render the augmented state unobservable from the new system output by utilizing a quantitative observability measure, thereby preventing disclosure of system state information to an eavesdropper. Subsequently, various optimization problems are formulated to maximize the unobservability index. **Finally**, we consider a multi-agent system (MAS) example from [11], implement the proposed

*This work was partially supported by the National Science Foundation under grant ECCS1711554 and by Naval Air Warfare Center Aircraft Division - Pax River, MD under contract N00421132M022.

Yimeng Dong and Nikhil Chopra are with the Department of Mechanical Engineering, University of Maryland, College Park, MD, 20740, USA ymdong@umd.edu nchopra@umd.edu

observability-based secure state encryption design method, and verify its efficacy through simulations.

The contributions of this paper are as follows: **(i)** the state encryption design problem for CPS with general nonlinear dynamics is formulated as an observability problem; **(ii)** By treating the dynamics and initial value of the encryption coefficient as optimization parameters, the design problem is achieved by solving various optimization problems that maximize the unobservability index; **(iii)** For an existing encryption coefficient design problem, we implement the proposed design procedure and verify that it can prevent the disclosure of the agent's state information as well as the encryption coefficient.

II. PRELIMINARIES

This section briefly reviews the nonlinear system observability based on [18].

Consider CPS with general nonlinear dynamics as,

$$\dot{x} = f(x), \quad y = h(x), \quad x(0) = x_0 \tag{1}$$

where $x \in \mathbb{R}^n$ is the system state, $y \in \mathbb{R}^p$ is the system output and $x(0) = x_0$ is the initial state.

For system (1), we adopt a definition of observability for (1) from [18]:

***Definition** 1:* Consider system (1), if the mapping from initial state x_0 to output trajectories $y(0,T)$ (mapping from t to $y(t)$ for $t \in (0,T]$) is one to one, then system is observable at x_0 over $[0,T]$. If the mapping is locally one to one, then system is local observable at x_0 over $[0,T]$. If system is locally observable at x_0 for all $T > 0$, then it is short time locally observable at x_0. If system is short time locally observable at every $x_0 \in \mathbb{R}^n$, then system is called short time locally observable.

A well-known observability rank condition to ascertain short time local observability for (1) is discussed in [14], [15], [17]:

***Proposition** 1:* System (1) is short time locally observable if there exists certain $k = 0, 1, 2, \dots$ such that

$$\text{rank}(\frac{\partial \mathcal{O}}{\partial x}(x_0)) = n, \mathcal{O}(x) = [h(x)^T \ L_f h(x)^T \ \cdots \ L_f^k h(x)^T]^T \tag{2}$$

holds for all $x_0 \in \mathbb{R}^n$, where the superscript T denotes the transpose, $L_f h = \frac{\partial h}{\partial x} f$, $L_f^k h = \frac{\partial L_f^{k-1} h}{\partial x} f$ are the Lie derivatives.

Note that the above proposition states a sufficient condition for short time local observability of system (1). However, the rank condition cannot be used to determine the observability for a certain element of the state space as shown in a counterexample [17]. A necessary condition for short time local observability is discussed as Theorem 3.11 in [14] and Corollary 3.35 in [15]:

***Corollary** 1:* The system (1) is short time local observable only if $\text{rank}(\frac{\partial \mathcal{O}}{\partial x}(x_0)) = n$, where x_0 in an open and dense subset of $\mathbb{R}^n$.

III. PROBLEM FORMULATION

Consider again the CPS in (1). With knowledge of system output and system dynamics, it is possible for a malicious entity (attacker) to deduce the system state and launch associated attacks. To prevent disclosure of state information, the notion of observability is utilized to encrypt the system state by generating a new output which is a function of the original state x and a time-varying encryption coefficient λ. The main objective is to preserve secrecy of the new augmented state consisting of both x and λ.

Specifically, we design an encryption coefficient $\lambda \in \mathbb{R}^m$ with dynamics

$$\dot{\lambda} = g(\lambda), \quad \lambda(0) = \lambda_0 \tag{3}$$

where g and λ_0 are the dynamics and the initial value of λ to be designed, respectively.

Combining (1) and (3), define an augmented state $z = [x^T, \lambda^T]^T$ with dynamics

$$\dot{z} = F(z), \quad r = E(x, \lambda), \quad z(0) = z_0 = [x_0^T \ \lambda_0^T]^T \tag{4}$$

where E is the encryption function and $r \in \mathbb{R}^e$ is augmented system output. The original system state x can be decrypted as

$$x = D(r, \lambda) = D(E(x, \lambda), \lambda) \tag{5}$$

where E and D are pre-defined encryption-decryption function pair.

Assume that the attacker has the knowledge of dynamics F and output r of (4). If the system (4) is observable, it is then possible for the attacker to estimate the state z. From the notion of observability discussed in the previous section, it can be see that observability of (1) depends on the initial condition of the system. Additionally, note that x_0 cannot be selected, but λ_0 can be designed. To prevent disclosure of state information, the objective of this work is to design the dynamics g and λ_0 in (3) to render the augmented system (4) unobservable from output r.

IV. MOTIVATING EXAMPLE

[11] discussed a doubled integrator consensus seeking multi agent system (MAS) under a content modification attack. The attacker was able to arbitrarily modify the packet content transmitted between different agents.

In Section III B of [11], the doubled integrator MAS is modeled by undirected graph $\mathcal{G}$, where the dynamics of each agent is given by

$$\begin{bmatrix} \dot{q}_i \\ \ddot{q}_i \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} q_i \\ \dot{q}_i \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} u_i \tag{6}$$

With consensus input u_i given in (3) of [11], the dynamics of MAS can be written in a compact form as,

$$\dot{x} = \begin{bmatrix} \dot{q} \\ \ddot{q} \end{bmatrix} = \begin{bmatrix} \mathbf{0}_N & I_N \\ -L & -\beta L \end{bmatrix} x \tag{7}$$

where $q = [q_1, q_2, \dots, q_N]^T \in \mathbb{R}^N$ is the generalized coordinate vector for all N agent, L is the Laplacian matrix

for graph $\mathcal{G}$, $\beta > 0$ is a constant gain, and I_n, $\mathbf{0}_n$ denote the n by n identity matrix and n by n zero matrix respectively.

A state encryption based attack detection scheme is proposed in Section IV D of [11]. The scheme is based on the physical relationship between constituents of the transmitted data (see Section IV C of [11]), which in this case means for each node j that the received velocities $\dot{q}_i$ and positions q_i should be 'coherent' at all times. Suppose the attacker modifies $(q_i, \dot{q}_i)$ to $(\tilde{q}_i, \dot{\tilde{q}}_i)$, then the data was only accepted when the following detection condition was satisfied:

$$\dot{\tilde{q}}_i(t) = \dot{\tilde{q}}_i(t), \quad \forall t \geq 0. \tag{8}$$

The implementation details of the proposed encryption based attack detection scheme are summarized below.

For each agent i, the encrypted data packet (r_{i1}, r_{i2}) is transmitted instead of $(\dot{q}_i, q_i)$, where (r_{i1}, r_{i2}) are computed as

$$r_{i1} = \dot{q}_i + \lambda_1 q_i, \quad r_{i2} = \dot{q}_i + \lambda_2 q_i \tag{9}$$

with $\lambda = [\lambda_1 \ \lambda_2] \in \mathbb{R}^2$ is the encryption coefficient, and

$$\dot{\lambda} = g(\lambda) = \begin{bmatrix} g_1(\lambda) \\ g_2(\lambda) \end{bmatrix}, \quad \lambda(0) = \lambda_0 \tag{10}$$

where the function g is known to all agents and designed such that $\lambda_1 \neq \lambda_2, \forall t \geq 0$. The initial condition $\lambda_0 = [\lambda_1(0), \lambda_2(0)]$ is shared securely between the agents when consensus starts, thus the attacker cannot computed λ_1, λ_2 during consensus without the knowledge of the initial condition λ_0.

At the receiving end, $\dot{q}_i, q_i$ are obtained by decrypting (r_{i1}, r_{i2}) for receiving agent j as

$$q_i = a(r_{i1} - r_{i2}), \quad \dot{q}_i = br_{i1} - cr_{i2}, \tag{11}$$

where $a = 1/(\lambda_1 - \lambda_2), b = \lambda_2/(\lambda_2 - \lambda_1), c = \lambda_1/(\lambda_2 - \lambda_1)$.

Then the detection condition (8) is checked after the decryption. If the detection condition is not violated, then the signals $\dot{q}_i, q_i$ are used in the local controller receiving agent j. Otherwise, an attack is detected. It was demonstrated in Theorem 3 of [11] that if λ_1 and λ_2 are unknown to the attacker during the operation, then the content modification attack will be detected by (8).

Similar to (4), define an augmented state $z = [x^T, \lambda^T]^T \in \mathbb{R}^{2N+2}$ with dynamics

$$\begin{cases} \dot{x} = \begin{bmatrix} \dot{q} \\ \ddot{q} \end{bmatrix} = \begin{bmatrix} \mathbf{0}_N & I_N \\ -L & -\beta L \end{bmatrix} x \\ \dot{\lambda} = g(\lambda) \end{cases}, \ r = \begin{bmatrix} \dot{q} + \lambda_1 q \\ \dot{q} + \lambda_2 q \end{bmatrix} \tag{12}$$

Note that the output r is a nonlinear function of state z.

If we consider a more intelligent attacker that seeks to derive z from available observations r, then the attack detection algorithm proposed in [11] may fail. Thus, the following design problem is proposed to strengthen the attack detection scheme: design the function g and λ_0 in (12) such that z cannot be derived from observations r. To rephrase this as observability problem, the problem is how to design g and λ_0 in (12) such that the system state z is rendered unobservable based on available observations r.

V. ENCRYPTION DESIGN USING OBSERVABILITY RANK CONDITION

Corollary 1 implies that if the system (4) fails to satisfy the observability rank condition on an open dense subset of $\mathbb{R}^{n+m}$, then it is not short time locally observable. Intuitively, this result provides a handy solution to address the problem outlined in Section III. In other words, for system (4), one would like to design dynamics g and λ_0 such that the observability rank condition is not satisfied in an open dense subset of $\mathbb{R}^{n+m}$.

Now consider the MAS example given in previous section with only two connected agents, i.e., $x = [q_1 \ q_2 \ \dot{q}_1 \ \dot{q}_2]^T \in \mathbb{R}^4$ in (12). Then from (4) and (12), the system dynamics can be written as

$$\dot{z} = F(z) = \begin{bmatrix} q_1 \\ q_2 \\ -q_1 + q_2 - \beta\dot{q}_1 + \beta\dot{q}_2 \\ q_1 - q_2 + \beta\dot{q}_1 - \beta\dot{q}_2 \\ g_1(\lambda) \\ g_2(\lambda) \end{bmatrix}, r = E(z) = \begin{bmatrix} \dot{q}_1 + \lambda_1 q_1 \\ \dot{q}_2 + \lambda_1 q_2 \\ \dot{q}_1 + \lambda_2 q_1 \\ \dot{q}_2 + \lambda_2 q_2 \end{bmatrix} \tag{13}$$

Now according to Proposition 1, $\frac{\partial \mathcal{O}}{\partial z}$ can be computed as

$$\frac{\partial \mathcal{O}}{\partial z} = \begin{bmatrix} \frac{\partial E}{\partial z} \\ \frac{\partial L_F E}{\partial z} \\ \vdots \end{bmatrix} =$$

$$\begin{bmatrix} \lambda_1 & 0 & 1 & 0 & q_1 & 0 \\ 0 & \lambda_1 & 0 & 1 & q_2 & 0 \\ \lambda_2 & 0 & 1 & 0 & 0 & q_1 \\ 0 & \lambda_2 & 0 & 1 & 0 & q_2 \\ g_1 - 1 & 1 & \lambda_1 - \beta & \beta & \dot{q}_1 + \frac{\partial g_1}{\partial \lambda_1} q_1 & \frac{\partial g_1}{\partial \lambda_2} q_1 \\ 1 & g_1 - 1 & \beta & \lambda_1 - \beta & \dot{q}_2 + \frac{\partial g_1}{\partial \lambda_1} q_2 & \frac{\partial g_1}{\partial \lambda_2} q_2 \\ g_2 - 1 & 1 & \lambda_2 - \beta & \beta & \frac{\partial g_2}{\partial \lambda_1} q_1 & \dot{q}_1 + \frac{\partial g_2}{\partial \lambda_2} q_1 \\ 1 & g_2 - 1 & \beta & \lambda_2 - \beta & \frac{\partial g_2}{\partial \lambda_1} q_2 & \dot{q}_2 + \frac{\partial g_2}{\partial \lambda_2} q_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{bmatrix} \tag{14}$$

Note that for system (13) with (14), a methodology for obtaining g and λ_0 such that rank$(\frac{\partial \mathcal{O}}{\partial z}(z_0)) < 6$ for z_0 in an open dense subset of $\mathbb{R}^6$ is not evident. It is even difficult to show the existence of g and λ_0 to render rank deficiency. Additionally, when the system dimension scales up, then computing (14) and estimating the rank can be difficult. So through this example it is noted that the observability rank condition cannot provide a direct solution for designing g and λ_0 for (4).

The observability rank condition provides a boolean answer on system observability, but it does not characterize the difficulty of observing a system. Instead of using the rank condition, the works [18]–[21] are appealing wherein a quantitative measure of system observability degree is discussed. Following this idea, in next section, design of the dynamics g and λ_0 for (4) is studied such that the observability degree of (4) is minimized.

VI. ENCRYPTION DESIGN USING QUANTITATIVE MEASURE OF OBSERVABILITY

In this section, state encryption design is studied using a quantitative measure of observability called unobservability

index, which is the reciprocal of the smallest eigenvalue of the empirical observability grammian. Recall that the larger unobservability index indicates smaller observability degree. Hence, the dynamics g and λ_0 for (4) are desgined to maximize the unobservability index or minimize the smallest eigenvalue of the empirical observability grammian.

A. Algorithm Description

From [18], the empirical observability grammian for system (4) at z_0 is a $(n+m)\times(n+m)$ matrix $P(z_0)$ with the (i,j) component as

$$[P(z_0)]_{i,j} = \frac{1}{4\rho^2}\int_0^T (r^{+i}(t) - r^{-i}(t))^T (r^{+j}(t) - r^{-j}(t))dt \tag{15}$$

where $\rho > 0$ is small displacement from system state, $r^{\pm i}$ denotes the output of system trajectory starting from $z_0 \pm \rho e^i$, and e^i is the ith unit vector of $\mathbb{R}^{n+m}$.

Consider the dynamics (3) for λ. To facilitate solving the problem, assume g is a known parameterized function of a constant parameter a (to be designed), that is,

$$\dot{\lambda} = g(\lambda, a) \tag{16}$$

First, treat only a as a design parameter and fix λ_0. Then for a given initial condition $z_0 = [x_0^T \ \lambda_0^T]^T$, the empirical observability grammian is a function of a and the unobservability index is given by $1/\sigma_{min}(P(a))$, where σ_{min} denotes the smallest eigenvalue.

Next, an optimization problem is formulated to obtain the parameter a:

Optimization Problem 1:

$$\begin{aligned} &\underset{a}{\text{minimize}} \quad J_a = \sigma_{min}(P(a)) \\ &\text{subject to:} \quad a_{lower} \le a \le a_{upper} \end{aligned} \tag{17}$$

where a_{lower} and a_{upper} are the lower and upper bounds of the optimization variable, which characterize the search region.

As discussed in Section 2.2 of [21], the L-BFGS-B (limited memory Broyden-Fletcher-Goldfrab-Shanno for bound constraints) [22] algorithm can be well applied for this type of eigenvalue optimization problem. L-BFGS-B is a limited-memory quasi-Newton method for bound-constrained optimization problem. Note that L-BFGS-B can only provide a local optimal solution, hence it is judicious to randomly select multiple initial guesses for a to find a reasobale initial guess. To implement L-BFGS-B, cost function J_a and its gradient ∇J_a are required. As shown in [21], ∇J_a can be computed as:

$$\nabla J_a = v^T(\nabla P(a))v \tag{18}$$

where v is the eigenvector associated with $\sigma_{min}(P(a))$ and $v^T v = 1$ and $\nabla P(a)$ can be approximated by a central finite difference scheme.

It is worth noting that the empirical observability grammian (15) is actually also a function of the initial state $z_0 = [x_0^T \ \lambda_0^T]^T$. In optimization problem 1, z_0 is randomly pre-selected. It is evident that the selection z_0 will affect the optimal value of (17). Thus, if we consider a and x_0 as fixed and pre-selected, but treat λ_0 as an optimization parameter, then another optimization problem can be formulated as:

Optimization Problem 2:

$$\begin{aligned} &\underset{\lambda_0}{\text{minimize}} \quad J_{\lambda_0} = \sigma_{min}(P(\lambda_0)) \\ &\text{subject to:} \quad \lambda_{lower} \le \lambda_0 \le \lambda_{upper} \end{aligned} \tag{19}$$

If we combine optimization problem 1 and 2 and treat both a and λ_0 as optimization parameters, then the following optimization problem is obtained:

Optimization Problem 3:

$$\begin{aligned} &\underset{a,\lambda_0}{\text{minimize}} \quad J_{a,\lambda_0} = \sigma_{min}(P(a,\lambda_0)) \\ &\text{subject to:} \quad a_{lower} \le a \le a_{upper}, \quad \lambda_{lower} \le \lambda_0 \le \lambda_{upper} \end{aligned} \tag{20}$$

With more freedom in the optimization variables, (20) may achieve a better result than (17) and (19), which is verified later in the simulation section.

B. Application on MAS Example

In this section, the proposed design method in Section VI-A is utilized for a MAS consensus example with six nodes (see Fig. 1) from [11].

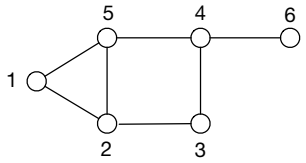


Fig. 1. Second order MAS with six nodes.

Assume λ dynamics as (16) is in a specific form of

$$\dot{\lambda} = G(a)\lambda = \begin{bmatrix} 0 & a_1 \\ -a_1 & a_2 \end{bmatrix}\lambda, \quad \lambda(0) = \lambda_0 \tag{21}$$

where $G(a)$ is 2×2 matrix and $a = [a_1 \ a_2]$ and λ_0 are the design parameters. Then the dynamics of the augmented state $z = [x^T \ \lambda^T]^T \in \mathbb{R}^{14}$ are given as

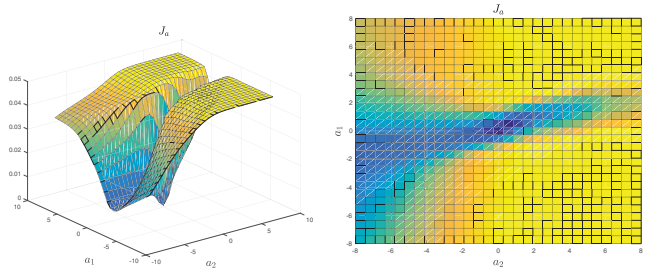
$$\begin{cases} \dot{x} = \begin{bmatrix} \dot{q} \\ \ddot{q} \end{bmatrix} = \begin{bmatrix} \mathbf{0}_6 & I_6 \\ -L & -\beta L \end{bmatrix} x \\ \dot{\lambda} = G(a)\lambda \end{cases}, r = \begin{bmatrix} \dot{q} + \lambda_1 q \\ \dot{q} + \lambda_2 q \end{bmatrix} \tag{22}$$

where L is the Laplacian matrix of graph in Fig. 1.

1) Solving Optimization Problem 1: First, λ_0 is preselected and the optimization problem 1 in (17) is solved using Matlab. Note that the original L-BFGS-B is written in Fortran, [23] converts the code from Fortran to C with a Matlab wrapper. The simulation parameters are set as $a_{lower} = [-8 \ -8]$ and $a_{upper} = [8 \ 8]$, initial condition z_0 is randomly chosen from $[-1, \ 1]$, $T = 2s$, $\beta = 8$, initial guess for a is $[-2 \ 2]$. The optimal variable is found as

$a^* = [0.0262\ 0.0177]$ and the local optimal value is obtained as $J_a^* = \sigma_{min}(P(a^*)) = 6.2673 \times 10^{-5}$ after 8 iterations.

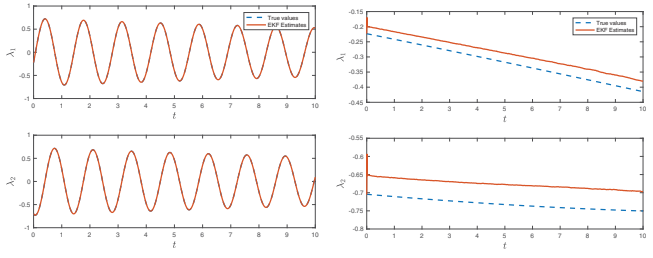
In order to verify the quality of the above optimization process, a search with various combinations of $[a_1\ \ a_2]$ is accomplished to compute the corresponding $J_a = \sigma_{min}(P(a))$.



(a) (b)

Fig. 2. Cost function $J_a = \sigma_{min}(P(a))$ with respect to a_1 and a_2. (a) 3D view (b) Top view

As shown in Fig. 2, the optimal value $J_a^s = 8.0337 \times 10^{-4}$ is achieved at $a^s = [0.2759\ 0.2759]$. To demonstrate the effectiveness of the obtained parameter a^* compared with other parameters a in the search region, an extended Kalman filter (EKF) is used to estimate the state of system (22). First, we choose $a = [-4.6\ -0.276]$, which is in the yellow region of Fig. 2. As seen in Fig. 3 (a), λ can be accurately estimated with this choice of the parameter vector a. Then, with the optimal choice $a = a^* = [0.0262\ 0.0177]$, as seen in Fig. 3 (b), the estimation error for λ does not converge. This comparison demonstrates that the obtained parameter a^* can indeed reduce the system observability, thereby deteriorating the EKF performance.

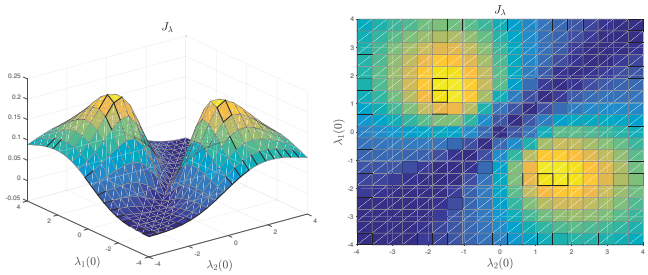


(a) (b)

Fig. 3. The estimate of λ from EKF with different parameter a: (a) $a = [-4.6\ \ -0.27]$ (b) $a = a^* = [0.0262\ 0.0177]$

2) Solving Optimization Problem 2: Now fix $a = [0\ 0]$ and take λ_0 as the optimization parameter as shown in (19). In this case, with $a = [0\ 0]$, encryption parameter λ is a constant. The simulation parameters are set as $\lambda_{lower} = [-4\ -4]$ and $\lambda_{upper} = [4\ 4]$, initial condition x_0 is randomly chosen from interval $[-1,\ 1]$, $T = 2s$ and $\beta = 1$. The optimization problem 2 stops after 5 iterations, the local optimal solution is $\lambda_0^* = [3.8507,\ 3.6214]$ and $J_{\lambda_0}^* = \sigma_{min}(P(\lambda_0^*)) = 4.0291 \times 10^{-5}$.

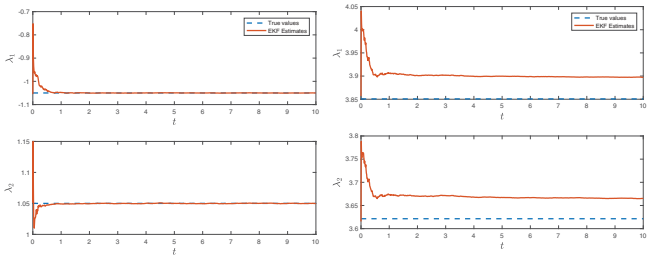
A simulation was also initiated to traverse through all the possible combinations of $\lambda_0 = [\lambda_1(0),\ \lambda_2(0)]$ within the search region. The plot of J_{λ_0} with respect to $\lambda_1(0),\ \lambda_2(0)$ is shown in Fig. 4. It can be noted that the obtained suboptimal solution $\lambda_0^* = [3.8507,\ 3.6214]$ is in the deep blue region.



(a) (b)

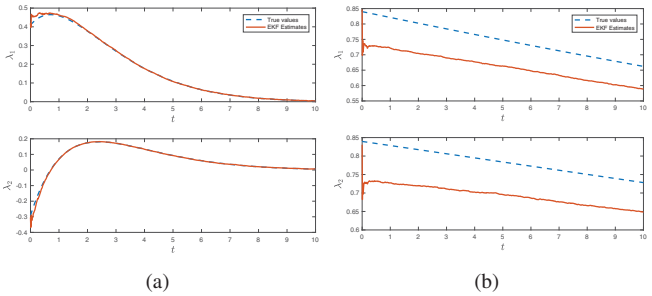
Fig. 4. Cost function $J_{\lambda_0} = \sigma_{min}(P(\lambda_0))$ with respect to $\lambda_1(0)$ and $\lambda_2(0)$: (a) 3D view (b) Top view

As before, the EKF is utilized with different values of λ_0. First, we choose $\lambda_0 = [-1.05,\ 1.05]$ in the yellow region of Fig. 4. As seen in Fig. 5 (a), λ is accurately estimated. Then, we choose $\lambda_0 = \lambda_0^* = [3.8507,\ 3.6214]$. The estimated λ is shown in Fig. 5 (b), wherein the estimation error for λ does not converge. From this comparison, it can be concluded that even a constant λ can reduce the observability of (22) by appropriately selection of λ_0.



(a) (b)

Fig. 5. The estimate of λ from EKF with different λ_0: (a) $\lambda_0 = [-1.05,\ 1.05]$ (b) $\lambda_0 = \lambda_0^* = [3.8507,\ 3.6214]$



(a) (b)

Fig. 6. The estimate of λ from EKF using different optimization problem with same x_0: (a) Optimization problem 1 (b) Optimization problem 3

3) Solving Optimization Problem 3: Since the optimal value of optimization problem 1 depends on the selection of initial state z_0, for certain z_0 the optimal value (smallest eigenvalue of empirical observability grammian) of optimiza-

tion problem 1 may not be close enough to zero, and thus system state can still be estimated by an EKF from attacker.

For instance, with one randomly generated $z_0 = [x_0^T \ \lambda_0^T]^T$, the optimization problem 1 is solved with simulation parameters as $a_{lower} = [-8 \ \ -8]$ and $a_{upper} = [8 \ 8]$, $T = 2s$ and $\beta = 8$. The local optimal solution is $a^* = [-0.6019 \ \ -1.1149]$ and the local optimal value $J_a^* = \sigma_{min}(P(a^*)) = 0.0095$. Compare this local optimal value with the one obtained earlier for optimization problem 1, note that J_a^* is much larger. Running the EKF again, it can be seen in Fig. 6 (a) that the estimated λ does converge to the true state.

Instead, now we fix the x_0 and treat λ_0 as an additional optimization parameter as considered in optimization problem 3 (20). Now we set parameter as $\lambda_{lower} = [-1 \ -1]$ and $\lambda_{upper} = [1 \ 1]$, $T = 2s$ and $\beta = 8$. Solving the optimization problem 3, the suboptimal solution $a^* = [-0.0227 \ \ -0.0359]$, $\lambda_0^* = [0.8401, \ 0.8395]$ and the suboptimal value $J_{a,\lambda_0}^* = \sigma_{min}(P(a^*, \lambda_0^*)) = 8.9161 \times 10^{-6}$. Now λ is estimated by the EKF is shown in Fig. 6 (b), wherein the estimation error for λ does not converge. This comparison verifies that optimization problem 3 can achieve a smaller optimal value than optimization problem 1, for the same x_0, by taking λ_0 as an additional optimization parameter.

4) Discussions: Through the simulation examples above, it can be seen that observability of system (4) can be minimized by designing dynamics g and the initial condition λ_0 of encryption coefficient λ. Specifically, for MAS with augmented dynamics (12), we can design g and λ_0 by solving various optimization problems such that the system state information is not disclosed, thereby leading to success of the detection algorithm in Section IV. Interestingly, by solving optimization problem 2, we find that even with constant λ that the system observability can be adjusted by appropriately choosing the value of λ. This provides an easy solution for the design problem stated in Section IV.

VII. CONCLUSIONS

In this paper, an observability-based secure state encryption design is proposed for cyber-physical systems with nonlinear dynamics. After determining the dynamics and initial condition of the encryption coefficient as design parameters, an optimization approach is adopted to minimize the smallest eigenvalue of the empirical observability grammian. For an existing state encryption design problem for multi-agent systems, we demonstrate that when using the proposed design, it is challenging for the attacker to estimate the system state and encryption coefficient by an extended Kalman filter.

REFERENCES

[1] K.-D. Kim and P. R. Kumar, "Cyber–physical systems: A perspective at the centennial," *Proceedings of the IEEE*, vol. 100, no. Special Centennial Issue, pp. 1287–1308, 2012.

[2] S. Amin, G. A. Schwartz, and A. Hussain, "In quest of benchmarking security risks to cyber-physical systems," *IEEE Network*, vol. 27, no. 1, pp. 19–24, 2013.

[3] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," *White paper, Symantec Corp., Security Response*, vol. 5, 2011.

[4] S. Amin, X. Litrico, S. Sastry, and A. M. Bayen, "Cyber security of water scada systemspart i: analysis and experimentation of stealthy deception attacks," *Control Systems Technology, IEEE Transactions on*, vol. 21, no. 5, pp. 1963–1970, 2013.

[5] H. S. Foroush and S. Martínez, "On event-triggered control of linear systems under periodic denial-of-service jamming attacks." in *CDC*, 2012, pp. 2551–2556.

[6] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on*. IEEE, 2009, pp. 911–918.

[7] ——, "Integrity attacks on cyber-physical systems," in *Proceedings of the 1st international conference on High Confidence Networked Systems*. ACM, 2012, pp. 47–54.

[8] A. Tsiamis, K. Gatsis, and G. J. Pappas, "State estimation with secrecy against eavesdroppers," *arXiv preprint arXiv:1612.04942*, 2016.

[9] H. Sandberg, S. Amin, and K. H. Johansson, "Cyberphysical security in networked control systems: An introduction to the issue," *IEEE Control Systems*, vol. 35, no. 1, pp. 20–23, 2015.

[10] Y. Dong, N. Gupta, and N. Chopra, "On content modification attacks in bilateral teleoperation systems," in *American Control Conference (ACC), 2016*. IEEE, 2016, pp. 316–321.

[11] ——, "Content modification attacks on consensus seeking multi-agent system with double-integrator dynamics," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 26, no. 11, p. 116305, 2016.

[12] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *Journal of medical systems*, vol. 36, no. 1, pp. 93–101, 2012.

[13] D. Goldschlag, M. Reed, and P. Syverson, "Hiding routing information," in *Information Hiding*. Springer, 1996, pp. 137–150.

[14] R. Hermann and A. Krener, "Nonlinear controllability and observability," *IEEE Transactions on automatic control*, vol. 22, no. 5, pp. 728–740, 1977.

[15] H. Nijmeijer and A. Van der Schaft, *Nonlinear dynamical control systems*. Springer, 1990, vol. 175.

[16] B. Tibken, "Observability of nonlinear systems-an algebraic approach," in *Decision and Control, 2004. CDC. 43rd IEEE Conference on*, vol. 5. IEEE, 2004, pp. 4824–4825.

[17] Y. Kawano and T. Ohtsuka, "Observability conditions by polynomial ideals," *Asian Journal of Control*, 2016.

[18] A. J. Krener and K. Ide, "Measures of unobservability," in *Decision and Control, 2009 held jointly with the 2009 28th Chinese Control Conference. CDC/CCC 2009. Proceedings of the 48th IEEE Conference on*. IEEE, 2009, pp. 6401–6406.

[19] W. Kang and L. Xu, "A quantitative measure of observability and controllability," in *Decision and Control, 2009 held jointly with the 2009 28th Chinese Control Conference. CDC/CCC 2009. Proceedings of the 48th IEEE Conference on*. IEEE, 2009, pp. 6413–6418.

[20] ——, "Computational analysis of control systems using dynamic optimization," *arXiv preprint arXiv:0906.0215*, 2009.

[21] S. King, W. Kang, and L. Xu, "Observability for optimal sensor locations in data assimilation," *International Journal of Dynamics and Control*, vol. 3, no. 4, pp. 416–424, 2015.

[22] C. Zhu, R. H. Byrd, P. Lu, and J. Nocedal, "Algorithm 778: L-bfgs-b: Fortran subroutines for large-scale bound-constrained optimization," *ACM Transactions on Mathematical Software (TOMS)*, vol. 23, no. 4, pp. 550–560, 1997.

[23] "https://github.com/stephenbeckr/l-bfgs-b-c."