<http://www.diva-portal.org>

Postprint

This is the accepted version of a paper presented at *55th IEEE Conference on Decision and Control, CDC 2016, ARIA Resort and Casino, Las Vegas, United States, 12 December 2016 through 14 December 2016*.

Citation for the original published paper:

Wiese, M., Johansson, K H., Oechtering, T J., Papadimitratos, P., Sandberg, H. et al. (2016)

Secure Estimation for Unstable Systems

In: *2016 IEEE 55th Conference on Decision and Control, CDC 2016*, 7799043 (pp. 5059-5064). Institute of Electrical and Electronics Engineers (IEEE)

IEEE Conference on Decision and Control

<https://doi.org/10.1109/CDC.2016.7799043>

N.B. When citing this work, cite the original published paper.

Permanent link to this version:

<http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-208568>

Secure Estimation for Unstable Systems

Moritz Wiese, Karl Henrik Johansson, Tobias J. Oechtering,
Panos Papadimitratos, Henrik Sandberg, Mikael Skoglund

Abstract—It is shown that instability of a system enables secure remote estimation. More precisely, suppose that an estimator obtains information about a system with uncertain initial state and/or disturbances through an uncertain wiretap channel. This means that both the estimator and an eavesdropper obtain their own (and in general different) uncertain versions of the channel inputs. If the zero-error secrecy capacity of the uncertain wiretap channel is large enough to track the dynamics of the system, then the estimator’s error can be bounded uniformly. Moreover, the instability of the system then permits that the volume of the set of states possible according to the eavesdropper’s information tends to infinity at exponential speed—either by itself (strong secrecy) or if divided by the volume of the set of states possible according to the estimator’s information (weak secrecy).

I. INTRODUCTION

With the increasing deployment and growing importance of cyber-physical systems, the question of their security has recently become a focus of research activity in control theory [1]. One central vulnerability of networked control or estimation is the communication channel between plant and controller/estimator and possibly the feedback channel from the controller to the plant. One type of attack on the channels is to actively interfere with transmitted information with the goal of degrading the control or estimation performance (e. g. [2], [3], [4], [5], [6]).

However, remote estimation of an unstable plant also entails the possibility of eavesdropping. An adversary might have the chance to overhear the transmitted information and to obtain its own system estimate. This paper addresses the question of what can be done to protect the transmitted information from such an attacker. It will turn out that the system’s instability actually helps to achieve security.

We consider plant noise which consists of arbitrary bounded disturbances, as is common in robust control. Then path-wise state estimation becomes a natural requirement. Path-wise state estimation means that the estimation error should be bounded along every path the system could possibly take. It was shown by Matveev and Savkin [7] that if a Discrete Memoryless Channel (DMC) is used for transmitting system information to the estimator, the zero-error capacity of this DMC has to exceed the sum of the logarithms of the plant’s unstable eigenvalues for path-wise estimation to be possible.

The zero-error capacity of a DMC [8], [9] is defined in terms of the number of messages which can be sent over the

Fig. 1. The problem setup. The pair $(\mathbf{T}_B, \mathbf{T}_C)$ of uncertain channels forms an uncertain wiretap channel.

channel with a strictly vanishing error probability. For DMCs as simple as the binary symmetric channel with crossing probability strictly between zero and one and the binary erasure channel with positive erasure probability, their zero-error capacity vanishes. It is a much stronger criterion than the classical Shannon capacity [10].

The zero-error capacity of a DMC only depends on which outputs can be generated by which inputs with positive probability, but not on the actual values of these probabilities. Thus every DMC induces what Nair [11] calls an *uncertain channel*, which can be regarded as a bipartite graph linking every channel input to those outputs which can be reached from this given input. In [11], this channel concept was applied to simplify the proof of the result of [7] in the case of nonstochastic arbitrary plant disturbances.

The present paper adapts Nair’s framework of bounded, nonstochastic plant disturbances (restricted to the scalar case) and uncertain channels. The basic problem setup is the same as in the authors’ previous work [12]. The estimator’s goal is path-wise state estimation. It is assumed that the quantized state is transmitted to the estimator from an encoder placed at the plant through an uncertain channel $\mathbf{T}_B$. Moreover, an eavesdropper obtains information about the sender’s channel input through another uncertain channel $\mathbf{T}_C$. This pair of uncertain channels constitutes an *uncertain wiretap channel*. In addition to state estimation, in [12] the encoder’s goal is to make the diameter of the set of states which are possible according to the eavesdropper’s information tend to infinity. If this goal is met, the eavesdropper’s estimation error is unbounded for every possible path no matter what estimation strategy it applies.

In [12] it was shown that surprisingly, the zero-error secrecy capacity $C_0(\mathbf{T}_B, \mathbf{T}_C)$ of the uncertain wiretap channel $(\mathbf{T}_B, \mathbf{T}_C)$ only has to be positive in addition to the requirement that the zero-error capacity $C_0(\mathbf{T}_B)$ of $\mathbf{T}_B$ be larger than the logarithm of the system’s unstable pole for secure estimation to be possible.

In the present paper, the security requirements are

The authors are with the ACCESS Linnaeus Centre, KTH Royal Institute of Technology, SE-10044 Stockholm, Sweden {moritzw, kallej, oech, papadim, hsan, skoglund}@kth.se

strengthened. Now the volume of the set of system states which are possible according to the eavesdropper's information should tend to infinity at exponential speed, at least if divided by the volume of the set of system states which are possible according to the estimator's information. In the former case, we call the security achieved *strong security*, in the latter case *weak security*.

We show in the case that the zero-error secrecy capacity $C_0(\mathbf{T}_B, \mathbf{T}_C)$ strictly exceeds the logarithm of the unstable pole of the plant, then weak or even strong security is achievable. The proposed scheme uses the fact that every output of the eavesdropper channel can be generated by multiple messages. If only the initial state is uncertain, it then suffices to count the number of message sequences that are candidates for being the true one according to the eavesdropper's information. The main difficulty in the case of system noise is that the quantizer does not partition the state space. At every point in time, the quantizer only partitions the set of states which are possible given the history so far. For different histories, the quantizing sets can overlap. Therefore it is not sufficient to just count the number of messages the eavesdropper confuses, as the corresponding volumes do not add up. However, by exploiting the instability of the plant, a sufficient number of message sequences can be found that are possible according to the eavesdropper's view for which the corresponding quantizing intervals do not intersect.

The outline of this paper is as follows. In Section II, the problem setup is defined and zero-error wiretap codes are defined. Section III gives the main results. It also describes the applied transmission schemes and proofs of the main theorems, together with an outline of the analysis behind these proofs. The main body of the paper closes with a short discussion section. The appendix on pages 7 and 8 contains the proofs of some technical lemmas.

Notation: For a real number x we define its *positive part* $|x|_+$ to equal x if $x \geq 0$ and 0 else. Logarithms are to the base 2. Given two sets $A, B \subset \mathbb{R}$ and a number λ , we define

$$\lambda A + B := \{c \in \mathbb{R} : c = \lambda a + b \text{ for some } a \in A, b \in B\}.$$

II. REMOTE ESTIMATION AND UNCERTAIN CHANNELS

Let $\lambda > 0$ and consider the unstable system

$$x(t+1) = \lambda x(t) + w(t). \quad (1)$$

The disturbance $w(t)$ is unknown a priori and can assume any value in the interval $[-\Omega/2, \Omega/2]$ for some $\Omega \geq 0$. The initial state $x(0)$ can attain any value in the bounded interval I_0 and is also unknown a priori.

An encoder quantizes and encodes the system state into a codeword. This codeword is sent to the estimator through the uncertain channel $\mathbf{T}_B$, where the estimator decodes and calculates an estimate. An eavesdropper obtains information about the codeword through the uncertain channel $\mathbf{T}_C$, see Fig. 1.

Definition 1: 1) An *uncertain channel* is a mapping $\mathbf{T} : \mathbf{A} \rightarrow 2_{*}^{\mathbf{B}}$, where $\mathbf{A}, \mathbf{B}$ denote arbitrary alphabets and $2_{*}^{\mathbf{B}}$ is the power set of $\mathbf{B}$ without the empty set.

Fig. 2. An uncertain wiretap channel. A line between a_i and b_j indicates that $b_j \in \mathbf{T}_B(a_i)$, similar for a_i and c_j .

- 2) An *uncertain wiretap channel* is a pair $(\mathbf{T}_B, \mathbf{T}_C)$ of uncertain channels, where $\mathbf{A}, \mathbf{B}, \mathbf{C}$ are finite alphabets and $\mathbf{T}_B : \mathbf{A} \rightarrow 2_{*}^{\mathbf{B}}$ and $\mathbf{T}_C : \mathbf{A} \rightarrow 2_{*}^{\mathbf{C}}$.

The reason why we only allow uncertain wiretap channels with finite alphabets is to exclude pathological cases. We define uncertain channels for general alphabets because we will eventually also define the quantization of the system states as an uncertain channel, where the input alphabet obviously is infinite.

For every input $a \in \mathbf{A}$, the uncertain channel $\mathbf{T}$ generates a nonempty set $\mathbf{T}(a)$ of possible outputs. These outputs are not weighted according to any probabilities. For every stochastic DMC one obtains an induced uncertain channel by mapping every channel input $a \in \mathbf{A}$ to the set of outputs $b \in \mathbf{B}$ which are the outputs of the DMC with positive probability given that a was input.

Note that every mapping $g : \mathbf{A} \rightarrow \mathbf{B}$ can be regarded as an uncertain channel each of whose output sets is a singleton. We also write

$$\text{ran}(\mathbf{T}) := \bigcup_{a \in \mathbf{A}} \mathbf{T}(a)$$

for the set of outputs of $\mathbf{T}$ which can be generated by $\mathbf{T}$. Given two uncertain channels $\mathbf{F} : \mathbf{M} \rightarrow 2_{*}^{\mathbf{A}}$ and $\mathbf{T} : \mathbf{A} \rightarrow 2_{*}^{\mathbf{B}}$, we define the concatenation $\mathbf{T} \circ \mathbf{F} : \mathbf{M} \rightarrow 2_{*}^{\mathbf{B}}$ of $\mathbf{F}$ and $\mathbf{T}$ by the rule

$$(\mathbf{T} \circ \mathbf{F})(m) := \mathbf{T}(\mathbf{F}(m)) := \bigcup_{a \in \mathbf{F}(m)} \mathbf{T}(a),$$

for every $m \in \mathbf{M}$.

If a sequence $a(0 : n-1)$ is to be transmitted over n time slots, where at each time i with $0 \leq i \leq n-1$, a different channel $\mathbf{T}_i$ is used, we define the set of possible outputs to be

$$\begin{aligned} &(\mathbf{T}_0 \times \dots \times \mathbf{T}_{n-1})(a(0 : n-1)) \\ &:= \mathbf{T}_0(a(0)) \times \dots \times \mathbf{T}_{n-1}(a(n-1)). \end{aligned} \quad (2)$$

$\mathbf{T}_0 \times \dots \times \mathbf{T}_{n-1} : \mathbf{A}^n \rightarrow 2_{*}^{\mathbf{B}^n}$ is an uncertain channel as well. If $\mathbf{T}_0 = \dots = \mathbf{T}_{n-1}$, then we write $\mathbf{T}^n := \mathbf{T}_0 \times \dots \times \mathbf{T}_{n-1}$. Property (2) implies that channel inputs at different times do not influence the outputs at other times.

An uncertain wiretap channel $(\mathbf{T}_B, \mathbf{T}_C)$ is shown in Fig. 2. It is interpreted in such a way that every channel input generates two outputs. The receiver of $\mathbf{T}_B$ should

be able to decode the transmitted information, whereas the eavesdropper which listens on channel $\mathbf{T}_C$ should obtain as little information as possible. We say that an output sequence $b(0 : n-1)$ of $\mathbf{T}_B^n$ and an output sequence $c(0 : n-1)$ of $\mathbf{T}_C^n$ are *compatible* if there exists an $a(0 : n-1) \in \mathbf{A}^n$ such that $b(0 : n-1) \in \mathbf{T}_B^n(a(0 : n-1))$ and $c(0 : n-1) \in \mathbf{T}_C^n(a(0 : n-1))$.

Next we describe how $\mathbf{T}_B$ is used to convey information about the system states to the estimator. We assume that for each step of the plant evolution, the channel can be used exactly once.

Definition 2: A *transmission scheme* is a sequence of triples $(n_k, f_k, \varphi_k)_{k=0}^\infty$, where $(n_k)_{k=0}^\infty \in \ell^\infty$ is a bounded sequence of positive integers and, setting $t_0 = 0$ and $t_k := n_0 + \dots + n_{k-1}$, for every $k \geq 0$

- the k -th encoder $f_k : \mathbb{R}^{t_k} \rightarrow 2_{*}^{\mathbf{A}^{n_k}}$ is an uncertain channel,
- the k -th decoder $\varphi_k : \mathbf{B}^{t_{k+1}} \rightarrow \mathbb{R}^{n_k}$ is an ordinary mapping.

f_k takes the system path until time t_k as input and maps this into a codeword of length n_k . We allow uncertain mappings for two reasons. One is that we do not have to distinguish between open and closed quantizing sets—if a path or state is on the boundary, we make an uncertain decision. The more important reason is that uncertain encoding has to be allowed in order for uncertain wiretap channels to achieve capacity [12]. The decoder φ_k takes the first t_{k+1} outputs of $\mathbf{T}_B$ and calculates an estimate of the states $x(t_{k-1}+1), \dots, x(t_k)$ (where we set $t_{-1} = -1$), which have not been estimated before. For example, the transmission of the codeword $f_0(x(0))$ of length n_0 generates an output sequence of length $n_0 = t_1$. When we define the performance criterion for a transmission scheme, it will be seen that by not allowing φ_k to be an uncertain channel we do not lose generality.

The minimal delay that has to be tolerated is $\max_k n_k$. With this delay, the receiver has good estimates for the states $x(t_k)$ but has to extrapolate for the states $x(t_k+1), \dots, x(t_{k+1}-1)$. A delay of $2 \max_k n_k$ would allow for interpolation and could possibly lead to a better estimate of $x(t_k+1), \dots, x(t_{k+1}-1)$. In any case, the estimation error will be bounded if it is bounded for the states at times t_k for all k . This will be sufficient for the purpose of this paper.

A transmission scheme only defines a decoder at the output of the estimator's channel $\mathbf{T}_B$. But every system path $x(0 : \infty)$ also generates a sequence $c(0 : \infty)$ of eavesdropper outputs. The security criterion will be such that transmitted information has to be secure no matter which decoding strategy the eavesdropper applies.

The performance of a transmission scheme $(n_k, f_k, \varphi_k)_{k=0}^\infty$ is measured by two criteria: *reliability* and (*weak* or *strong*) *security*. We now introduce the notation which is necessary to define these concepts.

Given a transmission scheme $(n_k, f_k, \varphi_k)_{k=0}^\infty$ and a sequence of channel outputs $b(0 : t_{k+1}-1) \in \mathbf{B}^{t_{k+1}}$, we write $\tilde{\mathbf{R}}_B^{(t_{k+1})}(b(0 : t_{k+1}-1))$ for the set of system paths $x(0 : t_k)$ which could have generated $b(0 : t_{k+1}-1)$, i.e., those paths

for which

$$(\mathbf{T}_B^{n_i} \circ f_i)(x(0 : t_i)) = b(t_i : t_{i+1}-1)$$

with $0 \leq i \leq k$. Further, for any $k \geq 0$, any $b(0 : t_{k+1}-1)$ and any $0 \leq s \leq t_k$, we set

$$\begin{aligned} \tilde{\mathbf{R}}_B^{(t_{k+1})}(b(0 : t_{k+1}-1))|_s \\ := \{x(s) : x(0 : t_k) \in \tilde{\mathbf{R}}_B^{(t_{k+1})}(b(0 : t_{k+1}-1))\}. \end{aligned}$$

Similarly, we define $\tilde{\mathbf{R}}_C^{(t_{k+1})}(c(0 : t_{k+1}-1))$ and $\tilde{\mathbf{R}}_C^{(t_{k+1})}(c(0 : t_{k+1}-1))|_s$.

Finally, for a set $S \subset \mathbb{R}$, we define $\text{vol}(S)$ to be the Lebesgue measure of S and $\text{diam}(S)$ to be the diameter of S , i.e., $\text{diam}(S) = \sup\{|s-s'| : s, s' \in S\}$.

Definition 3: 1) A transmission scheme $(n_k, f_k, \varphi_k)_{k=0}^\infty$ is called *reliable* if there exists a constant $\varrho \in [0, \infty)$ such that the two following properties are satisfied:

- a) $\text{diam}(\tilde{\mathbf{R}}_B^{(t_{k+1})}(b(0 : t_{k+1}-1))|_s) \leq \varrho$ for every $k \geq 0$, every $b(0 : t_{k+1}-1)$ and $0 \leq s \leq t_k$,
- b) the s -th component of $\varphi_k(b(0 : t_{k+1}-1))$ is contained in $\tilde{\mathbf{R}}_B^{(t_{k+1})}(b(0 : t_{k+1}-1))|_{t_{k-1}+s}$ for every $k \geq 0$ and $1 \leq s \leq n_k$.

- 2) For $\sigma > 0$, a transmission scheme $(n_k, f_k, \varphi_k)_{k=0}^\infty$ is called σ -*weakly secure* if there exists a $\tau > 0$ such that for sufficiently large k , all output sequences $b(0 : t_{k+1}-1) \in \text{ran}(\mathbf{T}_B^{t_{k+1}} \circ (f_0 \times \dots \times f_k))$ and every $c(0 : t_{k+1}-1) \in \mathbf{C}^{t_{k+1}}$ which is compatible with $b(0 : t_{k+1}-1)$,

$$\frac{\text{vol}(\tilde{\mathbf{R}}_C^{(t_{k+1})}(c(0 : t_{k+1}-1))|_{t_k})}{\text{vol}(\tilde{\mathbf{R}}_B^{(t_{k+1})}(b(0 : t_{k+1}-1))|_{t_k})} \geq \tau \cdot 2^{\sigma t_k}.$$

- 3) For $\sigma > 0$, a transmission scheme $(n_k, f_k, \varphi_k)_{k=0}^\infty$ is called σ -*strongly secure* if there exists a $\tau > 0$ such that for sufficiently large k and for all eavesdropper output sequences $c(0 : t_{k+1}-1) \in \text{ran}(\mathbf{T}_C^{t_{k+1}} \circ (f_0 \times \dots \times f_k))$,

$$\text{vol}(\tilde{\mathbf{R}}_C^{(t_{k+1})}(c(0 : t_{k+1}-1))|_{t_k}) \geq \tau \cdot 2^{\sigma t_k}.$$

The reason why the definition of reliability is split into two parts is that what has to be controlled is the diameter of the set of possible states, which is condition 1a). Condition 1b) mainly ensures that the estimation error does not exceed the diameter of this set.

The terms “weak” and “strong” are justified in combination with reliability. If the volume of the estimator's set tended to infinity, “weak security” would actually be a stronger requirement than “strong security”.

Our goal is to relate the existence of a transmission scheme which is both reliable and (weakly or strongly) secure to the secrecy capacity $C_0(\mathbf{T}_B, \mathbf{T}_C)$ of the uncertain wiretap channel $(\mathbf{T}_B, \mathbf{T}_C)$. This was introduced in [12] and will be defined next.

Definition 4: A *zero-error wiretap* (n, M) -code for $(\mathbf{T}_B, \mathbf{T}_C)$ is an uncertain channel $\mathbf{F} : \{1, \dots, M\} \rightarrow 2_{*}^{\mathbf{A}^n}$ satisfying

- 1) $\mathbf{T}_B^n(\mathbf{F}(m)) \cap \mathbf{T}_B^n(\mathbf{F}(m')) = \emptyset$ for all $m, m' \in \{1, \dots, M\}$ with $m \neq m'$,
- 2) for every $c(0 : n-1) \in \text{ran}(\mathbf{T}_C^n \circ \mathbf{F})$ there exist messages $m, m' \in \{1, \dots, M\}$ such that $m \neq m'$ and $c(0 : n-1) \in \mathbf{T}_C^n(\mathbf{F}(m)) \cap \mathbf{T}_C^n(\mathbf{F}(m'))$.

Definition 5: For $n \geq 1$, let $N(n)$ be the maximal M for which there exists a zero-error wiretap (n, M) -code for $(\mathbf{T}_B, \mathbf{T}_C)$. The number

$$C_0(\mathbf{T}_B, \mathbf{T}_C) := \sup_n \frac{N(n)}{n}$$

is then called the *zero-error secrecy capacity* of $(\mathbf{T}_B, \mathbf{T}_C)$.

By the superadditivity of the sequence $N(0 : \infty)$ and Fekete's lemma ([13], see also [14]), the supremum in the definition of $C_0(\mathbf{T}_B, \mathbf{T}_C)$ can be replaced by $\lim_{n \rightarrow \infty}$.

When zero-error wiretap codes are applied in the construction of secure transmission schemes, the achievable degree of security also depends on how many messages can possibly generate a given eavesdropper channel output.

Definition 6: An (n, M, ζ) -code is an (n, M) -code $\mathbf{F}$ where for every $c(0 : n-1) \in \text{ran}(\mathbf{T}_C \circ \mathbf{F})$,

$$|\{m : c(0 : n-1) \in \mathbf{T}_C^n(\mathbf{F}(m))\}| \geq \zeta.$$

Obviously $\zeta \geq 2$. With an (n, M, ζ) -code, the eavesdropper has for each of its outputs at least ζ messages that could have generated this output. The interplay between M and ζ is crucial for our main results.

Definition 7: By $R_0(\mathbf{T}_B, \mathbf{T}_C)$ we denote the set of pairs (r, z) of nonnegative real numbers which satisfy that for every $\varepsilon > 0$ and sufficiently large n there exists an (n, M, ζ) -code with

$$\frac{\log M}{n} \geq r - \varepsilon, \quad \frac{\log \zeta}{n} \geq z - \varepsilon.$$

If we concatenate an (n, M, ζ) -code with itself to form a zero-error wiretap code of blocklength $2n$, note that this is a $(2n, M^2, \zeta^2)$ -code. Therefore it makes sense to consider the exponential growth rate of the maximal ζ as n tends to infinity, which is positive if $C_0(\mathbf{T}_B, \mathbf{T}_C) > 0$. The set $R_0(\mathbf{T}_B, \mathbf{T}_C)$ actually contains those pairs of growth rates which can be achieved jointly by M and ζ . As $M \geq \zeta$, its interior is nonempty, and to every positive $r < C_0(\mathbf{T}_B, \mathbf{T}_C)$ there exists a positive z with $(r, z) \in R_0(\mathbf{T}_B, \mathbf{T}_C)$.

III. MAIN RESULTS AND PROOFS

A. Main Results

Theorem 1: Assume that $\Omega = 0$ and $C_0(\mathbf{T}_B, \mathbf{T}_C) > \log \lambda$.

- 1) For every $(r, z) \in R_0(\mathbf{T}_B, \mathbf{T}_C)$ with $r > \log \lambda$ and $z > 0$ and every sufficiently small $\varepsilon > 0$ there exists a transmission scheme $(n_k, f_k, \varphi_k)_{k=0}^\infty$ which is reliable and $(z - \varepsilon)$ -weakly secure.
- 2) For every $(r, z) \in R_0(\mathbf{T}_B, \mathbf{T}_C)$ with $r > \log \lambda$ and $z > r - \log \lambda$ and every sufficiently small $\varepsilon > 0$, there exists a transmission scheme $(n_k, f_k, \varphi_k)_{k=0}^\infty$ which is reliable and $(z - r + \log \lambda - \varepsilon)$ -strongly secure.

Theorem 2: Assume that $\Omega > 0$ and $C_0(\mathbf{T}_B, \mathbf{T}_C) > \log \lambda$. For every $(r, z) \in R_0(\mathbf{T}_B, \mathbf{T}_C)$ with $r > \log \lambda$, define

$$\sigma := \frac{z \log \lambda}{r + 3 \log \lambda}.$$

Then for every $0 < \varepsilon < \sigma$ there exists a transmission scheme $(n_k, f_k, \varphi_k)_{k=0}^\infty$ which is reliable and $(\sigma - \varepsilon)$ -strongly secure.

The constant ϱ in the definition of reliability heavily depends on the channel and the delay. We can give good bounds for the estimates of the states at times $x(t_k)$. Depending on the delay, one has to extrapolate at times between those observation times. How large the inter-observation periods are depends on how long the blocklength of the zero-error wiretap codes has to be in order to achieve a sufficiently large rate.

B. Analysis Without Channel

In this subsection, we analyze the system under the assumption that an zero-error wiretap $(1, M, \zeta)$ -code exists. This does not have to be the case even if $C_0(\mathbf{T}_B, \mathbf{T}_C) > 0$, as was shown in [12], but it allows us to concentrate on the properties of the dynamical system. In Subsection III-C, the results of this subsection will be applied to codes with larger blocklengths and the correspondingly subsampled dynamical system to obtain Theorems 1 and 2.

We assume the existence of a $(1, M, \zeta)$ -code (obviously with $M \geq \zeta \geq 2$). Once we have defined a quantizer, we are ready to derive the main technical results on which the proofs of Theorems 1 and 2 are based. For every $t \geq -1$ and every sequence $m(0 : t) \in M^{t+1}$ (where we define $m(0 : -1)$ to be the empty word), we define $[A(m(0 : -1)), B(m(0 : -1))] := I_0$ and $\hat{x}(m(0 : -1))$ to be the mid point of I_0 . Then recursively for $t \geq 0$

$$P(m(0 : t)) := A(m(0 : t-1)) \tag{3}$$

$$+ \frac{B(m(0 : t-1)) - A(m(0 : t-1))}{M} [m(t) - 1, m(t)],$$

$$\hat{x}(m(0 : t)) := \text{mid point of } P(m(0 : t)), \tag{4}$$

$$[A(m(0 : t)), B(m(0 : t))] := \lambda P(m(0 : t)) + \left[-\frac{\Omega}{2}, \frac{\Omega}{2}\right]. \tag{5}$$

For every $t \geq 0$, the interval $[A(m(0 : t-1)), B(m(0 : t-1))]$ is the set of states $x(t)$ that are possible according to the quantizer index sequence $m(0 : t-1)$ generated by the system until time $t-1$. In other words, it represents the estimator's knowledge about $x(t)$ after receiving the messages $m(0), \dots, m(t-1)$ and before receiving $m(t)$. After reception of $m(t)$, the estimator knows that $x(t) \in P(m(0 : t))$. The estimate of $x(t)$ then is $\hat{x}(m(0 : t))$. Clearly, every path $x(0 : \infty)$ generates an infinite sequence $m(0 : \infty)$. Moreover, note that for every message sequence $m(0 : \infty)$ there exists a system path $x(0 : \infty)$ which generates $m(0 : \infty)$.

The following lemma from [12] takes care of the estimation error by bounding the length of the quantization intervals.

Lemma 1: For every $t \geq 0$ and $m(0:t) \in \{1, \dots, M\}^t$,

$$|P(m(0:t+1))| = \frac{\lambda}{M} |P(m(0:t))| + \frac{\Omega}{M}. \quad (6)$$

In particular,

$$|P(m(0:t))| = \frac{\Omega}{M-\lambda} + \left(\frac{\lambda}{M}\right)^t \left(\frac{|I_0|}{M} - \frac{\Omega}{M-\lambda}\right). \quad (7)$$

and $\sup_t |P(m(0:t))| < \infty$ if and only if $\lambda < M$. In that case

$$\sup_t |P(m(0:t))| = \max \left\{ \frac{|I_0|}{M}, \frac{\Omega}{M-\lambda} \right\}. \quad (8)$$

Henceforth, we will frequently just write $|P(m(0:t))|$ without specifying which $m(0:t)$ is meant. This is justified by the fact that $|P(m(0:t))|$ only depends on t , as shown in Lemma 1. Security in the case $\Omega = 0$ uses the following lemma.

Lemma 2: If $\Omega = 0$, then at each time $t \geq 0$, the interiors of the intervals $P(m(0:t))$ are disjoint, where $m(0:t)$ ranges over $\{1, \dots, M\}^{t+1}$.

Proof: See Appendix. ■

With the above quantizer, the estimator will in each time step t receive one message $m(t)$ and know that the true state is contained in $P(m(0:t))$. In contrast to this, according to the eavesdropper's information, at each time step at least ζ messages could be the true one. Thus after $t+1$ steps, there are ζ^{t+1} possible message paths $m(0:t)$. As the interiors of the corresponding quantizer sets are disjoint according to Lemma 2, the volume of the set of possible states according to the eavesdropper's information therefore is at least $\zeta^{t+1} |P(m(0:t))|$. This will provide weak security and, if ζ is large enough, also strong security.

To obtain security in the case of $\Omega > 0$ is more complicated. This is due to the fact that the disjointness of the quantizer intervals as proved above for the case $\Omega = 0$ breaks down for $\Omega > 0$.

Example 1: Let $\lambda = 2$, $\Omega = 2$, $I_0 = [-1, 1]$ and $M = 4$. Then $P(2) = [-\frac{1}{2}, 0]$ and $P(3) = [0, \frac{1}{2}]$. In the next step, one has

$$P(2, 3) = \left[-1\frac{1}{2}, -\frac{3}{4}\right], \quad P(3, 2) = \left[-1\frac{1}{4}, -\frac{1}{2}\right],$$

so $P(2, 3)$ and $P(3, 2)$ are not disjoint. The closer a state $x(t)$ is to the origin (and the larger t), the more paths there are which can be in this particular state at time t .

The above example shows that one can only hope to obtain disjoint quantizer sets for a subset of message sequences. For every $t \geq 0$ let $\mathcal{M}_t := \{m_{t,1} < m_{t,2} < \dots < m_{t,\zeta}\} \subset \{1, \dots, M\}$ (where the $\mathcal{M}_t$ may differ from $\mathcal{M}_{t'}$ for $t \neq t'$). Every eavesdropper channel output sequence $c(0:\infty)$ gives rise to such a sequence of message subsets due to the application of the $(1, M, \zeta)$ -code. Write $\Xi := \{1, \dots, \zeta\}$ and fix a $T \geq 1$. For $j \geq 1$ and $\xi(1:j) \in \Xi^j$, we define the message sequence $m_{\xi(1:j)}(0:jT-1)$ by

$$m_{\xi(1:j)}(s) = m_{\xi(i),s}$$

if $1 \leq i \leq j$ and $(i-1)T \leq s \leq iT-1$. All of these message sequences are candidates for being the true sequence

according to the eavesdropper's information. In addition, on the j -th block of components $(j-1)T, \dots, jT-1$, the sequences with the same history $m_{\xi(1:j-1)}(0:(j-1)T-1))$ are a componentwise ordered set of ζ message sequences. The corresponding quantizer intervals $P(m_{\xi(1:j)}(0:jT-1))$, where $\xi(j) \in \Xi$, will therefore diverge.

Lemma 3: Let $\Omega > 0$ and choose a $T \in \mathbb{N}$ satisfying

$$T \geq 2 + \frac{2 \log M}{\log \lambda} - \frac{\log(M-\lambda)}{\log \lambda}. \quad (9)$$

Then for every $j \geq 1$, the interiors of the sets $P(m_{\xi(1:j)}(0:jT-1))$, where $\xi(1:j)$ ranges over Ξ^j , are disjoint.

Proof: See Appendix. ■

The idea behind the proof of this lemma is twofold. First, one has to show that T is large enough such that the sets $P(m_{\xi(1:j-1)\xi}(0:jT-1))$ are disjoint for ξ ranging over Ξ . Second, one has to show that system paths starting in different $P(m_{\xi(1:j)}(0:jT-1))$ and $P(m_{\xi'(1:j)}(0:jT-1))$ never meet at later times. The two assertions together then provide the proof of Lemma 3.

C. Proof of the Theorems

We begin by describing the transmission schemes, which are common for the cases $\Omega = 0$ and $\Omega > 0$. Let $(r, z) \in R_0(\mathbf{T}_B, \mathbf{T}_C)$ with $r > \log \lambda$ and let $\varepsilon < r - \log \lambda$. For sufficiently large n there is then a zero-error wiretap (n, M, ζ) -code $\mathbf{F}$ with

$$M > 2^{n(r-\varepsilon)}, \quad \zeta > 2^{n(z-\varepsilon)}. \quad (10)$$

In particular, $M > \lambda^n$. We now consider the system

$$x^{(n)}(k+1) = \lambda^n x^{(n)}(k) + w^{(n)}(k), \quad x^{(n)}(0) \in I_0,$$

where the plant disturbances $w^{(n)}(k)$ may assume any value in the interval $[-\tilde{\Omega}^{(n)}/2, \tilde{\Omega}^{(n)}/2]$ with

$$\tilde{\Omega}^{(n)} = \frac{\Omega}{\lambda-1} (\lambda^n - 1).$$

This is the n -sampled version of our original dynamical system. Next we define a transmission scheme $(n_k, f_k, \varphi_k)_{k=0}^\infty$. We set $n_k = n$ for all $k \geq 0$. The encoders f_k are the concatenation of the quantizer with $\mathbf{F}$. More precisely, we first recursively define a sequence of uncertain quantizing channels $q_k^{(n)}: \mathbb{R}^{t_k} \rightarrow \{1, \dots, M\}$. We set

$$q_0^{(n)}(x(0)) := \{m(0) : x(0) \in P^{(n)}(m(0))\}.$$

For $k \geq 1$, we set

$$q_k^{(n)}(x(0:kn)) := \{m(k) : x(kn) \in P^{(n)}(m(0:k))\}$$

if $q_i^{(n)}(x(0:in)) = m(i)$, for $0 \leq i \leq k-1$. For most states, $q_k^{(n)}(x(kn))$ contains a single element, except for those $x(kn)$ which lie on the boundary between two neighboring quantizer intervals. Given a quantizer output, we just encode this output using the zero-error wiretap channel $\mathbf{F}$. Hence we can write

$$f_k(x(kn)) = \mathbf{F}(q_k^{(n)}(x(kn))).$$

At the receiving end, the decoder φ_k maps the received message $m(k)$ to the mid point $\hat{x}^{(n)}(k)$ of $P(m(0 : k))$ given the history $m(0 : k-1)$.

The encoded values are transmitted error-less to the estimator. According to Lemma 1, the diameter of the sets $P^{(n)}(m(0 : kn))$ is upper-bounded by

$$\max \left\{ \frac{\tilde{\Omega}^{(n)}}{M - \lambda^n}, \frac{|I_0|}{M} \right\} = \max \left\{ \frac{\Omega}{\lambda - 1} \frac{\lambda^n - 1}{M - \lambda^n}, \frac{|I_0|}{M} \right\}.$$

Thus our transmission scheme is reliable. Next we prove the security assertions.

Security for $\Omega = 0$: Hardly anything remains to be proved here. By Lemma 2, for given k , the interiors of all possible $P^{(n)}(m(0 : k))$ are disjoint. Assume the true message sequence equals $m(0 : k)$ and that the eavesdropper obtains the channel output sequence $c(0 : (k+1)n-1)$. For every $0 \leq i \leq k$ and every received output block $c(in : (i+1)n-1)$, as the encoder applies an (n, M, ζ) -code, there are at least ζ possible messages which could have generated this output sequence. Thus after time $(k+1)n-1$, the eavesdropper has at least ζ^{k+1} possible message sequences to choose from, and the state could be in one of ζ^{k+1} possible intervals of length $|P^{(n)}(m(0 : k))|$. Upon observing that $t_k = (k+1)n$, this provides $\log \zeta^{1/n}$ -weak security, and hence with (10) also $(z - \varepsilon)$ -weak security.

For strong security, observe that by Lemma 1

$$\zeta^{k+1} |P(m(0 : kn))| = \left(\frac{\zeta}{M} \lambda^n \right)^{k+1} \frac{|I_0|}{\lambda^n}.$$

This tends to infinity at exponential speed if $\zeta > M/\lambda^n$. Again observing that $t_k = (k+1)n$, strong security follows with the sigma claimed in the statement of Theorem 1 and constant $\tau := |I_0|/\lambda^n$.

Security for $\Omega > 0$: Define

$$T^{(n)} := 2 + \left\lceil \frac{2 \log M}{\log \lambda^n} - \frac{\log(M - \lambda^n)}{\log \lambda^n} \right\rceil.$$

$T^{(n)}$ satisfies the requirements for Lemma 3 to be valid for the n -sampled system. For a given eavesdropper output sequence $c(0 : jT^{(n)}n - 1)$, there are $\zeta^{jT^{(n)}}$ possible message sequences which could have generated this output sequence. Out of these, the ζ^j message sequences of the form $m_{\xi(1:j)}(0 : jT^{(n)} - 1)$ produce quantizing sets $P^{(n)}(m_{\xi(1:j)}(0 : jT^{(n)} - 1))$ with disjoint interiors. This gives $\zeta^{1/(nT^{(n)})}$ -strong security with constant

$$\tau := \inf_{j \geq 1} |P(m(0 : jT^{(n)}n - 1))| > 0.$$

Without loss of generality we may assume in addition to (10) that $M < 2^{nr}$. Given an arbitrary $\delta > 0$, if n is large enough, then $\log(M - \lambda^n) \geq \log r - \delta$. Thus

$$T^{(n)} \leq 2 + \left\lceil \frac{r}{\log \lambda} + \delta \right\rceil \leq \frac{r}{\log \lambda} + 3 + \delta.$$

Therefore we obtain from (10)

$$\begin{aligned} \zeta^{1/(nT^{(n)})} &\geq \frac{z - \varepsilon}{T^{(n)}} \\ &\geq \frac{z \log \lambda}{r + (3 + \delta) \log \lambda} - \varepsilon' \geq \frac{z \log \lambda}{r + \log \lambda} - \varepsilon'', \end{aligned}$$

where $\varepsilon', \varepsilon''$ tend to 0 as δ and ε tend to zero. This shows strong security with the claimed parameter and concludes the proof of Theorem 2.

IV. DISCUSSION

The quantizer which is applied in the proof depends on λ . In particular, the analyses here only hold if the encoder has precise knowledge about λ . However, if the true λ is known to lie in a certain domain $[\lambda_-, \lambda_+]$, we expect all results to go through if $C_0(\mathbf{T}_B, \mathbf{T}_C) > \log \lambda_+$. Quantization would be done according to λ_+ , but the divergence parameter σ would be determined by λ_- .

For a better understanding of Theorems 1 and 2, the set $R_0(\mathbf{T}_B, \mathbf{T}_C)$ would have to be studied further. This would also be necessary to find out how much delay has to be tolerated in order to achieve a desired performance. However, this would be a purely information-theoretic analysis.

REFERENCES

- [1] *IEEE Control Systems Magazine*, vol. 35, no. 1, February 2015, special issue on Cyberphysical Security in Networked Control Systems.
- [2] C. De Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 2930–2944, Nov 2015.
- [3] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1467, June 2014.
- [4] A. Gupta, A. Nayyar, C. Langbort, and T. Basar, "A dynamic transmitter-jammer game with asymmetric information," in *51st IEEE Conference on Decision and Control (CDC)*, Dec 2012, pp. 6477–6482.
- [5] M. Pajic, P. Tabuada, I. Lee, and G. J. Pappas, "Attack-resilient state estimation in the presence of noise," in *54th IEEE Conference on Decision and Control (CDC)*, Dec 2015, pp. 5827–5832.
- [6] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135 – 148, 2015.
- [7] A. S. Matveev and A. V. Savkin, "Shannon zero error capacity in the problems of state estimation and stabilization via noisy communication channels," *Int. Jour. Contr.*, vol. 80, no. 2, pp. 241–255, 2007.
- [8] C. Shannon, "The zero error capacity of a noisy channel," *IRE Trans. Inf. Theory*, vol. 2, no. 3, pp. 8–19, September 1956.
- [9] J. Körner and A. Orlitsky, "Zero-error information theory," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2207–2229, Oct 1998.
- [10] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Wiley-Interscience, 2006.
- [11] G. Nair, "A nonstochastic information theory for communication and state estimation," *IEEE Trans. Autom. Control*, vol. 58, no. 6, pp. 1497–1510, June 2013.
- [12] M. Wiese, K. H. Johansson, T. J. Oechtering, P. Papadimitratos, H. Sandberg, and M. Skoglund, "Uncertain wiretap channels and secure estimation," January 2016, available online at <https://www.kth.se/social/files/56a37e38f276547a85a12c26/ISIT16-long.pdf>.
- [13] M. Fekete, "Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten," *Mathematische Zeitschrift*, vol. 17, no. 1, pp. 228–249, 1923.
- [14] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*. Cambridge University Press, 2001.

APPENDIX

The security analyses rely heavily on the following formula for the mid points of the quantizer intervals which was proved in [12].

Lemma 4: Let $t \geq 0$ and $m(0 : t) \in \{1, \dots, M\}^{t+1}$. Define

$$\sigma_t := \sum_{i=0}^t \left(\frac{\lambda}{M} \right)^i = \frac{M}{M-\lambda} \left(1 - \left(\frac{\lambda}{M} \right)^{t+1} \right).$$

Then

$$\hat{x}(m(0 : t)) = \lambda^t \left\{ \hat{x}(m(0 : -1)) + \frac{1}{2} \sum_{i=0}^t \left(\frac{\Omega \sigma_{i-1}}{\lambda^i} + \frac{|I_0|}{M^i} \right) \left(\frac{2m(i) - 1}{M} - 1 \right) \right\}.$$

Proof of Lemma 2: We show that the minimal distance between $\hat{x}(m(0 : t))$ and $\hat{x}(m'(0 : t))$ for $m(0 : t) \neq m'(0 : t)$ is lower-bounded by $|P(m(0 : t))|$. Let $m(0 : t) \neq m'(0 : t)$. Then by Lemma 4,

$$\begin{aligned} \hat{x}(m(0 : t)) - \hat{x}(m'(0 : t)) &= \lambda^t \frac{|I_0|}{M} \sum_{i=0}^t \frac{m(i) - m'(i)}{M^i} \geq \frac{|I_0|}{M} \left(\frac{\lambda}{M} \right)^t. \end{aligned}$$

By Lemma 1, the right-hand side of the above inequality equals $|P(m(0 : t))|$. Hence the lemma is proven.

The distance between $P(m_{\xi(1:k)}(0 : kT - 1))$ and $P(m'_{\xi'(1:k)}(0 : kT - 1))$ is evaluated based on the following lemma.

Lemma 5: Let $M \geq 2$ and for every $t \geq 0$ let $1 \leq m'(t) < m(t) \leq M$. Then

$$\begin{aligned} \hat{x}(m(0 : t)) - \hat{x}(m'(0 : t)) &\geq \lambda^t \left\{ \frac{\Omega}{M-\lambda} \left(\frac{1 - \lambda^{-(t+1)}}{1 - \lambda^{-1}} - \frac{1 - M^{-(t+1)}}{1 - M^{-1}} \right) \right. \\ &\quad \left. + \frac{|I_0|}{M} \frac{1 - M^{-(t+1)}}{1 - M^{-1}} \right\}. \end{aligned} \quad (11)$$

Proof: Due to Lemma 4,

$$\begin{aligned} \hat{x}(m(0 : t)) - \hat{x}(m'(0 : t)) &= \lambda^t \sum_{i=0}^t \left(\frac{\Omega \sigma_{i-1}}{\lambda^i} + \frac{|I_0|}{M^i} \right) \frac{m(i) - m'(i)}{M} \\ &\geq \frac{\lambda^t}{M} \sum_{i=0}^t \left(\frac{\Omega \sigma_{i-1}}{\lambda^i} + \frac{|I_0|}{M^i} \right). \end{aligned} \quad (12)$$

Now observe that

$$\frac{\sigma_{i-1}}{\lambda^i} = \frac{M}{M-\lambda} \left(\frac{1}{\lambda^i} - \frac{1}{M^i} \right).$$

Hence (12) equals (11). This completes the proof. $\blacksquare$

That system paths do not meet if they start in intervals which are sufficiently far apart is the content of the next lemma.

Lemma 6: Let I_0 and I'_0 be two intervals with $|I_0| = |I'_0|$. Consider two quantizer systems P and P' as in (3)-(5) with the same M , where the starting interval $[A(m(0 :$

$-1)), B(m(0 : -1))]$ for P equals I_0 and the starting interval $[A'(m'(0 : -1)), B'(m'(0 : -1))]$ for P' equals I'_0 . Denote the mid point of $P(m(0 : t))$ by $\hat{x}(m(0 : t))$ and the mid point of $P'(m'(0 : t))$ by $\hat{x}'(m'(0 : t))$, for $t \geq -1$. If

$$\hat{x}(m(0 : -1)) - \hat{x}'(m'(0 : -1)) \geq \frac{\Omega}{\lambda - 1} + |I_0|, \quad (13)$$

then for every t and all possible message sequences $m(0 : t), m'(0 : t)$, the interiors of the intervals $P(m(0 : t))$ and $P'(m'(0 : t))$ are disjoint.

Proof: Due to Lemma 1, it is now sufficient to show that for any message sequences $m(0 : t)$ and $m'(0 : t)$, it holds that

$$\begin{aligned} \hat{x}(m(0 : t)) - \hat{x}'(m'(0 : t)) &\geq \frac{\Omega}{M-\lambda} + \left(\frac{|I_0|}{M} - \frac{\Omega}{M-\lambda} \right) \left(\frac{\lambda}{M} \right)^t. \end{aligned} \quad (14)$$

This assertion is valid if the smallest states belonging to paths which start in $\hat{x}(m(0 : -1))$ never meet the largest states belonging to paths which start in $\hat{x}'(m'(0 : -1))$. Hence, to show (14) it is sufficient to consider the messages $m(0 : t)$ and $m'(0 : t)$ with $m(s) = 1$ for $1 \leq s \leq t$ and $m'(s) = M$ for $1 \leq s \leq t$. By Lemma 4, for these message sequences

$$\begin{aligned} \hat{x}(m(0 : t)) - \hat{x}'(m'(0 : t)) &= \lambda^t \left\{ \hat{x}(m(0 : -1)) - \hat{x}'(m'(0 : -1)) \right. \\ &\quad \left. - \frac{M-1}{M} \sum_{i=0}^t \left(\frac{\Omega \sigma_{i-1}}{\lambda^i} + \frac{|I_0|}{M^i} \right) \right\} \\ &= \lambda^t \left\{ \hat{x}(m(0 : -1)) - \hat{x}'(m'(0 : -1)) \right. \\ &\quad \left. - \frac{M-1}{M} \left(\Omega \frac{M}{M-\lambda} \left(\frac{1 - \lambda^{-(t+1)}}{1 - \lambda^{-1}} - \frac{1 - M^{-(t+1)}}{1 - M^{-1}} \right) \right. \right. \\ &\quad \left. \left. + |I_0| \frac{1 - M^{-(t+1)}}{1 - M^{-1}} \right) \right\}. \end{aligned}$$

It remains to show that the right-hand side of the above equality minus the right-hand side of (14) is nonnegative. Under assumption (13), some calculations reveal that this is equivalent to showing that $\Omega/(\lambda-1) + |I_0|$ is lower-bounded by

$$\frac{\Omega}{\lambda - 1} \left(1 - \frac{1}{\lambda^t} \right) + |I_0|.$$

This is obviously smaller than $\frac{\Omega}{\lambda-1} + |I_0|$, so the lemma is proven. $\blacksquare$

We now have all the ingredients to prove Lemma 3, which is the core of security in the case $\Omega > 0$.

Proof of Lemma 3: We prove by induction that for every $j \geq 1$, the two following statements are true:

- 1) For every $\xi(1 : j-1) \in \Xi^{j-1}$, the intervals $P(m_{\xi(1:j-1)\xi}(0 : jT-1))$ are disjoint, where ξ ranges over Ξ .

- 2) For all $\xi(1:j) \neq \xi'(1:j)$, all $\ell \geq 1$ and all $\xi(j+1:\ell), \xi'(j+1:\ell) \in \Xi^{\ell-j}$, the intervals $P(m_{\xi(1:\ell)}(1:\ell t-1))$ and $P(m_{\xi'(1:\ell)}(1:\ell t-1))$ are disjoint.

To prove this, first set $j = 1$. Note that if we observe our system until time $T-1$ and if it produces the quantizing sequence $m(0:T-1)$, then from this time it can be regarded as a system obeying the rule (1) but whose uncertain initial state is from the interval $[A(m(0:T-1)), B(m(0:T-1))]$ instead of I_0 . (We have to use $[A(m(0:T-1)), B(m(0:T-1))]$ as initial interval instead of $P(m(0:T))$ because the quantizer (3)-(5) quantizes the initial state.) Thus given two message sequences $m(0:T-1), m'(0:T-1)$, we can apply Lemma 6 to the systems started in $[A(m(0:T-1)), B(m(0:T-1))]$ and $[A(m'(0:T-1)), B(m'(0:T-1))]$, respectively, to deduce that their future paths do not cross, as follows.

Lemma 5 provides a lower bound on the minimal distance between $\hat{x}(m_\xi(0:T-1))$ and $\hat{x}(m_{\xi'}(0:T-1))$ for $\xi > \xi'$. According to Lemma 6, this distance has to be at least

$$\frac{\Omega}{\lambda-1} + M|P(m(0:T))|.$$

After some calculations, it turns out that this is the case if

$$\frac{1}{\lambda^{T-1}} \frac{M\lambda - \lambda + 1}{\lambda - 1} \leq \frac{M - \lambda}{(\lambda - 1)(M - 1)},$$

and

$$M^T \geq M\lambda - \lambda + 1.$$

Both inequalities hold because T satisfies (9). This proves the second assertion 2) in the case $j = 1$.

For the first assertion observe that by (6)

$$\begin{aligned} & \frac{\Omega}{\lambda-1} + M|P(m(0:T))| - |P(m(0:T-1))| \\ &= (\lambda-1)|P(m(0:T-1))| + \frac{\lambda\Omega}{\lambda-1} > 0. \end{aligned}$$

Hence by assertion 2), $\hat{x}(m_\xi(T-1))$ and $\hat{x}_{\xi'}(m(0:T-1))$ are further apart than $|P(m(0:T-1))|$, so the interiors of $P(m_\xi(0:T-1))$ and $P(m_{\xi'}(0:T-1))$ are disjoint. Thus assertion 1) is also proven for the case $j = 1$.

Next assume that assertions 1) and 2) have been proven for all $1 \leq i \leq j-1$. We will now prove it for the case j . Again we start with 2). To show that paths do not meet starting in $\xi(1:j)$ or $\xi'(1:j) \neq \xi(1:j)$, we may assume that $\xi'(1:j-1) = \xi(1:j-1)$. Otherwise, this follows from 2) for the case $i = j-1$.

Analogously to the case $j = 1$, it has to be proven that

$$\begin{aligned} & \hat{x}(m_{\xi(1:j)}(0:jT-1)) - \hat{x}(m_{\xi'(1:j)}(0:jT-1)) \\ & \geq \frac{\Omega}{\lambda-1} + M|P(m(0:jT))| \quad (15) \end{aligned}$$

if $\xi(1:j-1) = \xi'(1:j-1)$ and $\xi(j) > \xi'(j)$. The calculations are the same as in the case $j = 1$. Observing that the lower bound (9) on T is independent of the length of the initial interval, it is immediate that assertion 2) also holds for the case j . The disjointness of the quantizing intervals

$P(m_{\xi(1:j)}(0:jT-1)) : \xi(j) \in \Xi$ follows as in the case $j = 1$.

Thus 1) and 2) hold for every $j \geq 1$. Their combination immediately yields the assertion of the lemma.