Transactive Energy System Deployment Over Insecure Communication Links

Yang Lu, Jianming Lian, *Senior Member, IEEE*, Minghui Zhu, and Ke Ma, *Member, IEEE*

***Abstract*— In this paper, the privacy and security issues associated with the transactive energy system (TES) deployment over insecure communication links are addressed. In particular, it is ensured that 1) individual agents' bidding information is kept private throughout hierarchical market-based interactions; and 2) any extraneous data injection attack can be quickly and easily detected. An implementation framework is proposed to enable the cryptography-based enhancement of privacy and security for the deployment of any general hierarchical systems including TESs. Under the proposed framework, a unified cryptography-based approach is developed to achieve both privacy and security simultaneously. Specifically, privacy preservation is realized by an enhanced Paillier encryption scheme, where a block design is proposed to significantly improve computational efficiency. Attack detection is further achieved by an enhanced Paillier digital signature scheme, where a stamp-concatenation mechanism is proposed to enable detection of data replace and reorder attacks. Simulation results verify the effectiveness of the proposed cyber-resilient design for transactive energy systems.**

***Note to Practitioners*—This paper is motivated by addressing the issues of cyber resiliency for practically deploying transactive energy system (TES) but it is also applicable to the problem of enhancing the privacy and security for any general hierarchical control systems. TES is an emerging control approach that engages energy suppliers and customers through market operations and uses the price to optimally allocate energy resources. While it has been shown to be promising for power system applications, the underlying market-based interactions raise significant concerns of privacy (data leakage) and security (data tampering). However, existing TES works only focus on the coordination mechanism instead of privacy and security issues. This paper proposes a new cryptography-based TES design for practical deployment. Specifically, to protect privacy, individual supply and demand amounts to be exchanged are all encrypted in a particular way such that the original amounts cannot be inferred from the encrypted amounts, while the desired computation for setting the market clearing price can be carried out over the encrypted amounts, thus generating an encrypted result which, when decrypted, matches that of the same computation over the original amounts. To achieve security, for each exchanged data, its sender generates a particular digital signature which is exchanged together with the data. This enables the receiver to automatically detect the integrity by checking whether a mathematical relationship holds for the pair of data and signature. In our future research, we will investigate more challenging scenarios where some suppliers and customers themselves could be corrupted and purposely submit distorted amounts.**

***Index Terms*— Transactive energy system, privacy-preserving, security-aware, cyber resilience, cryptography.**

Manuscript received 29 January 2023; accepted 25 March 2023. Date of publication 4 May 2023; date of current version 8 August 2024. This article was recommended for publication by Associate Editor L. Xia and Editor Q. Zhao upon evaluation of the reviewers' comments. This work was supported in part by the Laboratory Directed Research and Development (LDRD) Program at the Oak Ridge National Laboratory (ORNL); in part by the National Science Foundation (NSF) through CAREER under Grant ECCS-1846706; and in part by UT-Battelle, LLC for the U.S. Department of Energy (DOE) under Grant DE-AC05-00OR22725. *(Corresponding author: Jianming Lian.)*

Yang Lu is with the School of Computing and Communications, Lancaster University, LA1 4YW Lancaster, U.K.

Jianming Lian is with the Grid Interactive Controls Group, Oak Ridge National Laboratory, Oak Ridge, TN 37831 USA (e-mail: lianj@ornl.gov).

Minghui Zhu is with the School of Electrical Engineering and Computer Science, The Pennsylvania State University, University Park, PA 16802 USA.

Ke Ma is with the Advanced Technology Solutions Group, ISO New England Inc., Holyoke, MA 01040 USA.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TASE.2023.3267034.

Digital Object Identifier 10.1109/TASE.2023.3267034

I. Introduction

A. Background and Motivation

TRANSACTIVE control has been emerging as a new type of control that incorporates economic concepts and principles into the decision making and controller design of individual entities of the system. Recently, various transactive energy system (TES) designs have been proposed for electric power system applications of transactive control by using the market clearing prices for the coordination and control of distributed energy resources (see [1] and the references therein). However, the market-based interactions among energy suppliers and customers inevitably raise significant concerns of privacy and security. The exchanged information on individual supply and demand curves can infer very crucial private information [2], e.g., business secrets or personal preferences. In addition, if the communication links are insecure, the exchanged information could also be tampered by extraneous data injection attacks. Hence, the privacy and security issues necessitate the novel TES designs that can execute transactive control while simultaneously protecting data privacy and detecting malicious attacks over insecure communication links.

B. Related Works

Various techniques have been proposed in the literature to protect data privacy in power systems. In [3] and [4], mutual information has been used to define data privacy of smart meters. This privacy metric quantifies the posterior information entropy of private data given statistical models of the source data and auxiliary information. In [5] and [6], the technique of obfuscation has been used to protect coefficient privacy in centralized optimal power flow (OPF) problems in cloud

1545-5955 © 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: Penn State University. Downloaded on March 03,2025 at 02:28:22 UTC from IEEE Xplore. Restrictions apply.

computing. This technique masks the original OPF problem by an obfuscation transformation. Once the obfuscated problem is solved, an optimal solution to the original problem can be obtained by inverting the transformation. Differential privacy [7], [8] has been applied to the OPF [9], [10], economic dispatch [11] and thermal inertial load management [12]. Differentially private schemes add random noises into individual data in such a way that they cannot be inferred by the adversaries who can access arbitrary auxiliary information. Our recent review paper [13] provides detailed comparisons of the aforementioned three techniques and homomorphic encryption (to be discussed soon) in the context of cyber-physical systems (CPSs).

On the other hand, digital signature has been widely used by the communication community for enhanced security [14], [15], [16]. It enables the receiver to easily verify whether the digital message from the sender has been tampered or not by checking certain mathematical relations for the message and the signature. Recently, digital signature has been applied for secure communications in data aggregation in smart meters [17]. However, the technique in [17] cannot detect data replace or reorder attacks. Please refer to Section IV-B for details of these two attacks. For the problem of [17], in each cycle, each smart meter only has one data to be communicated, and the gap between two cycles could be long. Hence, these two attacks can be avoided by using a fresh new key to perform digital signature for each cycle. In contrast, detection of these two attacks is crucial for TESs. This is because, for each supplier or customer, a large number of sampled points of its supply/demand curve need to be communicated within a short period of market cycle, and it is unrealistic to adopt a fresh new key to perform digital signature for each sampled point. If the same key is used to perform digital signature for multiple sampled data, then it is possible for an attacker to launch replace and reorder attacks.

In this paper, a cyber-resilient TES design is proposed for the first time to overcome both the privacy and security issues of TESs over insecure communication links. In particular, Paillier encryption and Paillier digital signature [18] are applied for the privacy-preserving and security-aware designs, respectively. Paillier encryption is an additively homomorphic encryption scheme. Homomorphic encryption is a cryptographic technique that allows algebraic operations to be carried out on ciphertexts, thus generating an encrypted result which, when decrypted, matches that of the same operations over plaintexts. It has an appealing advantage that it can achieve perfect correctness in secure multiparty computation, i.e., the computation process provides each party the correct result of its target computation without disclosing any information of its private data to the other entities. Homomorphic encryption has been increasingly used by the control community to achieve secure multiparty computation for optimization and control [19], [20], [21], [22], [23], [24], [25]. For power systems, it has been applied to data aggregation in smart meters [17], [26], [27], [28], and very recently in OPF problems [29]. All these works adopt point-wise encryption, i.e., an encryption operation has to been done for each private data sample. This limits their usage in applications such as TESs where a large number of data samples need to be encrypted in a short period of time. Specifically, in TESs, to maintain a high market clearing accuracy, a small sampling resolution should be adopted and hence a large number of sampled points need to be encrypted within a market cycle. In addition, the above works on smart meters only consider integer-valued data. The work presented in [29] claimed to be able to deal with real-valued data but did not provide the design details. Integer-valued data is enough for smart meters because smart meters readings are always integers. However, supply and demand in TESs are usually real numbers. Hence, it is necessary to customize standard homomorphic encryption schemes for dealing with real numbers.

C. Contributions

In this paper, the privacy and security issues associated with the TESs are first identified. Then a framework is proposed to enable the implementation of cryptography-based approaches for hierarchically designed TESs. Under the proposed framework, the market participants perform Paillier encryption over the sampled points of their supply or demand curves using the coordinator's public key, and a third party is introduced to aggregate those encrypted sampled values. After that, the coordinator decrypts the aggregated encrypted sampled values using its private key. Pre- and post-operations are integrated into the encryption scheme to deal with real-valued sampled points of supply and demand curves. It is worth noting that, no participant, including the coordinator and third party, is assumed to be trustworthy. In this process, the coordinator has no access to individual encrypted sampled values and thus cannot recover individual supply or demand curves. Without knowing the coordinator's private key, the third party and the eavesdroppers over insecure communication links, cannot recover individual supply or demand curves either.

Specifically, the implementation challenges are addressed herein to practically utilize Paillier encryption for the privacy-preserving TES designs. First, the computational overhead associated with Paillier encryption is directly proportional to the number of data points. When this number of data points is large, the process of encryption and decryption would be time-consuming and may not be suitable for real-time market operations. To address this computational issue, a block design is further proposed in this paper to improve the computational efficiency by the number of sampled points times while still maintaining the level of privacy.

Second, the security issue has not been addressed in the presence of potential data injection attacks over insecure communication links. In this paper, an attack detection mechanism based on Paillier digital signature is proposed. When sending the data over the insecure communication link, the sender first generates a digital signature for the data using its own private key and then sends the data together with its signature to the receiver. After receiving the data, the receiver can perform a verification operation using the sender's public key to detect whether the received data and signature has been tampered or not. Without knowing the sender's private key, it is nearly impossible for an attacker to generate a pair that can pass

Authorized licensed use limited to: Penn State University. Downloaded on March 03,2025 at 02:28:22 UTC from IEEE Xplore. Restrictions apply.

the receiver's verification.[1] Specifically, to detect data replace and reorder attacks, we customize the standard Paillier digital signature scheme by concatenating a stamp to each message to identify its unique index, and a digital signature is generated for the stamped message. With this mechanism, the data replace or reorder attacks can no longer pass the verification operation as the replaced or reordered pair of message and signature does not match the index.

A preliminary version of this paper was presented in [30]. Compared with [30], the current paper includes data injection attack and proposes a security-aware mechanism, and develops a block design that can improve computational efficiency.

D. Organization

The rest of this paper is organized as follows. In Section II, the TES is briefly introduced with the privacy and security issues identified. In Section III, a privacy-preserving TES design is developed based on the Paillier encryption scheme, while in Section IV, an attack detection algorithm based on the Paillier digital signature is proposed for security-aware TES design. In Section V, case studies are presented to illustrate the effectiveness of the proposed cyber-resilient TES design. Conclusions are found in Section VI.

E. Notations

Denote by $\mathbb{R}$ and $\mathbb{N}$ the sets of real and natural numbers (including 0), respectively. Given a positive integer n, let $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$ and let $\mathbb{Z}_n^*$ denote the set of positive integers that are smaller than and co-prime to n. Given positive integers x and y, denote by $\gcd(x, y)$ and $\mathrm{lcm}(x, y)$ the greatest common divisor and the least common multiple of x and y, respectively. Given $x, y \in \mathbb{N}$, denote by $x \leftrightarrow y$ the concatenation of x and y, e.g., $12 \leftrightarrow 345 = 12345$. Given $x \in \mathbb{N}$, denote by $\mathrm{num}(x)$ the number of digits in x, e.g., $\mathrm{num}(123) = 3$. Given $x \in \mathbb{N}$ and two positive integers $a \le b \le \mathrm{num}(x)$, denote by $[x]_{a:b}$ the part from the a-th digit to the b-th digit of x, with the first digit being the leftmost one, and denote by $[x]_{a:\mathrm{end}}$ the part from the a-th digit to the last digit of x, e.g., $[12345]_{2:4} = 234$ and $[12345]_{3:\mathrm{end}} = 345$. Given $a \in \mathbb{N}$, denote by $(0 \cdots 0)_a$ the concatenation of a zeros, e.g., $(0 \cdots 0)_3 = 000$.

II. Problem Statement

In this section, we first briefly introduce the concept of TES. Then, we assess the cyber vulnerabilities of TES to identify the privacy and security issues associated with the existing TES designs. Finally, we state the objective of this paper.

[1]The attackers can perform the verification operation as any other legitimate receivers, so they can deploy attacks by trying different pairs of data and signature with brutal force until a valid pair that can pass the verification operation is generated. However, this could only occur theoretically because such an attack with brutal force is computationally infeasible in practice. In other words, the probability of generating a valid pair is extremely small and can be neglected in practice.

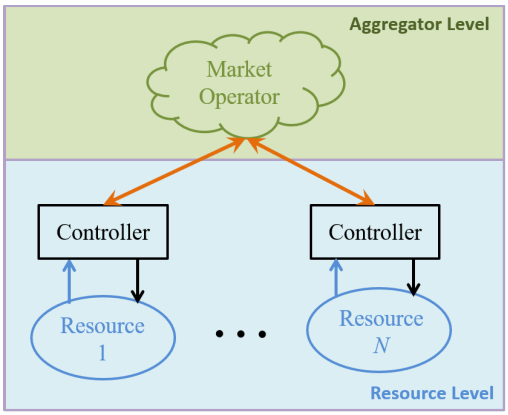


Fig. 1. Illustration of the underlying hierarchical structure of TESs.

A. Transactive Energy System

Within the TES, different entities can be classified into three types: coordinator (CO), supplier, and customer, where the coordinator is the market operator, a supplier is an energy seller, and a customer is an energy buyer. The TES can then be modeled as a multi-agent system with a hierarchical structure, as shown in Fig. 1. The coordinator aims to allocate energy resources to the suppliers and customers to ensure both individual and social objectives and constraints. This is referred to as the resource coordination problem. In transactive coordination, the coordinator achieves the optimal resource coordination by properly setting the resource price, which is called the market clearing price. We next present a typical TES to illustrate transactive coordination.

Denote by $\mathcal{V}_s$ and $\mathcal{V}_d$ be the set of suppliers and the set of customers, respectively. Let $N_s = |\mathcal{V}_s|$, $N_d = |\mathcal{V}_d|$, and $\mathcal{V} \triangleq \mathcal{V}_s \cup \mathcal{V}_d$. In the remaining of the paper, when it is necessary to differentiate between suppliers and customers, we will use "supplier $i \in \mathcal{V}_s$" or "customer $i \in \mathcal{V}_d$." Otherwise, we will use "agent $i \in \mathcal{V}$."

Given a market clearing price λ, each supplier $i \in \mathcal{V}_s$ aims to determine an optimal supply that maximizes its profit, which is defined as the difference between the revenue and cost of energy generation. Hence, the profit optimization problem of supplier $i \in \mathcal{V}_s$ can be formulated as

$$\max_{p_i^s \in \mathcal{L}_i^s} \lambda p_i^s - C_i(p_i^s),$$

where p_i^s is its supply, $C_i : \mathbb{R} \to \mathbb{R}$ is its cost function, λ is the market clearing price, and $\mathcal{L}_i^s$ is the feasible set of p_i^s.

Similarly, each customer $i \in \mathcal{V}_d$ aims to determine an optimal demand that maximizes its profit, which is defined as the difference between the utility and cost of energy consumption. Hence, the profit optimization problem of customer $i \in \mathcal{V}_d$ can be formulated as

$$\max_{p_i^d \in \mathcal{L}_i^d} U_i(p_i^d) - \lambda p_i^d,$$

where p_i^d is its demand, $U_i : \mathbb{R} \to \mathbb{R}$ is its utility function, and $\mathcal{L}_i^d$ is the feasible set of p_i^d.

As both the suppliers and customers try to maximize their profit, the coordinator aims to determine the optimal market

Authorized licensed use limited to: Penn State University. Downloaded on March 03,2025 at 02:28:22 UTC from IEEE Xplore. Restrictions apply.

clearing price that maximizes the social welfare of the entire system. Hence, the bi-level optimization problem of the coordinator can be formulated as

$$\max_{\lambda\in\mathbb{R}} \sum_{i\in\mathcal{V}_d} U_i\big(p_i^{d*}(\lambda)\big) - \sum_{i\in\mathcal{V}_s} C_i\big(p_i^{s*}(\lambda)\big) \tag{1a}$$

$$\text{s.t. } p_i^{s*}(\lambda) = \operatorname*{argmax}_{p_i^s\in\mathcal{L}_i^s} \lambda p_i^s - C_i(p_i^s),\ \forall i \in \mathcal{V}_s, \tag{1b}$$

$$p_i^{d*}(\lambda) = \operatorname*{argmax}_{p_i^d\in\mathcal{L}_i^d} U_i(p_i^d) - \lambda p_i^d,\ \forall i \in \mathcal{V}_d. \tag{1c}$$

The function $p_i^{s*}(\lambda)$ (resp. $p_i^{d*}(\lambda)$) in the optimization problem (1a) is referred to as the supply (resp. demand) function, and its graphical representation is the so-called supply (resp. demand) curve. For the majority of power system applications, the cost and utility functions, C_i and U_i, are often convex and concave, respectively, and the feasible sets $\mathcal{L}_i^s$ and $\mathcal{L}_i^d$ are convex. By deriving the Karush–Kuhn–Tucker (KKT) conditions for (1a), it can be shown that the optimal solution λ^* satisfies the following,

$$\sum_{i\in\mathcal{V}_s} p_i^{s*}(\lambda) = \sum_{i\in\mathcal{V}_d} p_i^{d*}(\lambda), \tag{2}$$

which implies that the total supply and demand are balanced at the optimal market clearing price. Both hierarchical and distributed market clearing approaches have been widely used to determine the optimal market clearing price λ^*. We next briefly discuss these two approaches.

Hierarchical market clearing. Hierarchical market clearing is implemented through auction. Individual suppliers $i \in \mathcal{V}_s$ and customers $i \in \mathcal{V}_d$ submit their entire supply or demand curves to the coordinator, respectively. Upon receiving all the individual curves, the coordinator first determines the aggregated supply and demand curves, and then find the market clearing price as the intersection between the aggregated supply and demand curves. Since it adopts the auction-based approach for market clearing, there is no price iteration.

Distributed market clearing. Unlike hierarchical market clearing that is iteration free, distributed market clearing works in an iterative manner. At the k-th iteration, the coordinator broadcasts an estimated price $\lambda(k)$ to the market participants. Individual suppliers $i \in \mathcal{V}_s$ and customers $i \in \mathcal{V}_d$ determine $p_i^s(k) = p_i^{s*}(\lambda(k))$ and $p_i^d(k) = p_i^{d*}(\lambda(k))$, respectively, and report them to the coordinator. Then the coordinator updates the price estimate for the next iteration until the price converges. In the literature, there are also many variants of the above basic algorithm. The readers can refer to [1] and the reference therein for a good review of existing algorithms and their convergence analysis.

Although distributed market clearing has been extensively explored in the literature, its practical applications to those time sensitive applications have been greatly limited because the price convergence could be time-consuming.

B. Cyber Vulnerabilities

TES is in fact a very typical CPS, where the market clearing prices are determined in the cyber space and the control tasks are performed in the physical world. Hence, TESs share the typical cyber vulnerabilities of general CPSs. In this paper, we consider the privacy and security issues associated with TESs. This subsection identifies these issues with respect to the two market clearing approaches introduced above.

1) Privacy Issue: The hierarchical market clearing requires individual agents to submit their supply or demand curves to the coordinator. With this information, the coordinator or an eavesdropper over the insecure communication links can easily infer individual cost or utility functions. In fact, the inverse supply or demand function is just the derivative of the corresponding cost or utility function [31]. Hence, individual cost or utility functions can be recovered by integrating the inverse of the corresponding supply or demand functions. This could potentially expose the business secrets (for suppliers) or personal preferences (for customers). We refer to the problem of private data leakage as the privacy issue.

The distributed market clearing can partially mitigate the privacy issue as individual agents do not submit their supply or demand curves to the coordinator, but only those quantities with respect to the broadcasted prices. However, the coordinator could make use of the iterative nature of the distributed approach to intentionally broadcast a large number of prices covering the entire admissible range. In this way, the coordinator or an eavesdropper could still recover individual supply or demand curves arbitrarily well.

2) Security Issue: Both market clearing approaches require information exchange between the coordinator and the agents. If the communication links are unauthenticated, extraneous attackers can send forged information to legitimate participants or tamper the information in transit to disrupt the market operation. This is termed as data injection attack (also known as data integrity attack or data tampering attack). In the presence of such attacks, the data received by the coordinator could be completely distorted, and the clearing price determined accordingly could arbitrarily deviate from the true clearing price and may lead to market chaos. We refer to the problem of data forging and tampering as the security issue.

C. Objectives

In this paper, we aim to develop a cyber-resilient TES design that simultaneously satisfies the following three properties:

(1) Correctness: The coordinator can determine the correct clearing price λ^* such that $\sum_{i\in\mathcal{V}_s} p_i^{s*}(\lambda^*) = \sum_{i\in\mathcal{V}_d} p_i^{d*}(\lambda^*)$;

(2) Privacy preservation: After the execution of the algorithm, for each supplier $i \in \mathcal{V}_s$ (resp. customer $i \in \mathcal{V}_d$), no other entity can infer the value of $p_i^{s*}(\lambda)$ (resp. $p_i^{d*}(\lambda)$) for any admissible λ;

(3) Security awareness: Any extraneous data injection attacks can be detected by legitimate message receivers.

For the purpose of illustration, only the hierarchical market clearing is considered in the following. However, the proposed design can be easily extended to distributed market clearing.

III. Privacy-Preserving Design

In this section, the privacy-preserving TES design is developed based on homomorphic encryption. We first propose a framework for practical deployment. Then we define the

Authorized licensed use limited to: Penn State University. Downloaded on March 03,2025 at 02:28:22 UTC from IEEE Xplore. Restrictions apply.

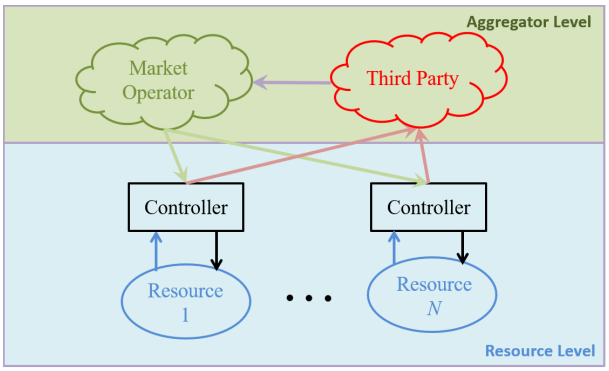


Fig. 2. Illustration of the proposed framework for TES deployment.

attacker model adopted in this section. After that, we present the details of the proposed privacy-preserving design. Finally, we propose an approach to ensure the computational efficiency for practical implementation.

A. Implementation Framework

In order to preserve the privacy, it requires that the coordinator should obtain the aggregated curve without knowing individual ones. In cryptography, homomorpihc encryption is a promising technique to fulfill this requirement. This technique requires that the entity who receives individual ciphertexts and carries out algebraic operations to be different from the entity who performs the decryptions. Hence, in order to enable the use of homomorphic encryption, we introduce an additional third party (TP) as the independent entity who is responsible of receiving individual ciphertexts and performing encrypted aggregations. The proposed framework is shown in Fig. 2, in which we assume that there is a communication link (i, TP) between each agent $i \in \mathcal{V}$ and the third party, and a communication link (TP, CO) between the third party and the coordinator. The third party can be implemented by an extraneous entity, e.g., a cloud service provider. Indeed, the third-party cloud service, for example, the IBM Power Virtual Server [32], has emerged in power systems to support thosee applications that are computationally intensive.

B. Attacker Model

We assume that any market participant $i \in \mathcal{V} \cup \{\text{CO}, \text{TP}\}$ is semi-honest, i.e., it correctly follows the designed algorithm but attempts to use received messages to infer other participants' private data ([33], pp-20). In addition, there could be external attackers that can eavesdrop the communication links. In this section, we assume that there are no data injection attacks. Such attacks are considered in the next section.

C. Algorithm Design

This subsection presents the proposed privacy-preserving auction-based algorithm. In plain auction-based clearing in Section II-A, individual supply or demand curves are sampled and discrete-valued versions are submitted. Denote by $\lambda_{\min}$ and $\lambda_{\max}$ the lower and upper bounds of resource price,

Algorithm 1 Privacy-Preserving Auction

1 **Key generation**
The CO runs $(\alpha, \beta, \nu, \pi) = \text{Alg}_{\text{key}}(n)$ such that $\alpha > \max\{10^{\sigma} N_s \delta_s, 10^{\sigma} N_d \delta_d\}$, broadcasts (α, β) and keeps (ν, π) private to itself;
for $\ell = 1;\ \ell \le N_p;\ \ell = \ell + 1$ **do**

2 **Encryption**
Each supplier $i \in \mathcal{V}_s$ runs

$$y^s_{i\ell} = \text{Alg}_{\text{enc}}(\alpha, \beta, 10^{\sigma} p^{s*}_{i\ell})$$

and sends $y^s_{i\ell}$ to the TP;
Each customer $i \in \mathcal{V}_d$ runs

$$y^d_{i\ell} = \text{Alg}_{\text{enc}}(\alpha, \beta, 10^{\sigma} p^{d*}_{i\ell})$$

and sends $y^d_{i\ell}$ to the TP;

3 **Computation over ciphertexts**
The TP computes

$$y^s_{\ell} = \prod_{i \in \mathcal{V}_s} y^s_{i\ell} \mod \alpha^2,$$
$$y^d_{\ell} = \prod_{i \in \mathcal{V}_d} y^d_{i\ell} \mod \alpha^2$$

and and sends (y^s_{ℓ}, y^d_{ℓ}) to the CO;

4 **Decryption**
The CO runs

$$\hat{y}^s_{\ell} = \text{Alg}_{\text{dec}}(\alpha, \nu, \pi, y^s_{\ell})/10^{\sigma},$$
$$\hat{y}^d_{\ell} = \text{Alg}_{\text{dec}}(\alpha, \nu, \pi, y^d_{\ell})/10^{\sigma};$$

5 **Setting clearing price**
The CO sets $\lambda^* = \lambda_{\min} + \ell\tau$ such that $\hat{y}^s_{\ell} = \hat{y}^d_{\ell}$, and sends λ^* to each agent $i \in \mathcal{V}$.

respectively. Denote by τ the sampling resolution and N_p the number of sampled values. For each supplier $i \in \mathcal{V}_s$ (resp. customer $i \in \mathcal{V}_d$), denote by $p^{s*}_{i\ell}$ (resp. $p^{d*}_{i\ell}$) its ℓ-th sampled value, i.e., $p^{s*}_{i\ell} = p^{s*}_i(\lambda_{\min} + \ell\tau)$ (resp. $p^{d*}_{i\ell} = p^{d*}_i(\lambda_{\min} + \ell\tau)$). Denote by $\sigma \in \mathbb{N}$ the precision level of the sampled values, i.e., for any $p^{s*}_{i\ell}$ and $p^{d*}_{i\ell}$, only the first σ decimal fraction digits are kept, while the rest are dropped. Assume that the coordinator and all the suppliers (resp. customers) know a strict upper bound δ_s (resp. δ_d) of individual supply (resp. demand) curves, i.e., $\delta_s > p^s_i$ for all $i \in \mathcal{V}_s$ and all $p^s_i \in \mathcal{L}^s_i$ (resp. $\delta_d > p^d_i$ for all $i \in \mathcal{V}_d$ and all $p^d_i \in \mathcal{L}^d_i$).

Our privacy-preserving auction-based design, Algorithm 1, is based on the Paillier encryption scheme. Preliminaries of Paillier encryption, including the sub-algorithms Alg_{key}, Alg_{enc}, and Alg_{dec}, are given in Appendix A.

At step 1, the coordinator generates a set of keys by the Paillier key-generation algorithm. The public keys are broadcasted while the private keys are kept private to itself. The bound on α is to guarantee decryption correctness. Roughly speaking, to ensure decryption correctness, the public key α must be larger than the computing result. Please refer to the statement of homomorphic property at the end of Appendix A, in which it requires $\alpha > \sum_{\ell=1}^{m} pt_{\ell}$. In our

Authorized licensed use limited to: Penn State University. Downloaded on March 03,2025 at 02:28:22 UTC from IEEE Xplore. Restrictions apply.

problem, $\max\{10^{\sigma}N_s\delta_s, 10^{\sigma}N_d\delta_d\}$ is a strict upper bound for all computing results, i.e., sampled values of aggregated supply and demand curves. Hence, the bound on α guarantees decryption correctness for all computing results at step 4. Actually, for the sake of privacy, α needs to be very large, e.g., in the magnitude of 2^{2000} [34]. Hence, the upper bound condition on α is usually automatically satisfied even if the participants do not know δ_s or δ_d. At step 2, each supplier $i \in \mathcal{V}_s$ (resp. customer $i \in \mathcal{V}_d$) encrypts its sampled value $10^{\sigma}p_{i\ell}^{s*}$ (resp. $10^{\sigma}p_{i\ell}^{d*}$) by the Paillier encryption algorithm with the public keys (α, β), and sends the ciphertext $y_{i\ell}^{s}$ (resp. $y_{i\ell}^{d}$) to the third party. Notice that $10^{\sigma}p_{i\ell}^{s*}$ and $10^{\sigma}p_{i\ell}^{d*}$ are both non-negative integers. At step 3, the third party performs computations over received ciphertexts according to the homomorphic property of the Paillier encryption scheme, i.e., multiplication of ciphertexts provides an encryption of sum of plaintexts. Hence, y_{ℓ}^{s} and y_{ℓ}^{d} are actually encryptions of the ℓ-th sampled values of the aggregated supply and demand curves, respectively. The third party then sends y_{ℓ}^{s} and y_{ℓ}^{d} to the coordinator. At step 4, the coordinator decrypts y_{ℓ}^{s} and y_{ℓ}^{d} by the Paillier decryption algorithm with its public key α and private keys (ν, π), and transforms the decrypted results back to real numbers via dividing them by 10^{σ}. At step 5, the coordinator sets and broadcasts the clearing price λ^*.

Algorithm 1 has the following properties:

(1) Correctness: For each $\ell \in \{1, \cdots, N_p\}$, it follows that $\hat{y}_{\ell}^{s} = \sum_{i\in\mathcal{V}_s} p_i^{s*}(\lambda_{\min} + \ell\tau)$ and $\hat{y}_{\ell}^{d} = \sum_{i\in\mathcal{V}_d} p_i^{d*}(\lambda_{\min} + \ell\tau)$.

The correctness property states that $\hat{y}_{\ell}^{s}$ and $\hat{y}_{\ell}^{d}$ are just the ℓ-th sampled values of the original aggregated supply and demand curves, respectively. This property directly follows from the homomorphic property of the Paillier encryption scheme (please refer to the end of Appendix A). Since λ^* is set as $\lambda^* = \lambda_{\min} + \ell\tau$ such that $\hat{y}_{\ell}^{s} = \hat{y}_{\ell}^{d}$, the correctness property leads to $\sum_{i\in\mathcal{V}_s} p_i^{s*}(\lambda^*) = \sum_{i\in\mathcal{V}_d} p_i^{d*}(\lambda^*)$. Hence, optimal market-based coordination is achieved.

(2) Privacy preservation: If the DCRA holds, then, after the execution of the algorithm, for each supplier $i \in \mathcal{V}_s$ (resp. customer $i \in \mathcal{V}_d$), for all $\ell \in \{1, \cdots, N_p\}$, the value of $p_i^{s*}(\lambda_{\min} + \ell\tau)$ (resp. $p_i^{d*}(\lambda_{\min} + \ell\tau)$) is semantically secure.

The privacy preservation property directly follows from the semantic security of the Paillier encryption scheme (please refer to the end of Appendix A). Specifically, after the execution of Algorithm 1, each agent $i \in \mathcal{V}$ only knows its own supply or demand curve and the market clearing price; the coordinator only knows the aggregated supply and demand curves and the market clearing price; the third party or an extraneous eavesdropper only knows the market clearing price. Therefore, any agent's individual supply or demand curve is not known to any other entity and privacy preservation is achieved.

D. Block Design for Improved Computational Efficiency

Algorithm 1 works in a point-wise manner, where all the cryptographic operations are performed for each sampled value of the supply or demand curves. Specifically, each agent i performs N_p times encryption, the third party performs $2N_p$ times computation over ciphertexts, and the coordinator performs $2N_p$ times decryption. When N_p is large, the implementation of Algorithm 1 would be time-consuming. In this subsection, we propose a design such that all the cryptographic operations are performed in a block-wise manner and the number of the operations becomes independent of N_p.

With the proposed block-wise design, each agent concatenates all its N_p sampled data to form a single block, and all the cryptographic operations are performed over the block. In this way, each agent only performs once encryption, the third party performs twice computation over ciphertexts, and the coordinator performs twice decryption. Hence, with the same key length, the computational complexity is reduced by approximately N_p times.

In order to ensure the correctness, we propose to pad enough zeros in each sampled value as the beginning digits to form an enlarged sub-block before concatenation. Roughly speaking, the number of zeros is carefully designed to be large enough so that the aggregated result over all the agents' corresponding data samples will not overflow the sub-block and hence will not affect the aggregated result of the preceding sub-block. This guarantees the aggregation correctness of each sub-block after deconcatenation.

In the following, we detail the block design and illustrate how to embed it into Algorithm 1.

At step 1, change the bound of α as

$$r'l\alpha > \max\left\{\frac{10^{N_p\times\mathrm{num}(10^{\sigma}N_s\delta_s)}-1}{10^{\mathrm{num}(10^{\sigma}N_s\delta_s)}-1}10^{\sigma}N_s\delta_s, \frac{10^{N_p\times\mathrm{num}(10^{\sigma}N_d\delta_d)}-1}{10^{\mathrm{num}(10^{\sigma}N_d\delta_d)}-1}10^{\sigma}N_d\delta_d\right\}.$$

Before step 2, individual suppliers and customers pad their $p_{i\ell}^{s*}$ and $p_{i\ell}^{d*}$ as

$$\bar{p}_{i\ell}^{s*} = (0\cdots0)_{\mathrm{num}(10^{\sigma}N_s\delta_s)-\mathrm{num}(10^{\sigma}p_{i\ell}^{s*})} \leftrightarrow 10^{\sigma}p_{i\ell}^{s*},$$
$$\bar{p}_{i\ell}^{d*} = (0\cdots0)_{\mathrm{num}(10^{\sigma}N_d\delta_d)-\mathrm{num}(10^{\sigma}p_{i\ell}^{d*})} \leftrightarrow 10^{\sigma}p_{i\ell}^{d*}$$

respectively, and then form the concatenation

$$\bar{p}_{i}^{s*} = \bar{p}_{iN_p}^{s*} \leftrightarrow \cdots \leftrightarrow \bar{p}_{i1}^{s*},$$
$$\bar{p}_{i}^{d*} = \bar{p}_{iN_p}^{d*} \leftrightarrow \cdots \leftrightarrow \bar{p}_{i1}^{d*}$$

respectively. After that, remove the loop over sampled values (i.e., remove the ℓ loop and drop ℓ from anywhere at steps 2–4). At step 2, replace $10^{\sigma}p_{i\ell}^{s*}$ and $10^{\sigma}p_{i\ell}^{d*}$ with $\bar{p}_{i}^{s*}$ and $\bar{p}_{i}^{d*}$, respectively. After step 4, the coordinator performs an additional cutting step by setting, for each $\ell = 1, \cdots, N_p$:

$$\hat{y}_{\ell}^{s} = [\hat{y}^{s}]_{(\mathrm{end}-\ell\times\mathrm{num}(10^{\sigma}N_s\delta_s)+1):(\mathrm{end}-(\ell-1)\times\mathrm{num}(10^{\sigma}N_s\delta_s))},$$
$$\hat{y}_{\ell}^{d} = [\hat{y}^{d}]_{(\mathrm{end}-\ell\times\mathrm{num}(10^{\sigma}N_d\delta_d)+1):(\mathrm{end}-(\ell-1)\times\mathrm{num}(10^{\sigma}N_d\delta_d))}.$$

IV. Security-Aware Design

In this section, the security-aware TES design is proposed by using the popular technique of digital signature. We first extend the attacker model defined in Section III to include data injection attacks. Then, we add to Algorithm 1 an attack detection mechanism so that we can further achieve objective (3) as stated in Section II-C.

Authorized licensed use limited to: Penn State University. Downloaded on March 03,2025 at 02:28:22 UTC from IEEE Xplore. Restrictions apply.

Algorithm 2 Attack Detection Mechanism

Syntax: $(\text{FLAG}, \bar{m}) = \text{Alg}_{\text{ad}}(i, j, \alpha_i, \beta_i, \nu_i, \pi_i, m, \ell)$.

1 **Signature**

Participant i runs

$$(s_1, s_2) = \text{Alg}_{\text{sig}}(\alpha_i, \beta_i, \nu_i, \pi_i, \ell \leftrightarrow m)$$

and sends $(\ell \leftrightarrow m, s_1, s_2)$ to participant j;

2 **Verification**

On receiving the ℓ-th triple $(\bar{z}, \bar{s}_1, \bar{s}_2)$ from (i, j), participant j sets $\bar{m} = [\bar{z}]_{\text{num}(\ell)+1:\text{end}}$ and FLAG $= 1$ if $\text{Alg}_{\text{ver}}(\alpha_i, \beta_i, \bar{z}, \bar{s}_1, \bar{s}_2) = 1$ and $[\bar{z}]_{1:\text{num}(\ell)} = \ell$, and sets $\bar{m} = \text{NULL}$ and FLAG $= 0$ otherwise.

A. Attacker Model

To proceed with the following security-aware TES design, all the market participants $\mathcal{V} \cup \{\text{CO}, \text{TP}\}$ have the same attacker model as defined in Section III-B. In addition, there could exist extraneous attackers that launch the data injection attacks. For example, the extraneous attackers can send arbitrarily forged information to other legitimate participants or arbitrarily tamper the information in transit as they desire. In this paper, we only focus on the data injection attacks over communication links, but do not consider Byzantine attacks, in which some legitimate participants arbitrarily deviate from the given algorithm. We leave the study of Byzantine attacks to our future works.

B. Algorithm Design

The security-aware design, Algorithm 2, is based on the Paillier digital signature scheme. Preliminaries of Paillier digital signature, including the sub-algorithms Alg_{sig} and Alg_{ver}, are given in Appendix B.

Consider the case where participant i aims to send a message m to participant j via link (i, j). Participant i generates Paillier keys $(\alpha_i, \beta_i, \nu_i, \pi_i)$, where (α_i, β_i) are sent over an authenticated link to participant j and (ν_i, π_i) are kept private to itself. Participants i and j perform an attack detection mechanism given by Algorithm 2. The inputs include the identity indicators i and j, participant i's keys $(\alpha_i, \beta_i, \nu_i, \pi_i)$, message m, and an index $\ell \in \mathbb{N}$. The outputs include a binary attack indicator FLAG and participant j's output message $\bar{m}$. In particular, the index ℓ is a stamp to identify which data m is. An example of setting ℓ is given later.

First, participant i generates a pair of signatures (s_1, s_2) for $\ell \leftrightarrow m$ by the Paillier signature algorithm and sends the triple $(\ell \leftrightarrow m, s_1, s_2)$ to participant j. Upon receiving the ℓ-th triple $(\bar{z}, \bar{s}_1, \bar{s}_2)$ from (i, j), participant j performs a verification operation to detect whether the triple has been attacked. The triple passes the verification if and only if: (1) the triple $(\bar{z}, \bar{s}_1, \bar{s}_2)$ passes the Paillier verification algorithm, and (2) the index matches, i.e., the first $\text{num}(\ell)$ digits of $\bar{z}$ matches ℓ. If the triple passes the verification, then participant j sets FLAG $= 1$ to indicate no attack and sets $\bar{m} = [\bar{z}]_{\text{num}(\ell)+1:\text{end}}$, which is just m. Otherwise, participant j sets FLAG $= 0$ to indicate attack and sets $\bar{m} = \text{NULL}$.

The detection is enabled by the property that, without knowing participant i's private keys (ν_i, π_i), an attacker cannot generate a triple that can pass participant j's verification. The index ℓ serves as the time stamp of message m. Without using the time stamp, a verification with FLAG $= 1$ only indicates that the received triple is or was generated by participant i. However, this alone does not tell whether the received triple is the current one. Indeed, an attacker could make use of this fact to launch two attacks that cannot be detected. First, the attacker could replace the current triple in (i, j) by a previously observed triple that had been sent over (i, j). Second, if there are multiple triples in (i, j) simultaneously, the attacker could swap their orders in the link. In these two attacks, since the replaced or reordered triple is a valid triple of message and signatures, it can pass the Paillier verification algorithm Alg_{ver} and the third party cannot detect the attacks. However, with the index ℓ, these two attacks cannot pass the verification operation in Algorithm 2, as a replaced or reordered triple does not match the index.

To proceed, we illustrate how to integrate Algorithm 2 into Algorithm 1. At step 1, each participant $i \in \mathcal{V} \cup \{\text{TP}, \text{CO}\}$ first generates a set of Paillier keys $(\alpha_i, \beta_i, \nu_i, \pi_i)$ by Alg_{key}, broadcasts (α_i, β_i) and keeps (ν_i, π_i) private to itself. All these key generation operations are only performed once. Without loss of generality, we assume that all the public keys are sent over authenticated links enabled by a public-key infrastructure (PKI) [35]. Between step 2 and step 3, insert a step so that supplier $i \in \mathcal{V}_s$ (resp. customer $i \in \mathcal{V}_d$) as well as the third party runs $(\text{FLAG}^s_{i\ell}, \bar{y}^s_{i\ell}) = \text{Alg}_{\text{ad}}(i, \text{TP}, \alpha_i, \beta_i, \nu_i, \pi_i, y^s_{i\ell}, \ell)$ (resp. $(\text{FLAG}^d_{i\ell}, \bar{y}^d_{i\ell}) = \text{Alg}_{\text{ad}}(i, \text{TP}, \alpha_i, \beta_i, \nu_i, \pi_i, y^d_{i\ell}, \ell)$). If $\text{FLAG}^s_{i\ell} = 1$ (resp. $\text{FLAG}^d_{i\ell} = 1$), then the third party adopts $\bar{y}^s_{i\ell}$ (resp. $\bar{y}^d_{i\ell}$) as $y^s_{i\ell}$ (resp. $y^d_{i\ell}$) at step 3. Then, between step 3 and step 4, insert another step so that the third party as well as the coordinator runs $(\text{FLAG}^s_\ell, \bar{y}^s_\ell) = \text{Alg}_{\text{ad}}(\text{TP}, \text{CO}, \alpha_{\text{TP}}, \beta_{\text{TP}}, \nu_{\text{TP}}, \pi_{\text{TP}}, y^s_\ell, 2(\ell - 1) + 1)$ (resp. $(\text{FLAG}^d_\ell, \bar{y}^d_\ell) = \text{Alg}_{\text{ad}}(\text{TP}, \text{CO}, \alpha_{\text{TP}}, \beta_{\text{TP}}, \nu_{\text{TP}}, \pi_{\text{TP}}, y^d_\ell, 2(\ell - 1) + 2)$). If $\text{FLAG}^s_\ell = 1$ (resp. $\text{FLAG}^d_\ell = 1$), then the coordinator adopts $\bar{y}^s_\ell$ (resp. $\bar{y}^d_\ell$) as y^s_ℓ (resp. y^d_ℓ) at step 4. After λ^* is derived at step 5, the coordinator and each agent $i \in \mathcal{V}$ run $(\text{FLAG}_i, \bar{\lambda}^*_i) = (\text{CO}, i, \alpha_{\text{CO}}, \beta_{\text{CO}}, \nu_{\text{CO}}, \pi_{\text{CO}}, 10^{\sigma_\lambda}\lambda^*, i)$, where $\sigma_\lambda \in \mathbb{N}$ is the precision level of price, i.e., for any price λ, only the first σ_λ decimal fraction digits are kept, while the rest are dropped. Hence, $10^{\sigma_\lambda}\lambda^*$ is a non-negative integer. If $\text{FLAG}_i = 1$, then agent i uses $\bar{\lambda}^*_i$ as λ^*.

The above attack detection mechanism guarantees that any data injection attack can be detected by legitimate message receivers. This property directly follows from the security of the Paillier digital signature scheme and the usage of index.

V. Case Studies

In this section, the proposed cyber-resilient design is tested on a TES that coordinates and controls residential air conditioners to manage the feeder congestion.

We consider the problem of real-time electricity allocation for a distribution feeder on a hot summer day (August 16, 2009) for Columbus, Ohio, USA. There are 1000 residential ACs under this feeder. A second-order equivalent thermal

Authorized licensed use limited to: Penn State University. Downloaded on March 03,2025 at 02:28:22 UTC from IEEE Xplore. Restrictions apply.

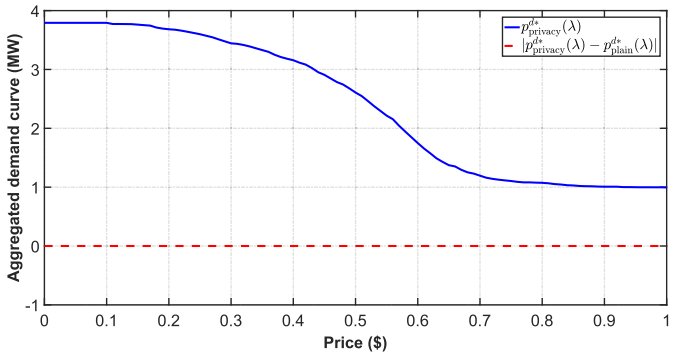


Fig. 3. Aggregated demand curve at the 200-th market cycle.

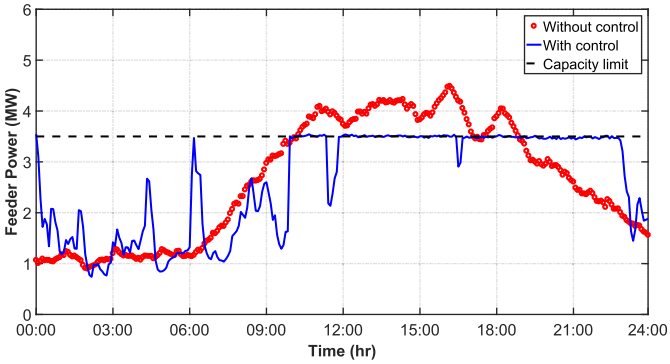


Fig. 4. Comparison of feeder power with and without control.

parameter (ETP) model is used to capture the load dynamics of the ACs. Detailed description of the ETP model parameters can be found in [36]. The simulation time step for the load dynamics is selected to be 30 seconds. The distribution feeder capacity limit is 3.5 MW. In this scenario, the feeder serves as both the coordinator and the only supplier while individual residential ACs serve as the customers.

The weather data as well as the Typical Meteorological Year (TMY2) data are adopted from [37] and [38]. The wholesale electricity price is adopted from the PJM market [39] and then modified to a retail rate plus a retail modifier as defined by American Electric Power (AEP)'s tariff [40]. We define this retail price as the base price.

In each market cycle, the feeder aims to obtain the aggregated demand curve and compares it with the feeder capacity limit to determine the market clearing price. If there is no congestion, then the clearing price is set to the base price. If there is congestion, the clearing price is set as the price corresponding to the feeder capacity limit on the aggregated demand curve. The range of the market clearing price is between $\lambda_{\min} = \$0.00$ and $\lambda_{\max} = \$1.00$. The sampling resolution is selected to be $\tau = \$0.01$ and thus $N_p = 101$. The length of a market cycle is set to be 5 minutes so there are total 288 market cycles in one day.

In our simulation studies, we first verify the correctness property of Algorithm 1 without data injection attacks. Denote by $p^{d*}(\lambda)$ the aggregated demand curve, i.e., $p^{d*}(\lambda) \triangleq \sum_{i\in\mathcal{V}_d} p_i^{d*}(\lambda)$. We simulate the TES both with and without the proposed privacy-preserving design and denote the aggregated demand curves in the two cases by $p^{d*}_{\text{privacy}}(\lambda)$ and $p^{d*}_{\text{plain}}(\lambda)$, respectively. In Fig. 3, the curve $p^{d*}_{\text{privacy}}(\lambda)$ (the solid blue line) shows the aggregated demand curve with the privacy-preserving design at the 200-th market cycle. Note that the number 200 is arbitrarily picked and any other market cycle can also be used for the purpose of illustration. At the same time, the curve $|p^{d*}_{\text{privacy}}(\lambda) - p^{d*}_{\text{plain}}(\lambda)|$ (the dashed red line) shows the difference between the aggregated demand curves with and without the privacy-preserving design at the 200-th market cycle. Since the difference is constant at 0, it implies that $p^{d*}_{\text{privacy}}(\lambda)$ is exactly equal to $p^{d*}_{\text{plain}}(\lambda)$ at all values of λ, which verifies the correctness of Algorithm 1.

The trajectory of feeder power over the day is shown in Fig. 4, where the solid blue line is obtained with the proposed

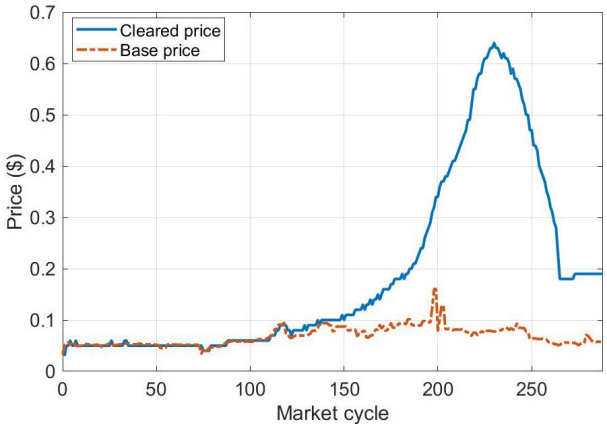


Fig. 5. Market clearing price over the day.

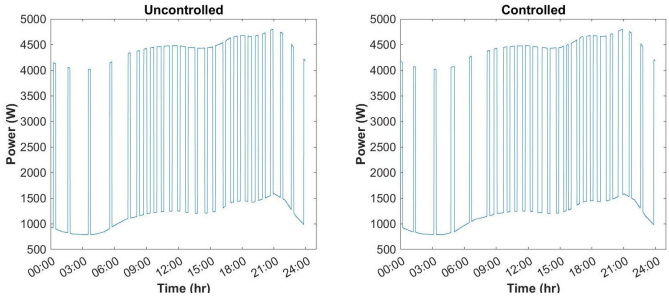


Fig. 6. Power comparison of a comfort-driven AC with and without control.

privacy-preserving TES design and the red dotted line without TES. It is clear that the TES can effectively maintain the feeder power at or below the capacity limit. The trajectory of market clearing price under TES over the day is shown in Fig. 5. It can be seen that the market clearing price is greater than the base price whenever the feeder congestion occurs.

In Fig. 6 and Fig. 7, the daily power profiles of two representative residential ACs are shown respectively to illustrate the difference between their power with and without TES. In Fig. 6, the power difference is small, which indicates that the operations of the corresponding AC is not very sensitive to the change in market clearing price. In other words, it is more comfort driven. In Fig. 7, the power difference is significant, which indicates that the operations of the corresponding AC is very sensitive to the change in market clearing price. In other words, it is more cost driven.

Authorized licensed use limited to: Penn State University. Downloaded on March 03,2025 at 02:28:22 UTC from IEEE Xplore. Restrictions apply.

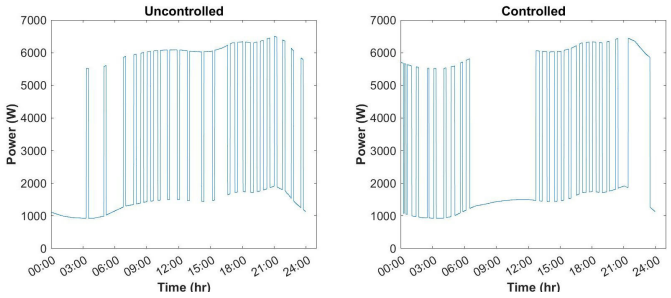


Fig. 7. Power comparison of a cost-driven AC with and without control.

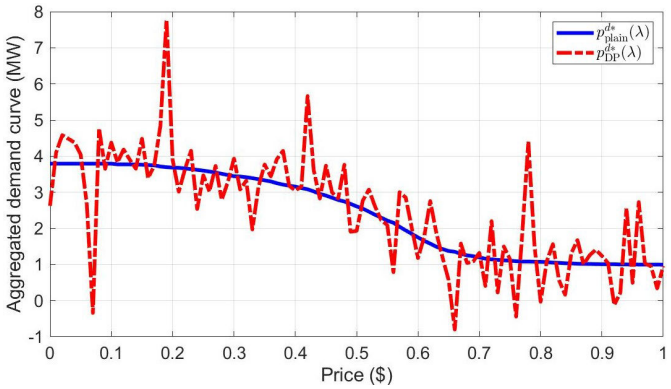


Fig. 8. Deviation of demand curve with differential privacy.

In order to further illustrate the effectiveness of the proposed privacy-preserving TES design, we also test the differential privacy scheme proposed in [41] on the above problem with the commonly-used 0.1-differential privacy. The aggregated demand curves at the 200-th market cycle with and without differential privacy are shown in Fig. 8. The solid blue line, $p^{d*}_{\text{plain}}(\lambda)$, denotes the ground truth of the aggregated demand curve derived without applying any privacy-enhancing technologies, which is the the same as the solid blue line in Fig. 3. The dashed red line, $p^{d*}_{\text{DP}}(\lambda)$, denotes the aggregated demand curve under 0.1-differential privacy. It can be seen that there is significant difference between $p^{d*}_{\text{DP}}(\lambda)$ and $p^{d*}_{\text{plain}}(\lambda)$, which is caused by the introduction of random noises. Decreasing the magnitude of the added noises leads to a smaller deviation but at the price of sacrificing the privacy level. Such utility-privacy trade-off is fundamental for differential privacy schemes [42]. The proposed homomorphic encryption-based scheme in this paper does not involve the use of any random noises and hence is free of utility-privacy trade-off.

We next examine the privacy preservation property of Algorithm 1. In Fig. 9, the left subfigure shows agent 100's demand curve at the 200-th market cycle, and the right subfigure shows its encryption under 500 bits of key length. Fig. 9 visually illustrates the privacy preservation of Algorithm 1, as the points of the encrypted demand curve look like pure random numbers within a large interval.

Next we verify the security awareness of the attack detection mechanism in Section IV. We consider four different attack modes. Mode 1 is no attack. Mode 2 uses a randomly chosen message to replace the true message. More specifically, in this

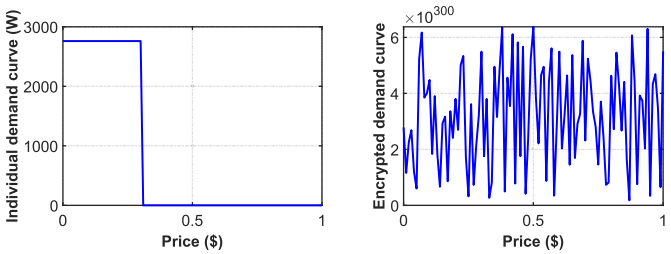


Fig. 9. Agent 100's demand curve at the 200-th market cycle.

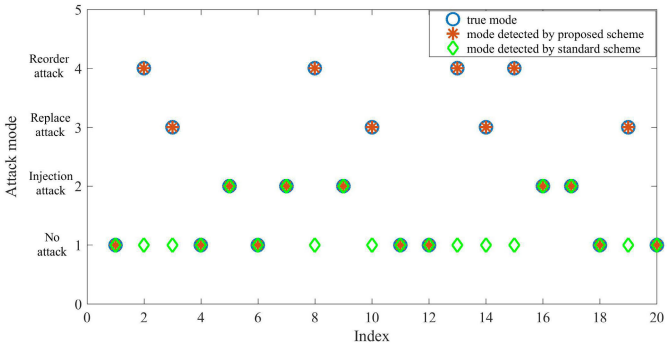


Fig. 10. Attack mode detection.

TABLE I
COMPARISON OF COMPUTATIONAL OVERHEAD

Key length (bit)	Point-wise (s)			Block-wise (s)		
	Agent	TP	CO	Agent	TP	CO
500	0.58	11.97	0.53	0.016	0.12	0.010
1000	2.55	21.19	3.28	0.035	0.16	0.035
1500	7.61	26.57	10.02	0.089	0.27	0.11
2000	16.79	42.36	22.14	0.18	0.41	0.23
2500	32.70	70.03	42.79	0.34	0.71	0.44
3000	55.23	107.35	76.10	0.58	1.09	0.76
3500	87.51	157.78	114.63	0.88	1.61	1.20
4000	128.66	223.32	172.57	1.40	2.34	1.96

mode, to tamper a triple $(\ell \leftrightarrow m, s_1, s_2)$, an attacker randomly chooses a message m' and generates a set of Paillier keys, and uses the keys to generate a pair of signatures (s'_1, s'_2) for $\ell \leftrightarrow m'$. The triple $(\ell \leftrightarrow m', s'_1, s'_2)$ is sent to the message receiver. Mode 3 is data replace attack and mode 4 is data reorder attack. Please refer to Section IV-B for details of these two attacks. We deploy these four modes of attacks to agent 100's 20 consecutive messages at the 200-th market cycle. The detection result is shown in Fig. 10. In the figure, the blue circle is the true attack mode, the red star is the attack mode detected by our proposed digital signature scheme, and the green diamond is the attack mode detected by the standard digital signature scheme in [17]. Fig. 10 shows that our scheme is able to detect all the four modes of attacks, while the scheme in [17] is only able to detect the attacks of modes 1 and 2.

Finally, we examine the efficiency of the integration of the proposed privacy-preserving and security-aware mechanisms. Table I summarizes the running time under different key lengths without and with the block design in Section III-D. The time for agent (columns 2 and 5) is the average time per

Authorized licensed use limited to: Penn State University. Downloaded on March 03,2025 at 02:28:22 UTC from IEEE Xplore. Restrictions apply.

agent per market cycle, and the time for the third party and the coordinator (columns 3, 4, 6 and 7) is the average time per market cycle. We can see that, under the same key length, the running time with the block design is much smaller than that without the block design. For large key lengths, the rate between the running time without and with the block design is approximately $N_p = 101$, which matches our expectation.

VI. Conclusion

This paper studied the privacy and security issues associated with the deployment of TESs. We addressed the privacy issue by developing a homomorphic encryption-based algorithm to achieve the optimal market-based coordination and privacy preservation simultaneously for TESs with hierarchical market clearing. A block design was then proposed to greatly improve the associated computational efficiency. After that, we moved to the security issue and proposed a digital signature-based mechanism that further ensures security awareness. Finally, the effectiveness of the proposed cyber-resilient TES design was verified by simulation studies on the transactive control of residential ACs to relieve feeder congestion.

Appendix

The appendix serves to briefly introduce Paillier encryption and Paillier digital signature. More detailed discussions on Paillier cryptosystem can be found in [18].

A. Paillier Encryption

The Paillier encryption scheme is an additive homomorphic encryption scheme. It consists of key generation, encryption and decryption operations, as illustrated next.

• Key generation: A set of keys $(\alpha, \beta, \nu, \pi)$ is generated by Algorithm 3, in which n is the security parameter to set the key length, (α, β) are public keys and broadcasted, while (ν, π) are private keys and kept secret to the executor itself.

Algorithm 3 Key Generation Algorithm

Syntax: $(\alpha, \beta, \nu, \pi) = \text{Alg}_{\text{key}}(n)$.
The executor randomly chooses two large prime numbers p and q such that $\gcd(pq, (p-1)(q-1)) = 1$ and $|\alpha| = n$ with $\alpha = pq$; computes $\nu = \text{lcm}(p-1, q-1)$; randomly selects an integer $\beta \in \mathbb{Z}^*_{\alpha^2}$ such that the following modular multiplicative inverse π exists

$$\pi = \left(\frac{(\beta^{\nu} \mod \alpha^2) - 1}{\alpha} \right)^{-1} \mod \alpha,$$

i.e., $\pi \frac{(\beta^{\nu} \mod \alpha^2)-1}{\alpha} \equiv 1 \mod \alpha$.

• Encryption: A plaintext $pt \in \mathbb{Z}_{\alpha}$ is encrypted as ct with public keys (α, β) by Algorithm 4.

• Decryption: A ciphertext $ct \in \mathbb{Z}_{\alpha^2}$ is decrypted as pt with public key α and private keys (ν, π) by Algorithm 5.

The correctness, privacy and homomorphic property of the Paillier encryption scheme are given as follows:

Algorithm 4 Encryption Algorithm

Syntax: $ct = \text{Alg}_{\text{enc}}(\alpha, \beta, pt)$.
The executor selects a random integer $r \in \mathbb{Z}^*_{\alpha}$ and computes $ct = \beta^{pt} \cdot r^{\alpha} \mod \alpha^2$.

Algorithm 5 Decryption Algorithm

Syntax: $pt = \text{Alg}_{\text{dec}}(\alpha, \nu, \pi, ct)$.
The executor computes $pt = \frac{(ct^{\nu} \mod \alpha^2)-1}{\alpha} \cdot \pi \mod \alpha$.

(i) Decryption correctness:

$$\text{Alg}_{\text{dec}}(\alpha, \nu, \pi, \text{Alg}_{\text{enc}}(\alpha, \beta, pt)) = pt.$$

(ii) Semantic security: If the decisional composite residuosity assumption (DCRA)[2] holds, then the Paillier encryption scheme is semantically secure. That is, it is computationally infeasible for one to infer any information of plaintexts by observing the corresponding ciphertexts. In other words, this scheme does not disclose any information of plaintexts.

(iii) Homomorphic property: Given any $pt_1, \cdots, pt_m \in \mathbb{Z}_{\alpha}$. If $\sum_{\ell=1}^{m} pt_{\ell} \in \mathbb{Z}_{\alpha}$, then

$$\text{Alg}_{\text{dec}}\left(\alpha, \nu, \pi, \prod_{\ell=1}^{m} \text{Alg}_{\text{enc}}(\alpha, \beta, pt_{\ell})\right) = \sum_{\ell=1}^{m} pt_{\ell}.$$

B. Paillier Digital Signature

The Paillier digital signature scheme consists of key generation, signature and verification operations, as illustrated next.

• Key generation: Same as the key generation operation of the Paillier encryption scheme.

• Signature: A pair of signatures (s_1, s_2) is generated for a message $m \in \mathbb{Z}_{\alpha^2}$ with keys $(\alpha, \beta, \nu, \pi)$ by Algorithm 6.

Algorithm 6 Signing Algorithm

Syntax: $(s_1, s_2) = \text{Alg}_{\text{sig}}(\alpha, \beta, \nu, \pi, m)$.
The executor computes $s_1 = \frac{(m^{\nu} \mod \alpha^2)-1}{\alpha} \cdot \pi \mod \alpha$ and $s_2 = (m \cdot \beta^{-s_1})^{1/\alpha \mod \nu} \mod \alpha$.

• Verification: A triple (m, s_1, s_2) is verified with public keys (α, β) by Algorithm 7.

Algorithm 7 Verification Algorithm

Syntax: $\text{FLAG} = \text{Alg}_{\text{ver}}(\alpha, \beta, m, s_1, s_2)$.
The executor sets $\text{FLAG} = 1$ if $m = \beta^{s_1} s_2^{\alpha} \mod \alpha^2$, and sets $\text{FLAG} = 0$ otherwise.

The security of the Paillier digital signature is illustrated as follows: If the DCRA holds, then, after obtaining signatures to any messages of its choice, an attacker cannot generate a pair of signatures for a new message that can pass the verification with non-negligible probability.

[2]DCRA: Given a composite C and an integer z, it is computationally intractable to decide whether z is a C-residue modulo C^2 or not, i.e., whether there exists y such that $z = y^C \mod C^2$.

Authorized licensed use limited to: Penn State University. Downloaded on March 03,2025 at 02:28:22 UTC from IEEE Xplore. Restrictions apply.

ACKNOWLEDGMENT

The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for U.S. Government purposes. The DOE will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan (http://energy.gov/downloads/doe-public-access-plan).

REFERENCES

[1] S. Li, J. Lian, A. J. Conejo, and W. Zhang, "Transactive energy systems: The market-based coordination of distributed energy resources," *IEEE Control Syst.*, vol. 40, no. 4, pp. 26–52, Aug. 2020.

[2] Y. Gong, Y. Cai, Y. Guo, and Y. Fang, "A privacy-preserving scheme for incentive-based demand response in the smart grid," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1304–1313, May 2016.

[3] O. Tan, D. Gündüz, and H. V. Poor, "Increasing smart meter privacy through energy harvesting and storage devices," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1331–1341, Jul. 2013.

[4] S. Han, U. Topcu, and G. J. Pappas, "Event-based information-theoretic privacy: A case study of smart meters," in *Proc. Amer. Control Conf. (ACC)*, Jul. 2016, pp. 2074–2079.

[5] A. R. Borden, D. K. Molzahn, B. C. Lesieutre, and P. Ramanathan, "Power system structure and confidentiality preserving transformation of optimal power flow problem," in *Proc. 51st Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2013, pp. 1021–1028.

[6] A. R. Borden, D. K. Molzahn, P. Ramanathan, and B. C. Lesieutre, "Confidentiality-preserving optimal power flow for cloud computing," in *Proc. 50th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2012, pp. 1300–1307.

[7] C. Dwork, "Differential privacy," in *Proc. 3rd Int. Colloq. Automata, Lang. Program.*, 2006, pp. 1–12.

[8] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Found. Trends Theor. Comput. Sci.*, vol. 9, nos. 3–4, pp. 211–407, Aug. 2014.

[9] Z. Yang, P. Cheng, and J. Chen, "Differential-privacy preserving optimal power flow in smart grid," *IET Generat., Transmiss. Distrib.*, vol. 11, no. 15, pp. 3853–3861, 2017.

[10] F. Zhou, J. Anderson, and S. H. Low, "Differential privacy of aggregated DC optimal power flow data," in *Proc. Amer. Control Conf.*, 2019, pp. 1307–1314.

[11] X. Lou, R. Tan, D. K. Y. Yau, and P. Cheng, "Cost of differential privacy in demand reporting for smart grid economic dispatch," in *Proc. IEEE Conf. Comput. Commun.*, May 2017, pp. 1–9.

[12] A. Halder, X. Geng, P. R. Kumar, and L. Xie, "Architecture and algorithms for privacy preserving thermal inertial load management by a load serving entity," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3275–3286, Jul. 2017.

[13] Y. Lu and M. Zhu, "A control-theoretic perspective on cyber-physical privacy: Where data privacy meets dynamic systems," *Annu. Rev. Control*, vol. 47, pp. 423–440, 2019.

[14] D. Stevenson, N. Hillery, and G. Byrd, "Secure communications in ATM networks," *Commun. ACM*, vol. 38, no. 2, pp. 45–52, Feb. 1995.

[15] L. Me and G. R. Arce, "A class of authentication digital watermarks for secure multimedia communication," *IEEE Trans. Image Process.*, vol. 10, no. 11, pp. 1754–1764, Nov. 2001.

[16] T. Jiang, Y. Hou, and S. Zheng, "Secure communication between set-top box and smart card in DTV broadcasting," *IEEE Trans. Consum. Electron.*, vol. 50, no. 3, pp. 882–886, Aug. 2004.

[17] C.-I. Fan, S.-Y. Huang, and Y.-L. Lai, "Privacy-enhanced data aggregation scheme against internal attackers in smart grid," *IEEE Trans. Ind. Informat.*, vol. 10, no. 1, pp. 666–675, Feb. 2014.

[18] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, vol. 1999, pp. 223–238.

[19] Y. Lu and M. Zhu, "Secure cloud computing algorithms for discrete constrained potential games," in *Proc. 5th IFAC Workshop Distrib. Estimation Control Networked Syst.*, Sep. 2015, vol. 48, no. 22, pp. 180–185.

[20] Y. Lu and M. Zhu, "Privacy preserving distributed optimization using homomorphic encryption," *Automatica*, vol. 96, pp. 314–325, May 2018.

[21] Y. Shoukry et al., "Privacy-aware quadratic optimization using partially homomorphic encryption," in *Proc. IEEE 55th Conf. Decis. Control (CDC)*, Dec. 2016, pp. 5053–5058.

[22] K. Kogiso and T. Fujita, "Cyber-security enhancement of networked control systems using homomorphic encryption," in *Proc. 54th IEEE Conf. Decision Control (CDC)*, Dec. 2015, pp. 6836–6843.

[23] F. Farokhi, I. Shames, and N. Batterham, "Secure and private control using semi-homomorphic encryption," *Control Eng. Pract.*, vol. 67, pp. 13–20, Oct. 2017.

[24] N. M. Freris and P. Patrinos, "Distributed computing over encrypted data," in *Proc. 54th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Sep. 2016, pp. 1116–1122.

[25] M. Ruan, H. Gao, and Y. Wang, "Secure and privacy-preserving consensus," *IEEE Trans. Autom. Control*, vol. 64, no. 10, pp. 4035–4049, Oct. 2019.

[26] R. Petrlic, "A privacy-preserving concept for smart grids," in *Proc. Sicherheit Vernetzten Systemen*, 2010, pp. B1–B14.

[27] F. D. Garcia and B. Jacobs, "Privacy-friendly energy-metering via homomorphic encryption," in *Proc. Int. Workshop Secur. Trust Manage.*, 2010, pp. 226–238.

[28] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 327–332.

[29] T. Wu, C. Zhao, and Y.-J.-A. Zhang, "Privacy-preserving distributed optimal power flow with partially homomorphic encryption," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4506–4521, Sep. 2021.

[30] Y. Lu, J. Lian, and M. Zhu, "Privacy-preserving transactive energy system," in *Proc. Amer. Control Conf. (ACC)*, Jul. 2020, pp. 3005–3010.

[31] J. Lian, H. Ren, Y. Sun, and D. J. Hammerstrom, "Performance evaluation for transactive energy systems using double-auction market," *IEEE Trans. Power Syst.*, vol. 34, no. 5, pp. 4128–4137, Sep. 2019.

[32] R. Gordon. *Power Systems in the IBM Cloud—IBM Enterprise Level Cloud Support*. Accessed: Jul. 29, 2019. [Online]. Available: https://mainline.com/power-systems-in-the-ibm-cloud-enterprise-level-cloud-support/

[33] C. Hazay and Y. Lindell, *Efficient Secure Two-Party Protocols—Techniques and Constructions*. New York, NY, USA: Springer, 2010.

[34] D. Giry, "Cryptographic key length recommendation," BlueKrypt, Neuve, Belgium, Version 32.3, May 2020. [Online]. Available: https://www.keylength.com/en/8/

[35] C. Paar and J. Pelzl, *Understanding Cryptography*. Cham, Switzerland: Springer, 2010.

[36] *GridLAB-D Residential Module User's Guide*. Accessed: Jul. 29, 2019. [Online]. Available: http://www.eps.ee.kth.se/personal/luigiv/pst/

[37] *Weather Unidergrounds: Weather Record for Columbus*. Accessed: Jul. 29, 2019. [Online]. Available: https://www.wunderground.com/

[38] W. Marion and K. Urban, "User's manual for TMY2s: Typical meteorological years: Derived from the 1961–1990 National Solar Radiation Data Base," Nat. Renew. Energy Lab., Golden, CO, Tech. Rep., 1995.

[39] *PJM Wholesale Market Energy Price*. Accessed: Jul. 29, 2019. [Online]. Available: http://pjm.com/markets-and-operations/energy.aspx

[40] *AEP Ohio Power Company Standard Tariff*. Accessed: Jul. 29, 2019. [Online]. Available: https://aepohio.com/account/bills/rates/AEPOhioRatesTariffsOH.aspx

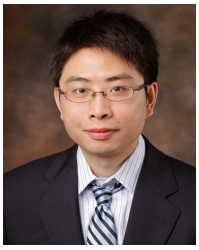
[41] J. L. Ny and G. J. Pappas, "Differentially private filtering," *IEEE Trans. Autom. Control*, vol. 59, no. 2, pp. 341–354, Feb. 2014.

[42] Q. Geng and P. Viswanath, "Optimal noise adding mechanisms for approximate differential privacy," *IEEE Trans. Inf. Theory*, vol. 62, no. 2, pp. 952–969, Feb. 2016.

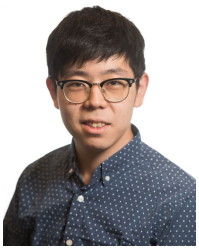
Authorized licensed use limited to: Penn State University. Downloaded on March 03,2025 at 02:28:22 UTC from IEEE Xplore. Restrictions apply.

Yang Lu received the B.E. and M.E. degrees in electrical engineering from Shanghai Jiao Tong University in 2010 and 2013, respectively, the M.S. degree in electrical engineering from the Georgia Institute of Technology in 2013, and the Ph.D. degree in electrical engineering from The Pennsylvania State University (PSU) in 2020. From March 2013 to June 2014, he worked as a Visiting Scholar with the School of Electrical and Computer Engineering, Georgia Institute of Technology. From January 2019 to May 2019, he worked as a Ph.D. Intern with the Pacific Northwest National Laboratory. From September 2020 to August 2021, he worked as a Post-Doctoral Scholar with the School of Electrical Engineering and Computer Science, PSU. He is currently a Lecturer (Assistant Professor) with the Systems Security Group, School of Computing and Communications, Lancaster University. His research interests include cyber-physical privacy and security, distributed control and optimization of multi-agent networks, and machine learning. He was a recipient of the Dr. Nirmal K. Bose Dissertation Excellence Award from PSU in 2019.

Jianming Lian (Senior Member, IEEE) received the B.S. degree (Hons.) from the University of Science and Technology of China, Hefei, China, in 2004, and the M.S. and Ph.D. degrees in electrical engineering from Purdue University, West Lafayette, IN, USA, in 2007 and 2009, respectively. He is currently a Distinguished Research and Development Staff and the Group Leader of the Grid-Interactive Controls Group of Energy Science and Technology Directorate with the Oak Ridge National Laboratory (ORNL). Prior to that, he was a Chief Engineer and a Team Lead of the Energy and Environment Directorate with the Pacific Northwest National Laboratory. He served as the project manager, a PI/Co-PI, and a key technical contributor for many large projects focusing on the engagement and integration of various distributed energy resources (DERs) into the future distribution management system. He has established the theoretical foundation of market-based control (aka. transactive control) for future transactive energy system. His research interests include diverse methods from control, optimization, economics, game theory, and data analytics and machine learning to improve the reliability and resilience as well as security and sustainability of complex energy systems, including power grid and building systems.



Minghui Zhu received the Ph.D. degree in engineering science (mechanical engineering) from the University of California at San Diego in 2011. He is currently an Associate Professor with the School of Electrical Engineering and Computer Science, The Pennsylvania State University (Penn State). Prior to joining Penn State in 2013, he was a Post-Doctoral Associate with the Laboratory for Information and Decision Systems, Massachusetts Institute of Technology. He is the coauthor of the book *Distributed Optimization-Based Control of Multi-Agent Networks in Complex Environments* (Springer, 2015). His research interests include distributed control and decision-making of multi-agent networks with applications in robotic networks, security and the smart grid. He was a recipient of the Dorothy Quiggle Career Development Professorship in engineering from Penn State in 2013, the Outstanding Reviewer of Automatica Award in 2013 and 2014, and the National Science Foundation CAREER Award in 2019. He is an Associate Editor of the IEEE OPEN JOURNAL OF CONTROL SYSTEMS and the *IET Cyber-Systems and Robotics* and the Conference Editorial Board of the IEEE Control Systems Society.



Ke Ma (Member, IEEE) received the B.E. degree in automation from Tsinghua University, Beijing, China, in 2012, and the Ph.D. degree in electrical and computer engineering from the Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX, USA, in 2018. He is currently a Senior Analyst in Advanced Technology Solutions, ISO New England Inc. Prior to that, he was an Electrical Engineer with the Pacific Northwest National Laboratory (PNNL). His research interests include dynamic mechanism design and its application in electricity market, and market-based (transactive) coordination and control of distributed energy resources (DERs).

Authorized licensed use limited to: Penn State University. Downloaded on March 03,2025 at 02:28:22 UTC from IEEE Xplore. Restrictions apply.