Asymptotic Learning Requirements for Stealth Attacks on Linearized State Estimation

Ke Sun, *Member, IEEE*, Iñaki Esnaola, *Member, IEEE*, Antonia M. Tulino, *Fellow, IEEE*, and H. Vincent Poor, *Life Fellow, IEEE*

***Abstract*—Information-theoretic stealth attacks are data injection attacks that minimize the amount of information acquired by the operator about the state variables, while simultaneously limiting the Kullback-Leibler divergence between the distribution of the measurements under attack and the distribution under normal operation with the aim of controling the probability of attack detection. For Gaussian distributed state variables, attack construction requires knowledge of the second order statistics of the state variables, which is estimated from a finite number of past realizations using a sample covariance matrix. Within this framework, the attack performance is studied for the attack construction with the sample covariance matrix. This results in an analysis of the amount of data required to learn the covariance matrix of the state variables used on the attack construction. The ergodic attack performance is characterized using asymptotic random matrix theory tools and the variance of the attack performance is bounded. The ergodic performance and the variance bounds are assessed with simulations on IEEE test systems.**

***Index Terms*—Data injection attack, information-theoretic stealth attacks, statistical learning, random matrix theory, ergodic performance, variance of performance.**

I. Introduction

DATA injection attacks (DIAs) are a type of cyber-security threat that aim to modify the data exchange between the components of a power system by exploiting existing vulnerabilities of the sensing and communication systems [1]. Specifically, DIAs alter the measurements acquired by monitoring equipment, such as remote terminal units, to corrupt state estimates without triggering bad data detection mechanism used by the operator [2]. Attack construction strategies vary for different estimation frameworks and abnormal data detection approaches. For the conventional framework consisting of least squares estimation and residual-based detection, it is shown in [2] that attacks that lie in the column space of the system Jacobian matrix are undetectable. However, the rapid growth of the cyber layer in the smart grid enables novel estimation and detection methods that incorporate system model knowledge and integration of multiple data sources. As a result, efficient attack strategies need to adapt in this changing landscape to multiple estimation paradigms. For instance, within a Bayesian framework with minimum mean square error (MMSE) estimation, the attack trades off mean square error disruption for probability of detection [3], [4]. In particular, the attack construction leverages the linear MMSE estimate to identify the signal subspace that is most vulnerable to additive distortion while minimizing the probability of detection of a likelihood ratio test (LRT).

There are also multiple variants that incorporate different operational constraints for the attacker. For instance, introducing the ℓ_0 norm of the attack vector as minimization objective yields sparse attacks that decrease the number of sensors that need to be compromised by the attacker to decrease the difficulty of launching the attack [5], [6], [7], [8]. Sparse attacks are constructed in a distributed settings with multiple attackers in [9] and [10]. Information-theoretic attack constructions [11], [12] stem from the aspiration of targeting universal disruption measures that pose a data-integrity threat for the operator under a wide range of estimation frameworks. In this setting, the attacker aims to limit the amount of information acquired by the operator from the grid measurements by constructing random attacks that minimize the mutual information between the measurements and the state variables. These attack constructions require prior knowledge about the power system, specifically the Jacobian matrix of the power system and the distribution of the state variables, to determine the distribution of the attack vectors. Under a Gaussian assumption for the state variables [3], [4], [12], the knowledge required reduces to the second order statistics of the state variables. Naturally, perfect knowledge of the second order statistics of the state variables is not attainable in practice, and as a result, the performance of such attacks degrades as a result of having imperfect statistics. With that motivation, we study the performance loss faced by an attacker as a result of having

Manuscript received 9 November 2021; revised 31 March 2022, 22 July 2022, and 3 November 2022; accepted 3 December 2022. Date of publication 13 January 2023; date of current version 21 June 2023. This work was supported through the project FRACTAL under grant agreement No. E59C20001020005, by the U.S. National Science Foundation under Grant ECCS-2039716, and by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, partnership on "Telecommunications of the Future" (PE00000001 - program "RESTART"). Paper no. TSG-01798-2021. *(Corresponding author: Ke Sun.)*

Ke Sun was with the Department of Automatic Control and Systems Engineering, The University of Sheffield, S1 3JD Sheffield, U.K. He is now with the School of Computer Engineering and Science, Shanghai University, Shanghai 200444, China (e-mail: ke_sun@shu.edu.cn).

Iñaki Esnaola is with the Department of Automatic Control and Systems Engineering, The University of Sheffield, S1 3JD Sheffield, U.K., and also with the Department of Electrical and Computer Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: esnaola@sheffield.ac.uk).

Antonia M. Tulino is with the DIETI, Università degli Studi di Napoli Federico II, 80138 Naples, Italy, and also with the ECE Department, New York University Tandon School of Engineering, Brooklyn, NY 11201 USA (e-mail: antoniamaria.tulino@unina.it).

H. Vincent Poor is with the Department of Electrical and Computer Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: poor@princeton.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSG.2023.3236785.

Digital Object Identifier 10.1109/TSG.2023.3236785

access to imperfect knowledge about the distribution of the state variables. Specifically, we study the setting in which the attacker has access to a finite number of realizations of the state variables, for instance obtained from historical data, and learns the distribution of the state variables from them.

Imperfect system knowledge has been studied in different settings. For example, it is shown in [13] that stealthy attacks can be constructed when the attacker has only partial information about the grid. Undetectable attack constructions that rely on imprecise branch parameters are studied in [14]. Historical operation data can also be leveraged to infer the power system parameters and obtain a statistical description of the system, which can be capitalized by the attacker. For instance, historical data is exploited to learn the topology of the grid in [15]. Furthermore, different statistical learning algorithms, such as principal component analysis [16] and independent component analysis [17], can successfully be used to infer the statistical distribution of the state variables and the measurements.

In this paper, we characterize the learning requirements for the information-theoretic stealth attacks proposed in [11] and [12] via asymptotic analysis tools from random matrix theory (RMT). To that end, we adopt a sample covariance matrix estimation framework as in [18]. In this setting, the attacker computes the sample covariance matrix from past realizations of the state variables and uses the estimate of the covariance matrix to construct the attack vector. Since the sample covariance estimate is asymptotically unbiased and the information-theoretic attack construction is linear in the covariance matrix [11], the attack construction resulting from using the sample covariance matrix is asymptotically optimal. Assuming that the historical samples form a sequence of independent and identically distributed (i.i.d.) random variables, the sample covariance matrix is a *random matrix* and the performance of the attacks is a *random variable*. The non-asymptotic performance, i.e., the case with a finite number of realizations to compute the sample covariance matrix, is studied in [18] but the study using RMT tools in [18] only provides bounds on the expected value of the performance. In this paper, we focus on the asymptotic regime and characterize analytically the ergodic attack performance and its variance. In doing so, we establish performance tradeoffs between the size of the data set used for computing the sample covariance matrix and the performance of the attacks. We also obtain variance bounds on the attack performance to characterize the distribution of the attack performance.

Asymptotic RMT tools are well suited for modeling power systems with incomplete state information and provide good performance evaluations of finite dimensional systems given their rapid convergence properties [19]. RMT tools have been successfully used in the analysis of power systems before, for instance in [20], [21], [22], and [23] for the measurements from the IEEE test systems. Specifically, [20] and [21] show that the distribution of the singular values or eigenvalues of voltage data from IEEE test systems satisfies the Marčenko–Pastur law and the circular law, which are used in [22] to detect abnormal events and in [23] for data visualization. In a cybersecurity context, RMT tools are used in [24] to characterize the tradeoff between the sparsity of the attacks and the probability of passing the detection mechanism when a limited number of measurements are available for the attacker.

The rest of the paper is organized as follows: In Section II, a Bayesian framework with linearized dynamics for DIAs is presented. The learning scenario and some auxiliary asymptotic RMT results are presented in Section III. Using these results, a closed-form expression for the ergodic attack performance and bounds for the variance of the performance are proposed in Section IV and Section V, respectively, for the attack constructed using imperfect information. Section VI numerically evaluates the results in Section IV and Section V on IEEE test systems. The paper ends with conclusions in Section VII.

II. System Model

A. Bayesian Framework With Linearized Dynamics

The measurement model for state estimation with linearized dynamics is given by

$$Y^m = \mathbf{H}X^n + Z^m, \tag{1}$$

where $Y^m \in \mathbb{R}^m$ is a vector of random variables describing the measurements; $X^n \in \mathbb{R}^n$ is a vector of random variables describing the state variables; $\mathbf{H} \in \mathbb{R}^{m\times n}$ is the linearized Jacobian measurement matrix that is given by

$$\mathbf{H} = \frac{\partial H(X^n)}{\partial X^n}\Big|_{X^n=\mathbf{x}_0}, \tag{2}$$

in which $H : \mathbb{R}^n \to \mathbb{R}^m$ models the nonlinear dynamics between the state variables and the measurements and $\mathbf{x}_0$ is the operating point; and $Z^m \in \mathbb{R}^m$ is the additive white Gaussian noise with distribution $\mathcal{N}(\mathbf{0}, \sigma^2\mathbf{I})$ that is introduced by the sensors as a result of the thermal noise, in which $\mathbf{I}$ denotes the identity matrix of proper dimension and σ^2 is the variance of the noise [25], [26].[1]

In the remaining of the paper, we assume that the vector of state variables follows a zero-mean multivariate Gaussian distribution given by

$$X^n \sim \mathcal{N}(\mathbf{0}, \mathbf{\Sigma}_{XX}), \tag{3}$$

where $\mathbf{\Sigma}_{XX} \in \mathcal{S}_+^n$ is the covariance matrix of the distribution of the state variables and $\mathcal{S}_+^n$ denotes the set of positive semidefinite matrices of size $n \times n$. As a result of the linearized model in (1), the vector of measurements also follows a multivariate Gaussian distribution denoted by

$$Y^m \sim \mathcal{N}(\mathbf{0}, \mathbf{\Sigma}_{YY}), \tag{4}$$

where $\mathbf{\Sigma}_{YY} = \mathbf{H}\mathbf{\Sigma}_{XX}\mathbf{H}^\mathsf{T} + \sigma^2\mathbf{I}$ is the relative covariance matrix.

The formulation of the problem in a Bayesian setting demands the introduction of a modeling assumption on the distribution of the state variables. The rationale for adopting a Gaussian distribution over the state variables in this

[1] Note that the linearized model is not limited to the direct current (DC) model in the power system state estimation. This model allows the operator to include both bus voltage magnitudes and angles as state variables, such as PMU-based state estimation case, in the linearized model, see [26, Table 15.4, Table 15.5].

paper stems from a maximum entropy [27] approach. Indeed, the distribution that maximizes the entropy for given second order moments is the Gaussian distribution [28]. As a result, by adopting a Gaussian model, we introduce the minimum amount of bias into our modeling, i.e., we adopt the distribution that is maximally non-committal over the state variables. From a modeling perspective, this is the distribution that assumes the least amount of prior over the problem formulation given that we only have information about the second order statistics. Gaussian models have been previously used in power flow problems [29], [30] and DIAs [3], [4], [12]. Interestingly, Gaussian distributions have also been observed in some of the smart grid processes. For instance, real data suggests that distribution networks are well described by Gaussian models for both state variables [31] and consumption measurements [32]. This suggests that nodal active power injections can be modeled as Gaussian but the fitness of the model to other state variables, such as reactive power or PMU measurements, requires further study. It is worth noting, therefore, that the insight provided by the analytical results in this paper is more reliable the closer the state variables are to following a Gaussian distribution. In any case, the linear observation model in (1) gives rise to Gaussian distributions over the state variables whenever the observations follow a Gaussian distribution or when the deviations with respect to the operation point of the state variables can be modeled by Gaussian distributions.

Under our setting, DIAs corrupt the measurements available to the operator by adding an attack vector of random variables to the measurements. The resulting vector of compromised measurements is given by

$$Y_A^m = \mathbf{H}X^n + Z^m + A^m, \tag{5}$$

where $A^m \in \mathbb{R}^m$ is the attack vector and $Y_A^m \in \mathbb{R}^m$ is the vector containing the compromised measurements [2]. Following the setting of [11] and [12], an attack vector which is independent of the state variables is constructed under the assumption that the attack vector follows a multivariate Gaussian distribution denoted by

$$A^m \sim \mathcal{N}(\mathbf{0}, \mathbf{\Sigma}_{AA}), \tag{6}$$

where $\mathbf{\Sigma}_{AA} \in \mathcal{S}_+^m$ is the associated covariance matrix. Because of the Gaussianity of the attack distribution, the vector of compromised measurements is distributed as

$$Y_A^m \sim \mathcal{N}(\mathbf{0}, \mathbf{\Sigma}_{Y_A Y_A}), \tag{7}$$

where $\mathbf{\Sigma}_{Y_A Y_A} = \mathbf{H}\mathbf{\Sigma}_{XX}\mathbf{H}^\mathsf{T} + \sigma^2\mathbf{I} + \mathbf{\Sigma}_{AA}$.

The operator of the power system makes use of the acquired measurements to detect the attack. The detection problem is cast as a hypothesis testing problem with hypotheses

$$\mathcal{H}_0 : Y^m \sim \mathcal{N}(\mathbf{0}, \mathbf{\Sigma}_{YY}), \quad \text{versus} \tag{8}$$

$$\mathcal{H}_1 : Y^m \sim \mathcal{N}\big(\mathbf{0}, \mathbf{\Sigma}_{Y_A Y_A}\big). \tag{9}$$

The null hypothesis $\mathcal{H}_0$ describes the case in which the power system is not compromised, while the alternative hypothesis $\mathcal{H}_1$ describes the case in which the power system is under attack. Note that by assuming that the operator knows the distribution of the attack vector, the attacker aims to induce a probability of detection that is close to the probability of false alarm. When the probability of false alarm is comparable to the probability of attack detection, the operator is unable to distinguish between bad data events during normal operation and bad data resulting from DIAs.

For the binary hypothesis testing problem in (8) and (9), Neyman-Pearson lemma states that LRT is the most powerful test under a prefixed significance level α, i.e., LRT achieves the maximum probability of detection among all the tests with probability of false alarm smaller that α [33, Proposition II.D.1]. As a result, the LRT is used to decide between $\mathcal{H}_0$ and $\mathcal{H}_1$ based on the available measurements. The LRT between $\mathcal{H}_0$ and $\mathcal{H}_1$ takes following form:

$$L(\mathbf{y}) \triangleq \frac{f_{Y_A^m}(\mathbf{y})}{f_{Y^m}(\mathbf{y})} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \tau, \tag{10}$$

where $\mathbf{y} \in \mathbb{R}^m$ is a realization of the vector of random variables modeling the measurements; $f_{Y_A^m}$ and f_{Y^m} denote the probability density functions of Y_A^m and Y^m, respectively; and τ is the decision threshold set by the operator to meet a given false alarm constraint.

B. Information-Theoretic Stealth Attacks

The probabilistic modeling of the system variables enables an information-theoretic analysis of the DIAs [11], [12]. The measurement model in (1) characterizes an information acquisition procedure, in which the operator acquires the information about the state variables from the gathered measurements. To that end, the attacker disrupts the information acquisition procedure by minimizing the amount of information acquired by the operator, or mathematically, by minimizing the mutual information between the vector of state variables and the vector of compromised measurements, i.e., minimizing $I(X^n; Y_A^m)$ in (5), where $I(\cdot\,;\,\cdot)$ denotes the mutual information. Given that the smart grid paradigm envisions a large array of data-driven processes taking place in the system, the use of mutual information as the measure of the utility of the data is reasonable given the fundamental character of the mutual information. Indeed, the links of mutual information to detection [34], estimation theory [35], and machine learning [36] problems facilitate results in an attack disruption metric with operational meaning on a wider range of applications.

From the perspective of the attacker, the attacker also needs to guarantee the attacks to be stealthy under the detection approach, which requires the minimization of the probability of detection under the detection approach. In particular, minimizing the probability of detection under the LRT in (10) is achieved by minimizing the asymptotic value of the probability, and as a result of the Chernoff-Stein lemma [28, Th. 11.7.3] [12, (10)], it is equivalent to minimizing $D(P_{Y_A^m} \| P_{Y^m})$, where $P_{Y_A^m}$ and P_{Y^m} denote the probability distributions of Y_A^m and Y^m, respectively, and $D(\cdot\|\cdot)$ denotes the Kullback-Leibler (KL) divergence.

The *stealth attacks* minimize the amount of information acquired by the operator and the probability of attack detection

simultaneously by minimizing the *data integrity* cost function given by

$$\min_{A^m} I\big(X^n; Y_A^m\big) + D\Big(P_{Y_A^m} \| P_{Y^m}\Big), \tag{11}$$

which is equivalent to

$$\min_{A^m} D\Big(P_{X^n Y_A^m} \| P_{X^n} P_{Y^m}\Big) \tag{12}$$

after some algebraic operations [37], where $P_{X^n Y_A^m}$ is the joint distribution of (X^n, Y_A^m). The unweighted sum in (11) is generalized into a weighted sum in [12]. Under the Gaussian assumption for the state variables and the attack, it is shown in [11] that the data integrity cost function in (12) is a convex function of the attack covariance matrix $\mathbf{\Sigma}_{AA}$ with optimal solution

$$\mathbf{\Sigma}_{AA}^{\star} = \mathbf{H}\mathbf{\Sigma}_{XX}\mathbf{H}^{\mathsf{T}}. \tag{13}$$

A detailed account of information-theoretic stealth attacks and the tradeoff between disruption and probability of detection are provided in [11], [12], and [38].

III. Learning Scenario for Stealth Attacks

A. Learning Scenario Setting

As shown in (13), the attacker needs to get access to the system Jacobian matrix $\mathbf{H}$ and the covariance matrix of the state variables $\mathbf{\Sigma}_{XX}$. Note that the setting in this paper differs from the setting in [2] in that the attacker exploits knowledge of the second order statistics of the state variables. To that end, the attacker estimates the covariance matrix $\mathbf{\Sigma}_{XX}$ based on the available training data. The amount of training data governs the accuracy of the covariance matrix estimate, and therefore, in practical settings in which the attacker has access to a finite number of historical data samples, the attack is constructed with partial knowledge of the covariance matrix.

In the following, we study the performance of the attack when the covariance matrix is not perfectly known by the attacker but the linearized Jacobian measurement matrix is known. We model the partial knowledge by assuming that the attacker has access to a sample covariance matrix of the state variables. Specifically, a training dataset consisting of an i.i.d. sequence of k samples of the state variables, i.e., of $\{X_i^n\}_{i=1}^k$, is available to the attacker. This assumes that the attacker has access to noiseless realizations of the state variables that can be used to estimate the state variables without any error. While in practical settings access to noiseless realizations is not feasible, this assumption aims to model the worst-case scenario attack for the operators, i.e., the case in which the attacker has access to perfect historical data of the state variables.

That being the case, the attacker computes the unbiased estimate of the mean and the covariance matrix of the state variables via

$$k\bar{X}^n = \sum_{i=1}^{k} X_i^n, \tag{14}$$

$$(k-1)\mathbf{S}_{XX} = \sum_{i=1}^{k} X_i^n (X_i^n)^{\mathsf{T}} - k\bar{X}^n(\bar{X}^n)^{\mathsf{T}}, \tag{15}$$

where $\bar{X}^n$ is the sample mean and $\mathbf{S}_{XX}$ is the sample covariance matrix. Given that the vector of the state variables follows a multivariate normal distribution, it is shown in [39, Proposition 7.1] that the sample covariance matrix in (15) is a random matrix with a central Wishart distribution given by

$$(k-1)\mathbf{S}_{XX} \sim \mathcal{W}_n(k-1, \mathbf{\Sigma}_{XX}), \tag{16}$$

where $\mathcal{W}_n(k-1, \mathbf{\Sigma}_{XX})$ denotes the central Wishart distribution with $k-1$ degrees of freedom and covariance matrix $\mathbf{\Sigma}_{XX}$.

Given the optimal stealth attacks expression in (13), the stealth attacks constructed using the sample covariance matrix follow a multivariate Gaussian distribution conditioned on the sample covariance matrix $\mathbf{S}_{XX}$, which is given by

$$\tilde{A}^m \sim \mathcal{N}(\mathbf{0}, \mathbf{\Sigma}_{\tilde{A}\tilde{A}}) \tag{17}$$

with $\mathbf{\Sigma}_{\tilde{A}\tilde{A}} = \mathbf{H}\mathbf{S}_{XX}\mathbf{H}^{\mathsf{T}}$; and as a result of (16) and [39, Proposition 7.4], it holds that

$$(k-1)\mathbf{\Sigma}_{\tilde{A}\tilde{A}} = (k-1)\mathbf{H}\mathbf{S}_{XX}\mathbf{H}^{\mathsf{T}} \sim \mathcal{W}_m(k-1, \mathbf{H}\mathbf{\Sigma}_{XX}\mathbf{H}^{\mathsf{T}}). \tag{18}$$

To that end, the measurements that are under attack are given by

$$Y_{\tilde{A}}^m = \mathbf{H}X^n + Z^m + \tilde{A}^m, \tag{19}$$

in which $Y_{\tilde{A}}^m \in \mathbb{R}^m$ is the vector containing the measurements that are compromised by the attacks in (17). As a result, the compromised measurements follow a multivariate Gaussian distribution conditioned on the sample covariance matrix $\mathbf{S}_{XX}$, i.e.,

$$Y_{\tilde{A}}^m \sim \mathcal{N}(\mathbf{0}, \mathbf{\Sigma}_{Y_{\tilde{A}}Y_{\tilde{A}}}) \tag{20}$$

with $\mathbf{\Sigma}_{Y_{\tilde{A}}Y_{\tilde{A}}} = \mathbf{H}\mathbf{\Sigma}_{XX}\mathbf{H}^{\mathsf{T}} + \sigma^2\mathbf{I} + \mathbf{\Sigma}_{\tilde{A}\tilde{A}}$. Similarly, the cost function in (12) is described in this case as

$$D\Big(P_{X^n Y_{\tilde{A}}^m} \| P_{X^n} P_{Y^m}\Big), \tag{21}$$

where $P_{X^n Y_{\tilde{A}}^m}$ is the joint distribution of $(X^n, Y_{\tilde{A}}^m)$. Under the Gaussianity assumption, (21) is equivalent to [12, Proposition 1]

$$F\big(\mathbf{\Sigma}_{\tilde{A}\tilde{A}}\big) \triangleq \frac{1}{2}\Big(\mathrm{tr}(\mathbf{\Sigma}_{YY}^{-1}\mathbf{\Sigma}_{\tilde{A}\tilde{A}}) - \log|\mathbf{\Sigma}_{\tilde{A}\tilde{A}} + \sigma^2\mathbf{I}| + \log|\mathbf{\Sigma}_{YY}|\Big). \tag{22}$$

Given the Wishart distribution of the attack covariance matrix in (18), the KL divergence objective in (21) and the cost functions in (22) are both *random variables*. Following on the same steps as in [18], we defined the *ergodic performance* of the attack as the performance obtained by averaging over all realizations of the training data set, i.e., as $\mathbb{E}[F(\mathbf{\Sigma}_{\tilde{A}\tilde{A}})]$.

The characterization of the objective and the cost function using RMT can be conducted in the non-asymptotic scenario and the asymptotic scenario. Note that under both scenarios the characterization that uses the distribution of the Wishart random matrices directly is not manageable, so we turn to the distribution of the eigenvalues of Wishart random matrices,[2] which is more tractable. The non-asymptotic scenario

[2]The expression in right-hand side of (22) can be rewritten as a function of the eigenvalues of $\mathbf{\Sigma}_{\tilde{A}\tilde{A}}$. We will show this later in Theorem 5.

focuses on the case when the dimensions of the random matrices are finite value, i.e., $k-1$ and n are finite integers. Under this scenario, only probabilistic bounds are available for the eigenvalues of random matrices. To that end, we can only provide upper and lower bounds on the non-asymptotic ergodic performance [18].

Unlike the non-asymptotic scenario, the asymptotic scenario focuses on the case when the dimension of the random matrices goes to infinite, i.e., when $k-1\to\infty$ and $n\to\infty$. The rapid convergence of the non-asymtotic results to the asymptotic results guarantees that the asymptotic results approximate the non-asymptotic results well even for small values of $k-1$ and n, which will be shown later by the numerical simulation result in Fig. 1. The eigenvalue distributions that arise for these types of matrices in the asymptotic case are simpler to describe, and therefore, amenable to be studied analytically. In fact for this case, we are able to obtain a closed-form expression for the ergodic performance, rather than bounds as in the non-asymptotic case [18]. Also the variance of the performance, i.e., $\mathrm{var}[F(\mathbf{\Sigma}_{\tilde{A}\tilde{A}})]$, can also be characterized by the corresponding bounds.

In the following, we analyze the performance of the attack constructed using the sample covariance matrix for the asymptotic scenario. Before that, we introduce some auxiliary asymptotic results from RMT to aid the analysis.

B. Auxiliary Results From RMT

Asymptotic RMT mainly investigates the spectral properties of random matrices when the dimension tends to infinity [40]. As the dimension increases to infinity, the distribution of the eigenvalues of random matrices converges to the fixed distributions, such as the Marčenko–Pastur law for Wishart random matrices. We first introduce some definitions from RMT.

Definition 1 [41]: The η-transform of a nonnegative random variable X is

$$\eta_X(\gamma)=\mathbb{E}\left[\frac{1}{1+\gamma X}\right], \tag{23}$$

where $\gamma\geq 0$ and thus $1\geq\eta_X(\gamma)>0$.

Definition 2 [41]: The Shannon transform of a nonnegative random variable X is defined as

$$\mathcal{V}_X(\gamma)=\mathbb{E}\big[\log(1+\gamma X)\big]. \tag{24}$$

Definition 3 [41]: The asymptotic eigenvalue distribution (AED), $\mathsf{F}_{\mathbf{A}}(\cdot)$, of an $n\times n$ Hermitian random matrix $\mathbf{A}$ is defined as

$$\mathsf{F}_{\mathbf{A}}(x)=\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\mathbb{1}_{\{\lambda_i(\mathbf{A})\leq x\}}, \tag{25}$$

where $\mathbb{1}_{\{\cdot\}}$ is the indicator function and $\lambda_1(\mathbf{A}),\ldots,\lambda_n(\mathbf{A})$ are the eigenvalues[3] of $\mathbf{A}$.

The following theorems characterize the Shannon transform of the spectral distribution of a certain type of random matrices and the variance of the logarithm of the spectral distribution. These results enable us to characterize the asymptotic case better.

[3]The eigenvalues $\lambda_1,\ldots,\lambda_n$ are unordered eigenvalues.

Theorem 1 [41, Th. 2.39]: Let $\mathbf{L}$ be an $n\times(k-1)$ matrix whose entries are zero-mean i.i.d. random variables with variance $\frac{1}{k-1}$. Let $\mathbf{T}$ be an $n\times n$ symmetric nonnegative random matrix, independent of $\mathbf{L}$, whose AED converges almost surely to a nonrandom limit. The AED of $\mathbf{L}^{\mathsf{T}}\mathbf{T}\mathbf{L}$ converges almost surely, as $k-1,n\to\infty$ with $\frac{k-1}{n}\to\beta$, to a distribution whose η-transform satisfies

$$\frac{1}{\beta}=\frac{1-\eta}{1-\eta_{\mathbf{T}}(\gamma\eta)}, \tag{26}$$

where for notational simplicity we have abbreviated $\eta_{\mathbf{L}^{\mathsf{T}}\mathbf{T}\mathbf{L}}(\gamma)=\eta$. The corresponding Shannon transform satisfies

$$\mathcal{V}_{\mathbf{L}^{\mathsf{T}}\mathbf{T}\mathbf{L}}(\gamma)=\frac{\mathcal{V}_{\mathbf{T}}(\gamma\eta)}{\beta}+\log\frac{1}{\eta}+(\eta-1)\log e. \tag{27}$$

Note that the definition of β here is the reciprocal of the definition in [41].

Theorem 2 [42, Th. 4]: Let $\mathbf{L}$ be an $n\times(k-1)$ matrix defined as in Theorem 1. Let $\mathbf{T}$ be an $n\times n$ matrix defined as in Theorem 1 whose the spectral norm is bounded. As $k-1$, $n\to\infty$ with $\frac{k-1}{n}\to\beta$, the random variable

$$\Delta_{k-1}=\log|\mathbf{I}+\gamma\mathbf{L}^{\mathsf{T}}\mathbf{T}\mathbf{L}|-(k-1)\mathcal{V}_{\mathbf{L}^{\mathsf{T}}\mathbf{T}\mathbf{L}}(\gamma) \tag{28}$$

is asymptotically zero-mean Gaussian with variance

$$\mathbb{E}\Big[\Delta^2\Big]=-\log\left(1-\frac{1}{\beta}\mathbb{E}\left[\left(\frac{T\gamma\eta_{\mathbf{L}^{\mathsf{T}}\mathbf{T}\mathbf{L}}(\gamma)}{1+T\gamma\eta_{\mathbf{L}^{\mathsf{T}}\mathbf{T}\mathbf{L}}(\gamma)}\right)\right]\right), \tag{29}$$

where the expectation is over the nonnegative random variable T, whose distribution is the AED of $\mathbf{T}$.

To obtain the result in Theorem 2, a central limit theorem result is needed for the linear spectral statistics of random matrices. We introduce it in the following theorem.

Theorem 3 [42], [43]: Let $\mathbf{L}$ be an $n\times(k-1)$ matrix defined as in Theorem 1. Let $\mathbf{T}$ be an $n\times n$ matrix defined as in Theorem 1 whose the spectral norm is bounded. Let $g(\cdot)$ be a continuous function on the real line with bounded and continuous derivatives, analytic on an open set containing the interval

$$\left[\liminf_n \phi_n\max\left\{0,1-\sqrt{1/\beta}\right\}^2,\ \limsup_n \phi_1(1+\sqrt{1/\beta})^2\right] \tag{30}$$

where $\phi_1\geq\cdots\geq\phi_n$ are the eigenvalues of $\mathbf{T}$. Denoting the i-th eigenvalue and asymptotic AED of $\mathbf{L}^{\mathsf{T}}\mathbf{T}\mathbf{L}$ by $\lambda_i(\mathbf{L}^{\mathsf{T}}\mathbf{T}\mathbf{L})$ and $\mathsf{F}_{\mathbf{L}^{\mathsf{T}}\mathbf{T}\mathbf{L}}(\cdot)$, the random variable

$$\Delta_{k-1}=\sum_{i=1}^{k-1}g\Big(\lambda_i(\mathbf{L}^{\mathsf{T}}\mathbf{T}\mathbf{L})\Big)-(k-1)\int g(x)\mathrm{d}\mathsf{F}_{\mathbf{L}^{\mathsf{T}}\mathbf{T}\mathbf{L}} \tag{31}$$

converges, as $k-1,n\to\infty$ with $\frac{k-1}{n}\to\beta$, to a zero-mean Gaussian random variable with variance

$$\mathbb{E}\Big[\Delta^2\Big]=-\frac{1}{2\pi^2}\oint\oint\frac{\dot{g}(\mathcal{Z}(u_1))g(\mathcal{Z}(u_2))}{u_2-u_1}\mathrm{d}u_1\mathrm{d}u_2 \tag{32}$$

or

$$\mathbb{E}\Big[\Delta^2\Big]=-\frac{1}{2\pi^2}\oint\oint\frac{g(\mathcal{Z}(u_1))g(\mathcal{Z}(u_2))}{(u_2-u_1)^2}\mathrm{d}u_1\mathrm{d}u_2, \tag{33}$$

where $\dot{g}(x) = \frac{\mathrm{d}}{\mathrm{d}x} g(x)$ while

$$\mathcal{Z}(u) = -\frac{1}{u}\left(1 - \frac{1-\eta_{\mathbf{T}}(u)}{\beta}\right). \tag{34}$$

In (32) and (33), the integration variables u_1 and u_2 follow closed contours, which we may take to be non-overlapping and conterclockwise, such that the corresponding contours mapped through $\mathcal{Z}(u)$ enclose the support of $\mathsf{F}_{\mathbf{L}^\mathsf{T}\mathbf{T}\mathbf{L}}(\cdot)$.

Here (32) follows from [42, Th. 3] and (33) follows from [43, Th. 1.1]. These two expressions are equivalent. The difference is that (32) is suitable for some logarithm functions, such as $g(x) = \log(1+\gamma x)$ that is used for Theorem 2 and (33) is suitable for some linear functions, such as $g(x) = x$ that we will discuss later in Theorem 4.

It is worth mentioning that the results in Theorem 1, 2, and 3, including Theorem 4 in the following section, are general results, in which the distribution of entries in $\mathbf{L}$ is not specified. The only requirement is that the matrix $\mathbf{L}$ is composed of zero-mean i.i.d. entries with normalized variance.

C. Asymptotic Results for Trace Terms

Using the result in Theorem 3, we introduce an analytical expression for the variance of $\mathrm{tr}(\mathbf{L}^\mathsf{T}\mathbf{T}\mathbf{L})$, which we use later in the performance analysis.

Theorem 4: Let $\mathbf{L}$ be an $n \times (k-1)$ matrix defined as in Theorem 1. Let $\mathbf{T}$ be a symmetric nonnegative definite random matrix independent of $\mathbf{Z}$ with bounded spectral norm and whose asymptotic AED converges almost surely to a nonrandom limit. As $k-1, n \to \infty$ with $\frac{k-1}{n} \to \beta$, the random variable

$$\Delta_{k-1} = \mathrm{tr}\left(\mathbf{L}^\mathsf{T}\mathbf{T}\mathbf{L}\right) - (k-1)\frac{\mathbb{E}[T]}{\beta} \tag{35}$$

is asymptotically zero-mean Gaussian with variance

$$\mathbb{E}\left[\Delta^2\right] = \frac{2}{\beta}\mathbb{E}\left[T^2\right], \tag{36}$$

where the distribution of T is the AED of $\mathbf{T}$.

Proof: Firstly, we note that the mean of $\mathrm{tr}(\mathbf{L}^\mathsf{T}\mathbf{T}\mathbf{L})$ is given by

$$\mathbb{E}\left[\mathrm{tr}\left(\mathbf{L}^\mathsf{T}\mathbf{T}\mathbf{L}\right)\right] = \mathbb{E}\left[\mathrm{tr}\left(\mathbf{T}\mathbf{L}\mathbf{L}^\mathsf{T}\right)\right] = \mathbb{E}[\mathrm{tr}(\mathbf{T})] \to n\mathbb{E}[T], \tag{37}$$

where the first equality follows from the cyclic permutation property of the trace operator; the second equality follows from the fact that $\mathbf{T}$ is independent of $\mathbf{L}$, the trace is a linear operator, and $\mathbb{E}[\mathbf{L}\mathbf{L}^\mathsf{T}] = \mathbf{I}$.

Secondly, we turn to obtain the variance. Taking $g(x) = x$ into (33) yields

$$\mathbb{E}\left[\Delta^2\right] = -\frac{1}{2\pi^2}\oint\oint \frac{\mathcal{Z}(u_1)\mathcal{Z}(u_2)}{(u_2-u_1)^2}\mathrm{d}u_1\mathrm{d}u_2 \tag{38}$$

with $\mathcal{Z}(u)$ in (34). Without loss of generality, we assume that, besides satisfying the condition of Theorem 3, the u_1 and u_2 contours do not overlap and that the u_2 contour encloses the u_1 contour. Consequently, $\mathbb{E}[\Delta^2]$ is rewritten as

$$\mathbb{E}\left[\Delta^2\right] = -\frac{1}{2\pi^2}\oint \mathcal{Z}(u_2)\left[\oint \frac{\mathcal{Z}(u_1)}{(u_2-u_1)^2}\mathrm{d}u_1\right]\mathrm{d}u_2. \tag{39}$$

To calculate the inner integral, we need to use Cauchy's residue theorem. The first step is to find the zeros and poles of $\mathcal{Z}(u_1)$. Finding the zeros of $\mathcal{Z}(u_1)$ is equivalent to solving

$$-\frac{1}{u}\left(1 - \frac{1-\eta_{\mathbf{T}}(u)}{\beta}\right) = 0. \tag{40}$$

Note that, for the case $\gamma = 1$, (26) can be rewritten as

$$1 - \frac{1-\eta_{\mathbf{T}}(u)}{\beta} = \eta. \tag{41}$$

Given the fact that $\eta \in (0, 1]$, as Definition 1, so $\mathcal{Z}(u_1)$ has no zeros. Without lost of generality, the u_1 contour can be chosen such that only the simple pole at $u_1 = 0$ is enclosed. As a result, the inner integral is calculated using Cauchy's residue theorem and is given by

$$\oint \frac{\mathcal{Z}(u_1)}{(u_2-u_1)^2}\mathrm{d}u_1 = 2\pi i\frac{-1}{u_2^2}. \tag{42}$$

Taking the value of the inner integral into (39) yields

$$\mathbb{E}\left[\Delta^2\right] = -\frac{1}{\pi i}\oint\left(-\frac{1}{u_2}\left(1 - \frac{1-\eta_{\mathbf{T}}(u_2)}{\beta}\right)\right)\frac{1}{u_2^2}\mathrm{d}u_2. \tag{43}$$

The proof is completed by applying Cauchy's residue theorem again for (43), in which $u_2 = 0$ is a pole of order 3. ■

IV. Explicit Expression for the Asymptotic Ergodic Data Integrity

As shown in (22), the objective function of the stealth attacks constructed using the sample covariance matrix is given by

$$\begin{aligned} F &\triangleq F\left(\mathbf{\Sigma}_{\tilde{A}\tilde{A}}\right) \\ &= \frac{1}{2}\left(\mathrm{tr}(\mathbf{\Sigma}_{YY}^{-1}\mathbf{\Sigma}_{\tilde{A}\tilde{A}}) - \log|\mathbf{\Sigma}_{\tilde{A}\tilde{A}} + \sigma^2\mathbf{I}| + \log|\mathbf{\Sigma}_{YY}|\right), \end{aligned} \tag{44}$$

where

$$(k-1)\mathbf{\Sigma}_{\tilde{A}\tilde{A}} = (k-1)\mathbf{H}\mathbf{S}_{XX}\mathbf{H}^\mathsf{T} \sim \mathcal{W}_m(k-1, \mathbf{H}\mathbf{\Sigma}_{XX}\mathbf{H}^\mathsf{T}). \tag{45}$$

Note that the objective given in (44) is a *random variable*.

Here without loss of generality, we assume that the rank of matrix $\mathbf{H}\mathbf{\Sigma}_{XX}\mathbf{H}^\mathsf{T}$ is equal to n, which implies that $\mathbf{\Sigma}_{XX}$ is full rank. The rationale for this assumption comes from the observability check set by the operator, which guarantees that $\mathbf{H}$ is a full column rank matrix with $m \geq n$ for the state estimation procedure. As a result, it holds that $\mathrm{rank}(\mathbf{H}\mathbf{\Sigma}_{XX}\mathbf{H}^\mathsf{T}) = \mathrm{rank}(\mathbf{\Sigma}_{XX})$.

A. Distribution of the Data Integrity

To characterize the performance of the attacks, we obtain an equivalent expression for the performance in (44) that shares the same distribution.

Theorem 5: The data integrity performance of the attack constructed using the sample covariance matrix is equivalent in distribution to the random variable given by

$$F \overset{d}{=} \mathrm{tr}\left(\mathbf{Z}^\mathsf{T}\left(\tilde{\mathbf{\Lambda}} + \mathbf{I}\right)^{-1}\tilde{\mathbf{\Lambda}}\mathbf{Z}\right) - \log\left|\mathbf{Z}^\mathsf{T}\tilde{\mathbf{\Lambda}}\mathbf{Z} + \mathbf{I}\right| + \log\left|\tilde{\mathbf{\Lambda}} + \mathbf{I}\right|, \tag{46}$$

where $\stackrel{d}{=}$ denotes equivalence in distribution; $\mathbf{Z}$ is an $n\times(k-1)$ matrix whose entries are zero-mean i.i.d. Gaussian random variables with variance $\frac{1}{k-1}$; $\tilde{\mathbf{\Lambda}} \stackrel{\Delta}{=} \frac{1}{\sigma^2}\mathbf{\Lambda} \in \mathbb{R}^{n\times n}$, in which $\mathbf{\Lambda}$ is the diagonal matrix formed with the non-zero eigenvalues of $\mathbf{H}\mathbf{\Sigma}_{XX}\mathbf{H}^{\mathsf{T}}$.

Proof: Note that

$$F \stackrel{d}{=} \mathrm{tr}\left(\mathbf{\Sigma}_{YY}^{-1}\mathbf{V}\mathbf{\Lambda}_s^{\frac{1}{2}}\mathbf{Z}_m\mathbf{Z}_m^{\mathsf{T}}\mathbf{\Lambda}_s^{\frac{1}{2}}\mathbf{V}^{\mathsf{T}}\right) + \log|\mathbf{\Sigma}_{YY}| - \log\left|\mathbf{V}\mathbf{\Lambda}_s^{\frac{1}{2}}\mathbf{Z}_m\mathbf{Z}_m^{\mathsf{T}}\mathbf{\Lambda}_s^{\frac{1}{2}}\mathbf{V}^{\mathsf{T}} + \sigma^2\mathbf{I}\right| \tag{47}$$

$$\stackrel{d}{=} \mathrm{tr}\left(\left(\mathbf{\Lambda}_s + \sigma^2\mathbf{I}\right)^{-1}\mathbf{\Lambda}_s\mathbf{Z}_m\mathbf{Z}_m^{\mathsf{T}}\right) + \log\left|\frac{\mathbf{\Lambda}_s}{\sigma^2} + \mathbf{I}\right| - \log\left|\frac{\mathbf{\Lambda}_s}{\sigma^2}\,\mathbf{Z}_m\mathbf{Z}_m^{\mathsf{T}} + \mathbf{I}\right| \tag{48}$$

$$\stackrel{d}{=} \mathrm{tr}\left(\mathbf{Z}^{\mathsf{T}}\left(\tilde{\mathbf{\Lambda}} + \mathbf{I}\right)^{-1}\tilde{\mathbf{\Lambda}}\mathbf{Z}\right) - \log\left|\mathbf{Z}^{\mathsf{T}}\tilde{\mathbf{\Lambda}}\mathbf{Z} + \mathbf{I}\right| + \log\left|\tilde{\mathbf{\Lambda}} + \mathbf{I}\right|, \tag{49}$$

where (47) follows from the fact that $(k-1)\mathbf{\Sigma}_{\tilde{A}\tilde{A}} = (k-1)\mathbf{H}\mathbf{S}_{XX}\mathbf{H}^{\mathsf{T}} \sim \mathcal{W}_m(k-1, \mathbf{H}\mathbf{\Sigma}_{XX}\mathbf{H}^{\mathsf{T}})$, so it holds that

$$\mathbf{H}\mathbf{S}_{XX}\mathbf{H}^{\mathsf{T}} \stackrel{d}{=} \mathbf{V}\mathbf{\Lambda}_s^{\frac{1}{2}}\mathbf{Z}_m\mathbf{Z}_m^{\mathsf{T}}\mathbf{\Lambda}_s^{\frac{1}{2}}\mathbf{V}^{\mathsf{T}}, \tag{50}$$

in which $\mathbf{\Lambda}_s$ and $\mathbf{V}$ are the matrix of eigenvalues and the unitary matrix of corresponding eigenvectors, respectively, of $\mathbf{H}\mathbf{\Sigma}_{XX}\mathbf{H}^{\mathsf{T}}$, and $\mathbf{Z}_m$ is a matrix of dimension $m\times(k-1)$ whose entries are zero-mean i.i.d. Gaussian random variables with variance $\frac{1}{k-1}$; Given the fact that $\mathbf{\Sigma}_{YY} = \mathbf{H}\mathbf{\Sigma}_{XX}\mathbf{H}^{\mathsf{T}} + \sigma^2\mathbf{I}$ shares the same eigenvectors as $\mathbf{H}\mathbf{\Sigma}_{XX}\mathbf{H}^{\mathsf{T}}$ and $\log|\mathbf{\Sigma}_{YY}| = \log|\mathbf{\Lambda}_s + \sigma^2\mathbf{I}|$, (48) follows from applying the cyclic permutation to the trace term in (47) and applying the Sylvester's determinant identity for the logarithm of the determinant term in (47); (49) follows from the fact $\mathbf{\Lambda}_s$ is a rank deficient matrix with rank n and applying the cyclic permutation for the trace term and the logarithm determinant term. This completes the proof. ■

B. Asymptotic Behaviors of Matrices

To obtain the asymptotic performance, the asymptotic behavior of diagonal matrix $\tilde{\mathbf{\Lambda}} \in \mathbb{R}^{n\times n}$ needs to be defined. Given the definition of $\tilde{\mathbf{\Lambda}}$ in Theorem 5, the asymptotic behavior of $\tilde{\mathbf{\Lambda}}$ can be obtained by defining the asymptotic behavior of $\mathbf{H}$ and $\mathbf{\Sigma}_{XX}$. Increasing the number of buses and transmission lines in the power system leads to the increase in the dimensions of $\mathbf{H}$ and $\mathbf{\Sigma}_{XX}$, but the values of the additive entries in $\mathbf{H}$ and $\mathbf{\Sigma}_{XX}$ are determined by the arrangement and the admittance of the transmission lines that connect the added bus with the existing buses. To that end, there is no general model to characterize the behavior of $\mathbf{H}$ and $\mathbf{\Sigma}_{XX}$ when the dimensions increase. That being the case, we choose to define the asymptotic behavior of $\tilde{\mathbf{\Lambda}}$ directly.

Let n_0 denote the number of state variables within the practical power system that we are analysing and $\tilde{\mathbf{\Lambda}}_{n_0} \in \mathbb{R}^{n_0\times n_0}$ denote the corresponding $\tilde{\mathbf{\Lambda}}$ in this system. For example, when the voltage angles of the buses are chosen to be the state variables, there are 29 state variables for the IEEE 30-Bus test system, which implies that $n_0 = 29$. As a result, there are 29 positive eigenvalues of the matrix $\mathbf{H}\mathbf{\Sigma}_{XX}\mathbf{H}^{\mathsf{T}}$ and $\tilde{\mathbf{\Lambda}}_{n_0}$ is of dimension 29×29. The empirical cumulative distribution function (c.d.f.) of the diagonal elements of $\tilde{\mathbf{\Lambda}}_{n_0}$ is given by

$$\mathsf{F}_{\tilde{\mathbf{\Lambda}}_{n_0}}^{n_0}(x) = \frac{\sum_{i=1}^{n_0}\mathbb{1}_{\left\{\lambda_i(\tilde{\mathbf{\Lambda}}_{n_0})\le x\right\}}}{n_0}, \tag{51}$$

which is obtained from the parameters of the power system.

For the asymptotic scenario, we define

$$\tilde{\mathbf{\Lambda}} = \tilde{\mathbf{\Lambda}}_{n_0} \otimes \mathbf{I}, \tag{52}$$

where $\otimes$ is the Kronecker product. Under this setting, the dimension of $\tilde{\mathbf{\Lambda}}$ is $n\times n$ with $n = ln_0$, in which l is the dimension of the identity matrix $\mathbf{I}$. As a result, when $l\to\infty$ in (52), the AED of $\tilde{\mathbf{\Lambda}}$, i.e., $\mathsf{F}_{\tilde{\mathbf{\Lambda}}}(x)$, is given by

$$\mathsf{F}_{\tilde{\mathbf{\Lambda}}}(x) = \lim_{n\to\infty}\frac{\sum_{i=1}^{n}\mathbb{1}_{\left\{\lambda_i(\tilde{\mathbf{\Lambda}})\le x\right\}}}{n} = \frac{\sum_{i=1}^{n_0}\mathbb{1}_{\left\{\lambda_i(\tilde{\mathbf{\Lambda}}_{n_0})\le x\right\}}}{n_0}, \tag{53}$$

which states that the AED of $\tilde{\mathbf{\Lambda}}$ is the same as the empirical c.d.f. of the eigenvalues of $\tilde{\mathbf{\Lambda}}_{n_0}$.

Under the asymptotic setting in (52), we also have that

$$\log|\tilde{\mathbf{\Lambda}} + \mathbf{I}| = \frac{n}{n_0}\log|\tilde{\mathbf{\Lambda}}_{n_0} + \mathbf{I}| = n\Delta_c, \tag{54}$$

where

$$\Delta_c = \frac{\log|\tilde{\mathbf{\Lambda}}_{n_0} + \mathbf{I}|}{n_0}. \tag{55}$$

Given the fact that $\tilde{\mathbf{\Lambda}}_{n_0}$ and n_0 are determined by the power system, Δ_c is a constant for the asymptotic scenario.

C. Asymptotic Ergodic Data Integrity

The following theorem provides the asymptotic characterization of the ergodic performance of the attacks constructed using the sample covariance matrix.

Theorem 6: Let $k\to\infty$ with $\frac{n}{m}\to\alpha$ and $\frac{k-1}{n}\to\beta$, then the ergodic data integrity of the stealth attacks given by

$$\bar{F}_n \stackrel{\Delta}{=} \frac{1}{n}F \tag{56}$$

converges almost surely to

$$\bar{F}_\infty \stackrel{\Delta}{=} \frac{1}{2}\left(\lambda_{\mathbf{Z}^{\mathsf{T}}\left(\tilde{\mathbf{\Lambda}}+\mathbf{I}\right)^{-1}\tilde{\mathbf{\Lambda}}\mathbf{Z}} - \log\left(1+\lambda_{\mathbf{Z}^{\mathsf{T}}\tilde{\mathbf{\Lambda}}\mathbf{Z}}\right) + \Delta_c\right) \tag{57}$$

with

$$\mathbb{E}\left[\bar{F}_\infty\right] = \frac{1}{2}\left(\Theta + \Delta_c\right) - \frac{1}{2}\left(\mathcal{V}_{\tilde{\mathbf{\Lambda}}}(\eta) - \beta\log\eta + \beta(\eta-1)\log e\right), \tag{58}$$

where $\lambda_{\mathbf{A}}$ is the unordered eigenvalue of $\mathbf{A}$, Δ_c is defined in (55),

$$\Theta \stackrel{\Delta}{=} \lim_{n\to\infty}\frac{1}{n}\mathrm{tr}\left(\left(\tilde{\mathbf{\Lambda}} + \mathbf{I}\right)^{-1}\tilde{\mathbf{\Lambda}}\right) = \mathbb{E}\left[\frac{\tilde{\Lambda}}{\tilde{\Lambda}+1}\right] \tag{59}$$

with $\tilde{\Lambda}$ denoting a random variable distributed as the AED of $\tilde{\mathbf{\Lambda}}$ in (53), and η is the abbreviation for the η-transform of $\mathbf{Z}^{\mathsf{T}}\tilde{\mathbf{\Lambda}}\mathbf{Z}$ that is solved from (26) for $\gamma = 1$.

Proof: Starting from (46) and (56), we have that

$$\bar{F}_\infty = \lim_{n\to\infty}\frac{1}{n}F \tag{60}$$

$$= \frac{1}{2n}\Big(\mathrm{tr}\Big(\mathbf{Z}^\mathsf{T}\big(\tilde{\mathbf{\Lambda}}+\mathbf{I}\big)^{-1}\tilde{\mathbf{\Lambda}}\mathbf{Z}\Big) - \log\Big|\mathbf{Z}^\mathsf{T}\tilde{\mathbf{\Lambda}}\mathbf{Z}+\mathbf{I}\Big| + \log\Big|\tilde{\mathbf{\Lambda}}+\mathbf{I}\Big|\Big) \tag{61}$$

$$\to \frac{1}{2}\Big(\lambda_{\mathbf{Z}^\mathsf{T}\left(\tilde{\mathbf{\Lambda}}+\mathbf{I}\right)^{-1}\tilde{\mathbf{\Lambda}}\mathbf{Z}} - \log\big(1+\lambda_{\mathbf{Z}^\mathsf{T}\tilde{\mathbf{\Lambda}}\mathbf{Z}}\big) + \Delta_c\Big). \tag{62}$$

We now characterize the ergodic performance, i.e., the expected value of (62). Following the same procedure as in (37), we have

$$\mathbb{E}\Big[\lambda_{\mathbf{Z}^\mathsf{T}\left(\tilde{\mathbf{\Lambda}}+\mathbf{I}\right)^{-1}\tilde{\mathbf{\Lambda}}\mathbf{Z}}\Big] = \lim_{n\to\infty}\frac{1}{n}\mathbb{E}\Big[\mathrm{tr}\Big(\big(\tilde{\mathbf{\Lambda}}+\mathbf{I}\big)^{-1}\tilde{\mathbf{\Lambda}}\mathbf{Z}\mathbf{Z}^\mathsf{T}\Big)\Big] = \Theta. \tag{63}$$

Note that $\mathbb{E}[\log(1+\lambda_{\mathbf{Z}^\mathsf{T}\tilde{\mathbf{\Lambda}}\mathbf{Z}})]$ is the Shannon transform of the AED of $\mathbf{Z}^\mathsf{T}\tilde{\mathbf{\Lambda}}\mathbf{Z}$, which is characterized in Theorem 1. The proof is completed by taking (27) and (63) into (62). ∎

It follows from Theorem 6 that we need to obtain the η-transform of $\mathbf{Z}^\mathsf{T}\tilde{\mathbf{\Lambda}}\mathbf{Z}$ from (26) to finalize the asymptotic characterization of the ergodic performance. The following proposition shows that (26) has a unique solution of η.

Proposition 1: As a function of η, (26) in Theorem 1 has a unique solution.

Proof: Note that in (26) we have

$$\eta_{\mathbf{T}}(\gamma\eta) = \mathbb{E}\Big[\frac{1}{1+\gamma\eta T}\Big], \tag{64}$$

where $\eta_{\mathbf{L}^\mathsf{T}\mathbf{T}\mathbf{L}}(\gamma)$ is abbreviated as η and the expectation is over random variable T whose distribution is the AED of $\mathbf{T}$. After some algebraic manipulation, (26) can be expressed as

$$\beta\eta - \mathbb{E}\Big[\frac{1}{1+\gamma\eta T}\Big] = \beta - 1. \tag{65}$$

Note that $\gamma > 0$, $T \in \mathbb{R}^+$, and the range of η is within the interval $(0, 1]$, see Definition 1, the left-hand term of (65) is a monotonically increasing function of $\eta \in (0, 1]$ and its range contains the value $\beta - 1$. This completes the proof. ∎

V. Variance Bounds of the Asymptotic Data Integrity

In the previous section, Theorem 6 characterizes the ergodic performance of the attack, which is described via the equivalent distribution obtained in Theorem 5. However, the ergodic performance defined there only yields the average performance of the attacks. The variance of the performance provides insight into the probability that the performance concentrates around the averaged performance. In the following, we propose the lower and upper bounds for the variance of the asymptotic performance of attack.

Note that it would be ideal to characterize the distribution of F in (44) in a closed-form manner via Theorem 3. However, the diagonal matrix within the trace term in (46), i.e., $(\tilde{\mathbf{\Lambda}}+\mathbf{I})^{-1}\tilde{\mathbf{\Lambda}}$, is different from the one within the logarithm of the determinant term, i.e., from $\tilde{\mathbf{\Lambda}}$. So here we choose to bound the variance of the performance.

Given the fact that Δ_c defined in (54) and (55) is a constant term, we only need to characterize the variance introduced by the first two terms on the left-hand side of (46). Using the equivalent distribution in Theorem 5 and further denoting

$$F_a \triangleq \mathrm{tr}\Big(\mathbf{Z}^\mathsf{T}\big(\tilde{\mathbf{\Lambda}}+\mathbf{I}\big)^{-1}\tilde{\mathbf{\Lambda}}\mathbf{Z}\Big) \tag{66}$$

$$F_b \triangleq \log\Big|\mathbf{Z}^\mathsf{T}\tilde{\mathbf{\Lambda}}\mathbf{Z}+\mathbf{I}\Big|, \tag{67}$$

the variance of F in (44) is given by

$$\mathrm{var}[F] = \mathrm{var}[F_a] + \mathrm{var}[F_b] - 2\rho(F_a, F_b)\sqrt{\mathrm{var}[F_a]}\sqrt{\mathrm{var}[F_b]}, \tag{68}$$

where $\rho(\cdot,\cdot)$ denotes the Pearson correlation.

We proceed by proving that $\rho(F_a, F_b) \in [0, 1]$.

Lemma 1: Let $\mathbf{Z}$ is an $n\times(k-1)$ matrix whose entries are zero-mean i.i.d. Gaussian random variables with variance $\frac{1}{k-1}$. Let $\tilde{\mathbf{\Lambda}}$ be an $n\times n$ diagonal and nonnegative random matrix, which is independent of $\mathbf{Z}$. Then it holds that

$$0 \le \rho(F_a, F_b) \le 1, \tag{69}$$

where F_a and F_b are defined in (66) and (67), respectively.

Proof: Note that

$$F_a = \mathrm{tr}\Big(\big(\tilde{\mathbf{\Lambda}}+\mathbf{I}\big)^{-1}\tilde{\mathbf{\Lambda}}^{\frac{1}{2}}\mathbf{Z}\Big(\tilde{\mathbf{\Lambda}}^{\frac{1}{2}}\mathbf{Z}\Big)^\mathsf{T}\Big) = \sum_{i=1}^{n}\frac{1}{1+\lambda_{\boldsymbol{\sigma}(i)}(\tilde{\mathbf{\Lambda}}+\mathbf{I})}\bar{\lambda}_i, \tag{70}$$

where the first equality follows from the fact that $\tilde{\mathbf{\Lambda}}$ is a diagonal matrix and from applying cyclical permutation to the trace term; the second equality follows from [44, 6.57], in which $\boldsymbol{\sigma} \in \mathbb{N}^n$ is a permutation of $[1, 2, \ldots, n]^\mathsf{T}$, and $\bar{\lambda}_i$ is the i-th eigenvalue of $\tilde{\mathbf{\Lambda}}^{\frac{1}{2}}\mathbf{Z}(\tilde{\mathbf{\Lambda}}^{\frac{1}{2}}\mathbf{Z})^\mathsf{T}$.

Furthermore, we have

$$F_b = \log\Big|\tilde{\mathbf{\Lambda}}^{\frac{1}{2}}\mathbf{Z}(\tilde{\mathbf{\Lambda}}^{\frac{1}{2}}\mathbf{Z})^\mathsf{T}+\mathbf{I}\Big| = \sum_{i=1}^{n}\log(1+\bar{\lambda}_i), \tag{71}$$

where (71) follows from Sylvester's determinant identity.

From (70) and (71), it is easy to show that both F_a and F_b are coordinatewise monotonically increasing functions of the vector $\bar{\mathbf{\Lambda}} = [\bar{\lambda}_1, \ldots, \bar{\lambda}_n]^\mathsf{T}$. Note that $\bar{\mathbf{\Lambda}}$ is the vector of eigenvalues of a Wishart random matrix distributed as $\mathcal{W}_n(k-1, \tilde{\mathbf{\Lambda}})$. It is proved in [45, Th. 3] that the distribution of the eigenvalues of a Wishart random matrix is multivariate totally positive of order 2 (MTP_2). Adding the fact that two coordinatewise monotonically increasing or decreasing functions of a vector whose distribution is MTP_2 are positively correlated [46, (1.9)], the conclusion that $0 \le \rho(F_a, F_b) \le 1$ holds for any realizations of $\tilde{\mathbf{\Lambda}}$. The theorem follows from the independence between $\tilde{\mathbf{\Lambda}}$ and $\mathbf{Z}$. ∎

Using the result in Lemma 1, the upper bound in (68) is transformed into

$$\Big(\sqrt{\mathrm{var}[F_a]} - \sqrt{\mathrm{var}[F_b]}\Big)^2 \le \mathrm{var}[F] \le \mathrm{var}[F_a] + \mathrm{var}[F_b], \tag{72}$$

where the upper bound is achieved when $\rho(F_a, F_b) = 0$, and the lower bound is achieved when $\rho(F_a, F_b) = 1$.

The following theorem provides a lower bound and an upper bound for the variance of the performance.

Theorem 7: The variance of the data integrity of the attacks constructed using sample covariance matrix, i.e., var[F] with F defined in (44), is bound by

$$\frac{1}{4}\left(\sqrt{\text{var}[F_a]}-\sqrt{\text{var}[F_b]}\right)^2 \le \text{var}[F] \le \frac{1}{4}(\text{var}[F_a]+\text{var}[F_b]) \tag{73}$$

with

$$\text{var}[F_a] = \frac{2}{\beta}\mathbb{E}\left[\left(\frac{\tilde{\Lambda}}{\tilde{\Lambda}+1}\right)^2\right] \tag{74}$$

$$\text{var}[F_b] = -\log\left(1-\frac{1}{\beta}\mathbb{E}\left[\left(\frac{\tilde{\Lambda}\eta_{\mathbf{Z}^\top\tilde{\mathbf{\Lambda}}\mathbf{Z}}(1)}{1+\tilde{\Lambda}\eta_{\mathbf{Z}^\top\tilde{\mathbf{\Lambda}}\mathbf{Z}}(1)}\right)\right]\right), \tag{75}$$

where the expectation is over the nonnegative random variable $\tilde{\Lambda}$, whose distribution is the AED of $\tilde{\mathbf{\Lambda}}$ defined in (53); and the value of $\eta_{\mathbf{Z}^\top\tilde{\mathbf{\Lambda}}\mathbf{Z}}(1)$ is solved from (26), which is proved to be always solvable in Proposition 1.

Proof: Note that $F_a - F_b$ is the only term that introduces the randomness into the objective, as described in (68). As a result, the theorem follows directly from combining the results in Theorem 2 and Theorem 4 with (72). ■

For the variance bounds in Theorem 7, the difference between the upper bound and lower bound is further upper bounded by $\frac{1}{2}\sqrt{\frac{2}{\beta}}\sqrt{-\log(1-\frac{1}{\beta})}$, regardless of the distribution of $\tilde{\Lambda}$. In particular, the difference between the bounds is smaller than 0.0726 when $\beta = 10$ and is smaller than 0.0071 when $\beta = 100$ for the natural logarithm case.

VI. Numerical Simulation

In this section, we present simulations to evaluate the performance of the attacks constructed using the sample covariance matrix in practical state estimation settings. In particular, we use the IEEE 30-Bus and 118-Bus test systems, whose parameters and topology are obtained from MATPOWER [47]. We assume a DC state estimation scenario [25], [26], for which the bus voltage angle is chosen to be the state variables.

It is worth mentioning that our results in this paper hold for any covariance matrix of the state variable and for any $\beta > 0$, regardless of the structure of the matrix. In the simulations, the covariance matrix of the state variables is assumed to be a Toeplitz matrix with exponential decay parameter $r \in [0, 1]$, i.e., $\mathbf{\Sigma}_{XX} = [s_{ij} = r^{|i-j|}; i, j = 1, 2, \ldots, n]$, where the exponential decay parameter r determines the correlation strength between different entries of the state variable vector. And for β, we assume that the number of samples available to the attacker is larger than the dimension of the state variables, i.e., $k-1 \ge n$ or $\beta \ge 1$. This guarantees that the objective function in (22) is always computable for the nonasymptotic case, i.e., for the practical IEEE test systems. The Signal-to-Noise Ratio

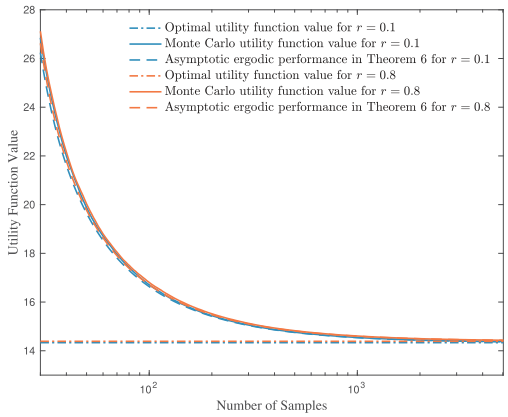


Fig. 1. Performance of the asymptotic ergodic data integrity in Theorem 6 for $r = 0.1$ and $r = 0.8$ when SNR = 30dB on IEEE 30-Bus test system.

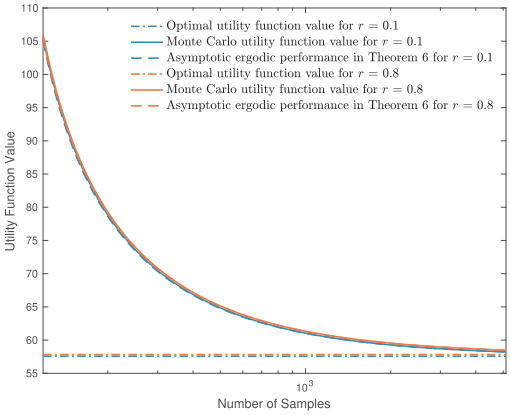


Fig. 2. Performance of the asymptotic ergodic data integrity in Theorem 6 for $r = 0.1$ and $r = 0.8$ when SNR = 30dB on IEEE 118-Bus test system.

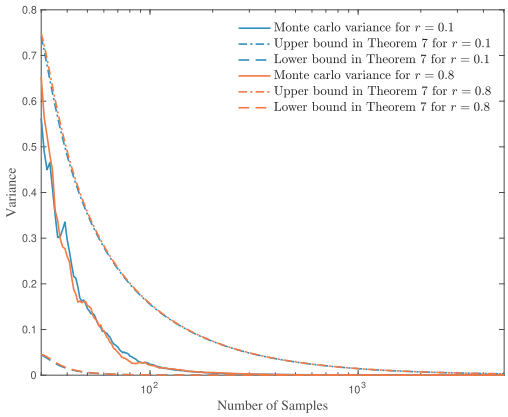


Fig. 3. Performance of the asymptotic ergodic data integrity in Theorem 7 for $r = 0.1$ and $r = 0.8$ when SNR = 30dB on IEEE 30-Bus test system.

(SNR) of the power system is defined as

$$\text{SNR} \triangleq 10\log_{10}\left(\frac{\text{tr}(\mathbf{H}\mathbf{\Sigma}_{XX}\mathbf{H}^\top)}{m\sigma^2}\right). \tag{76}$$

Fig. 1 depicts the performance of the asymptotic ergodic data integrity in Theorem 6 on IEEE 30-Bus test system for $r = 0.1$ and $r = 0.8$ when SNR = 30dB, in which the Monte Carlo performance value is the averaged performance

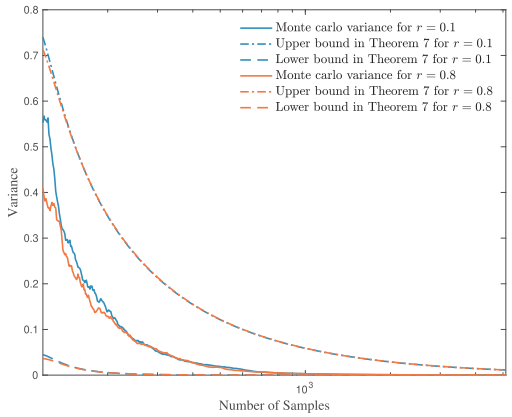


Fig. 4. Performance of the asymptotic ergodic data integrity in Theorem 7 for $r = 0.1$ and $r = 0.8$ when SNR = 30dB on IEEE 118-Bus test system.

through one thousand realizations, and the optimal utility function value is the utility function value when the attacker has perfect knowledge about the system. It is found that when the number of samples increases, the performance of the attacks constructed with the sample covariance matrix converges to the optimal value. More importantly, the asymptotic characterization approximates the non-asymptotic case described by the real power system well. It is worth to mentioning that the superb approximation still holds when the SNR changes. The same phenomenon is observed for the simulation on IEEE 118-Bus test system, which is shown in Fig. 2.

Fig. 3 depicts the performance of the bounds that are proposed in Theorem 7 for the IEEE 30-Bus test system when $r = 0.1$ and $r = 0.8$ with SNR = 30dB. Compared with the case when SNR = 10dB, it is found that the bounds, especially the lower bound, is tighter when the SNR value is high. Furthermore, the variance obtained by the Monte Carlo approach is closer to the upper bound when the number of samples is small compared with the dimension of the system, i.e., β is small, and when SNR is high. The same phenomenon is observed for the simulation on IEEE 118-Bus test system, which is shown in Fig. 4. Interestingly, the variance and the upper and lower bounds are comparable for both the IEEE 30-Bus test system and the IEEE 118-Bus test system. This suggests that the tightness of the bounds does not change with the size of the system.

It is worth mentioning that the conclusions in the preceding context also hold for the linearized AC model in (2). From a practical point of view, the results indicate that when the number of samples in the training set is at least 10 times larger than the dimension of the vector of state variables, the performance of the stealth attacks is close to that of the attack construction with perfect knowledge. Moreover, for that case the variance is smaller than 0.1, which suggests that the attack performance is close to the optimal case for most training data set realizations. This insight provides a guideline for operators on how much historical data is safe to share between different stakeholders in the power system. For instance, the historical data, such as voltage angle and magnitude, owned by Transmission System Operators or by Distribution System Operators might pose a risk depending on the size of the data set determined by β. Our analytical results provide a quantitative framework to assess the risk of sharing historical data in platforms such as the data exchange hubs of the National Regulatory Authority [48].

VII. Conclusion

In this paper, the learning requirements for information-theoretic DIAs have been analyzed using asymptotic RMT tools. Specifically, in this framework the attacker learns the second-order statistics of the state variables from a limited number of past realizations of the state variables and constructs the attacks using the estimated statistics. Since the sample covariance matrix is a random matrix, the performance of the attacks using the estimated statistics is a random variable. The ergodic performance of the attacks using the estimated statistics has been characterized in closed-form and the variance of the performance is bounded to obtain insight into the distribution of the performance. It is observed from the numerical simulations that the non-asymptotic ergodic performance exhibits an exponential convergence to the asymptotic case, and therefore, the asymptotic characterization provides practical insight into the performance of stealth attacks even with small datasets.

References

[1] A. Giani, S. Sastry, K. H. Johansson, and H. Sandberg, "The VIKING project: An initiative on resilient control of power networks," in *Proc. 2nd Int. Symp. Resilient Control Syst.*, Idaho Falls, ID, USA, Aug. 2009, pp. 31–35.

[2] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. ACM Conf. Comput. Commun. Security*, Chicago, IL, USA, Nov. 2009, pp. 21–32.

[3] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[4] I. Esnaola, S. M. Perlaza, H. V. Poor, and O. Kosut, "Maximum distortion attacks in electricity grids," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2007–2015, Jul. 2016.

[5] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Gaithersburg, MD, USA, Oct. 2010, pp. 214–219.

[6] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Proc. 1st Workshop Secure Control Syst.*, Stockholm, Sweden, Apr. 2010, pp. 1–6.

[7] K. C. Sou, H. Sandberg, and K. H. Johansson, "On the exact solution to a smart grid cyber-security analysis problem," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 856–865, Jun. 2013.

[8] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, Jun. 2011.

[9] A. Tajer, S. Kar, H. V. Poor, and S. Cui, "Distributed joint cyber attack detection and state recovery in smart grids," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Brussels, Belgium, Oct. 2011, pp. 202–207.

[10] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Sparse attack construction and state estimation in the smart grid: Centralized and distributed models," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1306–1318, Jul. 2013.

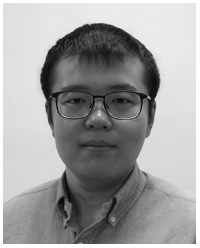
[11] K. Sun, I. Esnaola, S. M. Perlaza, and H. V. Poor, "Information-theoretic attacks in the smart grid," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Dresden, Germany, Oct. 2017, pp. 455–460.

[12] K. Sun, I. Esnaola, S. M. Perlaza, and H. V. Poor, "Stealth attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 1276–1285, Mar. 2020.

[13] J. Kim, L. Tong, and R. J. Thomas, "Subspace methods for data attack on state estimation: A data driven approach," *IEEE Trans. Signal Process.*, vol. 63, no. 5, pp. 1102–1114, Mar. 2015.

[14] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *Proc. IEEE Global Commun. Conf.*, Anaheim, CA, USA, Dec. 2012, pp. 3153–3158.

[15] X. Li, H. V. Poor, and A. Scaglione, "Blind topology identification for power systems," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Vancouver, BC, Canada, Oct. 2013, pp. 91–96.
[16] Z.-H. Yu and W.-L. Chin, "Blind false data injection attack using PCA approximation method in smart grid," *IEEE Trans. Smart Grid*, vol. 6, no. 3, pp. 1219–1226, May 2015.
[17] M. Esmalifalak, H. Nguyen, R. Zheng, L. Xie, L. Song, and Z. Han, "A stealthy attack against electricity market using independent component analysis," *IEEE Syst. J.*, vol. 12, no. 1, pp. 297–307, Mar. 2018.
[18] K. Sun, I. Esnaola, A. M. Tulino, and H. V. Poor, "Learning requirements for stealth attacks," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, Brighton, U.K., 2019, pp. 8102–8106.
[19] R. Vershynin, *High-Dimensional Probability: An Introduction With Applications in Data Science*. Cambridge, U.K.: Cambridge Univ. Press, 2018.
[20] X. He, Q. Ai, R. C. Qiu, W. Huang, L. Piao, and H. Liu, "A big data architecture design for smart grids based on random matrix theory," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 674–686, Mar. 2017.
[21] X. He, L. Chu, R. C. Qiu, Q. Ai, and Z. Ling, "A novel data-driven situation awareness approach for future grids—Using large random matrices for big data modeling," *IEEE Access*, vol. 6, pp. 13855–13865, 2018.
[22] X. He, R. C. Qiu, Q. Ai, L. Chu, X. Xu, and Z. Ling, "Designing for situation awareness of future power grids: An indicator system based on linear eigenvalue statistics of large random matrices," *IEEE Access*, vol. 4, pp. 3557–3568, 2016.
[23] D. Cai, X. He, Z. Yu, L. Wang, G. Xie, and Q. Ai, "3D power-map for smart grids—An integration of high-dimensional analysis and visualization," in *Proc. Int. Conf. Renew. Power Gener.*, Beijing, China, Oct. 2015, pp. 1–5.
[24] S. Lakshminarayana, A. Kammoun, M. Debbah, and H. V. Poor, "Data-driven false data injection attacks against power grids: A random matrix approach," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 635–646, Jan. 2021.
[25] A. Abur and A. G. Expósito, *Power System State Estimation: Theory and Implementation*. Boca Raton, FL, USA: CRC Press, Mar. 2004.
[26] J. J. Grainger and W. D. Stevenson, *Power System Analysis*. New York, NY, USA: McGraw-Hill, 1994.
[27] E. T. Jaynes, "Information theory and statistical mechanics," *Phys. Rev.*, vol. 106, no. 4, p. 620, 1957.
[28] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Somerset, U.K.: Wiley, Nov. 2012.
[29] G. E. Constante-Flores and M. S. Illindala, "Data-driven probabilistic power flow analysis for a distribution system with renewable energy sources using monte carlo simulation," *IEEE Trans. Ind. Appl.*, vol. 55, no. 1, pp. 174–181, Jan./Feb. 2019.
[30] A. Schellenberg, W. Rosehart, and J. Aguado, "Cumulant-based probabilistic optimal power flow (P-OPF) with Gaussian and gamma distributions," *IEEE Trans. Power Syst.*, vol. 20, no. 2, pp. 773–781, May 2005.
[31] C. Genes, I. Esnaola, S. M. Perlaza, L. F. Ochoa, and D. Coca, "Recovering missing data via matrix completion in electricity distribution systems," in *Proc. IEEE Workshop Signal Process. Adv. Wireless Commun.*, Edinburgh, U.K., Jul. 2016, pp. 1–6.
[32] N. C. Woolley and J. V. Milanovic, "Statistical estimation of the source and level of voltage unbalance in distribution networks," *IEEE Trans. Power Del.*, vol. 27, no. 3, pp. 1450–1460, Jul. 2012.
[33] H. V. Poor, *An Introduction to Signal Detection and Estimation*. New York, NY, USA: Springer, 1994.
[34] G. Vazquez-Vilar, A. T. Campo, A. G. I. Fàbregas, and A. Martinez, "Bayesian *M*-ary hypothesis testing: The meta-converse and Verdú-Han bounds are tight," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2324–2333, May 2016.
[35] D. Guo, S. Shamai, and S. Verdú, "The interplay between information and estimation measures," in *Foundations and Trends® in Signal Processing*, vol. 6. Hanover, MA, USA: Now, 2013, pp. 243–429.
[36] D. Russo and J. Zou, "How much does your data exploration overfit? Controlling bias via information usage," *IEEE Trans. Inf. Theory*, vol. 66, no. 1, pp. 302–323, Jan. 2020.
[37] J. Hou and G. Kramer, "Effective secrecy: Reliability, confusion and stealth," in *Proc. IEEE Int. Symp. Inf. Theory*, Honolulu, HI, USA, Jun. 2014, pp. 601–605.
[38] I. Esnaola, S. M. Perlaza, and K. Sun, "Data-injection attacks," in *Advanced Data Analytics for Power Systems*, A. Tajer, S. M. Perlaza, and H. V. Poor, Eds. Cambridge, U.K.: Cambridge Univ. Press, 2021, ch. 9, pp. 197–229.
[39] M. Bilodeau and D. Brenner, *Theory of Multivariate Statistics*. New York, NY, USA: Springer-Verlag, 1999.
[40] Z. Bai and J. W. Silverstein, *Spectral Analysis of Large Dimensional Random Matrices* (Springer Series in Statistics), 2nd ed. New York, NY, USA: Springer-Verlag, 2010.
[41] A. M. Tulino and S. Verdú, *Random Matrix Theory and Wireless Communications*. Delft, The Netherlands: Now Publ. Inc., 2004.
[42] A. M. Tulino and S. Verdú, "Asymptotic outage capacity of multiantenna channels," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, Philadelphia, PA, USA, Mar. 2005, pp. 825–828.
[43] Z. D. Bai and J. W. Silverstein, "CLT for linear spectral statistics of large-dimensional sample covariance matrices," *Ann. Probab.*, vol. 32, no. 1A, pp. 553–605, 2004.
[44] G. A. F. Seber, *A Matrix Handbook for Statisticians*. Hoboken, NJ, USA: Wiley, 2008.
[45] M.-T. Tsai, F.-J. Hsu, and C.-H. Tsai, "The ordering of Shannon entropies for the multivariate distributions and distributions of eigenvalues," *Entropy*, vol. 21, no. 2, p. 201, 2019.
[46] S. Karlin and Y. Rinott, "Classes of orderings of measures and related correlation inequalities. I. Multivariate totally positive distributions," *J. Multivariate Anal.*, vol. 10, no. 4, pp. 467–498, 1980.
[47] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.
[48] Å. Jenssen, T. Borsche, and J. Wolst. "Data exchange in electric power systems: European state of play and perspectives." 2017. [Online]. Available: https://eepublicdownloads.entsoe.eu/clean-documents/news/THEMA_Report_2017-03_web.pdf

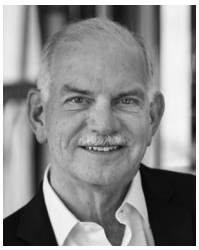


Ke Sun (Member, IEEE) received the B.Eng. degree from the Shandong University of Science and Technology, Qingdao, China, in 2012, the first M.Sc. degree from Tongji University, Shanghai, China, in 2015, the second M.Sc. degree from the University of Bologna, Bologna, Italy, in 2015, and the Ph.D. degree from the University of Sheffield, Sheffield, U.K., in 2020,

He is currently a Lecturer with the School of Computer Science and Engineering, Shanghai University, Shanghai, China. Prior to that, he was a Postdoctoral Researcher with the INRIA Centre at Université Côte d'Azur, INRIA, Sophia Antipolis, France, in 2022, and a Postdoctoral Research Associate with the University of Sheffield from 2019 to 2021. His research interests include the security of cyber-physical systems, information theory, random matrix theory, and game theory. Recognition of his work includes the 2020 ACSE Prize and the Honorable Mention Award within the Engineering Science Category in the 2020 Doctoral Research Award. He serves as a Reviewer for several journals and conferences, including *IET Smart Grid*, IEEE INTERNET OF THINGS JOURNAL, and IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS.

Iñaki Esnaola (Member, IEEE) received the M.S. degree in electrical engineering from the University of Navarra, Spain, in 2006, and the Ph.D. degree in electrical engineering from the University of Delaware, Newark, DE, USA, in 2011. He is currently a Senior Lecturer with the Department of Automatic Control and Systems Engineering, The University of Sheffield, U.K., and a Visiting Research Collaborator with the Department of Electrical Engineering, Princeton University, Princeton, NJ, USA. He was a Research Intern with Bell Laboratories, Alcatel-Lucent, Holmdel, NJ, USA, from 2010 to 2011, and a Postdoctoral Research Associate with Princeton University from 2011 to 2013. His research interests include information theory and statistical learning with an emphasis on the application to cyberphysical systems and data integrity security problems.

Antonia M. Tulino (Fellow, IEEE) received the Ph.D. degree in electrical engineering from the Seconda Università degli Studi di Napoli, Italy, in 1999. She held research positions with the Center for Wireless Communications, Finland; Princeton University, USA; and the Università degli Studi del Sannio, Benevento, Italy. From 2002 to 2016, she was an Associate Professor with the Università degli Studi di Napoli Federico II, where she has been a Full Professor since 2017. Since 2002, she has been collaborating with Nokia Bell Labs. Starting from October 2019, she is also a Research Professor with the Department of Electrical and Computer Engineering, New York University Tandon School of Engineering, NY, USA. In September 2020, she was appointed as a Teaching Director of the 5G Academy jointly organized by the Università degli Studi di Napoli Federico II in collaboration with Capgemini, Nokia, and TIM. She has received several paper awards and among the others the 2009 Stephen O. Rice Prize in the Field of Communications Theory for the Best Paper published in the IEEE TRANSACTIONS ON COMMUNICATIONS in 2008. She was a recipient of the UC3M-Santander Chair of Excellence from 2018 to 2019. From 2011 to 2013, she was a member of the editorial board of the IEEE TRANSACTIONS ON INFORMATION THEORY. She was selected by the National Academy of Engineering for the Frontiers of Engineering Program in 2013. Since 2019, she has been the Chair of the Information Theory Society Fellows Committee.



H. Vincent Poor (Life Fellow, IEEE) received the Ph.D. degree in EECS from Princeton University in 1977. From 1977 to 1990, he was on the faculty of the University of Illinois at Urbana-Champaign. Since 1990, he has been on the faculty at Princeton, where he is currently the Michael Henry Strater University Professor. From 2006 to 2016, he served as the Dean of Princeton's School of Engineering and Applied Science. He has also held visiting appointments at several other universities, including most recently at Berkeley and Cambridge. His research interests are in the areas of information theory, machine learning and network science, and their applications in wireless networks, energy systems, and related fields. Among his publications in these areas is the recent book *Advanced Data Analytics for Power Systems* (Cambridge University Press, 2021). Dr. Poor is a member of the National Academy of Engineering and the National Academy of Sciences and is a foreign member of the Chinese Academy of Sciences, the Royal Society, and other national and international academies. He received the IEEE Alexander Graham Bell Medal in 2017.