Secure state estimation over Markov wireless communication channels

Anastasia Impicciatore[1], Anastasios Tsiamis[2], Yuriy Zacchia Lun[1], Alessandro D'Innocenzo[1], George J. Pappas[3]

***Abstract*—This note studies state estimation in wireless networked control systems with secrecy against eavesdropping. Specifically, a sensor transmits a system state information to the estimator over a legitimate user link, and an eavesdropper overhears these data over its link independent of the user link. Each connection may be affected by packet losses and is modeled by a finite-state Markov channel (FSMC), an abstraction widely used to design wireless communication systems. This paper presents a novel concept of optimal mean square expected secrecy over FSMCs and delineates the design of a secrecy parameter requiring the user mean square estimation error (MSE) to be bounded and eavesdropper MSE unbounded. We illustrate the developed results on an example of an inverted pendulum on a cart whose parameters are estimated remotely over a wireless link exposed to an eavesdropper.**

***Index Terms*—Wireless networked control systems, finite-state Markov channel, optimal mean square expected secrecy**

I. Introduction

Wireless networked control systems (WNCSs) comprise spatially distributed networked sensors, actuators, and controllers providing closed-loop control over wireless communication media. These systems find applications in industrial automation, intelligent transportation, and smart grids, receiving considerable attention from industry and academia [1], [2]. The significant challenges of wireless connectivity, especially for the control applications, lie in the time-varying, unreliable and shared nature of this communication medium. The movement of people and objects in the propagation environment induces the shadow and small-scale fading that, paired with interference from other transmitters, causes information loss leading to performance and stability degradation [3]. Furthermore, due to the shared nature of the wireless medium, other agents in the vicinity can overhear the content of transmissions, and there is often a need to protect systems from eavesdroppers [4], [5].

The current defense mechanisms against eavesdropping in WNCSs involve encryption-based tools, wireless physical-layer security methods, and control-theoretic approaches [6]–[9]. Like [10], this paper relies on control theory to take advantage of the system dynamics to provide security guarantees by randomly withholding sensor information. However, unlike any other control-theoretic contribution, it does not consider the transmission over wireless links being modeled by an independent and identically distributed (i.i.d.) Bernoulli random variable or a time-homogeneous two-state Markov chain (MC) but by a finite-state Markov channel (FSMC). FSMC is an important model because traditionally, wireless communication systems designers use this mathematical abstraction for modeling error bursts in fading channels to analyze and improve performance measures in the physical or media access control layers. Moreover, several receivers' channel state estimation and decoding algorithms rely upon FSMC models [11].

In this work each agent (user or eavesdropper) estimates the process evolution of the Signal-to-Interference-plus-Noise Ratio (SINR) on its link, independently from the other. A finite-state MC (with more than two modes) approximates the SINR process over each link. A binary random variable standing for the outcome of the transmission is associated to each Markov mode, which determines the distribution of the binary random variable. The resulting FSMC allows for a tighter integration in the coupled design of the communication and estimation components of the WNCS.

Some procedures for control and estimation over packet dropping wireless links modeled by FSMCs can be related to the Markov jump [12] linear systems (MJLSs) theory [13]–[15] generalizing the fundamental results based on i.i.d. Bernoullian assumptions [16]. Nevertheless, most of the contributions on estimation and control over fading channels consider the two-state MC modeling a bursty packet erasure channel [17]. In this article, we choose a minimum mean square Markov jump filter instead of Kalman filter (see [17]), because the filter dynamics depends just on the current mode of the sensing channel (rather than on the entire past history of modes).

A. *Paper contribution*

This work brings the perfect expected secrecy notion in [10] to FSMCs. In contrast to [10], we study secrecy over estimation filters, whose gains can be pre-computed offline. The original notion of perfect expected secrecy requires implementations of the Kalman filter. However, under FSMCs, any offline computation of the Kalman filter gains would

[1] Department of Information Engineering, Computer Science and Mathematics, University of L'Aquila, L'Aquila 67100, Italy (e-mails:anastasia.impicciatore@graduate.univaq.it, yuriy.zacchialun@univaq.it, alessandro.dinnocenzo@univaq.it)

[2] Automatic Control Laboratory, ETH Zürich (e-mail: atsiamis@control.ee.ethz.ch)

[3] Department of Electrical and Systems Engineering University of Pennsylvania, 200 South 33rd Street, Philadelphia, PA 19104, United States (e-mail: pappasg@seas.upenn.edu)

require a combinatorially increasing, with the time-horizon, amount of memory. For this reason, here, we consider an alternative practical notion of expected secrecy; we consider the minimum MSE, but over filters with a finite number of offline-computed gains.

In particular, in this paper, we require the eavesdropper MSE to grow unbounded, while the user MSE remains bounded. This new definition, requires us to adopt a different approach and utilize tools for the stability analysis of MJLSs [13], [18].

We employ a secrecy mechanism, which, similar to [10], randomly withholds information with some probability. We prove that by properly tuning the withholding probability, we can achieve expected secrecy if an only if there is channel disparity between the user and the eavesdropper, i.e., the user has a higher probability of packet reception on average. Finally, we also provide novel covariance lower bounds for the eavesdropper MSE. Such a lower bound could be used as a guide to tune the withholding probability of the secrecy mechanism.

B. Notation and preliminaries

In the following, $\mathbb{N}_0$ denotes the set of non-negative integers, $\mathbb{R}$ denotes the set of reals, while $\mathbb{F}$ indicates the set of either real or complex numbers. The absolute value of a number is denoted by $|\cdot|$. For positive integers r and s, the symbol $\mathbf{O}_r$ denotes the vector containing all zeros of length r. $\mathbb{I}_r$ indicates the identity matrix of size r, while $\mathbb{O}_r$ represents the matrix of zeros of size $r \times r$. Consider a vector $x \in \mathbb{R}^r$ and a matrix $K \in \mathbb{R}^{r\times s}$. The transposition is denoted by x' and K', the complex conjugation is denoted by $\overline{x}$ and $\overline{K}$, the conjugate transposition is denoted by x^* and K^*, respectively. $\mathbb{F}_*^{r\times r}$ and $\mathbb{F}_+^{r\times r}$ represent the sets of Hermitian and positive semi-definite matrices, respectively. For any positive integers N, r, a sequence of matrices K_m, $m = 1, \dots, N$, denoted by $\mathbf{K} = [K_m]_{m=1}^N$, we define the following sets of sequences of Hermitian matrices and of positive semi-definite Hermitian matrices:

$$\mathbb{H}^{Nr,*} \triangleq \{\mathbf{K} = [K_m]_{m=1}^N; K_m \in \mathbb{F}_*^{r\times r}, m = 1, \dots, N\},$$
$$\mathbb{H}^{Nr,+} \triangleq \{\mathbf{K} \in \mathbb{H}^{Nr,*}; K_m \in \mathbb{F}_+^{r\times r}, m = 1, \dots, N\}.$$

We denote by $\rho(\cdot)$ the spectral radius of a square matrix, i.e., the largest absolute value of its eigenvalues, and by $\|\cdot\|$ either any vector norm or any matrix norm. The operator $\operatorname{vec}(\cdot)$ denotes the vectorization of a matrix. Given $\mathbf{K} = [K_m]_{m=1}^N$,

$$\operatorname{vec}^2(\mathbf{K}) = [\operatorname{vec}(K_1), \dots, \operatorname{vec}(K_N)]'.$$

Let $\otimes$, $\bigoplus$ denote the Kronecker product defined in the usual way (see for example [19]) and the direct sum, respectively.

C. Paper organization

The paper is organized as follows. The problem formulation is presented in Section II. The optimal mean square expected secrecy is provided by Section III and the main result is shown in Section IV. An eavesdropper characterization is presented in Section V. Finally, an example can be found in Section VI. Proofs and technical results are reported in the appendix.

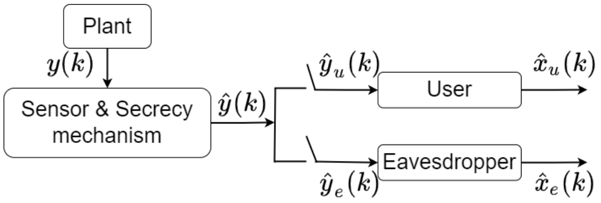

Fig. 1: Remote estimation architecture.

II. Problem formulation

The following discrete-time linear system describes the plant

$$\begin{cases} x(k+1) = Ax(k) + w(k), \\ y(k) = Lx(k) + v(k), \end{cases} \tag{1}$$

where $x(k) \in \mathbb{R}^{n_x}$ is the state and $y(k) \in \mathbb{R}^{n_y}$ is the system's output, while $k \in \mathbb{N}$ is the (discrete) time. The signals $w(k) \in \mathbb{R}^{n_x}$ and $v(k) \in \mathbb{R}^{n_y}$ are the process and measurement noise respectively: $w(k)$ and $v(k)$ are i.i.d. independent Gaussian random variables with zero mean and covariance matrices $Q, R \succ 0$ respectively. The initial state x_0 is Gaussian with zero mean and covariance matrix $\Sigma_0 \succ 0$.

Assumption 1. *The system described by* (1) *is unstable, i.e.,* $\rho(A) > 1$.

Even without eavesdroppers, estimation of unstable open-loop systems has been a problem of independent interest in control systems (see [20] for instance). The ultimate goal is to close the loop and apply control, but first, estimation of the open-loop system should be studied. Besides, if the system is stable, the eavesdropper can predict the state with more accuracy, even without eavesdropping, since the state remains close to the origin.

A. Secrecy mechanism

We adopt the secrecy mechanism introduced in [10]: the sensor transmits the output $y(k)$ with probability $\lambda \in [0, 1]$ and it transmits no information (denoted by the symbol ϵ) with probability $1 - \lambda$. Formally,

$$\hat{y}(k) = \begin{cases} y(k) & \text{if } \nu(k) = 1 \\ \epsilon & \text{if } \nu(k) = 0 \end{cases} \quad \forall k \geq 0, \tag{2}$$

$\nu(k)$ is the outcome of the secrecy mechanism, represented by a binary random variable with secrecy parameter λ defined as follows: $\mathbb{P}(\nu(k) = 1) = \lambda$, $\mathbb{P}(\nu(k) = 0) = 1 - \lambda$. In the rest of this note, we will use the subscript i to indicate an agent operating at the receiver's end.

Formally, $i \in \{u, e\}$, where u refers to the user and e marks the eavesdropper. We will also call the i-th link the wireless link between the plant and the agent i.

B. Wireless link

Let $\hat{y}_i(k)$ denote the measurement received by the agent i at time $k \in \mathbb{N}$. The general model for the agent's link is

$$\hat{y}_i(k) = \begin{cases} \hat{y}(k) & \text{if } \xi_i(k) = 1 \\ \epsilon & \text{if } \xi_i(k) = 0 \end{cases} \quad \forall k \geq 0, \tag{3}$$

where ϵ means no information. The i-th link is modeled exploiting the mathematical abstraction provided by the finite-state Markov channel (FSMC). The packet arrival process on the i-th link is described by the process $\xi_i(k)$, $k \in \mathbb{N}$: its value is $\xi_i(k) = 0$ if the packet is lost, $\xi_i(k) = 1$ if the packet is correctly delivered. The process $\xi_i(k)$ is a binary random variable and the probability of having a packet loss or a correct packet transmission over the link i depends on the SINR. The SINR is determined by physical phenomena and model parameters (see [21]) such as path loss, shadow fading, interference and also the nature of the environment (domestic or industrial). SINR is a stochastic process and can be approximated by a finite state MC, denoted as $\eta_i(k)$. Let $\mathbb{S} \triangleq \{1, \ldots, N\}$ be the index set of the Markov modes, then $\eta_i(k) \in \{s_{i,m}\}_{m \in \mathbb{S}}$ (see [21]). Each agent i estimates the SINR process during a learning phase and thus, it knows the number of modes, the transition probabilities, and the probability distribution of the MC η_i. For each mode of $\eta_i(k)$, the value of $\xi_i(k)$ can be either zero or one with certain probabilities. For $m \in \mathbb{S}$, let the variable $\hat{\gamma}_{i,m}$ denote the probability that $\xi_i(k) = 1$, given the mode of the MC $\eta_i(k)$ for $k \in \mathbb{N}$,

$$\begin{aligned} &\mathbb{P}\left(\xi_i(k) = 1 \mid \eta_i(k) = s_{i,m}\right) = \hat{\gamma}_{i,m}, \\ &\mathbb{P}\left(\xi_i(k) = 0 \mid \eta_i(k) = s_{i,m}\right) = 1 - \hat{\gamma}_{i,m}. \end{aligned}$$

When a packet loss on the i-th link has occurred or the secrecy mechanism has withheld the output information, the agent i interprets the system state message as lost. Specifically, based on error detection and correction mechanisms the receiver decides whether the packet is ϵ and should be dropped. For most communication protocols receiver also performs SINR estimation for each received packet and thus the agent i always knows the mode of the i-th link $\eta_i(k)$. From (2)-(3) the received measurement $\hat{y}_i(k)$ is different from ϵ if and only if $\nu(k)\xi_i(k) = 1$. We define the variable $\varphi_i(k) \triangleq \nu(k)\xi_i(k)$. For $i \in \{u, e\}$, $m \in \mathbb{S}$,

$$\begin{aligned} &\mathbb{P}\left(\varphi_i(k) = 1 | \eta_i(k) = s_{i,m}\right) = \lambda\hat{\gamma}_{i,m}, \\ &\mathbb{P}\left(\varphi_i(k) = 0 | \eta_i(k) = s_{i,m}\right) = 1 - \lambda\hat{\gamma}_{i,m}. \end{aligned}$$

The information set available to the agent i at time $k \in \mathbb{N}$ is given by $\mathcal{F}_i(k) = \{(\hat{y}_i(t))_{t=0}^k, (\varphi_i(t))_{t=0}^k, (\eta_i(t))_{t=0}^k\}$.

Remark 1. *Observing the information set $\mathcal{F}_i(k)$ and recalling the definition of $\hat{y}_i(k)$ in* (3) *and the secrecy mechanism* (2), *it is straightforward to see that with the knowledge of $\hat{y}_i(k)$ and $\varphi_i(k)$, the agent i is aware of $y(k)$.*

C. Probabilistic framework

Let $\pi_{i,m}(k) \triangleq \mathbb{P}\left(\eta_i(k) = s_{i,m}\right)$, with $0 < \pi_{i,m}(k) < 1$, for any k, for $m \in \mathbb{S}$, $i \in \{u, e\}$. A Transition Probability Matrix (TPM) associated with the MC $\eta_i(k)$ is denoted by $P_i \triangleq [p_{i,mn}]_{m,n=1}^N$,

$$p_{i,mn} = \mathbb{P}\left(\eta_i(k+1) = s_{i,n} | \eta_i(k) = s_{i,m}\right), \sum_{n=1}^N p_{i,mn} = 1.$$

Similarly to [18, Sec. 5.3], we make the following technical assumptions (with $i \in \{u, e\}$ and $k \in \mathbb{N}$):

i) the initial conditions $x_0, \eta_{i,0}$ are independent random variables,

ii) the white noise sequences $\{w(k)\}$ and $\{v(k)\}$ are independent of the initial conditions $(x_0, \nu(0))$ and of the processes $\xi_i(k)$, for any discrete-time $k \in \mathbb{N}$,

iii) the MCs $\{\eta_i(k)\}$ and the noise sequences $\{w(k)\}$ and $\{v(k)\}$ are independent,

iv) the MCs $\{\eta_i(k)\}$ are ergodic, with steady state probability distributions $\pi_{i,m}^\infty = \lim_{k \to \infty} \pi_{i,m}(k)$, $m \in \mathbb{S}$.

This work aims to design an estimator of the class of mean square Markov jump filters (see [18, Ch.5.3]) together with a secrecy mechanism, such that the user MSE remains bounded, while the eavesdropper MSE is unbounded. The formal guarantees of this secrecy notion can be found in Section III, see Definition 1. Here we introduce the variables ψ_i and ζ_i that will be useful for the statement and the proof of our main result. For $i \in \{u, e\}$, ψ_i denotes the average probability of intercepting a measurement on the i-th link when $\lambda = 1$, ζ_i is the average probability of intercepting a measurement for $\lambda \in [0, 1)$. Formally, $\psi_i \triangleq \sum_{m=1}^N \pi_{i,m}^\infty \hat{\gamma}_{i,m}$, $\zeta_i \triangleq \psi_i \lambda$.

III. Optimal mean square expected secrecy

We present the infinite horizon minimum mean square Markov jump filter (see [18, Ch.5.3] with the estimation technique provided by an estimator called current estimator [22, Ch. 8.2.4]). Specifically, the estimator provides at each step a model prediction obtained from the estimated state at the previous step. This prediction is corrected by the current measurement received $\hat{y}_i(k)$.

Remark 2. *It is well known that for the case in which the information on the output of the system and on the MC are available at each time step $k \in \mathbb{N}$, the best linear estimator of $x(k)$ is the Kalman filter (see [18, Remark 5.2]). An offline computation of the Kalman filter is inadvisable here as pointed out in [23]. The reason is that the solution of the difference Riccati equation and the time varying Kalman gain are sample path dependent and the number of sample paths grows exponentially in time. On the other hand, an online computation of the Kalman filter requires online matrix inversions which might require a lot of computation. For this reason, we consider a different class of estimators, for which we can pre-compute the filtering gains offline. This allows us to avoid online matrix inversions, thus, reducing the computational burden.*

Recalling that the agent i receives a quantity that is different from ϵ if and only if $\varphi_i(k) = 1$ (see Remark 1), the current estimated state dynamics can be written as follows (see also [22, eq. (8.33)-(8.34)]), for $i \in \{u, e\}$:

$$\hat{x}_i(k) = \overline{x}_i(k) - \varphi_i(k)\widehat{M}_{i,\eta_i(k)}\left[y(k) - L\overline{x}_i(k)\right], \quad (4)$$

$$\overline{x}_i(k+1) = A\hat{x}_i(k), \quad (5)$$

where $\widehat{M}_{i,\eta_i(k)}$ is the mode-dependent filtering gain, whose explicit expression can be found later in (9). Since the filtering gain depends on the mode of the MC at time k, and the MC has a given finite set of modes, it can be computed offline (see Remark 4). From (4)-(5), by defining the error as $\tilde{e}_i(k) = x(k) - \overline{x}_i(k)$, $i \in \{u, e\}$,

$$\begin{aligned}\tilde{e}_i(k+1) = \left(A + \varphi_i(k)A\widehat{M}_{i,\eta_i(k)}L\right)\tilde{e}_i(k) + w(k) \\ + \varphi_i(k)A\widehat{M}_{i,\eta_i(k)}v(k), \quad (6)\end{aligned}$$

see also [22, eq. (8.36)].

Remark 3. *The error system described by* (6) *is a discrete-time MJLS (see for instance [18]).*

The notation presented in [18] is adopted here: for $i \in \{u, e\}$, $m \in \mathbb{S}$, let us define $\mathbf{Z}_i(k) \triangleq [Z_{i,m}(k)]_{m=1}^{N} \in \mathbb{H}^{Nn_x,+}$,

$$Z_{i,m}(k) \triangleq \mathbb{E}\left[\tilde{e}_i(k)\tilde{e}_i^*(k)\mathbf{1}_{\{\eta_i(k)=s_{i,m}\}}\right],$$

with $\mathbf{1}_{\{\eta_i(k)=s_{i,m}\}}$ denoting the indicator function defined in the usual way.
The MSE can be written as follows (see for instance [18], [14]), $\mathbb{E}\left[\tilde{e}_i(k)\tilde{e}_i^*(k)\right] = \sum_{m=1}^{N} Z_{i,m}(k)$.
Given the MSE expression, we are ready to introduce the definition of optimal mean square expected secrecy over FSMCs.

Definition 1 (Secrecy over FSMCs). *Given the system described by* (1) *and the FSMCs* (3)*, we say that a secrecy mechanism* (2) *achieves optimal mean square expected secrecy over FSMCs if and only if, for any initial condition* $\mathbf{Z}_i(0) \in \mathbb{H}^{Nn_x,+}$, $i \in \{u, e\}$*, both of the following conditions hold:* $\lim_{k\to\infty} \mathbf{tr}\left\{\mathbb{E}\left[\tilde{e}_u(k)\tilde{e}_u^*(k)\right]\right\} < \infty$, $\lim_{k\to\infty} \mathbf{tr}\left\{\mathbb{E}\left[\tilde{e}_e(k)\tilde{e}_e^*(k)\right]\right\} = \infty$.

Assumption 2. *If the secrecy mechanism* $\hat{y}(k) = y(k)$ *is employed for all* $k \geq 0$*, i.e., when* $\lambda = \frac{\zeta_u}{\psi_u} = 1$*, the user MSE is bounded, i.e.,* $\lim_{k\to\infty} \mathbf{tr}\left\{\mathbb{E}\left[\tilde{e}_u(k)\tilde{e}_u^*(k)\right]\right\} < \infty$*, for any initial condition* $\mathbf{Z}_u(0) \in \mathbb{H}^{Nn_x,+}$.

The following operator is instrumental for the presentation of the Algebraic Riccati equation and for the technical results exploited in the proof of the main theorem. Let us define the operator $\mathcal{X}_\lambda : \mathbb{F}_+^{n_x \times n_x} \times \mathbb{R}^+ \times \mathbb{R}^+ \to \mathbb{F}_+^{n_x \times n_x}$, for $\lambda \in [0, 1]$, $X \in \mathbb{F}_+^{n_x \times n_x}$, $\alpha > 0$, $\phi \in \mathbb{R}^+$,

$$\begin{aligned}&\mathcal{X}_\lambda(X, \alpha, \phi) \triangleq (1 - \lambda\phi)\{AXA^* + \alpha Q\} + \\ &\lambda\phi\left(AXA^* + \alpha Q - AXL^*\left(LXL^* + \alpha R\right)^{-1}LXA^*\right). \quad (7)\end{aligned}$$

Proposition 1. *Consider the error system described by* (6)*. Under Assumption 2, for* $m, n \in \mathbb{S}$*,* $i \in \{u, e\}$*, the filtering coupled algebraic Riccati equations (CAREs) are*

$$Z_{i,n} = \sum_{m=1}^{N} p_{i,mn}\mathcal{X}_\lambda\left(Z_{i,m}, \pi_{i,m}^{\infty}, \hat{\gamma}_{i,m}\right), \quad (8)$$

$$\widehat{M}_{i,m} = -Z_{i,m}L^*\left(LZ_{i,m}L^* + \pi_{i,m}^{\infty}R\right)^{-1}. \quad (9)$$

Proof. See appendix. □

Remark 4. *The filtering gain can be computed offline from the minimization of the MSE, according to the procedure shown in [14]. Particularly, each agent i knows the matrices of the system, as well as the mode of the MCs* η_i*. Formally, for* $m \in \mathbb{S}$*, the filtering gain* $\widehat{M}_{i,m}$ *is given by* (9)*, where* $Z_{i,m}$ *is the solution of* (8).

IV. Main result

In this section we present necessary and sufficient conditions concerning the FSMCs probabilities such that optimal mean square expected secrecy is guaranteed.

Theorem 1. *Consider the system described by* (1)*, the secrecy mechanism given by* (2)*, and FSMCs described by* (3)*. Under Assumption 1 and Assumption 2, the secrecy mechanism achieves optimal mean square expected secrecy over FSMCs if and only if* $\psi_u > \psi_e$.
In particular, there exists a probability $\zeta_c \in [0, 1)$ *such that optimal mean square expected secrecy is guaranteed if and only if the probability* λ *in the secrecy mechanism satisfies the following inequalities*

$$\frac{\zeta_c}{\psi_u} < \lambda \leq \min\left\{\frac{\zeta_c}{\psi_e}, 1\right\}.$$

Remark 5. *The inequality* $\psi_u > \psi_e$ *is a reasonable condition for secrecy in many cases of interest. Indeed, it is plausible that the propagation environment leads to an average probability of intercepting the measurement over the eavesdropper link,* ψ_e*, which is strictly less than* ψ_u*, for instance because the eavesdropper might be further away from the source.*

Proof. Let us show the sufficiency part. Consider for $n \in \mathbb{S}$, $i \in \{u, e\}$, $k \in \mathbb{N}$, the following equality,

$$Z_{i,n}(k+1) = \sum_{m=1}^{N} p_{i,mn}\mathcal{X}_\lambda\left(Z_{i,m}(k), \pi_{i,m}(k), \hat{\gamma}_{i,m}\right).$$

Under Assumption 2, if $\lim_{k\to\infty} \mathbf{tr}\left\{\mathbb{E}\left[\tilde{e}_e(k)\tilde{e}_e^*(k)\right]\right\} = +\infty$, we can choose $\lambda = 1$. Otherwise, since Assumptions 1-2 hold, by [24, Lemma 3], for any $\mathbf{Z}_0 \in \mathbb{H}^{Nn_x,+}$, $m, n \in \mathbb{S}$, $i \in \{u, e\}$,

$$\lim_{k\to\infty} \mathbf{tr}\left\{Z_{i,n}(k)\right\} = +\infty, \quad \text{for } 0 \leq \lambda \leq \frac{\zeta_c}{\psi_i}, \quad (10)$$

$$\lim_{k\to\infty} \mathbf{tr}\left\{Z_{i,n}(k)\right\} < \infty, \quad \text{for } \frac{\zeta_c}{\psi_i} < \lambda \leq 1. \quad (11)$$

This implies that the probability λ in the secrecy mechanism should be designed such that $\lambda > \zeta_c/\psi_u$, in order to guarantee (11) for the user MSE. Since the user MSE is bounded by assumption when $\lambda = 1$, $\psi_u \times 1 > \zeta_c$, and thus $\psi_u > \zeta_c$ implying $\zeta_c/\psi_u < 1$.

Consider now the eavesdropper MSE. The secrecy parameter λ should be chosen sufficiently small such that the inequality $\lambda \leq \zeta_c/\psi_e$ is satisfied. Therefore, by choosing λ satisfying the following inequalities, $\zeta_c/\psi_u < \lambda \leq \min\{\zeta_c/\psi_e, 1\}$, the secrecy mechanism guarantees optimal mean square expected secrecy over FSMCs by [24, Lemma 3].

Notice that the interval $(\zeta_c/\psi_u, \min\{\zeta_c/\psi_e, 1\}]$ is nonempty: $\zeta_c/\psi_u < 1$, and $\psi_u > \psi_e$ implies that $\zeta_c/\psi_u < \zeta_c/\psi_e$.

Let us show the necessity part. If the optimal mean square expected secrecy over FSMCs is achieved by the secrecy mechanism in (2), by [24, Lemma 3] $\zeta_c/\psi_u < \lambda \leq 1$ and $\lambda \leq \zeta_c/\psi_e$, implying $\zeta_c/\psi_u < \lambda \leq \zeta_c/\psi_e$.

Consequently, $\lambda\psi_e < \lambda\psi_u$, and finally $\psi_e < \psi_u$.

The proof of the theorem is complete. □

V. Eavesdropper characterization

Given the propagation environment, a designer can deduce possible positions of eavesdroppers, decide which are of the most concern, and derive an eavesdropper's TPM.

In this section, we provide link quality constraints used to design the secrecy mechanism attempting to increase the eavesdropper MSE to infinity. More specifically, if the eavesdropper TPM P_e is known, the designer is able to construct the matrix $\mathcal{A}_e$, defined as follows,

$$\mathcal{A}_e \triangleq \left[P_e' \otimes \mathbb{I}_{n_x^2}\right] \left[\bigoplus_{m=1}^{N} (1 - \lambda\hat{\gamma}_{e,m}) \left(\overline{A} \otimes A\right)\right].$$

For $\mathbf{V} = [V_m]_{m=1}^{N} \in \mathbb{H}^{Nn_x,*}$ define for $n \in \mathbb{S}$,

$$\mathcal{S}_{e,n}(\mathbf{V}) \triangleq \sum_{m=1}^{N} p_{e,mn} (1 - \lambda\hat{\gamma}_{e,m}) A V_m A^* + \pi_{e,n}^{\infty} Q.$$

As we prove in the next proposition, it turns out that the operator $\mathcal{S}_{e,n}$ defined above provides a lower bound to the eavesdropper MSE, under the estimator defined in (4). Hence, we can use the above recursion to test whether the eavesdropper has MSE that increases to infinity.

Proposition 2. Consider the system described by (1) *and the secrecy mechanism* (2). *The following statements hold, for* $n \in \mathbb{S}$,

- *If* $\rho(\mathcal{A}_e) < 1$, *then* $\lim_{k\to\infty} \mathbf{tr}\{Z_{e,n}(k)\} \geq \mathbf{tr}\{S_{e,n}\}$, *with* $S_{e,n} = \mathcal{S}_{e,n}(\mathbf{S}_e)$, $\mathbf{S}_e = [S_{e,n}]_{n=1}^{N} \in \mathbb{H}^{Nn_x,+}$.
- *If* $\rho(\mathcal{A}_e) \geq 1$, *then* $\lim_{k\to\infty} \mathbf{tr}\{Z_{e,n}(k)\} = +\infty$.

Proof. See appendix. □

VI. Example

This section examines an inverted pendulum on a cart [25] whose parameters are estimated remotely over a wireless link exposed to an eavesdropper. The considered cart's and pendulum's masses are 0.5 kg and 0.2 kg, inertia about the pendulum's mass center is $0.006\ \mathrm{kg} \cdot \mathrm{m}^2$, distance from the pivot to the pendulum's mass center is 0.3 m, coefficient of friction for the cart is 0.1. The discrete-time system has been obtained from discretization with sampling $T_s = 0.01$ s and linearization of the dynamical continuous time nonlinear model around the unstable equilibrium points $\mathrm{x}^* = 0$ m, $\phi^* = 0$ rad. The resulting matrix A of the discrete-time system is such that $\rho(A) \approx 1.1 > 1$. This unstable plant evolves in open-loop.

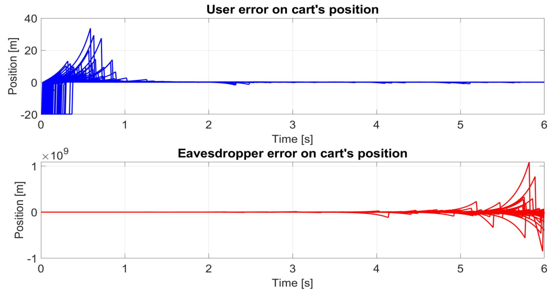

Fig. 2: Error trajectories on cart's position for the user (blue trajectories) and for the eavesdropper (red trajectories) obtained with $\lambda = 0.3$.

We recall that, when the propagation environment is known, a designer can deduce which are the possible eavesdropping configurations allowing to overhear the user's messages.

Consider two independent wireless links: one link for the user, the other one for the eavesdropper. The formal mathematical description of a propagation environment accounts for different parameters. The two main parameters we refer in this description are the transmitter/receiver couple and the transmitter/interferer couple: the transmitter/receiver couple is the couple of interest, while the transmitter/interferer couple models some interference that affects the propagation environment and that characterize both the user and the eavesdropper wireless link. Let d_u and d_e denote the distances of the couple of interest for the user and for the eavesdropper, respectively. Let $\tilde{d}_u$ and $\tilde{d}_e$ denote the distances of the couple transmitter/interferer for the user and for the eavesdropper, respectively.

Consider the following scenario (see [11], [13]): $d_u = 17$ m, $\tilde{d}_u = 15$ m, $d_e = 19$ m, $\tilde{d}_e = 13$ m. With this configuration for user and eavesdropper the secrecy parameter λ guaranteeing the optimal mean square expected secrecy over FSMCs belongs to the interval $(0.26, 0.48]$, and the limit probability $\zeta_c \approx 0.105$.

The results obtained in simulations are shown in Fig. 2 and in Fig. 3. Fig. 2 shows the error trajectories $\tilde{e}_i(k)$, $i \in \{u, e\}$, obtained from 1000 Montecarlo simulations for the user (blue lines) and the eavesdropper (red lines) with $\lambda = 0.3$. As the reader can see, the user error trajectories have a convergent behavior, while the eavesdropper error trajectories diverge. Consider now Fig. 3, that reports the eavesdropper MSE (red line) and the user MSE (blue line) on cart's position with $\lambda = 0.3$. The reader may notice that the eavesdropper MSE shows a worse behavior with respect to the user MSE: this is induced by the relation existing between the average probabilities of successfully receiving the system state message, ψ_e and ψ_u, over the

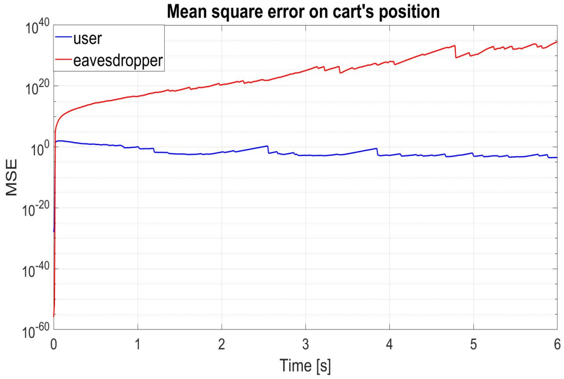

Fig. 3: The figure reports the MSE on cart's position for the user (blue line) and for the eavesdropper (red line) with $\lambda = 0.3$.

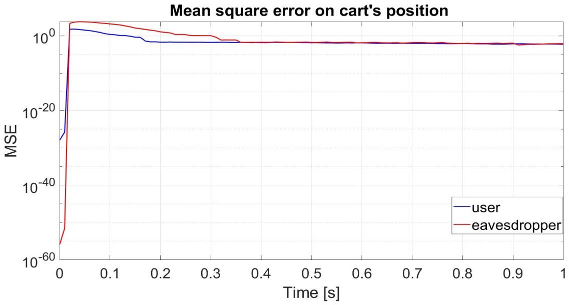

Fig. 4: The figure reports the MSE on cart's position for the user (blue line) and for the eavesdropper (red line) with $\lambda = 1$.

eavesdropper and the user link, respectively. Particularly, in the reported example $\psi_e = 0.219$, $\psi_u = 0.413$, and thus $\psi_e < \psi_u$, as required by Theorem 1. More specifically, by comparing Fig. 4 (obtained without a secrecy mechanism) and Fig. 3 (obtained with the proposed secrecy mechanism), the reader may notice that the secrecy mechanism makes the eavesdropper MSE go to infinity, while the user MSE remains bounded (see Fig. 3).

VII. Conclusion

In this paper we considered secure state estimation over Markov wireless communication channels. We bring the secrecy notion in [10] to FSMCs, which requires re-definition of estimation problem and a novel technical procedure for deriving the secrecy conditions. Moreover, we design a secrecy mechanism satisfying the described formal requirements over FSMCs, and we show the effectiveness of our result in the example of an inverted pendulum on a cart whose parameters are estimated remotely over a wireless link exposed to an eavesdropper.

References

[1] P. Park, S. Coleri Ergen, C. Fischione, C. Lu, and K. H. Johansson, "Wireless network design for control systems: A survey," *IEEE Commun. Surv. Tut.*, vol. 20, no. 2, pp. 978–1013, 2018.

[2] C. Lu, A. Saifullah, B. Li, M. Sha, H. Gonzalez, D. Gunatilaka, C. Wu, L. Nie, and Y. Chen, "Real-time wireless sensor-actuator networks for industrial cyber-physical systems," *IEEE Proc.*, vol. 104, no. 5, pp. 1013–1024, 2015.

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

[4] A. S. Leong, D. E. Quevedo, and S. Dey, "State estimation over markovian packet dropping links in the presence of an eavesdropper," in *IEEE 56th CDC*, 2017, pp. 6616–6621.

[5] M. S. Chong, H. Sandberg, and A. M. Teixeira, "A tutorial introduction to security and privacy for cyber-physical systems," in *18th ECC*, 2019, pp. 968–978.

[6] M. Schulze Darup, A. B. Alexandru, D. E. Quevedo, and G. J. Pappas, "Encrypted control for networked systems: An illustrative introduction and current challenges," *IEEE Contr. Syst. Mag.*, vol. 41, no. 3, pp. 58–78, 2021.

[7] A. B. Alexandru, A. Tsiamis, and G. J. Pappas, "Encrypted distributed lasso for sparse data predictive control," in *60th IEEE CDC*, 2021, pp. 4901–4906.

[8] A. S. Leong, D. E. Quevedo, D. Dolz, and S. Dey, "Transmission scheduling for remote state estimation over packet dropping links in the presence of an eavesdropper," *IEEE TAC*, vol. 64, no. 9, pp. 3732–3739, 2019.

[9] A. Tsiamis, K. Gatsis, and G. J. Pappas, "State-secrecy codes for networked linear systems," *IEEE TAC*, vol. 65, no. 5, pp. 2001–2015, 2020.

[10] ——, "State estimation with secrecy against eavesdroppers," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 8385–8392, 2017.

[11] P. Sadeghi, R. A. Kennedy, P. B. Rapajic, and R. Shams, "Finite-state Markov modeling of fading channels - a survey of principles and applications," *IEEE Signal Process. Mag.*, vol. 25, no. 5, pp. 57–80, 2008.

[12] A. Impicciatore, A. D'Innocenzo, and P. Pepe, "Sufficient Lyapunov conditions for *p*th moment ISS of discrete-time Markovian Switching Systems," in *Proc. IEEE 59th Conf. Decision Control (CDC)*. IEEE, Dec. 2020.

[13] Y. Zacchia Lun and A. D'Innocenzo, "Stabilizability of Markov jump linear systems modeling wireless networked control scenarios," *IEEE 58th CDC*, pp. 5766–5772, 2019.

[14] A. Impicciatore, Y. Zacchia Lun, P. Pepe, and A. D'Innocenzo, "Optimal output-feedback control and separation principle for Markov jump linear systems modeling wireless networked control scenarios," in *2021 ACC*, 2021, pp. 2700–2706.

[15] V. De Iuliis, A. D'Innocenzo, A. Germani, and C. Manes, "Stability conditions for linear discrete-time switched systems in block companion form," *IET Control Theory & Applications*, vol. 14, no. 19, pp. 3107–3115, 2020.

[16] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, and S. S. Sastry, "Foundations of Control and Estimation Over Lossy Networks," *Proc. IEEE*, vol. 95, no. 1, pp. 163–187, 2007.

[17] Y. Mo, E. Garone, and B. Sinopoli, "LQG control with Markovian packet loss," *ECC*, pp. 2380–2385, 2013.

[18] O. L. V. Costa, M. D. Fragoso, and R. P. Marques, "Discrete-Time Markov Jump Linear Systems," NY:Springer, New York, 2005.

[19] J. W. Brewer, "Kronecker products and matrix calculus in system theory," *IEEE Trans. Circuits Syst.*, vol. 25, no. 9, pp. 772–781, 1978.

[20] B. Sinopoli, L. Schenato, M. Franceschetti, K. Poolla, M. Jordan, and S. Sastry, "Kalman filtering with intermittent observations," *IEEE TAC*, vol. 49, no. 9, pp. 1453–1464, 2004.

[21] Y. Zacchia Lun, C. Rinaldi, A. D'Innocenzo, and F. Santucci, "On the impact of accurate radio link modeling on the performance of WirelessHART control networks," *39th IEEE INFOCOM*, pp. 2430–2439, 2020.

[22] G. F. Franklin, J. D. Powell, and M. L. Workman, *Digital Control of Dynamic Systems*, 3rd ed. Addison-Wesley, 1997.

[23] Y. Ji and H. J. Chizeck, "Jump linear quadratic gaussian control : Steady-state solution and testable conditions," 1990.

[24] A. Impicciatore, A. Tsiamis, Y. Zacchia Lun, A. D'Innocenzo, and G. J. Pappas, "Secure state estimation over Markov wireless communication channels (extended version)," 2022. [Online]. Available: http://arxiv.org/abs/2209.05146

[25] G. F. Franklin, J. D. Powell, and A. Emami-Naeini, *Feedback control of dynamic systems*, 6th ed. Prentice Hall: Prentice Hall, 2009.