2018 56th Annual Allerton Conference on Communication, Control, and Computing (Allerton)
Allerton Park and Retreat Center
Monticello, IL, USA, October 2-5, 2018

Model-Based Encryption: Privacy of States in Networked Control Systems

Nirupam Gupta and Nikhil Chopra

Abstract— **In this paper, we investigate model-based encryption scheme for privacy of states against eavesdroppers with unbounded computation power in one-channel feedback networked control system (NCSs). In the one-channel feedback NCS, the states of the plant are measured by remote sensors and the controller is co-located with the actuators. To emphasize the mechanics of the proposed approach, the model-based encryption scheme is referred to as masking with system kernel (MSK). In contrast to encryption approaches based on modern cryptography, MSK does not require generation and distribution of secret keys amongst sensors and the controller. It is demonstrated that MSK guarantees privacy of states against eavesdroppers with unbounded computation power if the system parameters of the considered one-channel feedback NCS are selected in an appropriate manner.**

Index Terms— **privacy of states in NCS; masking with system kernel**

I. Introduction

Near ubiquitous network accessibility has made it easier than ever before to employ remote sensing for network control of dynamical systems. These systems with remote sensing are commonly referred to as one-channel feedback networked control systems (NCSs) [1], [2]. Essentially, in a one-channel feedbacks NCSs the states of the plant are monitored or measured by sensors that are not co-located with the controller. The sensors transmit these state measurements to the controller over a network. The sensed measurements are transmitted to the controller over a network, wherein a controller/actuator pair collocated with plant drives the states of the plant. Common examples of these systems include remote control of mobile vehicles [3], [4] and supervisory control and data acquisition (SCADA) for smart homes or power grids [5], [6].

As the state of the plant in one-channel feedback NCSs is transmitted over a communication network, the privacy of the system state against eavesdroppers becomes a critical issue [13], [14]. The privacy issue is especially important in NCSs that are being used for public utility services like the smart power grids [15]. An obvious solution for preserving the privacy of states is encryption. The sensors can encrypt their state measurements using any of the existing symmetric or asymmetric encryption schemes[1] in cryptography [17]. However, in a typical cryptographic encryption the controller needs to decrypt the received encrypted state measurements in order to compute the control inputs. For this reason, the existing encryption techniques are always supported by equally sophisticated key management protocols [18] that manage generation and distribution of secret keys between the two communicating parties across the network. However, a key management protocol adds significant overhead to both computation and communication costs of any cryptographic encryption scheme.

In this paper, we investigate a model-based encryption scheme for encrypting the state measurements that does not require generation or distribution of secret keys between the sensors and the controller. The proposed encryption scheme exploits the nullity in the control parameters of the NCS to encrypt the state measurements. As the control parameters are a subset of the system parameters, the encryption scheme is referred to as masking with system kernel (MSK). Unlike a typical cryptographic encryption scheme, in MSK the controller can directly utilize the encrypted measurements (without any decryption) to compute the control inputs without affecting the states of the plant. It is rigorously shown that MSK is capable of preserving privacy of states against eavesdroppers with unbounded computation power.

As an alternative to encryption, researchers in control systems have proposed addition of locally generated random independent noise (Gaussian or Laplacian) to obfuscate the states for differential privacy[2] of states in distributed multi-agent consensus [20]–[22]. This technique of obfuscating the state measurements by noise can also be used for differential privacy of states in a one-channel feedback NCS, as is presented in detail in [15]. However, the obfuscation of the state measurements with noise leads to perturbation of the state-dynamics of the plant. As a result these techniques often suffer from unavoidable trade-offs between differential privacy and accuracy [15], [20]. On the other hand, MSK ensures that the state-dynamics are invariant to the proposed privacy mechanism.

A. Summary of Paper Contribution

In this paper, we propose and study a model-based encryption scheme, referred to as masking with system kernel (MSK), for privacy of states against eavesdroppers with unbounded computation power in a one-channel feedback NCS. The NCS consists of an LTI plant with co-located actuators-controller and remote sensors. In MSK, the state

This work was partially supported by the National Science Foundation under grant ECCS1711554.

Nirupam Gupta (nirupam@umd.edu) and Nikhil Chopra (nchopra@umd.edu) are with the Department of Mechanical Engineering, University of Maryland, College Park, 20742 MD, USA

[1]For NCS, it is often preferable to use symmetric encryption due to the strict communication time constraints [16]

[2]For further information on differential privacy refer to [19]

measurements are encrypted by adding random vectors[3] belonging to the nullspace of the control input parameters. The controller computes the control inputs by directly using the received encrypted states. Therefore, MSK does not require any key management protocol for generation and distribution of secret keys between the sensors and the controller. Furthermore, the state-dynamics of the plant remains preserved under MSK .

We formulate the definition of privacy of states using the concept of *perfect secrecy* in cryptography [17] to rigorously analyze the privacy provided by MSK to the states. As it turns out, MSK can not preserve privacy of states of the considered NCS with *any* system parameters. Therefore, the challenging part is to obtain necessary and sufficient condition under which MSK guarantees the privacy of states against eavesdroppers with unbounded computation power. In this paper we partially solve this problem by proposing a sufficient condition in Section V. Expectedly, the proposed sufficient condition implies unobservability of the NCS with control inputs being as the output and therefore, puts restrictions on the pole placement.

II. Notations

$\mathbb{N}$, $\mathbb{Z}_{\geq 0}$, $\mathbb{R}_{>0}$, $\mathbb{R}^n$ and $\mathbb{R}^{n\times m}$ represent the set of natural numbers, non-negative integers, positive real numbers, n-dimensional real-valued vectors and $n \times m$ dimensional real-valued matrices, respectively. $1_n(0_n)$ represents a vector of dimension n with all elements equal to $1(0)$. $\mathbf{0}_n$ represents an $n \times n$ matrix of all elements equal to 0. For any matrix $M \in \mathbb{R}^{m\times n}$, its nullspace is represented by $\mathcal{N}(M) \subset \mathbb{R}^n$. For any vector $x \in \mathbb{R}^n$, its i-th element is represented by $x[i]$. Let $x \in \mathbb{R}^n$ and $y \in \mathbb{R}^n$, then $[x, y]$ represents the set of all vectors in $\mathbb{R}^n$ that lie on the line segment joining x and y. A vector $x \in \mathbb{R}^n$ is said to have all non-zero elements if $x[i] \neq 0, \forall i \in \{1, \ldots, n\}$. $|\cdot|$ denotes the absolute value of any scalar value.

For a random vector X (over $\mathbb{R}^n$), its probability density at any point x is simply represented as $f_X(x)$ and $Pr(X \in \Gamma)$ represents the probability of X taking value in a compact set Γ. $f_{X\in\Gamma}(x)$ is the conditional probability density of X, given X belongs to the compact set Γ. Specifically,

$$f_{X\in\Gamma}(x) = \begin{cases} \frac{f_X(x)}{Pr(X\in\Gamma)} & \forall x \in \Gamma \\ 0 & \text{otherwise} \end{cases}$$

For two random vectors X and Y the conditional probability density of X at x given the Y is represented as $f_{X|Y}(x|y)$. $U(\Gamma)$ represents the uniform probability density over a compact set Γ.

III. Problem Formulation

This section contains the formal description of the problem addressed in the paper.

[3]The specifications on the probability distribution of these random vectors are presented in the sequel.

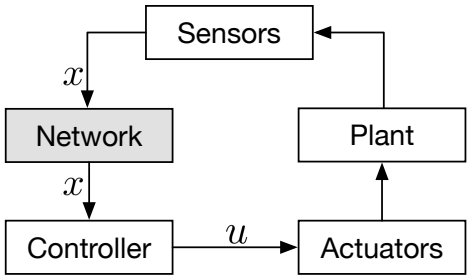

Fig. 1: Pictorial representation of a one-channel feedback NCS with co-located controller-actuators and remote sensors.

Consider a one-channel feedback networked control systems (NCS) as shown in Fig. 1. The NCS consists of a linear time-invariant (LTI) plant whose states are measured using remote sensors and driven by controller co-located with the actuators.

The mathematical model of system dynamics is as following.

$$x_{t+1} = Ax_t + Bu_t,\ u_t = Kx_t,\ \forall t \in \mathbb{Z}_{\geq 0} \tag{1}$$

where $x_t \in \mathbb{R}^n$ represents the state vector and $u_t \in \mathbb{R}^m$ represents the control input vector at any time t. The constant real-valued matrices $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$ and $K \in \mathbb{R}^{m\times n}$ constitute the system parameters. The matrix $A + BK$ is assumed to be non-singular.

In this paper, we consider eavesdroppers with unbounded computation power. In context of the aforementioned NCS, an eavesdropper is defined as following.

***Definition** 1:* (*Eavesdropper*) An eavesdropper is a passive adversary that can read all the messages being transmitted by the sensors over the network to the controller. An eavesdropper has precise knowledge of the system parameters (A, B and K) and the encryption scheme (if used) to encrypt the messages or state measurements. The eavesdropper is a passive adversary, implies it can not tamper with the messages or sensor measurements in any form.

The *objective* of this paper is to investigate a model-based encryption scheme that can prevent an eavesdropper from gathering any (or very limited) information about the states at any time $t \in \mathbb{Z}_{\geq 0}$ without affecting the closed-loop dynamics of the NCS.

To achieve this objective, in the subsequent section we propose a model-based encryption scheme.

IV. Model-Based Encryption

This section is divided into two subsections. In Subsection IV-A, we propose the model-based encryption scheme: *Masking With System Kernel* (MSK). In Subsection IV-B,

we present the formal definition of privacy of states.

A. Masking With System Kernel (MSK)

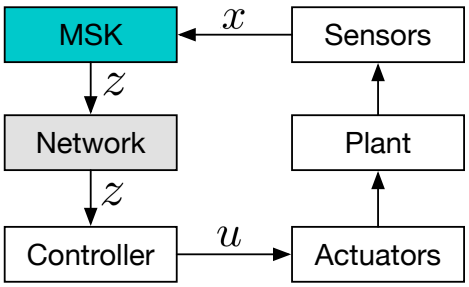

Fig. 2: Pictorial representation of masking with system kernel (MSK) for the considered NCS.

In MSK, the state vector x_t at each $t \in \mathbb{Z}_{\geq 0}$ is masked by adding a random vector from the kernel[4] of the matrix K to obtain masked state vector z_t as following.

$$z_t = x_t + w_t, \forall t \in \mathbb{Z}_{\geq 0} \tag{2}$$

Here, the random vector w_t is distributed over a compact set $N_t \subset \mathcal{N}(K)$ at each $t \in \mathbb{Z}_{\geq 0}$ with a known probability density. The specifications on the probability density of w_t and the set N_t are derived later in Section V as it requires the formal definition of privacy of states.

Now, instead of the x_t the sensors transmit z_t over the network to the controller. The controller computes the control input u_t as following.

$$u_t = Kz_t = Kx_t, \forall t \in \mathbb{Z}_{\geq 0}$$

Thus, substituting this value of u_t in (1) yields same state-dynamics.

Hence, it is quite clear that masking of the states x_t as z_t has no effect on the state-dynamics of the plant or on the state sequence $\{x_0, x_1, \ldots, x_t, \ldots\}$.

B. Privacy of States

In this section, we present the formal definition of the privacy of states using the concept of *perfect secrecy* in cryptography[5]. The definition is critical for deriving sufficient conditions under which MSK guarantees the privacy of states against eavesdroppers with unbounded computation power.

Notations: Let X_t, Z_t, W_t and U_t represent the random vectors corresponding to x_t, z_t, w_t and u_t. The sequences of random vectors Z_t and U_t are represented as $\mathcal{Z}_t = \{Z_0, \ldots, Z_t\}$ and $\mathcal{U}_t = \{U_0, \ldots, U_t\}$.

[4]A vector $v \in \mathbb{R}^n$ belongs to the kernel of the matrix $M \in \mathbb{R}^{n \times n}$ if and only if $Mv = 0$.

[5]For details on *perfect secrecy*, please refer to Chapter 2 in [17]

From (1), the random vectors X_t, Z_t, W_t and U_t are related as following.

$$X_t = (A + BK)^t X_0,\ Z_t = X_t + W_t \text{ and } U_t = KZ_t \tag{3}$$

for every $t \in \mathbb{Z}_{\geq 0}$.

As $U_t = KZ_t, \forall t \in \mathbb{Z}_{\geq 0}$, this implies that (as K is publicly known)

$$f_{X_r|\mathcal{Z}_t,\mathcal{U}_t}(x_r) = f_{X_r|\mathcal{Z}_t}(x_r),\ \forall r,\ t \in \mathbb{Z}_{\geq 0} \tag{4}$$

In other words, the control inputs u_t, $\forall t \in \mathbb{Z}_{\geq 0}$ provides no additional information on x_r (for any $r \in \mathbb{Z}_{\geq 0}$) than what is already available from the masked states z_t, $\forall t \in \mathbb{Z}_{\geq 0}$.

Let $Z_s = z_s$ at any time $s \in \{0, \ldots, t\}$. As $w_s \in N_s$, this implies that X_s is contained in the set $M_s(z_s)$, where

$$M_s(z_s) = (x_s \in \mathbb{R}^n;\ z_s - x_s \in N_s)$$

This further implies that X_0 is contained in $K_s(z_s)$ for given $Z_s = z_s$ as $x_s = (A + BK)^s x_0$, where

$$K_s(z_s) = (x_0 \in \mathbb{R}^n;\ z_s - (A + BK)^s x_0 \in N_s) \tag{5}$$

Inferentially, for a given sequence of masked states $\mathcal{Z}_t = \mathbf{z}_t = \{z_0, \ldots, z_t\}$ the random vector X_0 can only take values from the following set

$$\mathcal{K}_{t,0}(\mathbf{z}_t) = \bigcap_{s=0}^{t} K_s(z_s) \tag{6}$$

In other words,

$$f_{X_0|\mathcal{Z}_t}(x_0|\mathbf{z}_t) = 0,\ \forall x_0 \notin \mathcal{K}_{t,0}(\mathbf{z}_t) \tag{7}$$

This holds regardless of the probability distribution of w_t. Evidently, from (7) it is quite obvious that MSK can not prevent disparity between the *priori* (before observing the encrypted states) and *posteriori* (after observing the encrypted states) probability distributions of X_r for any $r \in \{0, \ldots, t\}$.

Inferentially from (7), an eavesdropper can determine the range of possible values of the state at 0 by observing the masked states from time 0 to t. However, privacy of x_0 can still be guaranteed if the knowledge of masked states does not effect the *posteriori* probability distribution of X_0 in $\mathcal{K}_{t,0}(\mathbf{z}_t)$. This intuition is used to formulate the following definition of privacy of states.

***Definition** 2:* MSK guarantees the *privacy of states* (against an eavesdropper with unbounded computation power) if both the following conditions, **C1** and **C2**, hold for every $t \in \mathbb{Z}_{\geq 0}$ and for any given sequence of encrypted states $\mathbf{z}_t = \{z_0, \ldots, z_t\}$.

C1 $f_{X_r|\mathcal{Z}_t}(x_r|\mathbf{z}_t) = f_{X_r \in \mathcal{K}_{t,r}(\mathbf{z}_t)}(x_r)$ for every $r \in \{0, \ldots, t\}$.

C2 For every $r \in \{0, \ldots, t\}$, there exists a vector $v_r \in \mathbb{R}^n$ with all non-zero elements ($0 < |v_r[i]|, \forall i$) such that

$$[z_r - v_r,\ z_r + v_r] \subseteq \mathcal{K}_{t,r}(\mathbf{z}_t)$$

Here, $\mathcal{K}_{t,\,r}(\mathbf{z}_t) = (x \in \mathbb{R}^n;\, (A+BK)^{-r}x \in \mathcal{K}_{t,\,0}(\mathbf{z}_t))$. The value $\delta_r = \min_{i=1}^{n} |v_r[i]|$ is the *degree of privacy* for state at time $r \in \{0, \ldots, t\}$.

Note: v_t for any time $t \in \mathbb{Z}_{\geq 0}$ in the definition above should not independent on the values of the encrypted states $\{z_0,\, z_1,\, \ldots\}$.

C1 ensures that for any given sequence of encrypted states $\mathcal{Z}_t = \mathbf{z}_t = \{z_0,\, \ldots,\, z_t\}$, $t \in \mathbb{Z}_{\geq 0}$, the *posteriori* probability distribution of X_r, $r \in \{0, \ldots, t\}$ should be the same as its *priori* probability distribution in $\mathcal{K}_{t,\,r}(\mathbf{z}_t)$. Clearly, **C1** is not as strong a condition as the *perfect secrecy*[6] which is impossible to achieve due to (7). However, if **C1** holds then we get the following equality for every $t \in \mathbb{Z}_{\geq 0}$ and $r \in \{0, \ldots, t\}$,

$$f_{\mathcal{Z}_t|X_r}\left(\mathbf{z}_t|x_r\right) = f_{\mathcal{Z}_t|X_r}\left(\mathbf{z}_t|x_r'\right) \tag{8}$$

where, x_r and x_r' are any two points in $\mathcal{K}_{t,\,r}(\mathbf{z}_t)$. The relationship above implies that it is impossible to distinguish between any two values of X_r, $r \in \{0, \ldots, t\}$ in $\mathcal{K}_{t,\,r}(\mathbf{z}_t)$ given the encrypted states $\mathbf{z}_t$.

Now, for a given sequence of encrypted states $\mathbf{z}_t$ the set of possible values of X_0 is given by $\mathcal{K}_{t,\,0}(\mathbf{z}_t)$ in (6). The set $\mathcal{K}_{t,\,0}(\mathbf{z}_t)$ is non-increasing with respect to t, that is

$$\mathcal{K}_{t+1,\,0}(\mathbf{z}_{t+1}) \subseteq \mathcal{K}_{t,\,0}(\mathbf{z}_t),\, \forall t \in \mathbb{Z}_{\geq 0}$$

So, it is very much possible that there exists a $T \in \mathbb{N}$ such that $\mathcal{K}_{t,\,0}(\mathbf{z}_t)$ is singleton[7] for all $t \geq T$. To further accentuate this point we present an example in Section V where $\mathcal{K}_{t,\,0}(\mathbf{z}_t)$ indeed reduces to singleton set for t greater than some particular value. Note that $\mathcal{K}_{t,\,0}(\mathbf{z}_t)$ is singleton if and only if $\mathcal{K}_{t,\,r}(\mathbf{z}_t)$ is singleton for all $r \in \{1, \ldots, t\}$.

Thus, **C2** is required to ensure a lower bound on the volume of $\mathcal{K}_{t,\,r}(\mathbf{z}_t)$, $\forall r \in \{0, \ldots, t\}$ that should hold for any sequence of encrypted states $\mathcal{Z}_t = \mathbf{z}_t$, $t \in \mathbb{Z}_{\geq 0}$. **C2** implies that for every $r \in \{0, \ldots, t\}$ there exists a vector v_r with all non-zero elements such that the set $[z_r - v_r,\, z_r + v_r]$ is contained in $\mathcal{K}_{t,\,r}(\mathbf{z}_t)$. The reason that we require v_r to have all non-zero elements is to ensure privacy of each and every element of the state at any time $r \in \{0, \ldots, t\}$.

The implication of ***Definition*** 2 (and perhaps a more natural definition) is summarized in the following remark.

Remark 1: If **C1** and **C2** hold then for any $t \in \mathbb{Z}_{\geq 0}$ and any given sequence of t encrypted states $\mathbf{z}_t$ there exists a vector $v_r \in \mathbb{R}^n$ with all non-zero elements, such that

$$f_{\mathcal{Z}_t|X_r}\left(\mathbf{z}_t|x_r\right) = f_{\mathcal{Z}_t|X_r}\left(\mathbf{z}_t|x_r'\right), \forall r \in \{0, \ldots, t\} \tag{9}$$

for all x_r, x_r' in $[z_r - v_r,\, z_r + v_r]$.

Thus, *privacy of states* as defined implies that it is impossible to distinguish between two state values of state at t from the set $[z_t - v_t,\, z_t + v_t]$ given the encrypted states.

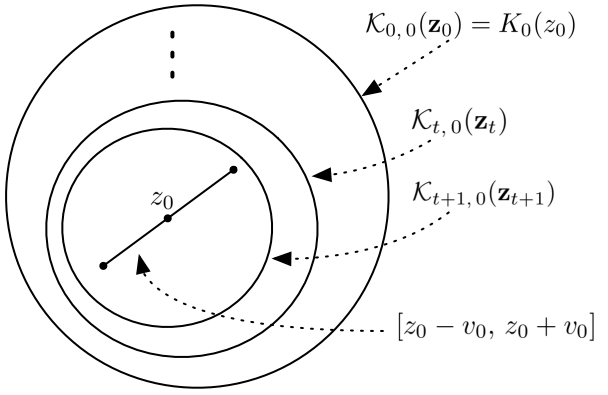

Fig. 3: A pictorial representation of a hypothetical scenario showing the evolution of sets $\mathcal{K}_{t,\,0}(\mathbf{z}_t)$ with time t and the implication of condition **C2**.

From (9), each element $X_r[i], i \in \{1, \ldots, n\}$ can take any value in $[z_r[i] - v_r[i],\, z_r[i] + v_r[i]]$ for a given sequence of encrypted states $\mathbf{z}_t$. Therefore, the size of the range of possible values for i-th element of state at time $r \in \{0, \ldots, t\}$ is equal to $2|v_r[i]|$. Hence, δ_r is the factor that determines lower bound[8] on the size of the set of possible values for each element of the state at r (as v_r at any time $r \in \mathbb{Z}_{\geq 0}$ is independent of the sequence of encrypted sates). Thus, *degree of privacy* δ_t is a critical measure of the extent of privacy of state at any time $t \in \mathbb{Z}_{\geq 0}$.

In the subsequent section we present a sufficient condition under which MSK guarantees privacy of states.

V. Sufficient Condition: Guaranteeing Privacy of States

From the results pertaining to the state estimation of an LTI system in the presence of uniformly distributed measurement noise in [24], we get the following result.

Lemma 1: (Modified version of the Theorem in [24]) If $W_t \sim U(N_t)$, $\forall t \in \mathbb{Z}_{\geq 0}$ with N_t being a compact subset of $\mathcal{N}(K)$ then MSK (2) satisfies condition **C1** given in Definition 2. ■

According to Lemma 1, if the mask vectors w_t are independently chosen from each other following a uniform distribution in some bounded subset in $\mathcal{N}(K)$ for all $t \in \mathbb{Z}_{\geq 0}$ then **C1** is satisfied. However, the following example shows that independent random selections of w_t from a compact set $N_t \subset \mathcal{N}(K)$ for all $t \in \mathbb{Z}_{\geq 0}$ does not guarantee condition **C2** and hence is not sufficient for the privacy of states.

Example I: Consider the following LTI state-dynamics of

[6]This is an obvious limitation as *perfect secrecy* is usually studied for the case of finite fields, whereas here we are dealing with state vectors in n-dimensional space of real numbers

[7]$\mathcal{K}_{t,\,r}(\mathbf{z}_t)$ is trivially guaranteed to be non-empty from the very design of the MSK.

[8]It is a lower bound as it is concerned with only the possible values along a single vector v_r at any time r.

the plant

$$x_{t+1} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} x_t + \begin{bmatrix} 0 \\ 1 \end{bmatrix} u_t,\ u_t = \begin{bmatrix} 1 & 1 \end{bmatrix} x_t$$

where $x_t \in \mathbb{R}^2$ for every $t \in \mathbb{Z}_{\geq 0}$. The system parameters are as follows

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix},\ B = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \text{ and } K = \begin{bmatrix} 1 & 1 \end{bmatrix}$$

Here, $\mathcal{N}(K) = \text{span}\{v_o\}$ with $v_o = \begin{bmatrix} -1 & 1 \end{bmatrix}^T$.

Let the states be masked using MSK as given by (2) with $W_t \in U(N_t)$, where N_t is a line segment of finite length along the vector v_o for $\forall t \in \mathbb{Z}_{\geq 0}$.

Now, in this case w_t is of the form $\lambda_t v_o$, $\lambda_t \in \mathbb{R}$ for all $t \in \mathbb{Z}_{\geq 0}$. Consider the mask vectors z_0 and z_1, given as following

$$z_0 = x_0 + w_0,\ z_1 = x_1 + w_1$$

As $x_1 = Ax_0$, $w_0 = \lambda_0 v_o$, $w_1 = \lambda_1 v_o$ and $v_o = \begin{bmatrix} -1 & 1 \end{bmatrix}^T$, we get the following set of equations

$$z_0[1] = x_0[1] - \lambda_0,\ z_0[2] = x_0[2] + \lambda_0$$
$$z_1[1] = x_0[1] + x_0[2] - \lambda_1,\ z_1[2] = x_0[2] + \lambda_1$$

or simply,

$$\begin{bmatrix} z_0[1] \\ z_0[2] \\ z_1[1] \\ z_1[2] \end{bmatrix} = \begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & -1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_0[1] \\ x_0[2] \\ \lambda_0 \\ \lambda_1 \end{bmatrix} \tag{10}$$

As the matrix in the RHS of (10) is non-singular, this implies that state vector x_0 can be uniquely determined for the given masked states z_0 and z_1. In other words, the set $\mathcal{K}_{t,0}(\mathbf{z}_t)$ is singular for all $t \geq 1$.

From Lemma 1, the masking of states in the form of MSK (2) with the aforementioned specifications on the masks w_t satisfies condition **C1** of Definition 2. However, it has been shown that the states can be uniquely determined from just observing the first 2 masked states. Therefore, not only this example explains the reason for condition **C2** in Definition 2, it also suggests that MSK can not preserve privacy of states for *any* NCS.

In the following theorem, we present a sufficient condition under which MSK guarantees the privacy of states, as defined in Definition 2.

***Theorem** 1:* For the considered NCS with state dynamics (1), *if* there exists a vector $v \in \mathcal{N}(K)$ with all non-zero elements such that $Av = \mu v$, $\mu \neq 0$ then MSK guarantees privacy of the states with degree of privacy

$$\delta_t = 2\mu^t d_o \min_{i=1}^{n} |v[i]|, \text{where}$$

1) $W_0 \sim U(N_0),\quad N_0 = [-d_o v,\ d_o v],\ d_o \in \mathbb{R}_{>0}$,
2) $w_t = \mu^t w_0,\ \forall t \in \mathbb{N}$

and d_o is any positive real-valued number.

Proof: Consider any $t \in \mathbb{Z}_{\geq 0}$ and sequence of encrypted states till time t, $\mathbf{z}_t = \{z_0, \ldots, z_t\}$.

As $w_t = \mu^t w_0$, we get

$$z_t = x_t + w_t = (A + BK)^t z_0,\ \forall t \in \mathbb{Z}_{\geq 0} \tag{11}$$

Consequentially,

$$Z_t = (A + BK)^t Z_0,\ \forall t \in \mathbb{Z}_{\geq 0}$$

The aforementioned relationship between the encrypted states in time implies that

$$f_{X_0|\mathcal{Z}_t}(x_0|\mathbf{z}_t) = f_{X_0|Z_0}(x_0|z_0),\ \forall t \in \mathbb{Z}_{\geq 0} \tag{12}$$

From Baye's rule, we know that

$$f_{X_0|Z_0}(x_0|z_0) = \frac{f_{Z_0|X_0}(z_0|x_0) f_{X_0}(x_0)}{\int_{x \in \mathbb{R}^n} f_{Z_0|X_0}(z_0|x) f_{X_0}(x) dx} \tag{13}$$

As $w_0 \sim U([-d_o v,\ d_o v])$ and is independent of x_0, this implies

$$f_{Z_0|X_0}(z_0|x_0) = \begin{cases} \gamma_0 & \forall x_0 \in K_0(z_0) \\ 0 & \text{otherwise} \end{cases} \tag{14}$$

where γ_0 is some positive real number (the actual value is not required for the proof). (From (5), the set $K_0(z_0) = (x \in \mathbb{R}^n; z_0 - x \in N_0)$.)

Thus,

$$\int_{x \in \mathbb{R}^n} f_{Z_0|X_0}(z_0|x) f_{X_0}(x) dx = \gamma_0 \int_{x \in K_0(z_0)} f_{X_0}(x) dx$$
$$= \gamma_0 Pr\left(X_0 \in K_0(z_0)\right) \tag{15}$$

Substituting (14) and (15) in (13) yields

$$f_{X_0|Z_0}(x_0|z_0) = \begin{cases} \frac{f_{X_0}(x_0)}{Pr(X_0 \in K_0(z_0))} & \forall x_0 \in K_0(z_0) \\ 0 & \text{otherwise} \end{cases}$$

or simply,

$$f_{X_0|Z_0}(x_0|z_0) = f_{X_0 \in K_0(z_0)}(x_0) \tag{16}$$

Now, we first show that $K_0(z_0)$ and $\mathcal{K}_{t,0}(\mathbf{z}_t)$ are indeed equivalent in this case.

As $w_0 \in N_0$ and $N_0 = [-d_o v,\ d_o v]$, this implies that for any $x_0 \in K_0(z_0)$ we can write

$$z_0 - x_0 = -\lambda d_o v + (1 - \lambda) d_o v \tag{17}$$

where, λ is some value in $[0,\ 1]$. As $v \in \mathcal{N}(K)$ is the right eigenvector of A with $Av = \mu v$, we get

$$(A + BK)^t v = \mu^t v,\ \forall t \in \mathbb{Z}_{\geq 0} \tag{18}$$

From (17) and (18), we get

$$(A + BK)^t z_0 - (A + BK)^t x_0 = -\lambda \mu^t v + (1 - \lambda) \mu^t v \tag{19}$$

for every $t \in \mathbb{Z}_{\geq 0}$. From (11) and the fact that $w_t = \mu^t w_0$, (19) is equivalent to the following

$$z_t - (A+BK)^t x_0 = w_t,\ \forall t \in \mathbb{Z}_{\geq 0} \tag{20}$$

Therefore, from (20) it is quite evident that if $x_0 \in K_0(z_0)$ then $x_0 \in K_t(z_t)$, $\forall t \in \mathbb{Z}_{\geq 0}$. Inferentially, $K_0(z_0) \subseteq \mathcal{K}_{t,0}(\mathbf{z}_t)$. However, $\mathcal{K}_{t,0}(\mathbf{z}_t) \subseteq K_0(z_0)$ as $\mathcal{K}_{t,0}(\mathbf{z}_t) = \bigcap_{s=0}^{t} K_s(z_s)$. This implies that

$$\mathcal{K}_{t,0}(\mathbf{z}_t) = K_0(z_0),\ \forall t \in \mathbb{Z}_{\geq 0} \tag{21}$$

Equation (21) has the following twofold implications.

(i) Combining (21) with (12) and (16) gives

$$f_{X_0|\mathcal{Z}_t}(x_0|\mathbf{z}_t) = f_{X_0 \in \mathcal{K}_{t,0}(\mathbf{z}_t)}(x_0)$$

As $A+BK$ is non-singular, the equality above implies that[9]

$$f_{X_r|\mathcal{Z}_t}(x_r|\mathbf{z}_t) = f_{X_r \in \mathcal{K}_{t,r}(\mathbf{z}_t)}(x_r)$$

for every $r \in \{0, \ldots, t\}$. Here, $\mathcal{K}_{t,r}(\mathbf{z}_t) = (x \in \mathbb{R}^n;\ (A+BK)^{-r}x \in \mathcal{K}_{t,0}(\mathbf{z}_t))$. Hence, condition **C1** of Definition 2 is satisfied.

(ii) From (21), we get $\mathcal{K}_{t,0}(\mathbf{z}_t) = [z_0 - d_0 v,\ z_0 + d_0 v]$. Now, using (11) and (18) here implies that

$$\mathcal{K}_{t,r}(\mathbf{z}_t) = [z_r - \mu^r d_0 v,\ z_r + \mu^r d_0 v],\ \forall r \in \{0, \ldots, t\} \tag{22}$$

Hence, condition **C2** of Definition 2 is satisfied with $v_r = \mu^r v$, $\forall r \in \mathbb{Z}_{\geq 0}$.

Note that the conclusions above holds for any $t \in \mathbb{Z}_{\geq 0}$ and any sequence of encrypted states $\mathbf{z}_t$ generated by the MSK (in (2)) with the given specifications.

Clearly, from (22) the degree of privacy of the state at time $t \in \mathbb{Z}_{\geq 0}$ is given by $\delta_t = 2\mu^t d_o \min_{i=1}^{n} |v[i]|$. ■

The result in Theorem 1 shows that MSK guarantees privacy of states for the considered NCS if the system parameters are related in the specified manner. **Note**, the condition given in the theorem above implies unobservability of the pair $(A+BK,\ K)$.

In the next section, we present an example to demonstrate MSK.

VI. Numerical Example

Consider the following state-dynamics of the plant

$$x_{t+1} = Ax_t + Bu_t,\ u_t = Kx_t,\ \forall t \in \mathbb{Z}_{\geq 0} \tag{23}$$

[9]If two random vectors S and R satisfy $S = TR$, where T is a (known) non-singular matrix (ref. [23]), then

$$f_S(s) = \frac{1}{|\det(T)|} f_R(T^{-1}s)$$

where $x_t \in \mathbb{R}^2$, $\forall t \in \mathbb{Z}_{\geq 0}$,

$$A = \begin{bmatrix} 1 & \epsilon \\ 0 & -\epsilon k_d + 1 \end{bmatrix},\ B = \begin{bmatrix} 0 \\ \epsilon \end{bmatrix} \text{ and } K = -[k_1,\ k_2].$$

Here k_d, k_1, k_2 and ϵ are positive real values such that

$$k_1 = k_d k_2 \text{ and } \epsilon \neq 1/k_d.$$

In this case,

$$\mathcal{N}(K) = \text{span}\{v\},\ v = \begin{bmatrix} -k_2 \\ k_1 \end{bmatrix} \tag{24}$$

Clearly, both the elements of v are non-zero (this is one of the required conditions in Theorem 1). From algebraic calculations, we get

$$Av = \begin{bmatrix} -k_2 + \epsilon k_1 \\ -\epsilon k_1 k_d + k_1 \end{bmatrix} = (1 - \epsilon k_d)v \tag{25}$$

where, $(1 - \epsilon k_d) \neq 0$. Also, note that

$$A + BK = \begin{bmatrix} 1 & \epsilon \\ -\epsilon k_d k_2 & 1 - \epsilon(k_2 + k_d) \end{bmatrix}$$

is non-singular with eigenvalues $1 - \epsilon k_d$ and $1 - \epsilon k_2$.

Therefore, the system parameters in this case satisfy the conditions prescribed in Theorem 1 with v as given in (24) and $\mu = (1 - \epsilon k_d)$. Hence, MSK as given by (2) or specifically the masking of x_t as following

$$z_t = x_t + w_t,\ \forall t \in \mathbb{Z}_{\geq 0}$$

where w_0 is chosen uniformly from the set $[-d_o v,\ d_o v]$ and $w_t = (1 - \epsilon k_d)^t w_0$, $\forall t \in \mathbb{N}$ guarantees privacy of state x_t at any time $t \in \mathbb{Z}_{\geq 0}$ against an eavesdropper with unbounded computation power with degree of privacy $d_o(1 - \epsilon k_d)^t \min\{k_2,\ k_d k_2\}$ for any $t \in \mathbb{Z}_{\geq 0}$. Here, d_o can any positive real number. Consequentially, the control input u_t in (23) is replaced by $u_t = Kz_t$, $\forall t \in \mathbb{Z}_{\geq 0}$.

VII. Conclusion

In this paper, a model-based encryption scheme (termed as masking with system kernel (MSK)) has been investigated, as alternative to cryptographic encryptions, for the privacy of states in a one-channel feedback networked control system (NCS) consisting of a linear-time invariant (LTI) plant. MSK does not require sharing or generation of secret keys and introduces minimal computation overhead (significantly light in comparison to existing cryptographic encryptions). The privacy of states is formally defined using the theory of *perfect secrecy* in cryptography [17] and assumes no bound on the computation power of the eavesdroppers. Based on this, we rigorously show that under certain conditions MSK *guarantees* privacy of states in the considered NCS.

REFERENCES

[1] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 138–162, 2007.

[2] N. Gupta and N. Chopra, "Stability analysis of a two-channel feedback networked control system," in *Control Conference (ICC), 2016 Indian*. IEEE, 2016, pp. 200–207.

[3] J. R. Allard, "Method and system for remote control of mobile robot," Mar. 18 2003, uS Patent 6,535,793.

[4] T. M. Chen and R. C. Luo, "Remote supervisory control of an autonomous mobile robot via world wide web," in *Industrial Electronics, 1997. ISIE'97., Proceedings of the IEEE International Symposium on*, vol. 1. IEEE, 1997, pp. SS60–SS64.

[5] Y.-P. Tsou, J.-W. Hsieh, C.-T. Lin, and C.-Y. Chen, "Building a remote supervisory control network system for smart home applications," in *Systems, Man and Cybernetics, 2006. SMC'06. IEEE International Conference on*, vol. 3. IEEE, 2006, pp. 1826–1830.

[6] F. Katiraei, R. Iravani, N. Hatziargyriou, and A. Dimeas, "Microgrids management," *IEEE power and energy magazine*, vol. 6, no. 3, 2008.

[7] W. Ren, "Consensus strategies for cooperative control of vehicle formations," *IET Control Theory & Applications*, vol. 1, no. 2, pp. 505–512, 2007.

[8] J. Shao, G. Xie, and L. Wang, "Leader-following formation control of multiple mobile vehicles," *IET Control Theory & Applications*, vol. 1, no. 2, pp. 545–552, 2007.

[9] N. Chopra, M. W. Spong, S. Hirche, and M. Buss, "Bilateral teleoperation over the internet: the time varying delay," in *Proceedings of the American Control Conference (ACC)*, 2003.

[10] P. F. Hokayem and M. W. Spong, "Bilateral teleoperation: An historical survey," *Automatica*, vol. 42, no. 12, pp. 2035–2057, 2006.

[11] N. Chopra and M. W. Spong, "On synchronization of networked passive systems with time delays and application to bilateral teleoperation," in *proceedings of the SICE annual conference*, 2005, pp. 3424–3429.

[12] R. Olfati-Saber, A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 215–233, 2007.

[13] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *Proceedings of the 52nd annual design automation conference*. ACM, 2015, p. 54.

[14] M. E. Tozal, Y. Wang, E. Al-Shaer, K. Sarac, B. Thuraisingham, and B.-T. Chu, "Adaptive information coding for secure and reliable wireless telesurgery communications," *Mobile Networks and Applications*, vol. 18, no. 5, pp. 697–711, 2013.

[15] H. Zhang, Y. Shu, P. Cheng, and J. Chen, "Privacy and performance trade-off in cyber-physical systems," *IEEE Network*, vol. 30, no. 2, pp. 62–66, 2016.

[16] K. A. McKay, K. A. McKay, L. Bassham, M. S. Turan, and N. Mouha, *Report on lightweight cryptography*. US Department of Commerce, National Institute of Standards and Technology, 2017.

[17] J. Katz and Y. Lindell, *Introduction to modern cryptography*. CRC press, 2014.

[18] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE wireless Communications*, vol. 18, no. 2, 2011.

[19] C. Dwork, M. Naor, T. Pitassi, and G. N. Rothblum, "Differential privacy under continual observation," in *Proceedings of the forty-second ACM symposium on Theory of computing*. ACM, 2010, pp. 715–724.

[20] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private average consensus with optimal noise selection," *IFAC-PapersOnLine*, vol. 48, no. 22, pp. 203–208, 2015.

[21] Y. Mo and R. M. Murray, "Privacy preserving average consensus," in *Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on*. IEEE, 2014, pp. 2154–2159.

[22] Z. Huang, S. Mitra, and G. Dullerud, "Differentially private iterative synchronous consensus," in *Proceedings of the 2012 ACM workshop on Privacy in the electronic society*. ACM, 2012, pp. 81–90.

[23] B. Lindgren, *Statistical theory*. Routledge, 2017.

[24] L. Servi and Y. Ho, "Recursive estimation in the presence of uniformly distributed measurement noise," *IEEE Transactions on Automatic Control*, vol. 26, no. 2, pp. 563–565, 1981.