Hindawi
Mobile Information Systems
Volume 2017, Article ID 3680671, 11 pages
https://doi.org/10.1155/2017/3680671

Research Article

Efficient and Privacy-Aware Power Injection over AMI and Smart Grid Slice in Future 5G Networks

Yinghui Zhang,[1,2,3] Jiangfan Zhao,[1] and Dong Zheng[1,3]

[1]*National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China*
[2]*State Key Laboratory of Cryptology, Beijing 100878, China*
[3]*Westone Cryptologic Research Center, Beijing 100070, China*

Correspondence should be addressed to Yinghui Zhang; yhzhaang@163.com and Dong Zheng; dzhengcrypto@hotmail.com

Received 20 October 2016; Revised 8 December 2016; Accepted 4 January 2017; Published 30 January 2017

Academic Editor: Jing Zhao

Smart grid is critical to the success of next generation of power grid, which is expected to be characterized by efficiency, cleanliness, security, and privacy. In this paper, aiming to tackle the security and privacy issues of power injection, we propose an efficient and privacy-aware power injection (EPPI) scheme suitable for advanced metering infrastructure and 5G smart grid network slice. In EPPI, each power storage unit first blinds its power injection bid and then gives the blinded bid together with a signature to the local gateway. The gateway removes a partial blind factor from each blinded bid and then sends to the utility company aggregated bid and signature by using a novel aggregation technique called hash-then-addition. The utility company can get the total amount of collected power at each time slot by removing a blind factor from the aggregated bid. Throughout the EPPI system, both the gateway and the utility company cannot know individual bids and hence user privacy is preserved. In particular, EPPI allows the utility company to check the integrity and authenticity of the collected data. Finally, extensive evaluations indicate that EPPI is secure and privacy-aware and it is efficient in terms of computation and communication cost.

1. Introduction

The fifth generation of mobile technology (5G) is positioned to provide a holistic end-to-end infrastructure that will include all aspects of the network. To be specific, the future 5G network is envisioned to provide higher data rates, enhanced end-user experience, and much lower latency and energy consumption. In particular, security and privacy preservation mechanisms are expected to be achieved besides the enhanced performance in 5G networks. Because wireless data services have witnessed an explosive growth driven by mobile Internet and smart devices, the new 5G mobile networks are expected to be deployed around 2020. The 5G architecture should include modular network functions that could be deployed and scaled on demand, to accommodate different use cases in a cost efficient and flexible manner.

As the next generation of power grid, smart grid belongs to a representative use case suggested in the Next Generation Mobile Network (NGMN) association's white paper [1]. Smart grid combines traditional grid with communication and information control technologies. It is expected to be characterized by efficiency, cleanliness, consumer involvement, security, privacy, and so forth. Indeed, as one of the main objectives of smart grid, the reduction of greenhouse gas emissions is greatly meaningful for the lives of the people [2]. This objective can be realized by widely deploying renewable energy generators and adaptively balancing the power demand and supply. Therefore, smart grid should have a large number of power storage units to store the excess power in certain cases, such as strong wind. Then, they inject the excess power to the grid when the utility company begins to collect energy at the period of reduced production. Both the utility company and the power storage units benefit from this process, where the utility company should be able to communicate with the power storage units. As important components of smart grid, smart meters (SMs) are two-way communication devices which are used to record power consumption periodically and collect real-time information on grid operations. The power storage units can be connected to the network of SMs through the existing

network infrastructure Advanced Metering Infrastructure (AMI). SMs can communicate with local gateways based on AMI networks and the communication between the gateways and the utility company could be realized through the 5G smart grid network slice.

Considering the issues of user privacy, communication efficiency, and so forth, it is meaningful for the gateways to aggregate the received requests before sending them to the utility company. Since transactions will be involved during power injection, data security and user privacy are of great importance. For one thing, all the data transmitted in the grid should be authenticated and be secure against unauthorized reading and malicious modifications. For another, user privacy related information must be protected against various attackers. For instance, during the communication process of power injection, individual power injection bids are sensitive and must be hidden. If some power storage units know that the other units do not inject power, they can deny selling power to force the utility company to offer a higher price. Furthermore, computation cost and communication overheads must be taken into account during power injection in smart grid. Therefore, the aggregation technique is important for addressing the above issues. As far as the authors' knowledge, however, most existing solutions cannot tackle the security issues of power injection in smart grid.

To solve the above problems, in this paper, we propose an Efficient and Privacy-aware Power Injection (EPPI) scheme suitable for AMI and 5G smart grid network slice. In EPPI, a novel data aggregation technique, named *hash-then-addition*, is proposed. Specifically, each power storage unit can generate two secret keys based on bilinear pairings and use the hash values of the keys to blind its power injection bid. Based on AMI networks, each power storage unit sends its blinded power bid and the corresponding signature to the local gateway. It also generates a message authentication code based on exponentiation operations and sends the result to the gateway. Upon receiving packets from all the units, the gateway first removes a partial blind factor from each blinded bid. Then it aggregates the bids and signatures to get an aggregated bid and an aggregated signature. The gateway also aggregates all the message authentication codes to achieve an aggregated code. All the aggregated values are sent by the gateway to the utility company through the 5G smart grid network slice. Upon receiving the packet, the utility company can generate some secret keys and get the total amount of injected power at each time slot by removing the sum of the secret keys from the aggregated bid. In the proposed EPPI system, only the utility company can know the total amount of injected power at each time slot, and it is able to ensure the integrity and authenticity of the data. In particular, individual power bids are hidden during the communications in AMI networks and the 5G smart grid network slice. Through extensive evaluations we show that EPPI is secure and privacy-aware under the discrete logarithm assumption and it is efficient in terms of computation and communication cost.

1.1. Related Work. The 5G system deployed initially in 2020 is expected to provide approximately 1000 times higher wireless area capacity compared with the current 4G system [3]. The advanced cloud radio access network (C-RAN) has been presented as a potential 5G solution. C-RAN has attracted intense research interest from both academia and industry [4]. Combined with cloud computing technologies, the 5G network will extend its capability to provide various cloud services, which provides the user a full smart life experience. Cloud computing security has been well studied [5–8] and various cloud services are provided [9–11]. The air interface and spectrum of the 5G system should be combined with the long term evolution (LTE) and WiFi to achieve seamless and consistent user experience across time and space [12]. Nikaein et al. [13] presented a slice-based 5G architecture that efficiently manages network slices. NGMN anticipates countless emerging use cases with a high variety of applications will be supported in 5G. As an important use case, smart grid has attracted many scholars' interest. In smart grid, in order to reduce communication overhead, it is essential to aggregate individual users' data at local intermediate nodes. The trivial method of decrypt-aggregate-encrypt is computationally expensive and is risky when intermediate nodes are not trusted. Castelluccia et al. [14] enabled efficient encrypted data aggregation based on homomorphic encryption techniques. Westhoff et al. [15] proposed a key predistribution scheme that is suitable for the end-to-end encryption in sensor networks. A symmetric homomorphic encryption can be used together with [15] to improve the efficiency and flexibility of data aggregation. In smart grid, each user has energy consumption data of multiple dimensions and each dimensional data is small in size. If homomorphic encryption techniques are used directly on each dimensional data, the communication overhead will be unaffordable. Lin et al. [16] proposed a multidimensional privacy-preserving data aggregation scheme for saving energy consumption in wireless sensor networks by integrating the super-increasing sequence and perturbation techniques into compressed data aggregation. Lu et al. [17] designed a compressed data aggregation scheme under the public key infrastructure to improve efficiency and achieve high reliability. To improve the performance of the power grid, several schemes have been proposed to coordinate power charging [18, 19].

In AMI networks, smart meters periodically send fine-grained power consumption data to the utility company. This data has a relation to the users' activities and hence is sensitive. Tonyali et al. [20] developed a meter data obfuscation scheme to protect consumer privacy from eavesdroppers and the utility company. In order to tackle the scalability of AMI networks, Rabieh et al. [21] divided the AMI network into clusters of SMs and proposed two certificate revocation schemes to identify and nullify the false positives when using bloom filters to reduce the size of the certificate revocation lists. Besides, privacy-aware schemes with various security characteristics have been investigated for different network environment and applications [22–27]. Note that these schemes are not focusing on the security and privacy issues in power injection. Recently, Mahmoud et al. [28] have proposed a power injection querying scheme over AMI and LTE cellular networks. In [28], two aggregation techniques, point addition aggregation and homomorphic encryption based aggregation, are adopted to enable the local gateway to

aggregate individuals' power bids, where the homomorphic encryption [29] is used. However, we found that the scheme [28] fails to achieve privacy protection in that it cannot preserve the power storage unit's bid. In fact, in [28], the utility company recovers the total amount of power by exhaustively computing jQ at different values of $j \in \mathbb{Z}_q^*$ until $jQ = \sum_{i=1}^{n} b_i Q$, where Q is a bilinear group element and b_i is an individual power injection bid. Obviously, this computation contradicts with the discrete logarithm assumption. In order to enable the utility company to get $\sum_{i=1}^{n} b_i$, the authors assume that $\sum_{i=1}^{n} b_i$ is a small number. Unfortunately, if $\sum_{i=1}^{n} b_i$ is a small number, then each b_i is a small number. In this case, any attacker can get b_i and hence violates the bid privacy in that $B_i = b_i Q$ is publicly sent by the power storage unit. More details can be found in [28]. The proposed EPPI realizes privacy preservation by using hash-then-addition aggregation technique and it does not constrain the power amount in any way.

1.2. Organization. The remaining of this work is organized as follows. We first review some preliminaries in Section 2. In Section 3, we present the system architecture and adversary models. We propose an efficient and privacy-aware power injection scheme over AMI and smart grid slice in 5G networks in Section 4. The security analysis and performance evaluations are described in Sections 5 and 6, respectively. Finally, we draw our conclusions in Section 7.

2. Preliminaries

In this section, we give a brief review on some cryptographic backgrounds.

2.1. Cryptographic Background

Definition 1 (bilinear pairings). Let $\mathbb{G}$, $\mathbb{G}_T$ be cyclic multiplicative groups of prime order q. Let $P \in \mathbb{G}$ be a generator. We call $\hat{e}$ a bilinear pairing if $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a map with the following properties [30]:

(1) bilinear: $\hat{e}(aP, bP) = \hat{e}(P, P)^{ab}$ for all $a, b \in \mathbb{Z}_q^*$,

(2) nondegenerate: there exists $P, Q \in \mathbb{G}$ such that $\hat{e}(P, Q) \neq 1$,

(3) computable: there is an efficient algorithm to compute $\hat{e}(P, Q)$ for all $P, Q \in \mathbb{G}$.

We define that $\mathcal{G}(\lambda)$ outputs $(q, P, \mathbb{G}, \mathbb{G}_T, \hat{e})$ where λ is a security parameter.

2.2. Discrete Logarithm Assumption

Definition 2 (discrete logarithm problem [31]). Let $\mathbb{G}$ be a group of prime order q, given two elements P and Q, to find an integer $x \in \mathbb{Z}_q^*$, such that $Q = xP$ whenever such an integer exists.

Definition 3 (discrete logarithm assumption [31]). In group $\mathbb{G}$, it is computationally infeasible to determine x from P and $Q = xP$.

3. System Architecture and Adversary Models

3.1. System Architecture. As shown in Figure 1, the system architecture of power injection over AMI and smart grid slice in 5G networks involves a number of communities and a utility company, and they are connected through a smart grid 5G network slice. In a community, there are many power storage units that are connected to AMI. Each AMI network connects to an access node and eventually to the utility company through a smart grid 5G network slice. The details are given as below.

(i) Power Storage Units. The power storage units can be home batteries or charging stations. They store power energy from the smart grid or other renewable energy sources. Each storage unit can buy power from the grid at a low-price period and inject excess power energy to the grid at a high-price period. Note that a storage unit communicates with a SM based on the IEEE 802.11s protocol.

(ii) AMI Network. The AMI network is an architecture for automated, two-way communication between SMs and a utility company. The goal of an AMI is to provides utility companies with real-time data about power consumption and allow users to make informed choices about energy usage based on the price at the time of use. In this paper, for the sake of efficiency, cleanliness, security, and privacy, smart meters communicate indirectly with the utility company by the gateway. The AMI network corresponding to a community comprises a group of SMs and a gateway. Similar to the work [28], two different AMI network topologies are considered: single hop AMI networks and multihop AMI networks. As shown in Figure 1, the SMs in the multihop AMI network are connected through a multihop wireless mesh topology, where each SM plays a role of relaying packets from other SMs. In the single-hop AMI network, the gateway can directly collect power injection related data from corresponding SMs, and then it aggregates the data and sends the result to the utility company. This process is performed periodically, for example, every 15 minutes. It can also receive the latest power data from the utility company and broadcast it to the SMs in the corresponding AMI network. Note that, similar to [28], the AMI network routes are created using the IEEE 802.11s mesh standard.

(iii) Smart Grid Slice in 5G Networks. A 5G network slice supports the communication service of a particular connection type with a specific way of handling the C- and U-plane for this service [1]. For this purpose, a 5G slice consists of a series of 5G network functions and specific radio access technology (RAT) settings that are combined together for the particular use case. Therefore, a 5G slice can span all domains of the network. Not all slices contain the same functions, and some functions that seem important for a mobile network might even be missing in other slices. After network function virtualization, the radio access network and the core network are called edge cloud and central cloud (or core cloud), respectively. The front haul between the access node and the edge cloud is based on software-define

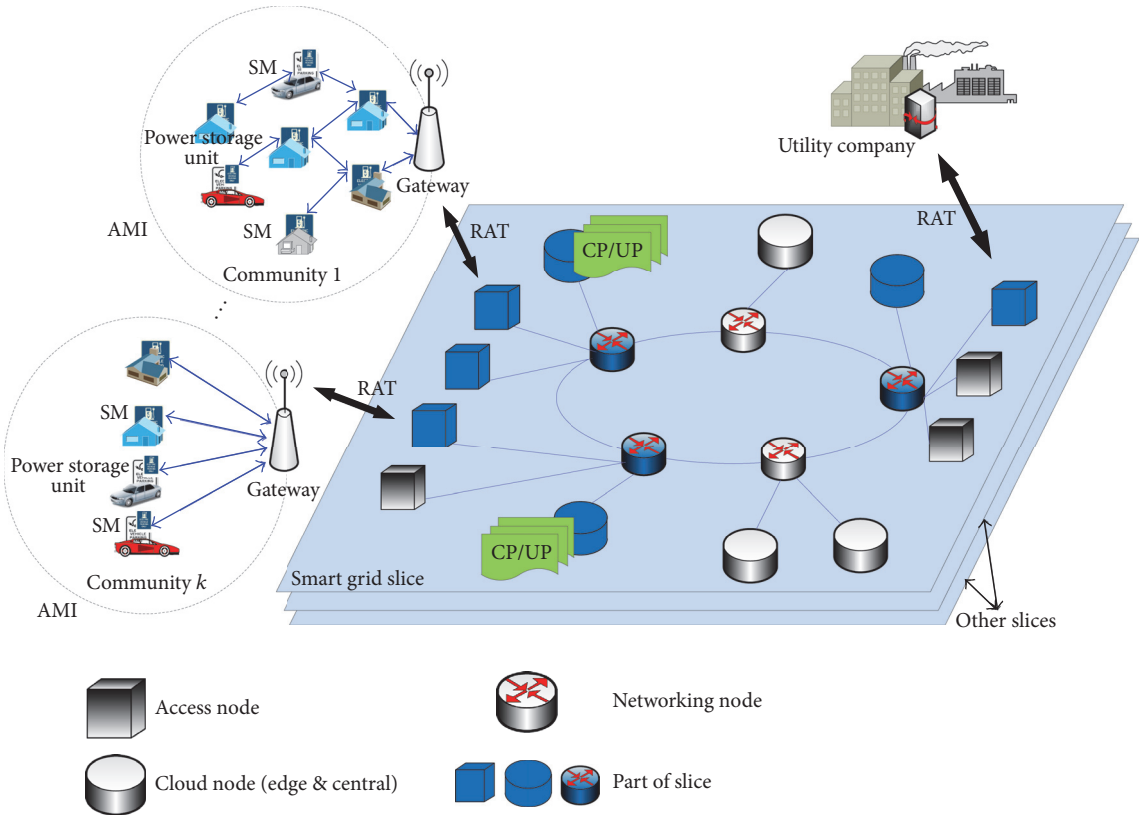

Figure 1: System architecture of power injection in future 5G networks.

networking (SDN). The backhaul between the edge cloud and the core cloud is also based on SDN. For a 5G slice supporting smart grid use case, security, privacy, reliability, and latency are of paramount importance. As shown in Figure 1, to tailor the network functions to suit the smart gird slice, all the necessary functions are instantiated at the cloud edge node.

(iv) Utility Company. If the power energy demand from communities is more than the supply, the utility company should contact electricity vendors or power storage units to buy power. Note that the utility company communicates with the power storage units via the AMI and 5G smart grid slice networks. It connects to the 5G slice through an access node.

3.2. Adversary Models. It is assumed that all the entities are "honest-but-curious." More precisely, they will honestly execute the tasks assigned by legitimate parties but try to find out as much private information as possible. Each power storage unit is curious to know the other units' bids to judge whether it is more profitable to inject power now. We assume that each power storage unit can only send packets in the corresponding community. The AMI network attackers, the smart grid 5G slice attackers, and outsiders are also interested in other's sensitive information, such as the amount and time of the power injection of each power storage unit. Similarly, the utility company does not disrupt the communication, but it tries to get private information on the owners of the power storage units and any other information that can help gain economic benefits. Note that the utility company does not collude with the power storage units in that they have conflicting interests. The utility wants to buy power at low prices but the storage units want to increase revenues. The power storage units will inject the amount of power as committed in their bids because this is more profitable.

3.3. Security Requirements and Design Goals. Considering the practical application environment, security and privacy are significant for the success of a power injection system. In order to prevent aforementioned adversaries from learning power storage units' individual bid and to detect the adversaries' malicious behaviors, the following security requirements should be satisfied in a secure power injection system.

(i) Confidentiality and Privacy Protection. Even if an adversary eavesdrops the communication on the AMI and smart grid slice networks, it fails to achieve the total amount of power injected from the community. The utility cannot know the contents of individual power storage unit's bid. In our scheme, aggregation at gateways is adopted to achieve these goals.

(ii) Authentication and Integrity. The utility company is able to authenticate the received packets to ensure that the packets are really from legal power storage units and have not been altered during the transmission; that is, if the adversary forges and/or modifies a packet, the malicious behavior should be

detected. Besides, the adversary should not impersonate the utility company, the gateway, or the storage units.

In general, under the proposed system architecture and security requirements, our design goal is to design an efficient and privacy-aware power injection scheme based on AMI and smart grid slice in 5G networks. To be specific, the following two objectives should be achieved. Firstly, the security requirements should be guaranteed in the proposed scheme. For one thing, a desirable scheme should provide robust security against various types of attacks including passive eavesdropping, impersonation attack, replay attack, and man-in-the-middle attack. For another, a desirable power injection scheme should enjoy some significant security benefits such as the assurance of session key freshness which enables the forward and backward secrecy. Secondly, the performance-related issue should be taken into consideration. The proposed power injection scheme should enjoy desirable efficiency in terms of the computation cost and the communication overhead.

4. Proposed EPPI Scheme

In this section, we propose an efficient and privacy-aware power injection scheme over AMI and smart grid slice in 5G networks, which comprises the following six phases: system initialization, registration, power collection request, privacy-aware bid generation, privacy-aware bid aggregation, and privacy-aware aggregated bid reading. Figure 2 presents the process of the proposed EPPI system. The details are given in the following.

4.1. System Initialization. The proposed EPPI system is initialized by the utility company. Specifically, in the system initialization phase, given the security parameter λ, the utility company first generates $(q, P_0, \mathbb{G}, \mathbb{G}_T, \hat{e})$ by running $\mathcal{G}(\lambda)$. It computes $Y = \hat{e}(P_0, P_0)$ and chooses two random elements $U, V \in \mathbb{G}$ and four secure cryptographic hash functions H, H_1, H_2, and H_3, where $H : \{0,1\}^* \to \mathbb{Z}_q^*$, $H_1 : \{0,1\}^* \to \mathbb{G}$, $H_2 : \mathbb{G}_T \to \mathbb{Z}_q^*$, and $H_3 : \mathbb{G}_T \to \{0,1\}^*$. Then, the utility company chooses a random element $\mathrm{sk}_u \in \mathbb{Z}_q^*$ as its secret key and calculates $\mathrm{PK}_u = \mathrm{sk}_u P_0$ as its public key. Finally, the utility company keeps sk_u secret and publishes the global public parameters

$$\mathrm{GPK} = \left(\mathbb{G}, \mathbb{G}_T, \hat{e}, q, P_0, U, V, \mathrm{PK}_u, H, H_1, H_2, H_3, Y\right). \quad (1)$$

4.2. Registration. In order to join the EPPI system, each gateway chooses a random element $\mathrm{sk}_g \in \mathbb{Z}_q^*$ as its secret key and calculates $\mathrm{PK}_g = \mathrm{sk}_g P_0$ as its public key. A power storage unit with identity ID_i chooses a random element $\mathrm{sk}_i \in \mathbb{Z}_q^*$ as its secret key and calculates $\mathrm{PK}_i = \mathrm{sk}_i P_0$ as its public key. Similar to [28], in the proposed EPPI system, all the gateways and power storage units should contact the utility company to receive corresponding certificates for public keys. Note that the existing public key infrastructure (PKI) can be used to generate certificates. Besides PKI, in the proposed scheme, the aggregated message authentication code and the aggregated signatures are necessary to ensure the authenticity and integrity of transaction data, which are shown in the privacy-aware bid aggregation phase.

4.3. Power Collection Request. During the peak hours, the utility company can collect power from related communities. To be specific, the utility company sends power collection request (*Power_Req*) packets to corresponding gateways. Upon receiving the packet, each gateway verifies the freshness and validity of the packet. Then the gateway broadcasts the valid packet in its community.

Suppose the utility company wants to collect power in the community corresponding to the gateway ID_g. As shown in Figure 2, the packet contains the identities of the utility company and the gateway, that is, ID_u and ID_g. It also has the power collection information of price per unit in each time slot, that is, $\mathrm{Info}_p = (p_1, p_2, \ldots, p_k)$, where k is the number of time slots. Then the utility company randomly chooses $r_u \in \mathbb{Z}_q^*$, computes $r_u P_0$, and attaches $r_u P_0$ in the packet *Power_Req*. Note that $r_u P_0$ is used by each power storage unit covered by the gateway ID_g in establishing a one-time key shared with the utility company. Besides, the packet contains a timestamp TS and a signature σ_u, where

$$\sigma_u = \mathrm{sk}_u H_1\left(\mathrm{ID}_u \parallel \mathrm{ID}_g \parallel \mathrm{Info}_p \parallel r_u P_0 \parallel \mathrm{TS}\right). \quad (2)$$

Both TS and σ_u will be used by the gateway in verification of the packet.

In fact, after receiving the packet *Power_Req*, the gateway ID_g first checks the freshness of *Power_Req* according to the difference between the current time and the timestamp TS. Then, it verifies the signature by checking if $\hat{e}(\sigma_u, P_0) = \hat{e}(H_1(\mathrm{ID}_u \parallel \mathrm{ID}_g \parallel \mathrm{Info}_p \parallel r_u P_0 \parallel \mathrm{TS}), \mathrm{PK}_u)$ holds. If and only if the equation holds, the gateway ID_g randomly chooses $r_g \in \mathbb{Z}_q^*$, computes $r_g P_0$, and attaches $r_g P_0$ in the packet *Power_Req*. Note that $r_g P_0$ is used by each power storage unit covered by the gateway ID_g in establishing a one-time key shared with the gateway. Then, the gateway broadcasts the packet in its community.

4.4. Privacy-Aware Bid Generation. Upon receiving the power collection request, each power storage unit should prepare a bid with the amount of power it can inject in each time slot. Then, it sends a power request response *Power_Res* packet to the corresponding gateway or its upstream smart meter. The bid format of the power storage unit ID_i is $b_i = (b_{i,1}, b_{i,2}, \ldots, b_{i,k})$, where $b_{i,x}$ represents the number of power units the power storage unit ID_i can inject in the x-th time slot at price p_x for $1 \le x \le k$. As shown in Figure 2, the packet *Power_Res* contains the identities of the gateway and the utility company, that is, ID_g and ID_u. The power storage unit ID_i randomly chooses $r_i \in \mathbb{Z}_q^*$, computes $r_i P_0$, and attaches $r_i P_0$ in the packet *Power_Res*. Note that $r_i P_0$ is used by ID_u in establishing a shared one-time key between ID_i and ID_u. The power storage unit ID_i computes two shared keys as $\hat{k}_i = H_2(\hat{e}(\mathrm{PK}_g, \mathrm{sk}_i r_i r_g P_0))$ and $k_i = H_2(\hat{e}(\mathrm{PK}_u, \mathrm{sk}_i r_i r_u P_0))$, which will be used to mask ID_i's bid and k_i can enable the utility company to ensure the authenticity and integrity of the aggregated bids without needing to read the individual bid.

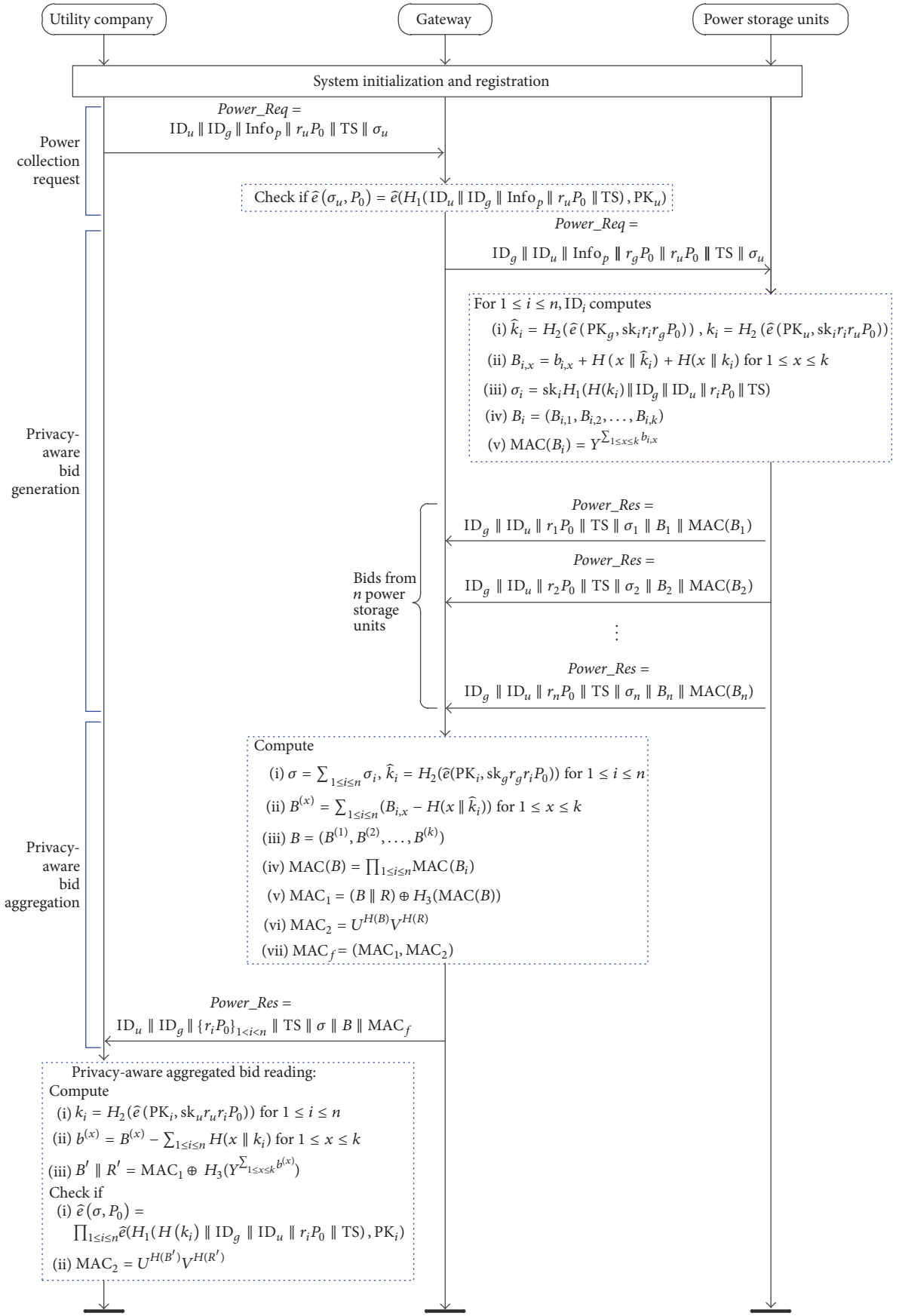

Figure 2: Six phases of the proposed EPPI system.

It is noted that we propose a novel bib aggregation method called *hash-then-addition* in the aggregation phase. Corresponding to this method, the power storage unit ID_i computes its masked bid as $B_i = (B_{i,1}, B_{i,2}, \ldots, B_{i,k})$, where $B_{i,x} = b_{i,x} + H(x \parallel \widehat{k}_i) + H(x \parallel k_i)$ for $1 \le x \le k$. It then calculates a signature $\sigma_i = \mathrm{sk}_i H_1(H(k_i) \parallel \mathrm{ID}_g \parallel \mathrm{ID}_u \parallel r_i P_0 \parallel \mathrm{TS})$ and a message authentication code $\mathrm{MAC}(B_i) = Y^{\sum_{1\le x\le k} b_{i,x}}$. Note that the masked bid can realize privacy protection in the sense of hiding individual bids.

4.5. Privacy-Aware Bid Aggregation. Upon receiving all the power request response packets, the gateway ID_g aggregates these packets and sends an aggregated response packet to the utility company ID_u. The aggregated packet enjoys the following benefits. Firstly, the power storage unit's bid privacy is preserved, which is very important in practical applications. For example, it can prevent the utility company from manipulating the power collection price. In fact, what the utility company needs is not the power storage units' individual power injection data, but the total power amount that can be collected from the community in each time slot. Secondly, the aggregated packet has smaller packet size and hence reduces the required bandwidth for transmitting the data to the utility company. Thirdly, instead of sending one message for each bid, all the bids in different time slots can be collected in one message. In the following, we show how to aggregate the packets considering two different scenarios: a single-hop AMI network and a multihop AMI network.

In the case of a single-hop AMI network, upon receiving all the *Power_Res* packets, ID_g computes a secret key $\widehat{k}_i = H_2(\widehat{e}(\mathrm{PK}_i, \mathrm{sk}_g r_g r_i P_0))$ shared with the power storage unit ID_i for $1 \le i \le n$. We note that $\widehat{k}_i = H_2(\widehat{e}(\mathrm{PK}_g, \mathrm{sk}_i r_i r_g P_0)) = H_2(\widehat{e}(\mathrm{PK}_i, \mathrm{sk}_g r_g r_i P_0))$. Then, ID_g aggregates the signatures, masked bids, and message authentication codes to generate an aggregated signature σ, an aggregated masked bid B, and an aggregated message authentication code $\mathrm{MAC}(B)$. The aggregated signature is $\sigma = \sum_{1\le i\le n} \sigma_i$. The aggregated bid is $B = (B^{(1)}, B^{(2)}, \ldots, B^{(k)})$, where $B^{(x)} = \sum_{1\le i\le n}(B_{i,x} - H(x \parallel \widehat{k}_i))$ for $1 \le x \le k$. The aggregated message authentication code is $\mathrm{MAC}(B) = \prod_{1\le i\le n}\mathrm{MAC}(B_i)$. Additionally, the gateway ID_g randomly chooses $R \in \mathbb{Z}_q^*$ and calculates the final message authentication code $\mathrm{MAC}_f = (\mathrm{MAC}_1, \mathrm{MAC}_2)$, where $\mathrm{MAC}_1 = (B \parallel R) \oplus H_3(\mathrm{MAC}(B))$ and $\mathrm{MAC}_2 = U^{H(B)} V^{H(R)}$. MAC_f will be used by the utility company ID_u to ensure that the aggregated bid in each time slot stems from the intended power storage units and it has not been modified in transit. Note that during the verification process, ID_u does not need to access the individual bid and hence the power storage unit's privacy is preserved.

In the case of a multihop AMI network, the aggregation process of the signatures and masked bids are done by the SMs in a bottom-up way, as shown in Figure 3. Once a SM receives *Power_Res* packets from its downstream SMs, it first aggregates them with its own data and then sends the aggregated packet to its upstream SM. For example, as shown in Figure 3, SM_2 and SM_3 send their *Power_Res* packets to their upstream smart meter SM_4. After receiving packets from SM_2 and SM_3, SM_4 aggregates its signature to the received signatures of SM_2 and SM_3 to generate aggregated signature $\sigma_{2-4} = \sigma_2 + \sigma_3 + \sigma_4$. Then, SM_4 aggregates its masked bid to the received masked bids of SM_2 and SM_3 to generate aggregated masked bid $B_{2-4} = (B_{2-4,1}, B_{2-4,2}, \ldots, B_{2-4,k})$, where $B_{2-4,x} = B_{2,x} + B_{3,x} + B_{4,x}$ for $1 \le x \le k$. SM_4 also aggregates its message authentication code to the received message authentication codes of SM_2 and SM_3 to generate an aggregated message authentication code $\mathrm{MAC}(B_{2-4}) = \mathrm{MAC}(B_2) \cdot \mathrm{MAC}(B_3) \cdot \mathrm{MAC}(B_4)$. Similarly, SM_5 generates $\sigma_{1-5} = \sigma_1 + \sigma_{2-4} + \sigma_5$, $B_{1-5} = (B_{1-5,1}, B_{1-5,2}, \ldots, B_{1-5,k})$, where $B_{1-5,x} = B_{1,x} + B_{2-4,x} + B_{5,x}$ for $1 \le x \le k$, and $\mathrm{MAC}(B_{1-5}) = \mathrm{MAC}(B_1) \cdot \mathrm{MAC}(B_{2-4}) \cdot \mathrm{MAC}(B_5)$. SM_8 generates $\sigma_{6-8} = \sigma_6 + \sigma_7 + \sigma_8$, $B_{6-8} = (B_{6-8,1}, B_{6-8,2}, \ldots, B_{6-8,k})$, where $B_{6-8,x} = B_{6,x} + B_{7,x} + B_{8,x}$ for $1 \le x \le k$, and $\mathrm{MAC}(B_{6-8}) = \mathrm{MAC}(B_6) \cdot \mathrm{MAC}(B_7) \cdot \mathrm{MAC}(B_8)$. Upon receiving response packets from SM_5 and SM_8, the gateway ID_g computes $\widehat{k}_i = H_2(\widehat{e}(\mathrm{PK}_i, \mathrm{sk}_g r_g r_i P_0))$ for $1 \le i \le 8$, $\sigma = \sigma_{1-8} = \sigma_{1-5} + \sigma_{6-8}$, $B_{1-8} = (B_{1-8,1}, B_{1-8,2}, \ldots, B_{1-8,k})$, where $B_{1-8,x} = B_{1-5,x} + B_{6-8,x}$ for $1 \le x \le k$, $B = (B^{(1)}, B^{(2)}, \ldots, B^{(k)})$, where $B^{(x)} = B_{1-8,x} - \sum_{1\le i\le 8} H(x \parallel \widehat{k}_i)$ for $1 \le x \le k$, and $\mathrm{MAC}(B) = \mathrm{MAC}(B_{1-5}) \cdot \mathrm{MAC}(B_{6-8})$. Additionally, the gateway ID_g randomly chooses $R \in \mathbb{Z}_q^*$ and calculates the final message authentication code $\mathrm{MAC}_f = (\mathrm{MAC}_1, \mathrm{MAC}_2)$, where $\mathrm{MAC}_1 = (B \parallel R) \oplus H_3(\mathrm{MAC}(B))$ and $\mathrm{MAC}_2 = U^{H(B)} V^{H(R)}$.

In any cases, the gateway ID_g attaches $\{r_i P_0\}_{1\le i\le n}$ to the aggregated response packet, where n is the number of power storage units covered by ID_g. Finally, the aggregated response packet is sent to the utility company. Note that only the final message authentication code MAC_f is sent to the utility company by the gateway.

4.6. Privacy-Aware Aggregated Bid Reading. After receiving the power request response packet from the gateway ID_g, the utility company computes a secret key $k_i = H_2(\widehat{e}(\mathrm{PK}_i, \mathrm{sk}_u r_u r_i P_0))$ shared with the power storage unit ID_i for $1 \le i \le n$. We note that $k_i = H_2(\widehat{e}(\mathrm{PK}_i, \mathrm{sk}_u r_u r_i P_0)) = H_2(\widehat{e}(\mathrm{PK}_u, \mathrm{sk}_i r_i r_u P_0))$. For $1 \le x \le k$, the utility company computes $b^{(x)} = B^{(x)} - \sum_{1\le i\le n} H(x \parallel k_i) = \sum_{1\le i\le n} b_{i,x}$, which is the power amount the utility company can collect from the community of ID_g in the x-th time slot at price p_x. Then, the utility company ensures the authenticity and integrity of the recovered data by checking if $\widehat{e}(\sigma, P_0) = \prod_{1\le i\le n} \widehat{e}(H_1(H(k_i) \parallel \mathrm{ID}_g \parallel \mathrm{ID}_u \parallel r_i P_0 \parallel \mathrm{TS}), \mathrm{PK}_i)$. Finally, in order to ensure that the recovered aggregated bids stem from the intended power storage units and they have not been modified in transition, the utility company computes $B' \parallel R' = \mathrm{MAC}_1 \oplus H_3(Y^{\sum_{1\le x\le k} b^{(x)}})$ and checks whether $\mathrm{MAC}_2 = U^{H(B')} V^{H(R')}$.

5. Security and Privacy Analysis

In this section, we show EPPI can achieve the expected security and privacy goals.

5.1. Confidentiality. In the privacy-aware aggregated bid reading phase, for $1 \le x \le k$, the utility company computes $b^{(x)} = B^{(x)} - \sum_{1\le i\le n} H(x \parallel k_i) = \sum_{1\le i\le n} b_{i,x}$, which is

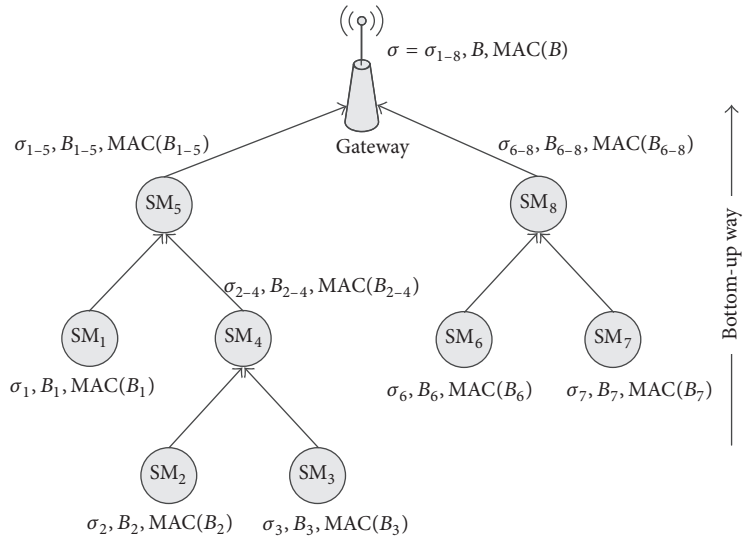

Figure 3: The aggregation way in multihop AMI networks.

the power amount the utility company can collect from the community of ID_g in the x-th time slot at price p_x. Then the utility company can know the total amount of power $\sum_{1\le x\le k} b^{(x)}$ injected from the community of ID_g. Obviously, the secret keys $\{k_i\}_{1\le i\le n}$ are necessary for the computation of the total amount of power. Therefore, adversaries cannot know the total amount of power. On the other hand, based on the discrete logarithm assumption, it is infeasible for attackers to compute $\sum_{1\le x\le k} b_{i,x}$ from $\mathrm{MAC}(B_i) = Y^{\sum_{1\le x\le k} b_{i,x}}$. Also, the gateway fails to recover $\sum_{1\le x\le k} b^{(x)}$ from $\mathrm{MAC}(B) = Y^{\sum_{1\le x\le k} b^{(x)}}$.

5.2. Privacy Protection. In the privacy-aware bid generation phase, the power storage unit ID_i computes its masked bid as $B_i = (B_{i,1}, B_{i,2}, \ldots, B_{i,k})$, where $B_{i,x} = b_{i,x} + H(x \parallel \widehat{k}_i) + H(x \parallel k_i)$ for $1 \le x \le k$. Because the secret keys $\widehat{k}_i$ and k_i are involved in the computation of B_i, any adversaries without knowing $\widehat{k}_i$ or k_i cannot know the original bid $b_{i,x}$ even if B_i is given. Although the utility company has the value k_i, it fails to recover $b_{i,x}$ in that $H(x \parallel \widehat{k}_i)$ cannot be removed from $B_{i,x}$. On the other hand, because the utility company only has the aggregated value $B^{(x)} = \sum_{1\le i\le n}(B_{i,x} - H(x \parallel \widehat{k}_i))$, it just gets the sum $\sum_{1\le i\le n} b_{i,x}$ by computing $b^{(x)} = B^{(x)} - \sum_{1\le i\le n} H(x \parallel k_i)$. In this case, the individual bid privacy is still preserved.

Furthermore, The use of one-time keys $\widehat{k}_i$ and k_i in hash-then-addition aggregation can boost the privacy protection because when the power storage units send the same bids in different cases, the masked bids are completely different and the attacker cannot distinguish the bids. In particular, the time slot parameter x is used in the generation of $B_{i,x}$, which makes it impossible for the attacker to calculate the difference between related bids.

5.3. Authentication and Integrity. The utility company ensures the authenticity and integrity of the recovered data by checking if $\widehat{e}(\sigma, P_0) = \prod_{1\le i\le n} \widehat{e}(H_1(H(k_i) \parallel \mathrm{ID}_g \parallel \mathrm{ID}_u \parallel r_i P_0 \parallel \mathrm{TS}), \mathrm{PK}_i)$. Any modification to a packet content, such as power price, will result in the failure of the signature verification. Signatures can also be used to resist impersonation attacks and external attacks such as denial of service by sending false packets. The attackers cannot impersonate the utility, gateway, or the power storage units because the generation of a valid signature needs a secret key. Based on the discrete logarithm assumption, it is infeasible to compute the secret key sk_i from the corresponding public key $\mathrm{PK}_i = \mathrm{sk}_i P_0$ and the signature $\sigma_i = \mathrm{sk}_i H_1(H(k_i) \parallel \mathrm{ID}_g \parallel \mathrm{ID}_u \parallel r_i P_0 \parallel \mathrm{TS})$. Besides, we developed a message authentication code based on signature techniques. The gateway ID_g randomly chooses $R \in \mathbb{Z}_q^*$ and calculates the final message authentication code $\mathrm{MAC}_f = (\mathrm{MAC}_1, \mathrm{MAC}_2)$, where $\mathrm{MAC}_1 = (B \parallel R) \oplus H_3(\mathrm{MAC}(B))$ and $\mathrm{MAC}_2 = U^{H(B)} V^{H(R)}$. MAC_f can be used by the utility company ID_u to ensure that the aggregated bid in each time slot stems from the intended power storage units and it has not been modified in transit.

5.4. Replay Attacks. In the proposed EPPI system, if attackers record valid packets and replay them in a different community or time slot, these replayed packets will be identified and dropped. For one thing, time stamps are used to protect against this replay attacks. For another, the verification of MAC_f fails if an attacker replays packets associated with old secret keys. In EPPI, we adopt a key management procedure to enable the utility company to share keys with power storage units. The attackers cannot calculate the keys because the secret number r_i is used, which is selected by each power storage unit. It is infeasible to retrieve r_i from $r_i P_0$. Particularly, even if the gateway and some power storage units collude, they cannot achieve the shared secret key between the utility company and a victim because the secret key computation is controlled jointly by the power storage unit and the utility company.

5.5. Man-in-the-Middle Attacks. In the proposed EPPI system, suppose an attacker resides between a power storage unit and the utility company. It tries to establish two secret keys to fool the power storage unit and the utility company to believe that they communicate directly, where one key is shared with the utility company and the other is shared with the power storage unit. The secret key agreement procedure is resilient to this attack because $r_i P_0$ and $r_u P_0$ are signed by the power storage unit and the utility company, respectively.

5.6. Session Key Freshness. It is a very desirable practice to periodically refresh the shared secret keys. In the proposed EPPI system, the secret key management procedure can achieve both forward and backward secrecy, where the attacker cannot derive the previously used session keys nor the future session keys even if the current key is exposed. This is because each time the utility company requests power injection, a new key is computed using one-time random numbers r_u and r_i. Therefore, if an attacker could get one key, this does not help him to know the old or new ones.

6. Performance Evaluation

In this section, we evaluate the performance of the proposed EPPI scheme in terms of the computation complexity and the communication overhead.

6.1. Computation Complexity. As for computation complexity, we will focus on measuring the time required for performing the cryptographic operations in EPPI. Denote the computational costs of a bilinear pairing operation, an exponentiation operation in $\mathbb{G}$, an exponentiation operation in $\mathbb{G}_T$, a multiplication operation in $\mathbb{G}$, a multiplication operation in $\mathbb{G}_T$, and an addition operation in $\mathbb{G}$ by C_p, C_e, C_{et}, C_m, C_{mt}, and C_a, respectively.

In the proposed EPPI scheme, in order to generate a power collection request $Power\_Req = \mathrm{ID}_u \parallel \mathrm{ID}_g \parallel \mathrm{Info}_p \parallel r_u P_0 \parallel \mathrm{TS} \parallel \sigma_u$, the utility company needs $2C_e$ computation cost. In the privacy-aware aggregated bid reading phase, the computation cost for the utility company is $(2n+1)C_p+(n+2)C_e+C_{et}+C_m$. In fact, the computation of the secret key $k_i = H_2(\widehat{e}(\mathrm{PK}_i, \mathrm{sk}_u r_u r_i P_0))$ shared with the power storage unit ID_i involves one C_p and one C_e. The authenticity and integrity of the recovered data based on $\widehat{e}(\sigma, P_0) = \prod_{1\le i\le n}\widehat{e}(H_1(H(k_i) \parallel \mathrm{ID}_g \parallel \mathrm{ID}_u \parallel r_i P_0 \parallel \mathrm{TS}), \mathrm{PK}_i)$ involves $(n+1)C_p$. To compute $B' \parallel R' = \mathrm{MAC}_1 \oplus H_3(Y^{\sum_{1\le x\le k} b^{(x)}})$, one C_{et} is needed. The verification based on $\mathrm{MAC}_2 = U^{H(B')}V^{H(R')}$ involves $2C_e$ and C_m. After receiving the packet *Power_Req*, the gateway verifies the signature by checking if $\widehat{e}(\sigma_u, P_0) = \widehat{e}(H_1(\mathrm{ID}_u \parallel \mathrm{ID}_g \parallel \mathrm{Info}_p \parallel r_u P_0 \parallel \mathrm{TS}), \mathrm{PK}_u)$ holds. Then it computes $r_g P_0$. The computation cost in this process is $2C_p+C_e$. In the privacy-aware bid aggregation phase, the computation cost for the gateway is $nC_p+(n+2)C_e+C_m+(n-1)C_{mt}+(n-1)C_a$. Specifically, the aggregated signature is $\sigma = \sum_{1\le i\le n}\sigma_i$ and it needs $(n-1)C_a$. The computation of the secret key $\widehat{k}_i = H_2(\widehat{e}(\mathrm{PK}_g, \mathrm{sk}_i r_i r_g P_0))$ involves one C_p and one C_e. The aggregated message authentication code is $\mathrm{MAC}(B) = \prod_{1\le i\le n}\mathrm{MAC}(B_i)$ and it needs $(n-1)C_{mt}$. The final message authentication code MAC_f needs $2C_e$ and C_m. In EPPI, the computation cost for each power storage units is $2C_p+4C_e+C_{et}$. We present the computation cost in Table 1, where UC, GW, and PSU represent the utility company, the gateway, and a power storage unit, respectively.

Table 1: Computation complexity of EPPI.

	Computation complexity
UC	$(2n+1)C_p + (n+4)C_e + C_{et} + C_m$
GW	$(n+2)C_p + (n+3)C_e + C_m + (n-1)C_{mt} + (n-1)C_a$
PSU	$2C_p + 4C_e + C_{et}$

Table 2: Communication overhead of EPPI.

	Communication overhead (bytes)
UC-to-GW	$0.5k + 89$
GW-to-PSU	$0.5k + 129$
PSU-to-GW	$20k + 129$
GW-to-UC	$40n + 40k + 109$

6.2. Communication Overhead. In the proposed EPPI system, the communications can be divided into four parts, that is, UC-to-GW communication, GW-to-PSU communication, PSU-to-GW communication, and GW-to-UC communication. We assign two bytes for each identity, four bits for each price p_i, five bytes for TS, 20 bytes for q, and 40 bytes for each group element in $\mathbb{G}$ and $\mathbb{G}_T$. We first consider the UC-to-GW communication, where the utility company generates a power collection request *Power_Req* and delivers the request to the gateway. The *Power_Req* packet is of the form $\mathrm{ID}_u \parallel \mathrm{ID}_g \parallel \mathrm{Info}_p \parallel r_u P_0 \parallel \mathrm{TS} \parallel \sigma_u$. Its size should be $k/2 + 89$ bytes if k time slots are adopted. In the GW-to-PSU communication, the *Power_Req* packet is of the form $\mathrm{ID}_g \parallel \mathrm{ID}_u \parallel \mathrm{Info}_p \parallel r_g P_0 \parallel r_u P_0 \parallel \mathrm{TS} \parallel \sigma_u$ and the size is $k/2 + 129$ bytes. In the PSU-to-GW communication, the power request response *Power_Res* packet is of the form $\mathrm{ID}_g \parallel \mathrm{ID}_u \parallel r_i P_0 \parallel \mathrm{TS} \parallel \sigma_i \parallel B_i \parallel \mathrm{MAC}(B_i)$ for the i-th power storage unit. The packet size should be $20k + 129$ bytes. It is noted that, instead of sending n signatures with a total of $56n$ bytes, the aggregated signature needs only 56 bytes for any number of storage units. In the GW-to-UC communication, the response message is of the form $\mathrm{ID}_u \parallel \mathrm{ID}_g \parallel \{r_i P_0\}_{1\le i\le n} \parallel \mathrm{TS} \parallel \sigma \parallel B \parallel \mathrm{MAC}_f$ and the size is $40n+40k+109$ bytes where n represents the number of power storage units. We present the communication cost in Table 2. As shown in Figures 4 and 5, we plot the communication overhead in terms of the time slot number k and the power storage unit number n.

In general, the proposed EPPI scheme is the first secure and privacy-aware power injection scheme and the above analysis indicates that EPPI is efficient in terms of computation and communication cost.

7. Conclusions

Aiming to tackle the security and privacy issues of power injection over AMI and 5G, we propose an efficient and privacy-aware power injection scheme based on 5G smart

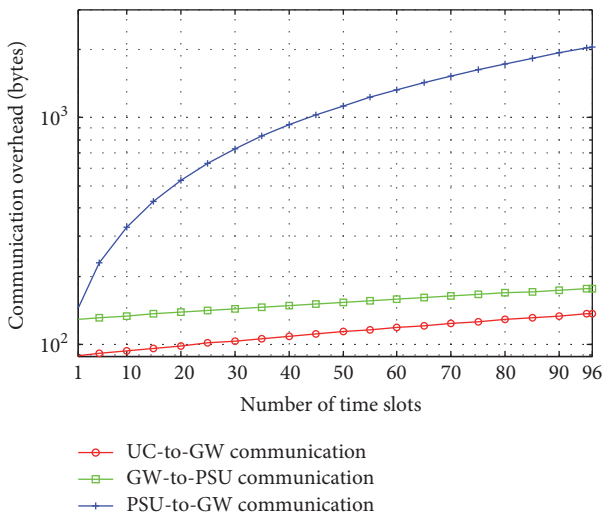

Figure 4: The UC-to-GW, GW-to-PSU, and PUS-to-GW communication overheads of EPPI.

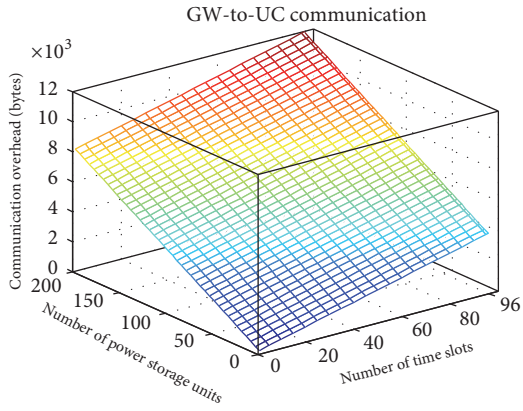

Figure 5: The GW-to-UC communication overhead of EPPI.

grid network slice. The proposed scheme allows the utility company to recover the total amount of collected power and resists any attacker to read individual power injection bid. Each power storage unit blinds its power injection bid, and all the bids will be aggregated by the local gateway based on a novel aggregation technique called *hash-then-addition*. In particular, the utility company can ensure the integrity and authenticity of the collected data. Extensive evaluations indicate that our scheme is secure and privacy-aware and it is efficient in terms of computation and communication cost.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work is supported by National Natural Science Foundation of China (nos. 61402366, 61472472, and 61272037), Natural Science Basic Research Plan in Shaanxi Province (nos. 2015JQ6236, 2016JM6033, and 2013JZ020), and Scientific Research Program Funded by Shaanxi Provincial Education Department (no. 15JK1686). Yinghui Zhang is supported by New Star Team of Xi'an University of Posts and Telecommunications.

References

[1] N. Alliance, "5 g white paper," White paper, Next Generation Mobile Networks, Frankfurt, Germany, 2015.

[2] G. Locke and P. D. Gallagher, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, National Institute of Standards and Technology, 2010.

[3] M. Peng, Y. Li, Z. Zhao, and C. Wang, "System architecture and key technologies for 5G heterogeneous cloud radio access networks," *IEEE Network*, vol. 29, no. 2, pp. 6–14, 2015.

[4] M. Peng, S. Yan, and H. V. Poor, "Ergodic capacity analysis of remote radio head associations in cloud radio access networks," *IEEE Wireless Communications Letters*, vol. 3, no. 4, pp. 365–368, 2014.

[5] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: opportunities and challenges," *Information Sciences*, vol. 305, pp. 357–383, 2015.

[6] J. Li, J. Li, X. Chen, C. Jia, and W. Lou, "Identity-based encryption with outsourced revocation in cloud computing," *IEEE Transactions on Computers*, vol. 64, no. 2, pp. 425–437, 2015.

[7] L. M. Kaufman, "Data security in the world of cloud computing," *IEEE Security and Privacy*, vol. 7, no. 4, pp. 61–64, 2009.

[8] Y. Zhang, X. Chen, J. Li, D. S. Wong, H. Li, and I. You, "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing," *Information Sciences*, vol. 379, pp. 42–61, 2017.

[9] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 2, pp. 340–352, 2016.

[10] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 9, pp. 2546–2559, 2016.

[11] J. Li, X. Chen, M. Li, P. P. Lee, and W. Lou, "Secure deduplication with efficient and reliable convergent key management," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 6, pp. 1615–1625, 2014.

[12] J. G. Andrews, S. Buzzi, W. Choi et al., "What will 5G be?" *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1065–1082, 2014.

[13] N. Nikaein, E. Schiller, R. Favraud et al., "Network store: exploring slicing in future 5G networks," in *Proceedings of the 10th International Workshop on Mobility in the Evolving Internet Architecture (MobiArch '15)*, pp. 8–13, Paris, France, September 2015.

[14] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient aggregation of encrypted data in wireless sensor networks," in *Proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems-Networking and Services (MobiQuitous '05)*, pp. 109–117, July 2005.

[15] D. Westhoff, J. Girao, and M. Acharya, "Concealed data aggregation for reverse multicast traffic in sensor networks: encryption, key distribution, and routing adaptation," *IEEE Transactions on Mobile Computing*, vol. 5, no. 10, pp. 1417–1431, 2006.

[16] X. Lin, R. Lu, and X. S. Shen, "MDPA: multidimensional privacy-preserving aggregation scheme for wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 10, no. 6, pp. 843–856, 2010.

[17] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: an efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621–1631, 2012.

[18] C. Wu, H. Mohsenian-Rad, and J. Huang, "Vehicle-to-aggregator interaction game," *IEEE Transactions on Smart Grid*, vol. 3, no. 1, pp. 434–442, 2012.

[19] L. Gan, U. Topcu, and S. H. Low, "Optimal decentralized protocol for electric vehicle charging," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 940–951, 2013.

[20] S. Tonyali, O. Cakmak, K. Akkaya, M. M. Mahmoud, and I. Guvenc, "Secure data obfuscation scheme to enable privacy-preserving state estimation in smart grid AMI networks," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 709–719, 2016.

[21] K. Rabieh, M. Mahmoud, K. Akkaya, and S. Tonyali, "Scalable certificate revocation schemes for smart grid AMI networks using bloom filters," *IEEE Transactions on Dependable and Secure Computing*, 2015.

[22] Y. H. Zhang, X. F. Chen, H. Li, and J. Cao, "Identity-based construction for secure and efficient handoff authentication schemes in wireless networks," *Security and Communication Networks*, vol. 5, no. 10, pp. 1121–1130, 2012.

[23] J. Cao, M. Ma, and H. Li, "A group-based authentication and key agreement for MTC in LTE networks," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM '12)*, pp. 1017–1022, Anaheim, Calif, USA, December 2012.

[24] M. M. E. A. Mahmoud and X. Shen, "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 10, pp. 1805–1818, 2012.

[25] Y. Zhang, X. Chen, J. Li, and H. Li, "Generic construction for secure and efficient handoff authentication schemes in EAP-based wireless networks," *Computer Networks*, vol. 75, pp. 192–211, 2014.

[26] H. Li, X. Lin, H. Yang, X. Liang, R. Lu, and X. Shen, "EPPDR: an efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 8, pp. 2053–2064, 2014.

[27] P. Guo, J. Wang, X. H. Geng, C. S. Kim, and J.-U. Kim, "A variable threshold-value authentication architecture for wireless mesh networks," *Journal of Internet Technology*, vol. 15, no. 6, pp. 929–935, 2014.

[28] M. Mahmoud, N. Saputro, P. Akula, and K. Akkaya, "Privacy-preserving power injection over a hybrid AMI/LTE smart grid network," *IEEE Internet of Things Journal*, 2016.

[29] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in cryptology—(EUROCRYPT '99)*, vol. 1592 of *Lecture Notes in Comput. Sci.*, pp. 223–238, Springer, Berlin, Germany, 1999.

[30] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology-CRYPTO 2001*, pp. 213–229, Springer, Berlin, Germany, 2001.

[31] W. Stallings, *Cryptography and Network Security: Principles and Practices*, Pearson Education, New Delhi, India, 2006.