Detecting Generalized Replay Attacks via Time-Varying Dynamic Watermarking

Matthew Porter, Pedro Hespanhol, Anil Aswani, Matthew Johnson-Roberson, and Ram Vasudevan

***Abstract*—Cyber-physical systems (CPS) often rely on external communication for supervisory control or sensing. Unfortunately, these communications render the system vulnerable to cyber-attacks. Attacks that alter messages, such as replay attacks that record measurement signals and then play them back to the system, can cause devastating effects. Dynamic Watermarking methods, which inject a private excitation into control inputs to secure resulting measurement signals, have begun addressing the challenges of detecting these attacks, but have been restricted to linear time invariant (LTI) systems. Though LTI models are sufficient for some applications, other CPS, such as autonomous vehicles, require more complex models. This paper develops a linear time-varying (LTV) extension to previous Dynamic Watermarking methods by designing a matrix normalization factor to accommodate the temporal changes in the system. Implementable tests are provided with considerations for real-world systems. The proposed method is then shown to be able to detect generalized replay attacks both in theory and in simulation using a LTV vehicle model.**

***Index Terms*—Dynamic watermarking, cyber-physical systems (CPS), networked control systems, linear time varying (LTV), secure control.**

I. Introduction

Cyber-physical systems (CPS) combine both networked computing and sensing resources with physical control systems in an effort to increase efficiency, manage complexity, or provide convenience. Whether it is industrial control applications or smart devices, CPS require secure networked communications to operate safely and correctly. Malicious attacks on such systems can cause devastating results [1]–[4]. CPS are often protected by traditional cyber security tools, but these methods are insufficient due to the addition of networked physical infrastructure. [5], [6]. A growing body of work has started to address these challenges by developing new detection algorithms, analyzing potentially stealthy attack models, and finding ways of reducing the effect of attacks. One particular detection method, Dynamic Watermarking, has been shown to detect various attack models while making few assumptions about system structure. Despite these developments, detection algorithms, including Dynamic Watermarking, have only focused on CPS that can be modeled as linear time invariant (LTI) systems. While LTI models can be sufficient for steady state or slow moving applications, many emerging CPS such as autonomous vehicles require models that change over time. This paper develops methods to accommodate such CPS by extending Dynamic Watermarking to linear time-varying (LTV) systems.

This work was supported by a grant from Ford Motor Company via the Ford-UM Alliance under award N022977, the National Science Foundation under Grants CMMI-1751093 and CMMI-1847666, the Office of Naval Research under award number N00014-18-1-2575, and the UC Berkeley Center for Long-Term Cybersecurity.

M. Porter and R. Vasudevan are with the Department of Mechanical Engineering, University of Michigan, Ann Arbor, MI 48103 USA (e-mail: matthepo@umich.edu; ramv@umich.edu).

A. Aswani and P. Hespanhol are with the Department of Industrial Engineering and Operations Research, University of California Berkeley, Berkeley, CA 94720 USA (e-mail: aaswani@berkeley.edu; pedrohespanhol@berkeley.edu).

M. Johnson-Roberson is with the Department of Naval Architecture, University of Michigan, Ann Arbor, MI 48103 USA (e-mail: mattjr@umich.edu).

A. Attack Models

Attacks are divided into three categories: *denial of service* (DOS) *attacks*, where the control or measurement signal is stopped, *direct attacks*, where the plant, actuators or sensors are physically attacked, and *deception attacks*, where the control or measurement signal are altered. [7]. DOS attacks can be detrimental, but are trivial to detect if they stop all communication. Furthermore, when only a portion of communication is stopped, their effects can be minimized using graceful degradation [8]. The result of direct attacks often causes anomalies in the measurement signal and can therefore be detected by methods used to detect deception attacks. Consequentially, this work focuses on the detection of deception attacks.

A variety of deception attacks have been proposed. The simplest deception attacks add noise using arbitrary or random strategies [9]. On the other hand, bias injection attacks, the attacker injects a constant bias into the system [10], while routing attacks send measurement signals through a linear transform [11]. Other deception attacks attempt to decouple the system such that the measurements are unaltered while certain states of the system are attacked [12]. For instance, zero-dynamics attacks take advantage of un-observable states or remove the effects of their attacks in the measurement signal [10], and replay attacks involve an attacker replaying recorded measurements while possibly altering control as well [10].

The amount of knowledge of the system dynamics and detection scheme along with the capability of the attacker to alter certain signals necessary to carry out these attacks varies greatly. While random, bias injection, routing, and replay attacks do not require any knowledge of the underlying system dynamics, decoupling and zero-dynamics attack require almost full knowledge. This knowledge can be difficult to obtain for non-insider attackers but it is not impossible [13], [14]. Nonetheless, this work focuses on a generalization of a replay attack due to the simplicity of implementation and because it has already been applied during real-world attacks [1]. Furthermore, we consider attacks that only alter measurement signals, since many of the systems we care about use local controllers while operating using externally received measurements.

B. Attack Detection Algorithms

The *measurement residual*, defined as the difference between the measurement and the expected measurement, is used by most detection schemes. For each detector, a metric based on the measurement residual is generated. If at any time the metric exceeds a user-defined threshold, the detector raises an alarm. Generally, these metrics can be separated into two categories: those that only observe the system, called *passive methods*, and those that alter the system while observing, called *active methods*. While passive methods do not degrade control performance, active methods accept a small amount of performance degradation in exchange for the ability to detect more complex attacks [15]–[17]. These categories can be further subdivided into *stateless* metrics, which only consider the current measurement residual, and *stateful* metrics, which rely on previous measurement residuals as well.

1) Passive Methods: The χ^2 detector's metric is the inner product of the normalized measurement residual, which follows a χ^2 distribution. Due to its simplicity, the χ^2 detector has been studied in several works [18]–[21]. Though the χ^2 is widely used, it is a stateless detector. Two stateful alternatives are the cumulative sum (CUSUM) detector and the multivariate exponentially weighted moving average (MEWMA) detector. When comparing these stateful detectors to the χ^2 detector, it has been shown that the stateful detectors can often provide stronger guarantees on detection while the χ^2 detector boasts both simpler implementation and generally takes less time to detect attacks [22], [23]. While passive detectors can detect random attacks, they are unable to detect more sophisticated attacks such as replay attacks. In addition, they have only been developed for LTI systems.

2) Active Methods: Most active methods fall into one of two categories: *moving target defense*, which change system parameters to keep attackers from obtaining the current configuration, and *watermarking-based methods*, which encrypt measurement signals with a watermark that is added to the control input.

The concept of moving target defenses is a topic of continued interest for the field of cyber security and includes randomizing the order of code execution and physical memory storage locations [24]. In CPS, moving target defense can take the form of switching between redundant measurements [25]–[29], altering control strategy [25], [29], or by changing plant dynamics [25]–[27], [30]–[33]. Switching measurement signals works well when an attacker is only hacking a few measurements, but otherwise performs similar to passive methods. Altering the control strategy is arguably similar to watermarking-based methods and can allow for detection of most attack models except zero-dynamics attacks. While some methods alter the physical plant dynamics directly [25]–[27], others append the plant dynamics with an auxiliary system with possibly more complex dynamics [30]–[33]. Despite the consideration of more complex dynamics for the auxiliary systems, moving target defense has only been applied to systems that have LTI dynamics. Although complex dynamics cause the behavior of the test metric to change in time, methods for selecting a time-varying threshold involve hand tuning. Moving target defenses can allow for detection of all attack models, but the method makes certain assumptions about the system. Note, the auxiliary system must take the form of an additional physical system that is coupled with the underlying system, or a simulated system that requires secure knowledge of the underlying system's state. Also, when an auxiliary system is not used, it is assumed that the plant dynamics are changeable.

The introduction of a watermark was first proposed as a way of making the χ^2 detector robust to replay attacks [34] and other more advanced attacks [35]. Here, the watermark takes the form of independent identically distributed (IID) Gaussian noise that is added to the control input. Robustness to replay attacks is then achieved by properly selecting the watermark covariance, while the χ^2 detector itself remains unchanged. Dynamic Watermarking uses a metric that relies on both the covariance of the residuals and the correlation between the residuals and the watermark. The covariance of the watermark is allowed to be an arbitrary symmetric full rank matrix [36]–[40]. In these works, the metric uses the measurement residuals contained in a temporally sliding window. Guarantees of detection are then made as the window size tends to infinity. Extensions to a limited subset of nonlinear systems have been implemented [38], [41], but otherwise Dynamic Watermarking has been limited to LTI systems. Though the addition of the watermark causes a degradation in system performance, the degradation can be minimized [42], [43]. Other work has considered allowing the watermark signal to be auto-correlated [44] or to have distributions that are not Gaussian [45], [46]. Furthermore, other forms of watermarks include intentional package drops [47], [48], using parameterized transforms on measurements [11], [49], [50], and B-splines added to feed forward inputs [51]. Though Dynamic Watermarking is unable to detect zero-dynamics attacks, it does not require the assumption of changeable plant dynamics, the ability to add physical auxiliary systems that are coupled with vulnerable states, or locally secure knowledge of plant state. This paper focuses on Dynamic Watermarking as described in Hespanhol et al. [37] due to its ability to be applied to a wide range of LTI systems including both fully and partially observable systems.

C. Contributions

The contributions of this paper are threefold. First, the tests used in Hespanhol et al. [37] are extended to LTV systems. To the best of our knowledge, the proposed method is the first detection scheme to focus on systems with time-varying characteristics. This is done using a carefully designed matrix normalization factor to accommodate the temporal changes in the system. These tests are then proven to detect generalized replay attacks. Second, a model is developed for time-varying generalized replay attacks. Third, LTV Dynamic Watermarking is applied to a simulated system to provide proof of concept.

The remainder of this paper is organized as follows. Section I-D introduces notation. Section II reviews the methods in Hespanhol et al. [37] to motivate the need for LTV Dynamic Watermarking. Asymptotic guarantees and implementable tests for LTV Dynamic Watermarking are provided in Sections III and IV respectively. Simulated results are presented in Section V. The appendix covers statistical background for the proofs in this paper in addition to several proofs of intermediate results.

D. Notation

This section briefly introduces the notation used in this paper. The 2-norm of a vector x is denoted $\|x\|$. Similarly, the 2-norm of a matrix X is denoted $\|X\|$. The trace of a matrix X is denoted $\text{tr}(X)$. Zero matrices of dimension $i \times j$ are denoted $0_{i\times j}$, and in the case that $i = j$, the notation is simplified to 0_i. Identity matrices of dimension i are denoted I_i. Block diagonal matrices using blocks $X_1,\ X_2,\ \ldots$ are denoted $\text{blkdiag}(X_1,\ X_2, \ldots)$.

The Wishart distribution with scale matrix Σ and i degrees of freedom is denoted $\mathcal{W}(\Sigma, i)$ [52, Section 7.2]. The multivariate Gaussian distribution with mean μ and covariance Σ is denoted $\mathcal{N}(\mu, \Sigma)$. The chi-squared distribution with i degrees of freedom is denoted $\chi^2(i)$. The expectation of a random variable a is denoted $\mathbb{E}[a]$. The probability of an event E is denoted $\mathbb{P}(E)$. Given a sequence of random variables $\{a_i\}_{i=1}^{\infty}$, convergence in probability is denoted $\text{p-lim}_{i\to\infty} a_i$ and almost sure convergence is denoted $\text{as-lim}_{i\to\infty} a_i$ [53, Definition 7.2.1].

II. Inspiration for LTV Watermarking

This section describes the inspiration for LTV dynamic watermarking by summarizing the method described in Hespanhol et al. [37] for LTI systems. Consider an LTI system with state x_n, measurement y_n, process noise w_n, measurement noise z_n, watermark e_n, additive attack v_n, and stabilizing feedback that uses the observed state $\hat{x}$

$$x_{n+1} = Ax_n + BK\hat{x}_n + Be_n + w_n \tag{1}$$

$$\hat{x}_{n+1} = (A + BK + LC)\hat{x}_n + Be_n - Ly_n \tag{2}$$

$$y_n = Cx_n + z_n + v_n \tag{3}$$

where $x_n, \hat{x}_n, w_n \in \mathbb{R}^p$, $e_n \in \mathbb{R}^q$, $y_n, z_n, v_n \in \mathbb{R}^r$, and $x_0 = 0_{p\times 1}$. The process noise w_n, measurement noise z_n, and watermark e_n are mutually independent and take the form $w_n \sim \mathcal{N}(0_{p\times 1}, \Sigma_w)$, $z_n \sim \mathcal{N}(0_{r\times 1}, \Sigma_z)$, and $e_n \sim \mathcal{N}(0_{q\times 1}, \Sigma_e)$. While the process and measurement noise are unknown to the controller, the watermark signal is generated by the controller and is known. The following assumption is made on the controller, observer, and watermark design.

Assumption II.1. *Assume $\|A + BK\| < 1$, $\|A + LC\| < 1$, and Σ_e is full rank.*

The measurement residual for this system takes the form $C\hat{x}_n - y_n$. When an attack is not present, the distribution of the measurement residuals converge to a zero mean Gaussian distribution with covariance Σ where

$$\Sigma = \lim_{n\to\infty} \mathbb{E}[(C\hat{x}_n - y_n)(C\hat{x}_n - y_n)^{\mathsf{T}}]. \tag{4}$$

Note, for a LTV system, the limit in (4) may not exist.

Next, consider a generalization of a replay attack satisfying

$$v_n = \alpha(Cx_n + z_n) + C\xi_n + \zeta_n \tag{5}$$

$$\xi_{n+1} = (A + BK)\xi_n + \omega_n \tag{6}$$

where $\alpha \in \mathbb{R}$ is called the *attack scaling factor*, the false state $\xi_n \in \mathbb{R}^p$ has process noise $\omega_n \in \mathbb{R}^p$ and measurement noise $\zeta_n \in \mathbb{R}^r$ that take the form $\omega_n \sim \mathcal{N}(0_{p\times 1}, \Sigma_\omega)$ and $\zeta_n \sim \mathcal{N}(0_{r\times 1}, \Sigma_\zeta)$, and are mutually independent with each other and with w_n and z_n. Though this attack structure does not include all forms of deception attacks, it does allow an attacker to carry out a variety of documented attacks. For example, selecting $\Sigma_\omega = 0_p$ and an attack scaling factor α of 0 results in independent identically distributed noise being added to the measurement. Moreover, when Σ_ω and Σ_ζ are selected such that the covariance of the measurement residual is unaltered and the attack scaling parameter is -1, this model can approximate a replay attack. While attackers may have the ability to start and stop attacks at will, attacks that are only present for finite time are not guaranteed to be detected. Therefore, when considering asymptotic guarantees of detection, the assumption of persistence is made. To formally describe these persistent attacks, consider the following definition.

Definition II.2. *The asymptotic attack power is defined as*

$$\underset{i\to\infty}{\text{as-lim}}\ \frac{1}{i}\sum_{n=0}^{i-1} v_n^{\mathsf{T}} v_n. \tag{7}$$

Under this definition, an attack with non-zero asymptotic power is deemed to be persistent.

The asymptotic claims of LTI dynamic watermarking take the form of the following theorem.

Theorem II.3. *[37, Theorem 1] Consider an attacked LTI system satisfying* (1)-(3)*, an attack model satisfying* (5)-(6)*, and Σ satisfying* (4)*. Let $k' = \min\{k \geq 0 \mid C(A+BK)^k B \neq 0_{r\times q}\}$ be finite. Then the asymptotic attack power is 0 if*

$$\underset{i\to\infty}{\text{as-lim}}\ \frac{1}{i}\sum_{n=0}^{i-1}(C\hat{x}_n - y_n)(C\hat{x}_n - y_n)^{\mathsf{T}} = \Sigma, \tag{8}$$

$$\underset{i\to\infty}{\text{as-lim}}\ \frac{1}{i}\sum_{n=0}^{i-1}(C\hat{x}_n - y_n)e_{n-k'-1}^{\mathsf{T}} = 0_{r\times q}. \tag{9}$$

Here, the first test checks for changes in the covariance of the residual while the second test ensures that the attack is uncorrelated with the true measurement and cannot avoid changing this covariance. The delay of the watermark by k' in (9) ensures that the effect of the watermark is present in the measurement signal. Note, the contrapositive of Theorem II.3 states that for attacks with non-zero asymptotic power, (8) and (9) cannot both be satisfied. Therefore, considering the LHS of (8) and (9), generalized replay attacks of non-zero asymptotic power are guaranteed to be detected in infinite time.

To make these tests implementable in real time, a statistical test is derived using a sliding window of fixed size. At each step, the combined partial sums in (8)-(9) take the form

$$S_n = \sum_{i=n+1}^{n+\ell} \begin{bmatrix} (C\hat{x}_i - y_i) \\ e_{i-k'-1} \end{bmatrix} \begin{bmatrix} (C\hat{x}_i - y_i)^{\mathsf{T}} & e_{i-k'-1}^{\mathsf{T}} \end{bmatrix}. \tag{10}$$

Under the assumption of no attack, S_n converges asymptotically to the Wishart distribution with scale matrix $S =$

blkdiag(Σ, Σ_e) and ℓ degrees of freedom as $\ell \to \infty$. Furthermore, for a generalized replay attack of non-zero asymptotic power, Theorem II.3 gives us that the scale matrix for S_n is no longer S, since either (8) or (9) is not satisfied. Given the sampled matrix S_n, the test then uses the negative log likelihood of the scale matrix

$$\mathcal{L}(S_n) = (m + q + 1 - \ell)\log(|S_n|) + \operatorname{tr}\left(S^{-1}S_n\right). \quad (11)$$

Negative log likelihood values that exceed a user-defined threshold signal an attack.s

For LTV systems, the limits in (8)-(9) may not exist. Furthermore, the sampled matrices S_n may no longer be approximated as a Wishart distribution since the vectors used to create it in (10) are not necessarily identically distributed. To accommodate these changes in distribution, it is necessary to develop a new method.

III. LTV Dynamic Watermarking

This section derives the limit-based formulation of Dynamic Watermarking for a discrete-time LTV system. In Section III-A, the LTV dynamics and necessary assumptions are given. In Section III-B, the limit based tests and corresponding claims are defined. Subsequently, Section III-C provides intermediate results to prove these claims.

A. LTV System

Consider an LTV system with state x_n, measurement y_n, process noise w_n, measurement noise z_n, watermark e_n, additive attack v_n, and stabilizing feedback that uses the observed state $\hat{x}$ and control gain K_n

$$x_{n+1} = A_n x_n + B_n K_n \hat{x}_n + B_n e_n + w_n \quad (12)$$

$$y_n = C_n x_n + z_n + v_n \quad (13)$$

where $x_n, \hat{x}_n, w_n \in \mathbb{R}^p$, $e_n \in \mathbb{R}^q$, $y_n, z_n, v_n \in \mathbb{R}^r$, and $x_0 = 0_{p\times 1}$. The process noise w_n, measurement noise z_n, and watermark e_n are mutually independent and take the form $w_n \sim \mathcal{N}(0_{p\times 1}, \Sigma_{w,n})$, $z_n \sim \mathcal{N}(0_{r\times 1}, \Sigma_{z,n})$, and $e_n \sim \mathcal{N}(0_{q\times 1}, \Sigma_e)$. While the process and measurement noise are unknown to the controller, the watermark signal is generated by the controller and is known. For simplicity, define $\bar{A}_n = (A_n + B_n K_n)$ and $\bar{A}_{(n,m)} = \bar{A}_n \cdots \bar{A}_m$ for $n \geq m$ and $\bar{A}_{(n,n+1)} = I_p$. We make the following assumption.

Assumption III.1. *The covariances Σ_e, $\Sigma_{w,n}$, and $\Sigma_{z,n}$, of the random variables used in (12)-(13), are full rank. Furthermore, there exists positive constants $\eta_w, \eta_z, \eta_{\bar{A}}, \eta_B, \eta_C \in \mathbb{R}$ such that $\|\Sigma_{w,n}\| < \eta_w$, $\|\Sigma_{z,n}\| < \eta_z$, $\|\bar{A}_n\| < \eta_{\bar{A}} < 1$, $\|B_n\| < \eta_B$, and $\|C_n\| < \eta_C$, for all $n \in \mathbb{N}$.*

The assumption of bounded full rank covariances for the process and measurement noise are satisfied for most systems by modeling error and sensor noise. Furthermore, the input and output matrices are often constrained to be finite by sensor and actuator limits. Note to satisfy the assumption on $\bar{A}_n$, one could for instance assume that the controllabilty matrix constructed from A_n and B_n for all $n \geq 0$ was full rank. Under that assumption one could design K_n using eigenvalue assignment and selecting real distinct eigenvalues that are less than 1 [54, Section 4.4.1]. Since the watermark is user-defined, the remaining assumption can be satisfied by proper selection of Σ_e. We make the following assumption.

Assumption III.2.

$$\lim_{i\to\infty} \tfrac{1}{i} \textstyle\sum_{n=0}^{i-1} C_n B_{n-1} \neq 0_{r\times q}. \quad (14)$$

Here, (14) guarantees an asymptotic correlation between the measurement signal y_n and the watermark signal e_{n-1}, which has been delayed by a single time step. This ensures that the watermark has a persistent measurable effect on the measurement signal, which can then be used for validation purposes. This is similar to assuming k' is equal to 0 for the LTI case.

The observer and the corresponding observer error, defined as $\delta_n = \hat{x}_n - x_n$, satisfy

$$\hat{x}_{n+1} = (\bar{A}_n + L_n C_n)\hat{x}_n + B_n e_n - L_n y_n \quad (15)$$

$$\delta_{n+1} = (A_n + L_n C_n)\delta_n - w_n - L_n(z_n + v_n), \quad (16)$$

where $\hat{x}_0 = \delta_0 = 0_{p\times 1}$ and L_n is the observer gain. For simplicity, define $\underline{A}_n = (A_n + L_n C_n)$ and $\underline{A}_{(n,m)} = \underline{A}_n \cdots \underline{A}_m$ for $n \geq m$ and $\underline{A}_{(n,n+1)} = I_p$. Furthermore, let

$$\bar{\delta}_{n+1} = \underline{A}_n \bar{\delta}_n - w_n - L_n z_n \quad (17)$$

$$\hat{\delta}_{n+1} = \underline{A}_n \hat{\delta}_n - L_n v_n \quad (18)$$

where $\bar{\delta}_0 = \hat{\delta}_0 = 0_{p\times 1}$. Note that $\delta_n = \bar{\delta}_n + \hat{\delta}_n$ and that when $v_n = 0_{r\times 1},\ \forall n$ we have that $\hat{\delta}_n = 0_{p\times 1},\ \forall n$. Here $\bar{\delta}_n$ can be thought of as the portion of the observer error that results from the original noise of the system, while $\hat{\delta}_n$ is the contribution of the attack to the observer error.

Next, consider the expected value $\Sigma_{\delta,n} = \mathbb{E}[\bar{\delta}_n \bar{\delta}_n^\intercal] = \mathbb{E}[\delta_n \delta_n^\intercal \mid v_n = 0_{r\times 1},\ \forall n]$, which can be written as

$$\Sigma_{\delta,n} = \textstyle\sum_{i=0}^{n} \underline{A}_{(n-1,n-i+1)}(\Sigma_{w,n-i} + \\ + L_{n-i}\Sigma_{z,n-i}L_{n-i}^\intercal)\underline{A}_{(n-1,n-i+1)}^\intercal. \quad (19)$$

The *matrix normalization factor* is then defined as

$$V_n = (C_n \Sigma_{\delta,n} C_n^\intercal + \Sigma_{z,n})^{-1/2}, \quad (20)$$

which exists since $\Sigma_{z,n}$ is full rank. For an LTI system, the matrix $V_n = \Sigma^{-1/2}$ where Σ is as defined in (4). For the LTV system, the matrix normalization factor can be thought of as a time-varying normalization for the measurement residual. To generate V_n using (19)-(20), one would need to know the covariance of the noise variables. However, in Section IV we cover a pragmatic approach to estimating V_n more directly. Next, we make the following assumption about the observer.

Assumption III.3. *There exists positive constants $\eta_{\underline{A}}$, η_L, η_δ, $\eta_V \in \mathbb{R}$ such that $\|\underline{A}_n\| < \eta_{\underline{A}} < 1$, $\|L_n\| < \eta_L$, $\|\Sigma_{\delta,n}\| < \eta_\delta$, and $\|V_n\| < \eta_V$, for all $n \in \mathbb{N}$.*

Note to satisfy the assumption on $\underline{A}_n$, one could for instance assume that the observability matrix constructed from A_n and C_n for all $n \geq 0$ was full rank. Under that assumption one could design L_n using eigenvalue assignment and selecting real distinct eigenvalues that are less than 1 [54, Section 4.8.1].

Previous assumptions imply the assumptions on L_n, $\Sigma_{\delta,n}$, and V_n are satisfied, but the bounds here simplify notation.

Next, we alter the attack defined in (5)-(6) to create a time-varying equivalent. Consider an attack v_n that satisfies

$$v_n = \alpha(C_n x_n + z_n) + C_n \xi_n + \zeta_n \tag{21}$$

$$\xi_{n+1} = \bar{A}_n \xi_n + \omega_n, \tag{22}$$

where $\alpha \in \mathbb{R}$ is called the *attack scaling factor*, the *false state* $\xi_n \in \mathbb{R}^p$ has process noise $\omega_n \in \mathbb{R}^p$ and measurement noise $\zeta_n \in \mathbb{R}^r$ that take the form $\omega_n \sim \mathcal{N}(0_{p\times 1}, \Sigma_{\omega,n})$ and $\zeta_n \sim \mathcal{N}(0_{r\times 1}, \Sigma_{\zeta,n})$ and are mutually independent with each other and with w_n and z_n. Similar to the LTI case, when $\Sigma_{\omega,n}$ and $\Sigma_{\zeta,n}$ are selected properly and the attack scaling parameter is -1, this model can approximate a replay attack. The results of such an attack can have devastating results as shown in Figure 1. While an attacker could choose to allow the noise to have unbounded covariance, the resulting attack would be trivial to detect. Therefore, we make the following assumption about the attack model.

Assumption III.4. *When there is an attack, v_n follows the dynamics* (21)-(22) *with the attack scaling factor remaining constant. Furthermore, there exists positive constants $\eta_\omega, \eta_\eta \in \mathbb{R}$ such that $\|\Sigma_{\omega,n}\| < \eta_\omega$, $\|\Sigma_{\zeta,n}\| < \eta_\zeta$, for all $n \in \mathbb{N}$.*

To make asymptotic guarantees of detection, we also assume the persistence of attacks using the following definition.

Definition III.5. *The asymptotic attack power is defined as*

$$\operatorname*{p-lim}_{i\to\infty} \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} v_n^\intercal v_n. \tag{23}$$

B. Asymptotic Tests

Similar to prior research in Dynamic Watermarking, we first define the asymptotic tests.

Theorem III.6. *Consider an attacked LTV system satisfying the dynamics in* (12)-(18)*. Let V_n be as defined in* (20)*. If $v_n = 0_{r\times 1}$, for all $n \in \mathbb{N}$, then*

$$\operatorname*{p-lim}_{i\to\infty} \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} V_n(C_n\hat{x}_n - y_n)e_{n-1}^\intercal = 0_{r\times q}, \tag{C1}$$

$$\operatorname*{p-lim}_{i\to\infty} \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} V_n(C_n\hat{x}_n - y_n)(C_n\hat{x}_n - y_n)^\intercal V_n^\intercal = I_r. \tag{C2}$$

Furthermore, if the attack follows the dynamics in (21)-(22) *and has non-zero asymptotic power as defined in Definition III.5, then* (C1) *and* (C2) *cannot both be satisfied.*

From Theorem III.6, the LHS of (C1) and (C2) can be used to guarantee detection of generalized replay attacks with non-zero asymptotic power in infinite time. Note, (C1), (C2), and (23) use limits in probability as opposed to the almost sure limits used in their LTI counterparts. This change removes the guarantee of detection via the asymptotic tests for certain pathological examples of attacks. Given an arbitrary real number ϵ, almost sure convergence states that with probability 1 the sequence will remain a distance of less than ϵ from the limit after a finite number of steps while convergence in probability states that the probability that an element of the sequence is within a distance of ϵ from the limit converges to 1 as you continue along the sequence. These asymptotic tests provide infinite time guarantees, but as formulated require the entire history of measurements. However, these tests motivate the finite-time statistical tests that are implemented in Section IV which consider a finite sample window. As the window size grows the sequence of sample averages is more likely to be closer to the limit when no attack is present. This is reflected in the distribution used to generate the test metric. As a result, the test becomes more sensitive.

C. Intermediate Results

To prove Theorem III.6, several intermediate results must first be provided. The proofs of these results are available in the appendix. First, we consider the asymptotic limit (C1) and show that it implies that the attack scaling factor α is equal to 0. This allows us to assume that α is equal to 0 for the remainder of the intermediate results.

Lemma III.7. *Consider an attacked LTV system satisfying* (12)-(18) *and the attack model satisfying* (21)-(22)*. Let V_n be as defined in* (20)*.* (C1) *holds if and only if the attack scaling factor α is equal to 0.*

In a sense, (C1) checks that the attack v_n is uncorrelated with the true measurement, which is true only when the attack scaling factor α is zero.

Assuming α is equal to 0, we show that (C2) is equivalent to another condition that is only dependent on the attack v_n and its contribution to the observer error $\hat{\delta}_n$. Note, $\hat{\delta}_n$ is not computable given the available knowledge of the system, but the provided condition is an amenable surrogate to (C2).

Lemma III.8. *Consider an attacked LTV system satisfying* (12)-(18) *and an attack model satisfying* (21)-(22)*. Let V_n be as defined in* (20)*. Assume the attack scaling factor α is equal to 0.* (C2) *holds if and only if*

$$\operatorname*{p-lim}_{i\to\infty} \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} V_n(C_n\hat{\delta}_n - v_n)(C_n\hat{\delta}_n - v_n)^\intercal V_n^\intercal = 0_r. \tag{24}$$

Here (24) can be thought of as that contribution of the attack to the value of the LHS of (C2).

For an attack scaling factor α of 0, the attack v_n is only dependent on the random vectors ξ_n and ζ_n. Similar to Lemma III.8, these vectors are not computable by the controller, but can be used to connect (C2) to the asymptotic attack power.

Lemma III.9. *Consider an attacked LTV system satisfying* (12)-(18) *and an attack model satisfying* (21)-(22)*. Assume that the attack scaling factor α is equal to 0. The asymptotic attack power as defined in* (23) *is 0 if and only if*

$$\operatorname*{p-lim}_{i\to\infty} \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} \zeta_n\zeta_n^\intercal = 0_r, \tag{25}$$

$$\operatorname*{p-lim}_{i\to\infty} \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} C_n\xi_n\xi_n^\intercal C_n^\intercal = 0_r. \tag{26}$$

Each of the prior equations can be thought of as the contribution of each random vector to the asymptotic attack power.

Next, we start to complete the connection between (C2) and zero asymptotic attack power by proving (24) implies (25). Furthermore, we prove a related result that makes it simpler to prove that (24) implies (26).

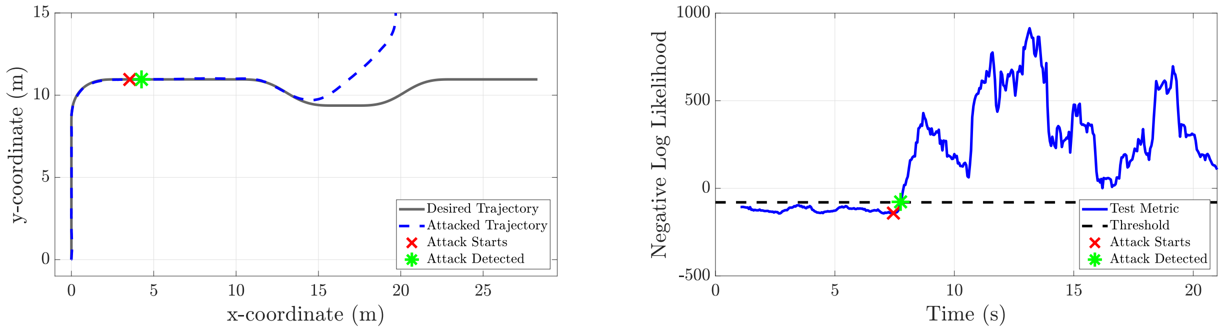


Fig. 1. Desired and attacked trajectory of an LTV car model showing attack start and detection (Left); Corresponding LTV Dynamic Watermarking test metric showing attack start and detection (right)

Lemma III.10. *Consider an attacked LTV system satisfying* (12)-(18) *and an attack model satisfying* (21)-(22)*. Let* V_n *be as defined in* (20)*. Assume the attack scaling factor* α *is equal to 0. If* (24) *holds, then* (25) *holds as well and*

$$\underset{i\to\infty}{\text{p-lim}}\tfrac{1}{i}\sum_{n=0}^{i-1}(C_n\hat{\delta}_n - C_n\xi_n)(C_n\hat{\delta}_n - C_n\xi_n)^\intercal = 0_r. \quad (27)$$

Since ζ_n adds additional noise to the measurement signal, the link between (24) and (25) is clear. In particular, (27) is constructed by removing ζ_n's effect from (24).

Next we claim that (24) implies (26) to complete the relation between (C2) and the asymptotic attack power.

Lemma III.11. *Consider an attacked LTV system satisfying* (12)-(18) *and an attack model satisfying* (21)-(22)*. Let* V_n *be as defined in* (20)*. Assume the attack scaling factor* α *is equal to 0. If* (24) *holds then* (26) *holds as well.*

The proof of Lemma III.11 makes use of Lemma III.10 and instead shows that (27) implies (26). Despite the removal of ζ_n in (27), the correlation between $\hat{\delta}_n$ and ξ_n introduces a potential complication. To address this challenge, we prove the contrapositive statement. Assuming that (26) does not hold, we make the following assertion.

Lemma III.12. *Consider an attacked LTV system satisfying* (12)-(18) *and an attack model satisfying* (21)-(22)*. Let* V_n *be as defined in* (20)*. Assume the attack scaling factor* α *is equal to 0. If* (26) *does not hold then there exists* $m \in \mathbb{N}$ *for which*

$$\underset{i\to\infty}{\text{p-lim}}\tfrac{1}{i}\sum_{n=0}^{i-1}\left(C_n\sum_{j=1}^{m_n}\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right)\times \times\left(C_n\sum_{j=1}^{m_n}\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right)^\intercal \neq 0_r. \quad (28)$$

where $m_n = \min\{n, m\}$*. Furthermore, there exists an* $m' \in \mathbb{N}$ *such that* $m' \leq m$ *and*

$$\underset{i\to\infty}{\text{p-lim}}\tfrac{1}{i}\sum_{n=0}^{i-1}C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\times \times\,\omega_{n-j}^\intercal\bar{A}_{(n-1,n-j+1)}^\intercal C_n^\intercal \neq 0_r \quad (29)$$

for $j = m'$ *but not for* $j < m'$*.*

Here (26) is expanded into a summation over a triangular array. Splitting ξ_n in (27), allows us to modify the cross terms and complete the proof.

Having proven several intermediate results, we are now able to formally prove Theorem III.6.

Proof. **(Theorem III.6)** When no attack is present, (C1) holds using Lemma III.7 since the attack scaling factor α is equal to 0. Furthermore, (C2) holds since the observer error $\delta = \overline{\delta}$.

Now assume that an attack of non-zero asymptotic power is present and consider the following cases.

Case 1 ($\alpha \neq 0$): Using Lemma III.7, (C1) does not hold.

Case 2 ($\alpha = 0$): Note, (C2) implies zero asymptotic attack power as follows.

$$\text{(C2)} \underset{\text{Lm. III.8}}{\Longleftrightarrow} (24) \begin{array}{l} \overset{\Longrightarrow}{\scriptstyle\text{Lm. III.10}} (25) \\ \underset{\text{Lm. III.11}}{\Longrightarrow} (26) \end{array} \underset{\text{Lm. III.9}}{\Longleftrightarrow} \begin{pmatrix}\text{zero asymptotic} \\ \text{attack power}\end{pmatrix}$$

Under our assumption of non-zero asymptotic power, the contrapositive implies that (C2) does not hold. ∎

IV. Implementable Statistical Tests

While Section III provides a necessary background for LTV Dynamic Watermarking, infinite limits are not well suited for real time attack detection. This section derives a statistical test using a sliding window approach. Let

$$\psi_n = \begin{bmatrix} V_n(C_n\hat{x}_n - y_n) \\ e_{n-1}\end{bmatrix} \quad (30)$$

$$Q_n = [\psi_{n-\ell} \;\ldots\; \psi_n][\psi_{n-\ell} \;\ldots\; \psi_n]^\intercal. \quad (31)$$

where $\ell+1$ is the window size, $\ell \in \mathbb{N}$, and $\ell \geq q+r-1$. Note, ψ_n is asymptotically uncorrelated and identically distributed such that $\psi_n \sim \mathcal{N}(0_{q+r\times 1}, S)$, for $n = 1, 2, 3, \cdots$ where $S = \text{blkdiag}(I_r, \Sigma_e)$. Therefore, under the assumption of no attack, the distribution of Q_n approaches a Wishart distribution with $\ell+1$ degrees of freedom and scale matrix S as ℓ goes to infinity. Furthermore, for a generalized replay attack with non-zero asymptotic power, Theorem III.6 proves that the scale matrix for Q_n is no longer S since either (C1) or (C2) is not satisfied. The Wishart distribution can then be used to define a statistical test using the negative log likelihood of the scale matrix S given the sampled matrix Q_n:

$$\mathcal{L}(Q_n) = (q + r - \ell)\log(|Q_n|) + tr(S^{-1}Q_n). \quad (32)$$

A negative log likelihood that exceeds a user-defined threshold signals an attack. Generally, the threshold is picked to minimize the frequency of false alarms while maintaining a desired level of sensitivity for the detection scheme. This tradeoff is dependent on the system under evaluation and can be studied through empirical or analytical means [15].

In theory, if the process and measurement noise covariances $\Sigma_{w,n}$ and $\Sigma_{z,n}$ are known, V_n can be calculated using (19)-(20). In practice, these covariances are difficult to estimate which can lead to error in the estimate of V_n. To reduce this error, V_n can be directly estimated using an ensemble average of i realizations such that

$$V_n \approx \left(\frac{1}{i}\sum_{j=1}^{i}(C_n\hat{x}_n^{(j)} - y_n^{(j)})(C_n\hat{x}_n^{(j)} - y_n^{(j)})^\intercal\right)^{-1/2} \quad (33)$$

where the superscript (j) is the index of the realization. This approximation is appropriate since by the weak law of large numbers we have that when no attack is present

$$\underset{i\to\infty}{\text{p-lim}}\ \frac{1}{i}\sum_{j=1}^{i}(C_n\hat{x}_n^{(j)} - y_n^{(j)})(C_n\hat{x}_n^{(j)} - y_n^{(j)})^\intercal = \\ = C_n\Sigma_{\delta,n}C_n^\intercal + \Sigma_{z,n} \quad (34)$$

and V_n is defined as in (20).

V. Simulated Results

To provide proof of concept, we use a simplified car model

$$\begin{bmatrix}\dot{x} & \dot{y} & \dot{\phi} & \dot{s} & \dot{\phi}\end{bmatrix}^\intercal = \begin{bmatrix}s\cos(\phi) & s\sin(\phi) & \dot{\phi} & a & \ddot{\phi}\end{bmatrix}^\intercal, \quad (35)$$

where the car has ground plane coordinates (x, y), heading ϕ, forward velocity s, and angular velocity $\dot{\phi}$. Using the desired trajectory shown in Figure 1, (35) is linearized and discretized using a step size of 0.05 and zero order hold on the current state and input. Note, for the discretized system, Assumption III.2 holds. The controller and observer for the resulting LTV system are found using a linear quadratic regulator (LQR) to stabilize the system, by enforcing a bound on $\bar{A}$ and $\underline{A}$ as stated in Assumptions III.1 and III.3. While linearizing non-linear stochastic systems often results in noise that is not independent zero mean Gaussian distributed, for this example we approximate it as such where $w_n \sim \mathcal{N}(0_{5\times1}, 10^{-5}I_5)$, $z_n \sim \mathcal{N}(0_{5\times1}, \text{diag}(4I_2 \times 10^{-3}, 3.6 \times 10^{-5}, s_n^2 \times 10^{-3}, 1.6 \times 10^{-7}))$. Note that the vehicle maintain a speed of 1.5 m/s to 3 m/s. As a result, this measurement noise over-approximates that of a vehicle relying upon RTK GNSS (within 20 km of a base station and using multiple antenna spaced 1 m apart) for measuring the ground plane positioning, heading, and velocity and an IMU for measuring angular velocity. Table I shows both the expected and over-approximated standard deviations of the measurement noise.

To compare LTI and LTV Dynamic Watermarking, a time invariant matrix normalization factor is calculated using the average of the residual covariance, while the time-varying matrix normalization factor is calculated using (33) with 100 realizations. For both cases, we run 100 simulations with a window size of 20 and calculate the test metric and the average test metric as shown in Figure 2. Note, while the LTV Dynamic Watermarking metric remains consistent over the simulation, the LTI counterpart has a repeatable time-varying pattern.

Measurement	Expected Std Dev	Over-approx. Std Dev
(x, y)	≤ 3 cm [55]	$2\sqrt{10} \approx 6.3$ cm
ψ	$< 3 \times 10^{-3}$ rad [56]	6×10^{-3} rad
s	0.2 cm/s to 5 cm/s [57]	$\sqrt{10}s_n \approx 3.2s_n$ cm/s
$\dot{\psi}$	2×10^{-4} rad/s [58]	4×10^{-4} rad/s

TABLE I

The standard deviation of measurement noise from a real-world RTK GNSS and an IMU system and the standard deviation of measurement noise used in the experiment. Note that the measurement noise used in the experiment over-approximates the noise one would expect to see in the real-world.

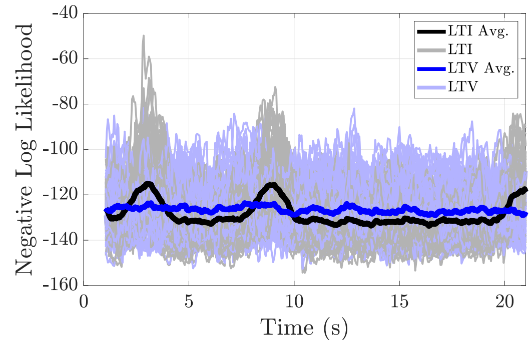


Fig. 2. Simulated LTI and LTV Dynamic Watermarking test metrics for LTV car model under no attack

Using the un-attacked data, a threshold for the LTV case is found such that the rate at which false alarms occur does not exceed once per every 50 seconds of run time. Next consider an attack model satisfying (12)-(18), with α equal to -1 and the measurement and process noise matching that of the true system. The results of this attack on the system, and the ability of LTV Dynamic Watermarking to quickly detect it, are shown in Figure 1.

VI. Conclusion

This paper derives Dynamic Watermarking for LTV systems, and provides asymptotic guarantees in addition to implementable tests. A LTV generalized replay attack is defined and shown to be detectable by the Dynamic Watermarking method developed in this work. Furthermore, a vehicle model with LTV Dynamic Watermarking is simulated to provide proof of concept of the implementable tests. Using these simulations, the LTV Dynamic Watermarking is compared to its LTI counterpart and is shown to provide a more consistent test metric. Potential future work includes analysis of robustness under approximation error in the matrix normalizing factor V_n, consideration for other potential test characteristics such as average time to detection and attack capability, and extensions to LTV systems under even less stringent assumptions.

References

[1] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, May 2011.

[2] M. Abrams and J. Weiss, "Malicious control system cyber security attack case study - Maroochy water services, australia," *MITRE*, 2008.

[3] R. M. Lee, M. J. Assante, and T. Conway, "German steel mill cyber attack," *Industrial Control Systems*, vol. 30, p. 62, 2014.

[4] ——, "Analysis of the cyber attack on the ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, 2016.

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

[6] A. A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems," in *Proceedings of the 3rd Conference on Hot Topics in Security*, ser. HOTSEC'08. Berkeley, CA, USA: USENIX Association, 2008, pp. 1–6.

[7] A. A. Cárdenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *The 28th International Conference on Distributed Computing Systems Workshops*, June 2008, pp. 495–500.

[8] S. Amin, A. A. Cárdenas, and S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *International Workshop on Hybrid Systems: Computation and Control*. Berlin, Heidelberg: Springer, 2009, pp. 31–45.

[9] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 13:1–13:33, Jun. 2011.

[10] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson, "Attack models and scenarios for networked control systems," in *Proceedings of the 1st International Conference on High Confidence Networked Systems*, ser. HiCoNS '12. New York, NY, USA: ACM, 2012, pp. 55–64.

[11] R. M. Ferrari and A. M. Teixeira, "Detection and isolation of routing attacks through sensor watermarking," in *2017 Annual American Control Conference (ACC)*, May 2017, pp. 5436–5442.

[12] R. S. Smith, "A decoupled feedback structure for covertly appropriating networked control systems," *IFAC Proceedings Volumes*, vol. 44, no. 1, pp. 90 – 95, 2011.

[13] Y. Yuan and Y. Mo, "Security in cyber-physical systems: Controller design against known-plaintext attack," in *54th IEEE Conference on Decision and Control (CDC)*, Dec 2015, pp. 5814–5819.

[14] D. Umsonst, E. Nekouei, A. M. Teixeira, and H. Sandberg, "On the confidentiality of linear anomaly detector states," in *2019 Annual American Control Conference (ACC)*, July 2019, pp. 397–403.

[15] M. Porter, A. Joshi, P. Hespanhol, R. Vasudevan, and A. Aswani, "Simulation and real-world evaluation of attack detection schemes," in *2019 Annual American Control Conference (ACC)*, July 2019, pp. 551–558.

[16] S. Weerakkody, O. Ozel, P. Griffioen, and B. Sinopoli, "Active detection for exposing intelligent attacks in control systems," in *2017 IEEE Conference on Control Technology and Applications (CCTA)*, Aug 2017, pp. 1306–1312.

[17] S. Weerakkody, B. Sinopoli, S. Kar, and A. Datta, "Information flow for security in control systems," in *55th IEEE Conference on Decision and Control (CDC)*, Dec 2016, pp. 5065–5072.

[18] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in *49th IEEE Conference on Decision and Control (CDC)*, Dec 2010, pp. 5967–5972.

[19] Y. Mo and B. Sinopoli, "Integrity attacks on cyber-physical systems," in *Proceedings of the 1st International Conference on High Confidence Networked Systems*, ser. HiCoNS '12. New York, NY, USA: ACM, 2012, pp. 47–54.

[20] C. Kwon, W. Liu, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks," in *2013 Annual American Control Conference (ACC)*, June 2013, pp. 3344–3349.

[21] N. Hashemi and J. Ruths, "Generalized chi-squared detector for lti systems with non-gaussian noise," in *2019 Annual American Control Conference (ACC)*, July 2019, pp. 404–410.

[22] C. Murguia and J. Ruths, "CUSUM and Chi-squared Attack Detection of Compromised Sensors," in *2016 IEEE Conference on Control Applications (CCA)*, Sep 2016, pp. 474–480.

[23] D. Umsonst and H. Sandberg, "Anomaly Detector Metrics for Sensor Data Attacks in Control Systems," in *2018 Annual American Control Conference (ACC)*, June 2018, pp. 153–158.

[24] S. Jajodia, A. K. Ghosh, V. Swarup, C. Wang, and X. S. Wang, *Moving target defense: creating asymmetric uncertainty for cyber threats*. Springer Science & Business Media, 2011, vol. 54.

[25] A. M. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "Revealing stealthy attacks in control systems," in *2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Oct 2012, pp. 1806–1813.

[26] M. A. Rahman, E. Al-Shaer, and R. B. Bobba, "Moving target defense for hardening the security of the power system state estimation," in *Proceedings of the First ACM Workshop on Moving Target Defense*, ser. MTD '14. New York, NY, USA: ACM, 2014, pp. 59–68.

[27] J. Tian, R. Tan, X. Guan, and T. Liu, "Hidden moving target defense in smart grids," in *Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids*, ser. CPSR-SG'17. New York, NY, USA: ACM, 2017, pp. 21–26.

[28] J. Giraldo, A. A. Cárdenas, and R. G. Sanfelice, "A moving target defense to detect stealthy attacks in cyber-physical systems," in *2019 Annual American Control Conference (ACC)*, July 2019, pp. 391–396.

[29] A. Kanellopoulos and K. Vamvoudakis, "Switching for unpredictability: A proactive defense control approach," in *2019 Annual American Control Conference (ACC)*, July 2019, pp. 4338–4343.

[30] S. Weerakkody and B. Sinopoli, "Detecting integrity attacks on control systems using a moving target approach," in *54th IEEE Conference on Decision and Control (CDC)*, Dec 2015, pp. 5820–5826.

[31] C. Schellenberger and P. Zhang, "Detection of covert attacks on cyber-physical systems by extending the system dynamics with an auxiliary system," in *56th IEEE Conference on Decision and Control (CDC)*, Dec 2017, pp. 1374–1379.

[32] M. Ghaderi, K. Gheitasi, and W. Lucia, "A novel control architecture for the detection of false data injection attacks in networked control systems," in *2019 Annual American Control Conference (ACC)*, July 2019, pp. 139–144.

[33] P. Griffioen, S. Weerakkody, and B. Sinopoli, "An optimal design of a moving target defense for attack detection in control systems," in *2019 Annual American Control Conference (ACC)*, July 2019, pp. 4527–4534.

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

[35] S. Weerakkody, Y. Mo, and B. Sinopoli, "Detecting integrity attacks on control systems using robust physical watermarking," in *53rd IEEE Conference on Decision and Control (CDC)*, Dec 2014, pp. 3757–3764.

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

[37] P. Hespanhol, M. Porter, R. Vasudevan, and A. Aswani, "Dynamic watermarking for general lti systems," in *56th IEEE Conference on Decision and Control (CDC)*, Dec 2017, pp. 1834–1839.

[38] B. Satchidanandan and P. Kumar, "Defending cyber-physical systems from sensor attacks," in *International Conference on Communication Systems and Networks*. Springer, 2017, pp. 150–176.

[39] P. Hespanhol, M. Porter, R. Vasudevan, and A. Aswani, "Statistical watermarking for networked control systems," in *2018 Annual American Control Conference (ACC)*, June 2018, pp. 5467–5472.

[40] J. Rubio-Hernan, L. De Cicco, and J. Garcia-Alfaro, "Event-triggered watermarking control to handle cyber-physical integrity attacks," in *Nordic Conference on Secure IT Systems*. Springer, 2016, pp. 3–19.

[41] W. H. Ko, B. Satchidanandan, and P. R. Kumar, "Theory and implementation of dynamic watermarking for cybersecurity of advanced transportation systems," in *2016 IEEE Conference on Communications and Network Security (CNS)*, 2016, pp. 416–420.

[42] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on scada systems," *IEEE Transactions on Control Systems Technology*, vol. 22, no. 4, pp. 1396–1407, July 2014.

[43] M. Hosseini, T. Tanaka, and V. Gupta, "Designing optimal watermark signal for a stealthy attacker," in *European Control Conference (ECC)*, June 2016, pp. 2258–2262.

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

[45] B. Satchidanandan and P. R. Kumar, "On the design of security-guaranteeing dynamic watermarks," *IEEE Control Systems Letters*, vol. 4, no. 2, pp. 307–312, April 2020.

[46] P. Hespanhol, M. Porter, R. Vasudevan, and A. Aswani, "Sensor switching control under attacks detectable by finite sample dynamic watermarking tests," *arXiv preprint arXiv:1909.00014*, 2019.

[47] O. Ozel, S. Weerakkody, and B. Sinopoli, "Physical watermarking for securing cyber physical systems via packet drop injections," in *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct 2017, pp. 271–276.

[48] S. Weerakkody, O. Ozel, and B. Sinopoli, "A bernoulli-gaussian physical watermark for detecting integrity attacks in control systems," in *2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Oct 2017, pp. 966–973.

[49] R. M. Ferrari and A. M. Teixeira, "Detection and isolation of replay attacks through sensor watermarking," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 7363–7368, 2017.

[50] A. M. Teixeira and R. M. Ferrari, "Detection of sensor data injection attacks with multiplicative watermarking," in *European Control Conference (ECC)*, June 2018, pp. 338–343.

[51] R. Romagnoli, S. Weerakkody, and B. Sinopoli, "A model inversion based watermark for replay attack detection with output tracking," in *2019 Annual American Control Conference (ACC)*, July 2019, pp. 384–390.

[52] T. Anderson, *An Introduction to Multivariate Statistical Analysis*, ser. Wiley Series in Probability and Statistics. Wiley, 2003.

[53] G. Grimmett and D. Stirzaker, *Probability and random processes*, 3rd ed. Oxford university press, 2001.

[54] E. Hendricks, O. Jannerup, and P. H. Sørensen, *Linear systems control: deterministic and stochastic methods*. Springer, 2008.

[55] W. Henning, "User guidelines for single base real time gnss positioning," *National Geodetic Survey*, version 3.1, April 2014.

[56] Septentrio, "AsteRx SB ProDirect datasheet," 2020, BBr: 06/2020.

[57] S. Ye, Y. Yan, and D. Chen, "Performance analysis of velocity estimation with bds," *The Journal of Navigation*, vol. 70, no. 3, p. 580, 2017.

[58] VectorNav Technologies, "Industrial Series datasheet," 2017, version 12-0009-R3.

[59] D. R. Brillinger, *Time series: data analysis and theory*. Siam, 1981, vol. 36.

[60] P. Billingsley, *Probability and Measure*, 3rd ed. Wiley, 1995.

APPENDIX

This section outlines the relevant background in statistics used in the paper and provides several of the proofs from the intermediate results.

A. Statistical Background

First, we provide inequalities for functions of random variables using the following three theorems.

Theorem A.1. *Let $(a_i)_{i=1}^s$ be a finite set of random variables then*

$$\mathbb{P}\left(\sum_{i=1}^s a_i > \epsilon\right) \leq \sum_{i=1}^s \mathbb{P}\left(a_i > \tfrac{\epsilon}{s}\right). \tag{36}$$

Proof. Assume $a_i < \frac{\epsilon}{s}\ \forall i$. This would imply that

$$\sum_{i=1}^s a_i < \sum_{i=1}^s \tfrac{\epsilon}{s} = \epsilon, \tag{37}$$

$$\left\{\sum_{i=1}^s a_i > \epsilon\right\} \subseteq \bigcup_{i=1}^s \left\{a_i > \tfrac{\epsilon}{s}\right\}. \tag{38}$$

Furthermore,

$$\mathbb{P}\left(\sum_{i=1}^s a_i > \epsilon\right) \leq \mathbb{P}\left(\bigcup_{i=1}^s \left\{a_i > \tfrac{\epsilon}{s}\right\}\right) \leq \leq \sum_{i=1}^s \mathbb{P}\left(a_i > \tfrac{\epsilon}{s}\right). \tag{39}$$

where the first inequality comes from the inclusion of the events and the final inequality comes from Boole's Inequality. ■

Theorem A.2. *Let $(a_i)_{i=1}^s$ be a finite set of random variables then*

$$\mathbb{P}\left(\prod_{i=1}^s |a_i| > \epsilon\right) \leq \sum_{i=1}^s \mathbb{P}\left(|a_i| > \epsilon^{\frac{1}{s}}\right). \tag{40}$$

Proof. Assume $|a_i| < \epsilon^{\frac{1}{s}}\ \forall i$. This would imply that

$$\prod_{i=1}^s |a_i| < \prod_{i=1}^s \epsilon^{\frac{1}{s}} = \epsilon. \tag{41}$$

The remainder of the proof follows closely to Theorem A.1. ■

Theorem A.3. *Let a and b be random variables then for $\epsilon, \gamma > 0$ we have*

$$\mathbb{P}\left(|ab| < \epsilon\right) \geq \mathbb{P}\left(|a| < \gamma\right) + \mathbb{P}\left(|b| < \tfrac{\epsilon}{\gamma}\right) - 1. \tag{42}$$

Proof. Note that

$$\mathbb{P}(|ab| < \epsilon) \geq \mathbb{P}\left(\{|a| < \gamma\} \cap \left\{|b| < \tfrac{\epsilon}{\gamma}\right\}\right) \tag{43}$$

since $|a| < \gamma$ and $|b| < \epsilon/\gamma$ implies $|ab| < \epsilon$. By expanding the RHS of (43) using inclusion exclusion and bounding the union term by 1, we get

$$\mathbb{P}(|ab| < \epsilon) \geq \mathbb{P}(|a| < \gamma) + \mathbb{P}\left(|b| < \tfrac{\epsilon}{\gamma}\right) - 1. \tag{44}$$

■

It is often helpful to split a probabilistic limit into components of the underlying random variable. While this is not possible for all cases, we provide sufficient conditions here.

Theorem A.4. *Given sequences of random variables a_i and b_i, and constants a and b, suppose that $\underset{i\to\infty}{\text{p-lim}}\ a_i + b_i = a + b$ and $\underset{i\to\infty}{\text{p-lim}}\ a_i = a$ then $\underset{i\to\infty}{\text{p-lim}}\ b_i = b$.*

Proof. Assume $\underset{i\to\infty}{\text{p-lim}}\ a_i + b_i = a + b$ and $\underset{i\to\infty}{\text{p-lim}}\ a_i = a$ hold. Given an $\epsilon > 0$, we have that

$$\mathbb{P}\left(\|b_i - b\| > \epsilon\right) \leq \mathbb{P}\left(\|a_i - a + b_i - b\| > \tfrac{\epsilon}{2}\right) + + \mathbb{P}\left(\|a_i - a\| > \tfrac{\epsilon}{2}\right) \tag{45}$$

where the inequality comes from triangle inequality and Theorem A.1. Since both terms in this upper bound converge to zero, their sum must as well. ■

Similarly we can combine probabilistic limits as follows.

Corollary A.5. *Consider sequences of random variables a_i and b_i and constants a and b. If $\underset{i\to\infty}{\text{p-lim}}\ b_i = b$ and $\underset{i\to\infty}{\text{p-lim}}\ a_i = a$ then $\underset{i\to\infty}{\text{p-lim}}\ a_i + b_i = a + b$.*

Proof. Let $a_i' = -a_i$, $a' = -a$, $b_i' = a_i + b_i$ and $b' = a + b$. Using Theorem A.4 on the new random variables gives us

$$\underset{i\to\infty}{\text{p-lim}}(a_i + b_i) = \underset{i\to\infty}{\text{p-lim}} b_i' = b' = a + b. \tag{46}$$

■

Since many of the limits in this paper deal with the average outer product of random vectors, it is important to know how and when these limits converge. The following theorem provides sufficient conditions for convergence.

Theorem A.6. *Consider the sequences of vectors $(f_i)_{i=1}^\infty$ and $(g_i)_{i=1}^\infty$ where $f_i \sim \mathcal{N}(0_{s\times 1}, \Sigma_{f,i})$ and $g_i \sim \mathcal{N}(0_{t\times 1}, \Sigma_{g,i})$. Let η and ϵ be scalar values such that $0 < \eta < \infty$ and $\epsilon > 1$. If*

$$\|\mathbb{E}[f_j f_i^\intercal]\|,\ \|\mathbb{E}[g_j g_i^\intercal]\|,\ \|\mathbb{E}[f_j g_i^\intercal]\| < \tfrac{\eta}{\epsilon^{|i-j|}}, \tag{47}$$

$\forall\ i, j \in \mathbb{N}$, then

$$\underset{i\to\infty}{\text{p-lim}}\quad \tfrac{1}{i}\sum_{j=1}^i f_j g_j^\intercal - \mathbb{E}[f_j g_j^\intercal] = 0_{s\times t}. \tag{48}$$

Proof. For (48) to hold, each of the element must also converge to 0 with probability 1. Therefore we will consider an arbitrary element and show it converges using an inequality derived from Chebyshev's inequality. Selecting the element in an arbitrary row m and column n such that $0 \leq m \leq s$ and $0 \leq n \leq t$, let

$$h_m^\intercal = \begin{bmatrix} 0_{1\times(m-1)} & 1 & 0_{1\times(s-m)} \end{bmatrix}, \quad (49)$$
$$h_n^\intercal = \begin{bmatrix} 0_{1\times(n-1)} & 1 & 0_{1\times(t-n)} \end{bmatrix}, \quad (50)$$

then the sum for this single element can be written as

$$\rho_i = \tfrac{1}{i}\textstyle\sum_{j=1}^{i} h_m^\intercal f_i g_i^\intercal h_n - h_m^\intercal \mathbb{E}[f_j g_j^\intercal] h_n. \quad (51)$$

In order to use Chebyshev's inequality we must first bound the second moment of ρ_i. We start by expanding ρ_i^2 using (51) and canceling like terms to get

$$\left|\mathbb{E}[\rho_i^2]\right| = \left|\tfrac{1}{i^2}\textstyle\sum_{j=1}^{i}\sum_{k=1}^{i} \mathbb{E}[h_m^\intercal f_j g_j^\intercal h_n h_m^\intercal f_k g_k^\intercal h_n] + \right.$$
$$\left. - h_m^\intercal \mathbb{E}[f_j g_j^\intercal] h_n h_m^\intercal \mathbb{E}[f_k g_k^\intercal] h_n\right|. \quad (52)$$

Expanding the expectation in the first term using [59, Equation 2.3.8] and once again canceling like terms results in

$$\left|\mathbb{E}[\rho_i^2]\right| = \left|\tfrac{1}{i^2}\textstyle\sum_{j=1}^{i}\sum_{k=1}^{i} h_m^\intercal \mathbb{E}[f_j g_k^\intercal] h_n h_m^\intercal \mathbb{E}[f_k g_j^\intercal] h_n + \right.$$
$$\left. + h_m^\intercal \mathbb{E}[f_j f_k^\intercal] h_m h_n^\intercal \mathbb{E}[g_j g_k^\intercal] h_n\right|. \quad (53)$$

Distributing the norm across the addition and multiplication using triangle inequality and the sub-multiplicative property of the 2 norm we then get the upper bound

$$\left|\mathbb{E}[\rho_i^2]\right| \leq \tfrac{1}{i^2}\textstyle\sum_{j=1}^{i}\sum_{k=1}^{i} \|h_m\|^2 \|h_n\|^2 \|\mathbb{E}[f_j g_k^\intercal]\| \times$$
$$\times \|\mathbb{E}[f_k g_j^\intercal]\| + \|h_m\|^2 \|h_n\|^2 \|\mathbb{E}[f_j f_k^\intercal]\| \; \|\mathbb{E}[g_j g_k^\intercal]\|. \quad (54)$$

Applying the bounds in (47) and the fact that $\|h_m\| = \|h_n\| = 1$ we can further upper bound resulting in

$$\left|\mathbb{E}[\rho_i^2]\right| \leq \tfrac{1}{i^2}\textstyle\sum_{j=1}^{i}\sum_{k=1}^{i} \frac{2\eta^2}{\epsilon^{2|j-k|}} \quad (55)$$

Furthermore,

$$\left|\mathbb{E}[\rho_i^2]\right| \leq \tfrac{1}{i^2}\textstyle\sum_{j=1}^{i}\sum_{k=1}^{\infty} \frac{4\eta^2}{\epsilon^{2k}} = \frac{4\eta^2}{i(1-\frac{1}{\epsilon^2})}. \quad (56)$$

where the inequality comes from the summation in (56) containing all of the summands in (55) and the fact that all summands are non-negative. Finally, using this bound and applying Chebyshev's Inequality [60, Equation 5.32] we have that, for an arbitrary choice of $\beta > 0$,

$$P(|\rho_i| > \beta) \leq \frac{\mathbb{E}[\rho_i^2]}{\beta^2} = \frac{4\eta^2}{i\beta^2(1-\frac{1}{\epsilon^2})}. \quad (57)$$

Therefore, ρ_i converges to 0 with probability 1. Since the matrix element was chosen arbitrarily, (48) must hold. ■

Using Theorem A.6, we can make similar claims for bounded linear transforms of Gaussian sequences.

Corollary A.7. *Consider a pair of sequences of vectors $(f_i)_{i=1}^{\infty}$ and $(g_i)_{i=1}^{\infty}$ where $f_i \sim \mathcal{N}(0_{s\times1}, \Sigma_{f,i})$ and $g_i \sim \mathcal{N}(0_{t\times1}, \Sigma_{g,i})$. Furthermore, consider the sequences of time varying matrices $(T_i)_{i=1}^{\infty}$ and $(U_i)_{i=1}^{\infty}$, where $T_i \in \mathbb{R}^{s'\times s}$ and $U_i \in \mathbb{R}^{t'\times t}$. Assume that*

$$\|T_i\| \leq \eta_T \quad \text{and} \quad \|U_i\| \leq \eta_U. \quad (58)$$

Let $\eta, \epsilon \in \mathbb{R}$ such that $0 < \eta < \infty$ and $\epsilon > 1$. If

$$\|\mathbb{E}[f_j f_i^\intercal]\|,\ \|\mathbb{E}[g_j g_i^\intercal]\|,\ \|\mathbb{E}[f_j g_i^\intercal]\| < \frac{\eta}{\epsilon^{|i-j|}}, \quad (59)$$

$\forall\ i, j \in \mathbb{N}$, then

$$\operatorname*{p-lim}_{i\to\infty} \ \tfrac{1}{i}\textstyle\sum_{j=1}^{i} T_j f_j g_j^\intercal U_j^\intercal - \mathbb{E}T_j \left[f_j g_j^\intercal\right] U_j^\intercal = 0_{s'\times t'}. \quad (60)$$

Proof. We prove this result by showing that the bounded linear transform generates new sequences that satisfy the conditions described in Theorem A.6. Let

$$f_i' = T_i f_i \ \forall i \ \text{ and } g_i' = U_i g_i \ \forall i \quad (61)$$

then $f_i' \sim \mathcal{N}(0_{s'\times1}, T_i\Sigma_{f,i}T_i^\intercal)$ and $g_i' \sim \mathcal{N}(0_{t'\times1}, U_i\Sigma_{g,i}U_i^\intercal)$. Furthermore, we have that

$$\|\mathbb{E}[f_j' f_i'^\intercal]\| \leq \|T_j\|\|T_i\|\|\mathbb{E}[f_j f_i^\intercal]\| < \frac{\eta_T^2\eta}{\epsilon^{|i-j|}} \quad (62)$$

where the first inequality comes from the submultiplicative property of the spectral norm and the second from applying (59) and (58). Similarly,

$$\|\mathbb{E}[g_j' g_i'^\intercal]\| < \frac{\eta_U^2\eta}{\epsilon^{|i-j|}} \quad \text{and} \quad \|\mathbb{E}[f_j' g_i'^\intercal]\| < \frac{\eta_U\eta_T\eta}{\epsilon^{|i-j|}}. \quad (63)$$

Let $\eta' = \max\{\eta_U^2\eta, \eta_T^2\eta, \eta_U\eta_T\eta\}$ and $\epsilon' = \epsilon$ then

$$\|\mathbb{E}[f_j' f_i'^\intercal]\|,\ \|\mathbb{E}[g_j' g_i'^\intercal]\|,\ \|\mathbb{E}[f_j' g_i'^\intercal]\| < \frac{\eta'}{\epsilon'^{|i-j|}} \quad (64)$$

which satisfies the conditions for using Theorem A.6 which implies that

$$\operatorname*{p-lim}_{i\to\infty} \ \tfrac{1}{i}\textstyle\sum_{j=1}^{i} f_j' g_j'^\intercal - \mathbb{E}[f_j' g_j'^\intercal] = 0_{s'\times t'}, \quad (65)$$

which completes the proof since

$$f_j' g_j'^\intercal - \mathbb{E}[f_j' g_j'^\intercal] = T_j f_j g_j^\intercal U_j^\intercal - T_j \mathbb{E}[f_j g_j^\intercal] U_j^\intercal. \quad (66)$$

■

To use Theorem A.6 and Corollary A.7, we provide sufficient conditions for a Gaussian sequence to satisfy conditions (47) and (59).

Theorem A.8. *Consider the Gaussian process*

$$a_{i+1} = M_i a_i + b_i \quad (67)$$

where $a_0 = 0_{s\times1}$ and b_i are independent gaussian distributed random vaiables such that $b_i \sim \mathcal{N}(0_{s\times1}, \Sigma_{b,i})$. If $\exists \epsilon_1, \epsilon_2$ such that $\|M_i\| < \epsilon_1 < 1$ and $\|\Sigma_{b,i}\| < \epsilon_2 < \infty \ \forall\ i$ then

$$\|\mathbb{E}\left[a_j a_i^\intercal\right]\| < \frac{\eta}{\epsilon^{|i-j|}}, \quad (68)$$

where $\eta = \frac{\epsilon_2}{1-\epsilon_1^2}$ and $\epsilon = \frac{1}{\epsilon_1}$.

Proof. Consider the LHS of (68) when $i = j$. We can expand $a_j a_j^T$ using (67) iterativley to get

$$\|\mathbb{E}[a_j a_j^\intercal]\| =$$
$$= \left\|\textstyle\sum_{i=1}^{j} M_{j-1}\ldots M_{j-i+1}\Sigma_{b,j-i}M_{j-i+1}^\intercal\ldots M_{j-1}^\intercal\right\|. \quad (69)$$

We upper bound this norm as follows

$$\|\mathbb{E}[a_j a_j^\intercal]\| \leq \textstyle\sum_{i=1}^{j} \|M_{j-1}\|\ldots\|M_{j-i+1}\| \times$$
$$\times \|\Sigma_{b,j-i}\| \ \|M_{j-i+1}^\intercal\|\ldots\|M_{j-1}^\intercal\|$$
$$< \textstyle\sum_{i=1}^{i} \epsilon_2\epsilon_1^{2(j-1)} \leq \frac{\epsilon_2}{1-\epsilon_1^2}, \quad (70)$$

where the first inequality comes from applying triangle inequality and the sub-multiplicative property of the spectral norm and the second inequality comes from applying the bounds on $\|M_i\|$ and $\|\Sigma_{b,i}\|$ and then bounding the resulting geometric series.

We now focus on (68) for when $i \neq j$. Consider the following which has been expanded using (67)

$$\|\mathbb{E}[a_{j+i}a_j^\intercal]\| = \|\mathbb{E}[a_j a_{j+i}^\intercal]\| = \|\mathbb{E}[a_j(M_{j+i-1}\dots M_j a_j + \\ + \textstyle\sum_{k=1}^{i} M_{j+i-1}\dots M_{j+i-k+1}b_{j+i-k})^\intercal]\|. \quad (71)$$

Since $\mathbb{E}[a_j b_{j+i-k}] = 0 \; \forall \; k \leq i$, this simplifies to

$$\|\mathbb{E}[a_{j+i}a_j^\intercal]\| = \|\mathbb{E}[a_j a_{j+i}^\intercal]\| \\ = \|\mathbb{E}[a_j a_j^\intercal] M_j^\intercal \dots M_{j+i-1}^\intercal\| < \tfrac{\eta}{\epsilon^i}, \quad (72)$$

where the inequality comes from (70) and $\|M_i\| < \epsilon_1$. ■

Next, we show that, when α being equal to 0, the full system state satisfies the conditions of Theorem A.8.

Theorem A.9. *Consider an attacked LTV system satisfying the dynamics in* (12)-(18) *and the attack model in* (21)-(22). *Assume the attack scaling factor α is equal to 0. Then $\exists\, \eta > 0$ and $\epsilon > 1$ such that*

$$\left\| \mathbb{E}\left[\begin{bmatrix} x_n \\ \bar{\delta}_n \\ \hat{\delta}_n \\ \xi_n \end{bmatrix} \begin{bmatrix} x_{n+i} \\ \bar{\delta}_{n+i} \\ \hat{\delta}_{n+i} \\ \xi_{n+i} \end{bmatrix}^\intercal \right] \right\| < \tfrac{\eta}{\epsilon^i}. \quad (73)$$

Proof. We prove this result using Theorem A.8. First note that using (12)-(18), (21)-(22), and assuming $\alpha = 0$ we can write

$$a_{n+1} = M_n a_n + b_n \quad (74)$$

where $a_n = \begin{bmatrix} x_n^\intercal & \bar{\delta}_n^\intercal & \hat{\delta}_n^\intercal & \xi_n^\intercal \end{bmatrix}^\intercal$,

$$M_n = \begin{bmatrix} \bar{A}_n & B_n K_n & B_n K_n & 0_p \\ 0_p & \underline{A}_n & 0_p & 0_p \\ 0_p & 0_p & \underline{A}_n & -L_n C_n \\ 0_p & 0_p & 0_p & \bar{A}_n \end{bmatrix}, \quad (75)$$

and $b_n = T_n \begin{bmatrix} e_n^\intercal & w_n^\intercal & z_n^\intercal & \zeta_n^\intercal & \omega_n^\intercal \end{bmatrix}^\intercal$ with

$$T_n = \begin{bmatrix} B_n & I_p & 0_{p\times r} & 0_{p\times r} & 0_p \\ 0_{p\times q} & -I_p & -L_n & 0_{p\times r} & 0_p \\ 0_{p\times q} & 0_p & 0_{p\times r} & -L_n & 0_p \\ 0_{p\times q} & 0_p & 0_{p\times r} & 0_{p\times r} & I_p \end{bmatrix}. \quad (76)$$

Let $\epsilon_1 = \max\{\eta_{A1}, \eta_{A2}\}$ then $\|M_n\| < \epsilon_1 < 1$ since the eigenvalues of upper block diagonal matrices are the set of eigenvalues of the block elements on the diagonal and $\|\bar{A}_n\| < \eta_{A1} < 1$ and $\|\underline{A}_n\| < \eta_{A2} < 1$. Furthermore, $b_n \sim \mathcal{N}(0, \Sigma_{b,n})$ where

$$\Sigma_{b,n} = T_n \text{ blkdiag}(\Sigma_e, \Sigma_{w,n}, \Sigma_{z,n}, \Sigma_{\zeta,n}, \Sigma_{\omega,n}) T_n^\intercal. \quad (77)$$

Since $B_n, L_n, \Sigma_e, \Sigma_{w,n}, \Sigma_{z,n}, \Sigma_{\zeta,n},$ and $\Sigma_{\omega,n}$ are all bounded we have that $\|\Sigma_{b,n}\| < \epsilon_2$ for some $0 \leq \epsilon_2 < \infty$. Using Theorem A.8 completes the proof. ■

Since the asymptotic attack power uses the inner product of v_n while most other limits use outer products, we relate these limits in the following Lemma.

Lemma A.10. *Consider a sequence of random vectors $(b_n)_{n=0}^{\infty}$ such that $b_n \in \mathbb{R}^s$.*

$$\underset{i\to\infty}{\text{p-lim}} \; \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} b_n b_n^\intercal = 0_s \;\Leftrightarrow\; \underset{i\to\infty}{\text{p-lim}} \; \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} b_n^\intercal b_n = 0. \quad (78)$$

Proof. Assume that the RHS of (78) holds. Note that

$$\left\| \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} b_n b_n^\intercal \right\| \leq \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} \|b_n b_n^\intercal\| = \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} b_n^\intercal b_n. \quad (79)$$

where the inequality comes from the triangle inequality and the equality comes from the matrix $b_n b_n^\intercal$ being singular. This implies that

$$\mathbb{P}\left(\left| \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} b_n^\intercal b_n \right| > \epsilon \right) \geq \mathbb{P}\left(\left\| \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} b_n b_n^\intercal \right\| > \epsilon \right). \quad (80)$$

Since the LHS of (80) converges to zero as $i \to \infty$ as a result of our assumption, the RHS must do so as well which directly implies the LHS of (78) holds.

Now assume that the LHS of (78) holds. Then since

$$\tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} b_n^\intercal b_n = \text{tr}\left(\tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} b_n b_n^\intercal \right), \quad (81)$$

and for the matrix to converge it must also converge element-wise, we have that the RHS of (78) also holds. ■

Next, we show that if conditions such as (C2) do not hold, linear transforms of the limit also do not converge to zero given the conditions in the following lemma hold.

Lemma A.11. *Consider a family of matrices $R_n \in \mathbb{R}^{t\times s}$ with full column rank. Assume there exists $\eta \in \mathbb{R}$ such that $0 < \eta \leq \lambda_n$, where λ_n is the smallest eigenvalue of $R_n^T R_n$. Furthermore, consider a sequence of random vectors $f_n \sim \mathcal{N}(0_{s\times 1}, \Sigma_f)$ such that $\Sigma_{f,n}$ is positive semi-definite. If*

$$\textstyle\sum_{i=1}^{\infty} \|\mathbb{E}[f_n f_{n+i}^\intercal]\| < \infty \;\forall n \quad (82)$$

$$\underset{i\to\infty}{\text{p-lim}} \; \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} f_n f_n^\intercal \neq 0_s, \quad (83)$$

then

$$\underset{i\to\infty}{\text{p-lim}} \; \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} R_n f_n f_n^\intercal R_n^\intercal \neq 0_t. \quad (84)$$

Proof. (Lemma A.11) Assume that (82)-(83) holds, but

$$\underset{i\to\infty}{\text{p-lim}} \; \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} R_n f_n f_n^\intercal R_n^\intercal = 0_t. \quad (85)$$

Applying Lemma A.10 we have that

$$\underset{i\to\infty}{\text{p-lim}} \; \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} f_n^\intercal R_n^\intercal R_n f_n = 0. \quad (86)$$

This implies that

$$\underset{i\to\infty}{\text{p-lim}} \; \frac{\eta}{i}\textstyle\sum_{n=0}^{i-1} f_n^\intercal f_n = 0 \quad (87)$$

since $\eta f_n^\intercal f_n \leq \lambda_n f_n^\intercal f_n \leq f_n^\intercal R_n^\intercal R_n f_n$. Since the limit is not affected by the constant η, and using Lemma A.10, this contradicts (83). Therefore, (84) must hold. ■

B. Proofs

Proof. **(Lemma III.7)** Assume that α is equal to 0. Rearranging the LHS of (C1) using (13), (16), and (21) results in

$$\begin{aligned}&\underset{i\to\infty}{\text{p-lim}}\ \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} V_n(C_n\hat{x}_n - y_n)e_{n-1}^{\mathsf{T}} = \\ &= \underset{i\to\infty}{\text{p-lim}}\ \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} V_n(C_n\delta_n - z_n - C_n\xi_n - \zeta_n)e_{n-1}^{\mathsf{T}}. \quad (88)\end{aligned}$$

Corollary A.5 says that to show that the RHS of (88) converges in probability to $0_{r\times q}$, it is sufficient to show that each term in the sum converges in probability to $0_{r\times q}$. Note that

$$\underset{i\to\infty}{\text{p-lim}}\ \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} V_n(C_n\delta_n - C_n\xi_n)e_{n-1}^{\mathsf{T}} = 0_{r\times q} \quad (89)$$

by Corollary A.7 since e_{n-1} is independent identically distributed with bounded covariance, and $V_n(C_n\delta_n - C_n\xi_n)$ is a bounded linear transform of a random vector that satisfies the necessary auto correlation bound as a result of Theorem A.9. Similarly,

$$\underset{i\to\infty}{\text{p-lim}}\ \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} V_n(-z_n - \zeta_n)e_{n-1}^{\mathsf{T}} = 0_{r\times q} \quad (90)$$

by Corollary A.7 since z_n, ζ_n, and e_{n-1} are mutually independent identically distributed with bounded covariances. Therefore $\alpha = 0$ implies (C1) holds.

Now assume that (C1) holds. Rearranging (C1) using (13), (16), and (21) results in

$$\begin{aligned}&\underset{i\to\infty}{\text{p-lim}}\ \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} V_n(C_n\hat{x}_n - y_n)e_{n-1}^{\mathsf{T}} = \\ &= \underset{i\to\infty}{\text{p-lim}}\ \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} V_n(C_n\delta_n - (1+\alpha)z_n + \\ &\qquad - \alpha C_n x_n - C_n\xi_n - \zeta_n)e_{n-1}^{\mathsf{T}}. \quad (91)\end{aligned}$$

Now since (90) holds by the same argument as before, we can use Theorem A.4 to cancel these terms resulting in

$$\begin{aligned}&\underset{i\to\infty}{\text{p-lim}}\ \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} V_n(C_n\hat{x}_n - y_n)e_{n-1}^{\mathsf{T}} = \\ &= \underset{i\to\infty}{\text{p-lim}}\ \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} V_n(C_n\delta_n - \alpha C_n x_n)e_{n-1}^{T}. \quad (92)\end{aligned}$$

Expanding x_n in (92) by one step using (12) then results in

$$\begin{aligned}&\underset{i\to\infty}{\text{p-lim}}\ \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} V_n(C_n\hat{x}_n - y_n)e_{n-1}^{\mathsf{T}} = \\ &= \underset{i\to\infty}{\text{p-lim}}\ \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} V_n(C_n\delta_n - \alpha C_n(A_{n-1}x_{n-1} + \\ &\quad + B_{n-1}K_{n-1}\hat{x}_{n-1} + B_{n-1}e_{n-1} + w_{n-1}))e_{n-1}^{\mathsf{T}}. \quad (93)\end{aligned}$$

Using Corollary A.7 we have that

$$\underset{i\to\infty}{\text{p-lim}}\ \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} -\alpha V_n C_n B_{n-1}(e_{n-1}e_{n-1}^{\mathsf{T}} - \Sigma_e) = 0_{q\times r}. \quad (94)$$

Therefore by Theorem, A.4 we have

$$\begin{aligned}&\underset{i\to\infty}{\text{p-lim}}\ \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} V_n(C_n\hat{x}_n - y_n)e_{n-1}^{\mathsf{T}} = \\ &= \underset{i\to\infty}{\text{p-lim}}\ \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} V_n(C_n\delta_n - \alpha C_n(A_{n-1}x_{n-1} + \\ &\quad + B_{n-1}K_{n-1}\hat{x}_{n-1} + w_{n-1}))e_{n-1}^{\mathsf{T}} + \alpha V_n C_n B_{n-1}\Sigma_e. \quad (95)\end{aligned}$$

Note, that all elements of

$$\begin{aligned}&V_n(C_n\delta_n - \alpha C_n(A_{n-1}x_{n-1} + \\ &\qquad + B_{n-1}K_{n-1}\hat{x}_{n-1} + w_{n-1}))e_{n-1}^{\mathsf{T}} \quad (96)\end{aligned}$$

are distributed symmetrically about 0 for all $n \in \mathbb{N}$. Consider an element of (95) for which the corresponding element in

$$\tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} V_n C_n B_{n-1}\Sigma_e \quad (97)$$

does not converge. For each i, the probability that the matrix element in (95) is farther away from 0 than the corresponding element in (97) is at least 0.5. Therefore the element cannot converge in probability to 0 completing the proof. ■

Proof. **(Lemma III.8)** Expanding (C2) using (13) and (16)-(18) gives us

$$\begin{aligned}&\underset{i\to\infty}{\text{p-lim}}\ \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} V_n(C_n\hat{x}_n - y_n)(C_n\hat{x}_n - y_n)^{\mathsf{T}}V_n^{\mathsf{T}} = \\ &= \underset{i\to\infty}{\text{p-lim}}\ \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} V_n(C_n\bar{\delta}_n - z_n)(C_n\bar{\delta}_n - z_n)^{\mathsf{T}}V_n^{\mathsf{T}} + \\ &\quad + V_n(C_n\bar{\delta}_n - z_n)(C_n\hat{\delta}_n - v_n)^{\mathsf{T}}V_n^{\mathsf{T}} + \\ &\quad + V_n(C_n\hat{\delta}_n - v_n)(C_n\bar{\delta}_n - z_n)^{\mathsf{T}}V_n^{\mathsf{T}} + \\ &\quad + V_n(C_n\hat{\delta}_n - v_n)(C_n\hat{\delta}_n - v_n)^{\mathsf{T}}V_n^{\mathsf{T}}. \quad (98)\end{aligned}$$

By Corollary A.7 and Theorem A.9,

$$\underset{i\to\infty}{\text{p-lim}}\ \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} V_n(C_n\bar{\delta}_n - z_n)(C_n\bar{\delta}_n - z_n)^{\mathsf{T}}V_n^{\mathsf{T}} = I_r, \quad (99)$$

$$\underset{i\to\infty}{\text{p-lim}}\ \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} V_n(C_n\bar{\delta}_n - z_n)(C_n\hat{\delta} - v_n)^{\mathsf{T}}V_n^{\mathsf{T}} = 0_r \quad (100)$$

since, by the definition of V_n in (20), the expectation for each summand in (99) is I_r, and $V_n(C_n\bar{\delta}_n - z_n)$ is uncorrelated with $V_n(C_n\hat{\delta} - v_n)$. First, assume that (C2) holds. By Theorem A.4, it follows from (98)-(100) that (24) must hold. Next, assume that (24) holds. By Corollary A.5, it follows from (98)-(100) that (C2) holds. ■

Proof. **(Lemma III.9)** Assume that $\alpha = 0$. Using Lemma A.10, the asymptotic attack power is 0 if and only if

$$\underset{i\to\infty}{\text{p-lim}}\tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} v_n v_n^{\mathsf{T}} = 0_r. \quad (101)$$

Expanding the LHS of (101) using (21)-(22) we get an equvalent condition.

$$\begin{aligned}&\underset{i\to\infty}{\text{p-lim}}\tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} C_n\xi_n\xi_n^{\mathsf{T}}C_n^{\mathsf{T}} + \\ &\quad + C_n\xi_n\zeta_n^{\mathsf{T}} + (C_n\xi_n\zeta_n^{\mathsf{T}})^{\mathsf{T}} + \zeta_n\zeta_n^{\mathsf{T}} = 0_r \quad (102)\end{aligned}$$

Since ξ_n and ζ_n are uncorrelated, from Theorem A.9 and Corollary A.7 we have

$$\underset{i\to\infty}{\text{p-lim}}\tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} C_n\xi_n\zeta_n^{\mathsf{T}} = 0_r. \quad (103)$$

First, assume that (25) and (26) hold. By Corollary A.5 we have that (102) must hold since, when separated, the limit for each term converges to 0_r. Next, assume that (102) holds. By Theorem A.4 we can rewrite (102) as

$$\underset{i\to\infty}{\text{p-lim}}\tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} \zeta_n\zeta_n^{\mathsf{T}} + C_n\xi_n\xi_n^{\mathsf{T}}C_n^{\mathsf{T}} = 0_r, \quad (104)$$

since (103) holds. Note, both terms are positive-semidefinite matrices. Therefore, for an arbitrary $\epsilon > 0$ we have that

$$\mathbb{P}\left(\left\|\frac{1}{i}\sum_{n=0}^{i-1}\zeta_n\zeta_n^{\intercal}\right\| > \epsilon\right) \leq \leq \mathbb{P}\left(\left\|\frac{1}{i}\sum_{n=0}^{i-1}\zeta_n\zeta_n^{\intercal} + C_n\xi_n\xi_n^{\intercal}C_n^{\intercal}\right\| > \epsilon\right) \quad (105)$$

Furthermore, (104) implies

$$\lim_{i\to\infty}\mathbb{P}\left(\left\|\frac{1}{i}\sum_{n=0}^{i-1}\zeta_n\zeta_n^{\intercal} + C_n\xi_n\xi_n^{\intercal}C_n^{\intercal}\right\| > \epsilon\right) = 0_r,\ \forall\epsilon > 0 \quad (106)$$

Then, by (105) and (106)

$$\lim_{i\to\infty}\mathbb{P}\left(\left\|\frac{1}{i}\sum_{n=0}^{i-1}\zeta_n\zeta_n^{\intercal}\right\| > \epsilon\right) = 0_r,\ \forall\epsilon > 0. \quad (107)$$

Therefore, (25) must hold. Applying Theorem A.4 to (104) using (25) implies (26) must also hold. ■

Proof. **(Lemma III.10)** Assume that (24) holds. Expanding the LHS of (24) using (21) we get

$$\operatorname*{p-lim}_{i\to\infty}\frac{1}{i}\sum_{n=0}^{i-1}V_n(C_n\hat{\delta}_n - C_n\xi_n)(C_n\hat{\delta}_n - C_n\xi_n)^{\intercal}V_n^{\intercal} + + V_n(C_n\hat{\delta}_n - C_n\xi_n)\zeta_n^{\intercal}V_n^{\intercal} + (V_n(C_n\hat{\delta}_n - C_n\xi_n)\zeta_n^{\intercal}V_n^{\intercal})^{\intercal} + + V_n\zeta_n\zeta_n^{\intercal}V_n^{\intercal} = 0_r. \quad (108)$$

Using Corollary A.7 and Theorem A.9 we have

$$\operatorname*{p-lim}_{i\to\infty}\frac{1}{i}\sum_{n=0}^{i-1}V_n(C_n\hat{\delta}_n - C_n\xi_n)\zeta_n^{\intercal}V_n^{\intercal} = 0_r. \quad (109)$$

Therefore, by applying Theorem A.4 to (108) we have

$$\operatorname*{p-lim}_{i\to\infty}\frac{1}{i}\sum_{n=0}^{i-1}V_n(C_n\hat{\delta}_n - C_n\xi_n)(C_n\hat{\delta}_n - C_n\xi_n)^{\intercal}V_n^{\intercal} + + V_n\zeta_n\zeta_n^{\intercal}V_n^{\intercal} = 0_r. \quad (110)$$

Note, both terms are positive-semidefinite matrices. Using the same method used on (104), we then have

$$\operatorname*{p-lim}_{i\to\infty}\frac{1}{i}\sum_{n=0}^{i-1}V_n\zeta_n\zeta_n^{\intercal}V_n^{\intercal} = 0_r, \quad (111)$$

$$\operatorname*{p-lim}_{i\to\infty}\frac{1}{i}\sum_{n=0}^{i-1}V_n(C_n\hat{\delta}_n - C_n\xi_n)(C_n\hat{\delta}_n - C_n\xi_n)^{\intercal}V_n^{\intercal} = 0_r. \quad (112)$$

We complete the proof using Lemma A.11 but we must first lower bound the eigenvalues of $V_n^{\intercal}V_n$. Let λ_n denote the smallest eignenvalue of $V_n^{\intercal}V_n$, then λ_n is lower bounded since

$$\lambda_n = \frac{1}{\|(V_n^{\intercal}V_n)^{-1}\|} = \frac{1}{\|C_n\Sigma_{\delta,n}C_n^{\intercal} + \Sigma_{z,n}\|} \geq \geq \frac{1}{\eta_C^2\eta_\delta + \eta_z} > 0. \quad (113)$$

If we assume that (25) does not hold then applying Lemma A.11 contradicts (111). Therefore (25) must hold. Similarly, assuming that (27) does not hold would result in a contradiction with (112). Therefore (27) must also hold. ■

Proof. **(Lemma III.12)** First, we prove the existence of m. Assume that (26) does not hold. Expanding the LHS of (26) using (22) results in

$$\operatorname*{p-lim}_{i\to\infty}\frac{1}{i}\sum_{n=0}^{i-1}\left(\sum_{j=1}^{n}C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right) \times \times \left(\sum_{j=1}^{n}C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right)^{\intercal} \neq 0_r. \quad (114)$$

Then, using Lemma A.10 we have that

$$\operatorname*{p-lim}_{i\to\infty}\frac{1}{i}\sum_{n=0}^{i-1}\left\|\sum_{j=1}^{n}C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right\|^2 \neq 0. \quad (115)$$

Since (26) does not hold there exists $\epsilon, \tau > 0$ such that

$$\mathbb{P}\left(\frac{1}{i}\sum_{n=0}^{i-1}\left\|\sum_{j=1}^{n}C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right\|^2 > \epsilon\right) > \tau \quad (116)$$

for infinitely many i. We prove that there exists an m such that for each i that (116) holds we have

$$\mathbb{P}\left(\frac{1}{i}\sum_{n=0}^{i-1}\left\|\sum_{j=1}^{m_n}C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right\|^2 > \frac{\epsilon}{6}\right) > \frac{\tau}{4} \quad (117)$$

which is equivalent to (28) as a result of Lemma A.10. To make statements on the truncated sum, we start by finding the relationship between the probability in the LHS of (116) and the probability in the LHS of (117). For each i such that (116) holds, we apply triangle inequality to get

$$\tau < \mathbb{P}\Bigg(\frac{1}{i}\sum_{n=0}^{i-1}\Bigg(\left\|\sum_{j=1}^{m_n}C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right\| + + \left\|\sum_{j=m_n+1}^{n}C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right\|\Bigg)^2 > \epsilon\Bigg). \quad (118)$$

Further expanding and applying Theorem A.1 result in

$$\tau < \mathbb{P}\left(\frac{1}{i}\sum_{n=0}^{i-1}\left\|\sum_{j=1}^{m_n}C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right\|^2 > \frac{\epsilon}{3}\right) + + \mathbb{P}\Bigg(\frac{2}{i}\sum_{n=0}^{i-1}\left\|\sum_{j=1}^{m_n}C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right\| \times \times \left\|\sum_{j=m_n+1}^{n}C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right\| > \frac{\epsilon}{3}\Bigg) + + \mathbb{P}\left(\frac{1}{i}\sum_{n=0}^{i-1}\left\|\sum_{j=m_n+1}^{n}C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right\|^2 > \frac{\epsilon}{3}\right). \quad (119)$$

Focusing on the center term in the RHS of (119), we can write

$$\mathbb{P}\Bigg(\frac{2}{i}\sum_{n=0}^{i-1}\left\|\sum_{j=1}^{m_n}C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right\| \times \times \left\|\sum_{j=m_n+1}^{n}C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right\| > \frac{\epsilon}{3}\Bigg) \leq \leq \mathbb{P}\Bigg(\sqrt{\frac{2}{i}\sum_{n=0}^{i-1}\left\|\sum_{j=1}^{m_n}C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right\|^2} \times \times \sqrt{\frac{2}{i}\sum_{n=0}^{i-1}\left\|\sum_{j=m_n+1}^{n}C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right\|^2} > \frac{\epsilon}{3}\Bigg) \leq \leq \mathbb{P}\left(\frac{2}{i}\sum_{n=0}^{i-1}\left\|\sum_{j=1}^{m_n}C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right\|^2 > \frac{\epsilon}{3}\right) + + \mathbb{P}\left(\frac{2}{i}\sum_{n=0}^{i-1}\left\|\sum_{j=m_n+1}^{n}C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right\|^2 > \frac{\epsilon}{3}\right), \quad (120)$$

where the first inequality comes from applying the Cauchy Schwarz Inequality and the second inequality comes from applying Theorem A.2. Then since

$$\mathbb{P}\left(\frac{1}{i}\sum_{n=0}^{i-1}\left\|\sum_{j=1}^{m_n} C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right\|^2 > \frac{\epsilon}{3}\right) \leq \\ \leq \mathbb{P}\left(\frac{2}{i}\sum_{n=0}^{i-1}\left\|\sum_{j=1}^{m_n} C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right\|^2 > \frac{\epsilon}{3}\right), \tag{121}$$

$$\mathbb{P}\left(\frac{1}{i}\sum_{n=0}^{i-1}\left\|\sum_{j=m_n+1}^{n} C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right\|^2 > \frac{\epsilon}{3}\right) \leq \\ \leq \mathbb{P}\left(\frac{2}{i}\sum_{n=0}^{i-1}\left\|\sum_{j=m_n+1}^{n} C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right\|^2 > \frac{\epsilon}{3}\right), \tag{122}$$

we can combine (119) with (120)-(122) to obtain

$$\tau < 2\mathbb{P}\left(\frac{1}{i}\sum_{n=0}^{i-1}\left\|\sum_{j=1}^{m_n} C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right\|^2 > \frac{\epsilon}{6}\right) + \\ + 2\mathbb{P}\left(\frac{1}{i}\sum_{n=0}^{i-1}\left\|\sum_{j=m_n+1}^{n} C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right\|^2 > \frac{\epsilon}{6}\right). \tag{123}$$

If we can upper bound the second term in the RHS or (123) by $\frac{\tau}{2}$ the first term must be lower bounded by $\frac{\tau}{2}$ completing the proof. To provide this bound we make use of Markov's Inequality. To this end, we first bound the expectation

$$\mathbb{E}\left(\frac{1}{i}\sum_{n=0}^{i-1}\left\|\sum_{j=m_n+1}^{n} C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right\|^2\right) = \\ = \mathbb{E}\Bigg(\frac{1}{i}\sum_{n=0}^{i-1}\sum_{j=m_n+1}^{n}\left(C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right)^\intercal \times \\ \times \left(C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right)\Bigg) \leq \\ \leq \mathbb{E}\Big(\frac{1}{i}\sum_{n=0}^{i-1}\sum_{j=m+1}^{\infty}\left(C_{n+j}\bar{A}_{(n+j-1,n+1)}\omega_n\right)^\intercal \times \\ \times \left(C_{n+j}\bar{A}_{(n+j-1,n+1)}\omega_n\right)\Big) \\ \leq \frac{1}{i}\sum_{n=0}^{i-1}\sum_{j=m+1}^{\infty} p\eta_C^2\eta_{A1}^{2(j-1)}\eta_\omega^2 = \frac{p\eta_C^2\eta_{A1}^{2m}\eta_\omega^2}{1-\eta_{A1}^2}, \tag{124}$$

where the the first equality comes from expanding the norm and ignoring uncorrelated terms, the first inequality comes from rearranging the summation and allowing the second summation to go to infinity, the second inequality comes from distributing the expectation and upper bounding each element, and the final equality comes from evaluating the summations. Since $\eta_{A1} < 1$, we can choose m sufficiently large such that

$$\frac{p\eta_C^2\eta_{A1}^{2m}\eta_\omega^2}{1-\eta_{A1}^2} < \frac{\tau\epsilon}{24}. \tag{125}$$

Using Markov's inequality [60, Equation 5.31] we have that

$$\mathbb{P}\left(\frac{1}{i}\sum_{n=0}^{i-1}\left\|\sum_{j=m_n+1}^{n} C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right\|^2 > \frac{\epsilon}{6}\right) \leq \\ \leq \frac{6p\eta_C^2\eta_{A1}^{2m}\eta_\omega^2}{(1-\eta_{A1}^2)\epsilon} < \frac{\tau}{4} \tag{126}$$

which completes the proof for the existence of m.

Next, to prove the existence of m' we expand (28)

$$\operatorname*{p-lim}_{i\to\infty}\frac{1}{i}\sum_{n=0}^{i-1} C_n\sum_{j=1}^{m_n}\sum_{k=1}^{m_n}\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\times \\ \times\omega_{n-k}^\intercal\bar{A}_{(n-1,n-k+1)}^\intercal C_n^\intercal \neq 0. \tag{127}$$

Considering the summands where $j \neq k$ we have that

$$\operatorname*{p-lim}_{i\to\infty}\frac{1}{i}\sum_{n=0}^{i-1} C_n\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\times \\ \times\omega_{n-k}^\intercal\bar{A}_{(n-1,n-k+1)}^\intercal C_n^\intercal = 0 \tag{128}$$

by Theorem A.6 since ω_n is independent and the dynamics are bounded and stable. If we further assume that there does not exist an m' for which (29) holds then by Theorem A.1 we have that (28) does not hold which is a contradiction. Therefore, the set of integers less than or equal to m for which (29) holds, is a non-empty finite set. The smallest element of this set then satisfies the conditions for m'. ■

Proof. **(Lemma III.11)** WLOG, in this proof, we allow summations to reference variables with negative index by assuming these values to be 0_r to ease notation. Assume that (24) holds but (26) does not. Since (26) does not hold, m' be chosen such that it satisfies the description in Lemma III.12. From Lemma III.10 we have that (24) implies (27). Expanding the LHS of (27) using (22) gives us

$$\operatorname*{p-lim}_{i\to\infty}\frac{1}{i}\sum_{n=0}^{i-1}(C_n\hat{\delta}_n - C_n\xi_n)(C_n\hat{\delta}_n - C_n\xi_n)^\intercal = \\ = \operatorname*{p-lim}_{i\to\infty}\frac{1}{i}\sum_{n=0}^{i-1}\left(C_n\left(\hat{\delta}_n - \sum_{j=1}^{n}\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right)\times \\ \times\left(\hat{\delta}_n - \sum_{k=1}^{n}\bar{A}_{(n-1,n-k+1)}\omega_{n-k}\right)^\intercal C_n^\intercal\right) = 0_r. \tag{129}$$

By separating the index m' we can write

$$\operatorname*{p-lim}_{i\to\infty}\frac{1}{i}\sum_{n=0}^{i-1}(C_n\hat{\delta}_n - C_n\xi_n)(C_n\hat{\delta}_n - C_n\xi_n)^\intercal = \\ = \operatorname*{p-lim}_{i\to\infty}\frac{1}{i}\sum_{n=0}^{i-1} C_n\left(\hat{\delta}_n - \sum_{\substack{1\leq j\leq n\\ j\neq m'}}\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right)\times \\ \times\left(\hat{\delta}_n - \sum_{\substack{0\leq k\leq n\\ k\neq m'}}\bar{A}_{(n-1,n-k+1)}\omega_{n-k}\right)^\intercal C_n^\intercal + \\ - C_n\left(\hat{\delta}_n - \sum_{\substack{1\leq j\leq n\\ j\neq m'}}\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right)\times \\ \times\omega_{n-m'}^\intercal\bar{A}_{(n-1,n-m'+1)}^\intercal C_n^\intercal - C_n\bar{A}_{(n-1,n-m'+1)}\omega_{n-m'}\times \\ \times\left(\hat{\delta}_n - \sum_{\substack{0\leq k\leq n\\ k\neq m'}}\bar{A}_{(n-1,n-k+1)}\omega_{n-k}\right)^\intercal C_n^\intercal + \\ + C_n\bar{A}_{(n-1,n-m'+1)}\omega_{n-m'}\times \\ \times\omega_{n-m'}^\intercal\bar{A}_{(n-1,n-m'+1)}^\intercal C_n^\intercal = 0_r. \tag{130}$$

For now suppose that

$$\operatorname*{p-lim}_{i\to\infty}\frac{1}{i}\sum_{n=0}^{i-1} -C_n\left(\hat{\delta}_n - \sum_{\substack{1\leq j\leq n\\ j\neq m'}}\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right)\times \\ \times\omega_{n-m'}^\intercal\bar{A}_{(n-1,n-m'+1)}^\intercal C_n^\intercal = 0_r. \tag{131}$$

Then by Theorem A.4 we have that

$$\operatorname*{p-lim}_{i\to\infty}\frac{1}{i}\sum_{n=0}^{i-1}(C_n\hat{\delta}_n - C_n\xi_n)(C_n\hat{\delta}_n - C_n\xi_n)^\intercal = \\ = \operatorname*{p-lim}_{i\to\infty}\frac{1}{i}\sum_{n=0}^{i-1} C_n\left(\hat{\delta}_n - \sum_{\substack{1\leq j\leq n\\ j\neq m'}}\bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right)\times$$

$$\times \left(\hat{\delta}_n - \textstyle\sum_{\substack{0\leq k\leq n\\ k\neq m'}} \bar{A}_{(n-1,n-k+1)}\omega_{n-k}\right)^{\mathsf{T}} C_n^{\mathsf{T}} + \\ + C_n \bar{A}_{(n-1,n-m'+1)}\omega_{n-m'} \times \\ \times \omega_{n-m'}^{\mathsf{T}} \bar{A}_{(n-1,n-m'+1)}^{\mathsf{T}} C_n^{\mathsf{T}} = 0_r. \quad (132)$$

Furthermore, by our choice of m' we have that

$$\operatorname*{p-lim}_{i\to\infty} \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} C_n \bar{A}_{(n-1,n-m'+1)}\omega_{n-m'} \times \\ \times \omega_{n-m'}^{\mathsf{T}} \bar{A}_{(n-1,n-m'+1)}^{\mathsf{T}} C_n^{\mathsf{T}} \neq 0_r, \quad (133)$$

and since the terms are all positive-semidefinite matrices

$$\mathbb{P}\big(\big\| \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} C_n \bar{A}_{(n-1,n-m'+1)}\omega_{n-m'} \times \\ \times \omega_{n-k}^{\mathsf{T}} \bar{A}_{(n-1,n-k+1)}^{\mathsf{T}} C_n^{\mathsf{T}} \big\| > \epsilon\big) \leq \\ \leq \mathbb{P}\left(\left\| \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} C_n \left(\hat{\delta}_n - \sum_{\substack{1\leq j\leq n\\ j\neq m'}} \bar{A}_{(n-1,n-j+1)}\omega_{n-j}\right) \times \right.\right. \\ \times \left(\hat{\delta}_n - \textstyle\sum_{\substack{0\leq k\leq n\\ k\neq m'}} \bar{A}_{(n-1,n-k+1)}\omega_{n-k}\right)^{\mathsf{T}} C_n^{\mathsf{T}} + \\ + C_n \bar{A}_{(n-1,n-m'+1)}\omega_{n-m'} \times \\ \left.\left. \times \omega_{n-m'}^{\mathsf{T}} \bar{A}_{(n-1,n-m'+1)}^{\mathsf{T}} C_n^{\mathsf{T}} \right\| > \epsilon \right). \quad (134)$$

This implies that (130) cannot hold which contradicts (24). Therefore (26) must hold since otherwise there exists an m' satisfying Lemma A.11.

To complete the proof, we now show that (131) indeed holds. By Corollary A.5 this is equivalent to proving

$$\operatorname*{p-lim}_{i\to\infty} \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} C_n \sum_{\substack{1\leq j\leq n\\ j\neq m'}} \bar{A}_{(n-1,n-j+1)}\omega_{n-j} \times \\ \times \omega_{n-m'}^{\mathsf{T}} \bar{A}_{(n-1,n-m'+1)}^{\mathsf{T}} C_n^{\mathsf{T}} = 0_r, \quad (135)$$

$$\operatorname*{p-lim}_{i\to\infty} \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} -C_n \hat{\delta}_n \omega_{n-m'}^{\mathsf{T}} \bar{A}_{(n-1,n-m'+1)}^{\mathsf{T}} C_n^{\mathsf{T}} = 0_r. \quad (136)$$

Note, (135) holds by Corollary A.7 since all ω_n are mutually independent, $\|C_n \bar{A}_{(n-1,n-m'+1)}\| \leq \|C_n\| < \eta_C$, and

$$\left\| \mathbb{E}\left[\left(\textstyle\sum_{\substack{1\leq j\leq n\\ j\neq m'}} \bar{A}_{(n-1,n-j+1)}\omega_{n-j} \right) \times \right.\right. \\ \left.\left. \times \left(\textstyle\sum_{\substack{1\leq k\leq n+i\\ k\neq m'}} \bar{A}_{(n+i-1,n+i-k+1)}\omega_{n+i-k} \right)^{\mathsf{T}} \right] \right\| = \\ = \left\| \textstyle\sum_{\substack{1\leq j\leq n\\ j\neq m'}} \bar{A}_{(n-1,n-j+1)} \Sigma_{\omega,n-j} \bar{A}_{(n+i-1,n-j+1)}^{\mathsf{T}} \right\| \leq \\ \leq \textstyle\sum_{j=1}^{\infty} \eta_{A1}^{2j-4+i} \eta_\omega = \frac{\eta_{A2}^{i-2}\eta_\omega}{1-\eta_{A1}^2}. \quad (137)$$

Here, the equality comes from evaluating the expectation, and the inequality comes from distributing the norm using the triangle inequality and the subadditivity of the spectral norm, bounding the individual terms, and allowing the summation to extend to infinity. Expanding the LHS of (136) using (18) gives us

$$\operatorname*{p-lim}_{i\to\infty} \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} -C_n \hat{\delta}_n \omega_{n-m'}^{\mathsf{T}} \bar{A}_{(n-1,n-m'+1)}^{\mathsf{T}} C_n^{\mathsf{T}} = \\ = \operatorname*{p-lim}_{i\to\infty} \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} C_n \big(\sum_{j=0}^{n-1} \underline{A}_{(n-1,j+1)} L_j \zeta_j \\ + \textstyle\sum_{k=1}^{n} \underline{A}_{(n-1,n-k+1)} L_{n-k} C_{n-k} \times \\ \times \textstyle\sum_{\ell=k+1}^{n} \bar{A}_{(n-k-1,n-\ell+1)}\omega_{n-\ell} \big) \times \\ \times \omega_{n-m'}^{\mathsf{T}} \bar{A}_{(n-1,n-m'+1)}^{\mathsf{T}} C_n^{\mathsf{T}} = 0_r. \quad (138)$$

To prove that (136) holds, we use Corollary A.5 on (138) and show that each term converges to 0_r. Note, by Theorem A.6,

$$\operatorname*{p-lim}_{i\to\infty} \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} C_n \big(\sum_{j=0}^{n-1} \underline{A}_{(n-1,j+1)} L_j \zeta_j \big) \times \\ \times \omega_{n-m'}^{\mathsf{T}} \bar{A}_{(n-1,n-m'+1)}^{\mathsf{T}} C_n^{\mathsf{T}} = 0_r, \quad (139)$$

since $\|C_n \bar{A}_{(n-1,n-m'+1)}\| \leq \eta_C$, ζ_n and ω_n are mutually independent, and

$$\left\| \mathbb{E}\left[\textstyle\sum_{j=0}^{n-1} \sum_{k=0}^{n+i-1} \underline{A}_{(n-1,j+1)} L_j \zeta_j \zeta_k^{\mathsf{T}} L_k^{\mathsf{T}} \underline{A}_{(n+i-1,k+1)}^{\mathsf{T}} \right] \right\| = \\ = \left\| \textstyle\sum_{j=0}^{n-1} \underline{A}_{(n-1,j+1)} L_j \Sigma_{\zeta_j} L_j^{\mathsf{T}} \underline{A}_{(n+i-1,j+1)}^{\mathsf{T}} \right\| \leq \\ \leq \textstyle\sum_{j=0}^{n-1} \eta_{A2}^{2(n-1-j)} \eta_{A2}^{i} \eta_L^2 \eta_\zeta \leq \frac{\eta_{A2}^{i}\eta_L^2\eta_\zeta}{1-\eta_{A2}^2}. \quad (140)$$

Furthermore, considering the portion of $\hat{\delta}_n$ not dependent on $\omega_{n-m'}$, by Theorem A.6,

$$\operatorname*{p-lim}_{i\to\infty} \tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} C_n \sum_{j=1}^{n} \underline{A}_{(n-1,n-j+1)} L_{n-j} C_{n-j} \times \\ \times \textstyle\sum_{\substack{k=j+1\\ k\neq m'}}^{n} \bar{A}_{(n-j-1,n-k+1)}\omega_{n-k} \times \\ \times \omega_{n-m'}^{\mathsf{T}} \bar{A}_{(n-1,n-m'+1)}^{\mathsf{T}} C_n^{\mathsf{T}} = 0_r, \quad (141)$$

since ω_n are independent, $\|C_n \bar{A}_{(n-1,n-m'+1)}\| \leq \eta_C$, and

$$\left\| \mathbb{E}\left[\left(C_n \textstyle\sum_{j=1}^{n} \underline{A}_{(n-1,n-j+1)} L_{n-j} C_{n-j} \times \right.\right.\right. \\ \left. \times \textstyle\sum_{\substack{k=j+1\\ k\neq m'}}^{n} \bar{A}_{(n-j-1,n-k+1)}\omega_{n-k} \right) \times \\ \times \left(C_{n+i} \textstyle\sum_{j=1}^{n+i} \underline{A}_{(n+i-1,n+i-j+1)} L_{n+i-j} C_{n+i-j} \times \right. \\ \left.\left.\left. \times \textstyle\sum_{\substack{k=j+1\\ k\neq m'}}^{n+i} \bar{A}_{(n+i-j-1,n+i-k+1)}\omega_{n+i-k} \right)^{\mathsf{T}} \right] \right\| = \\ = \left\| \textstyle\sum_{j=1}^{n} \sum_{\ell=1}^{n+i} C_n \underline{A}_{(n-1,n-j+1)} L_{n-j} C_{n-j} \times \right. \\ \times \textstyle\sum_{\substack{k=\max\{j+1,\ell+1\}\\ k\neq m'}}^{n} \bar{A}_{(n-j-1,n-k+1)} \Sigma_{\omega,n-k} \times \\ \times \bar{A}_{(n+i-\ell-1,n-k+1)}^{\mathsf{T}} C_{n+i-\ell}^{\mathsf{T}} L_{n+i-\ell}^{\mathsf{T}} \times \\ \left. \times \underline{A}_{(n+i-1,n+i-\ell+1)}^{\mathsf{T}} C_{n+i}^{\mathsf{T}} \right\| \leq \\ \leq \textstyle\sum_{j=1}^{n} \sum_{\ell=1}^{n} \eta_C^4 \eta_L^2 \eta_A^{\ell+j-2} \times \\ \times \textstyle\sum_{\substack{k=\max\{j+1,\ell+1\}\\ k\neq m'}}^{n} \eta_A^{2k-j-\ell-2+i} \eta_\omega \leq \\ \leq \eta_A^{i-4} \eta_C^4 \eta_L^2 \eta_\omega 2 \textstyle\sum_{j=1}^{\infty} \sum_{\ell=j}^{\infty} \sum_{k=\ell+1}^{\infty} \eta^{2k} = \frac{2\eta_A^{i}\eta_C^4\eta_L^2\eta_\omega}{(1-\eta_A^2)^3}, \quad (142)$$

where the first equality comes from evaluating the expectation, the first inequality comes from distributing the norm using the triangle inequality and the submultiplicative property of the spectral norm and then using the individual upper bounds, the second inequality comes from rearranging the sum and allowing the index to go to infinity, and the final equality comes from evaluating the geometric series. Now if

$$\begin{aligned}\underset{i\to\infty}{\text{p-lim}}\tfrac{1}{i}\textstyle\sum_{n=0}^{i-1} C_n \sum_{j=1}^{m'-1} \underline{A}_{(n-1,n-j+1)} L_{n-j} C_{n-j}\times\\ \times \bar{A}_{(n-j-1,n-m'+1)}\omega_{n-m'}\omega_{n-m'}^{\intercal}\bar{A}_{n-1,n-k+1}^{\intercal}C_n^{\intercal} = 0_r,\end{aligned} \tag{143}$$

we have completed the proof. To show this, we show that the trace of the matrix converges to 0 for each value of j.

$$\begin{aligned}&\underset{i\to\infty}{\text{p-lim}}\tfrac{1}{i}\textstyle\sum_{n=0}^{i-1}\big(\omega_{n-m'}^{\intercal}\bar{A}_{(n-1,n-m'+1)}^{\intercal}C_n^{\intercal}\times\\ &\quad\times C_n\underline{A}_{(n-1,n-j+1)}L_{n-j}C_{n-j}\times\\ &\quad\times \bar{A}_{(n-j-1,n-m'+1)}\omega_{n-m'}\big)\leq\\ &\leq \underset{i\to\infty}{\text{p-lim}}\Big(\tfrac{1}{i}\textstyle\sum_{n=0}^{i-1}\left\|C_n\bar{A}_{(n-1,n-m'+1)}\omega_{n-m'}\right\|^2\Big)^{1/2}\times\\ &\quad\times\Big(\tfrac{1}{i}\textstyle\sum_{n=0}^{i-1}\big\|C_n\underline{A}_{(n-1,n-j+1)}L_{n-j}\times\\ &\quad\times C_{n-j}\bar{A}_{(n-j-1,n-m'+1)}\omega_{n-m'}\big\|^2\Big)^{1/2}\end{aligned} \tag{144}$$

where the inequality follow from the Cauchy Schwarz Inequality. Let $\epsilon,\tau>0$ be chosen arbitrarily. By Markov's Inequality,

$$\begin{aligned}&\mathbb{P}\Big(\tfrac{1}{i}\textstyle\sum_{n=0}^{i-1}\left\|C_n\bar{A}_{(n-1,n-m'+1)}\omega_{n-m'}\right\|^2\geq\\ &\qquad\geq\tfrac{2\eta_C^2\eta_{A1}^{2(m'-1)}\eta_\omega}{1-\tau}\Big)\leq\\ &\leq\frac{(1-\tau)\mathbb{E}\left[\frac{1}{i}\sum_{n=0}^{i-1}\left\|C_n\bar{A}_{(n-1,n-m'+1)}\omega_{n-m'}\right\|^2\right]}{2\eta_C^2\eta_{A1}^{2(m'-1)}\eta_\omega}\leq\\ &\leq\frac{(1-\tau)\eta_C^2\eta_{A1}^{2(m'-1)}\eta_\omega}{2\eta_C^2\eta_{A1}^{2(m'-1)}\eta_\omega}=\frac{1-\tau}{2}.\end{aligned} \tag{145}$$

Furthermore by our choice of m', we have that there exists an N such that $i>N$ implies

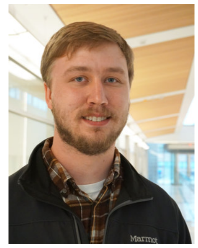
$$\begin{aligned}&\mathbb{P}\Big(\tfrac{1}{i}\textstyle\sum_{n=0}^{i-1}\left\|C_{n-j}\bar{A}_{(n-j-1,n-m'+1)}\omega_{n-m'}\right\|^2\leq\\ &\qquad\leq\frac{\epsilon^2}{2\eta_C^4\eta_{A1}^{2(m'-1)}\eta_{A2}^{2(j-1)}\eta_L^2\eta_\omega}\Big)\geq\frac{\tau+1}{2}.\end{aligned} \tag{146}$$

Finally, applying Theorem A.3

$$\begin{aligned}&\mathbb{P}\bigg(\Big(\tfrac{1}{i}\textstyle\sum_{n=0}^{i-1}\left\|C_n\bar{A}_{(n-1,n-m'+1)}\omega_{n-m'}\right\|^2\Big)^{1/2}\times\\ &\quad\times\Big(\tfrac{1}{i}\textstyle\sum_{n=0}^{i-1}\big\|C_n\underline{A}_{(n-1,n-j+1)}L_{n-j}\times\\ &\quad\times C_{n-j}\bar{A}_{(n-j-1,n-m'+1)}\omega_{n-m'}\big\|^2\Big)^{1/2}\leq\epsilon\bigg)\geq\\ &\geq\mathbb{P}\Big(\tfrac{1}{i}\textstyle\sum_{n=0}^{i-1}\left\|C_{n-j}\bar{A}_{(n-j-1,n-m'+1)}\omega_{n-m'}\right\|^2\\ &\quad\leq\frac{\epsilon^2}{2\eta_C^4\eta_{A1}^{2(m'-1)}\eta_{A2}^{2(j-1)}\eta_L^2\eta_\omega}\Big)+\\ &\quad+\Big(1-\mathbb{P}\Big(\tfrac{1}{i}\textstyle\sum_{n=0}^{i-1}\big\|C_n\bar{A}_{(n-1,n-m'+1)}\times\\ &\quad\times\omega_{n-m'}\big\|^2\geq 2\eta_C^2\eta_{A1}^2\eta_\omega\Big)\Big)-1\geq\end{aligned} \tag{147}$$

$$\geq\frac{\tau+1}{2}+1-\frac{1-\tau}{2}-1=\tau. \tag{148}$$

Therefore (143) must hold. ■



Matthew Porter received the B.S. degree in mechanical engineering from the Michigan Technological University, Houghton, MI, USA, in 2014, and the M.S. degree in mechanical engineering from the University of Michigan, Ann Arbor, MI, USA, in 2017, where he is currently pursuing the Ph.D. in mechanical engineering. His current research interests include the development and testing of algorithms for securing cyber-physical systems, through mathematical analysis and physical experimentation.

Pedro Hespanhol received the B.S. degree in Industrial Engineering from Pontifical Catholic University of Rio de Janeiro, Brazil, in 2014, the M.S. degree in Industrial Engineering and Operations Research (IEOR) from University of California at Berkeley in 2016, where he is currently pursuing the Ph.D. in IEOR. His research is focused on the interplay between control, learning and optimization, with emphasis on autonomous systems applications and computational optimization, from modeling techniques to practical implementations.

Anil Aswani is an associate professor in the department of industrial engineering and operations research (IEOR) at the University of California, at Berkeley. He received a BS in Electrical Engineering in 2005 from the University of Michigan, in Ann Arbor, and a PhD in Electrical Engineering and Computer Sciences with Designated Emphasis in Computational and Genomic Biology in 2010 from the University of California, at Berkeley. He has received an NSF CAREER award through the Operations Engineering program for his work on personalized healthcare, a Hellman Fellowship for his research on food insecurity, the Leon O. Chua award from Berkeley for outstanding achievement in an area of nonlinear science, and a William Pierskalla Runner-Up Award from the INFORMS Health Applications Society. His research interests include data-driven decision making, with particular emphasis on addressing inefficiencies and inequities in health systems and physical infrastructure.

Matthew Johnson-Roberson is an Associate Professor of Engineering in the Department of Naval Architecture & Marine Engineering and the Department of Electrical Engineering and Computer Science at the University of Michigan. He co-directs the UM Ford Center for Autonomous Vehicles (FCAV) and he founded and leads the DROP (Deep Robot Optical Perception) Lab, which researches 3D reconstruction, segmentation, data mining, and visualization. He received a PhD from the University of Sydney and he has held prior postdoctoral appointments with the Centre for Autonomous Systems - CAS at KTH Royal Institute of Technology in Stockholm and the Australian Centre for Field Robotics at the University of Sydney. He is a recipient of the NSF CAREER award (2015).

Ram Vasudevan received the B.S. degree in electrical engineering and computer sciences and the Honors degree in physics, the M.S. degree in electrical engineering, and the Ph.D. degree in electrical engineering from the University of California at Berkeley, Berkeley, CA, USA, in 2006, 2009, and 2012, respectively. He is currently an Assistant Professor in mechanical engineering with the University of Michigan, Ann Arbor, MI, USA, with an appointment in the University of Michigan's Robotics Program. His current research interests include the development and application of optimization and systems theory to quantify and improve human and robot interaction with one another and the environment.