11-2018

Privacy-preserving communication and power injection over vehicle networks and 5G smart grid slice

Yinghui ZHANG

Jin LI

Dong ZHENG

Ping LI

Yangguang TIAN
Singapore Management University, ygtian@smu.edu.sg

Privacy-preserving communication and power injection over vehicle networks and 5G smart grid slice

Yinghui Zhang[ab] Jin Li[c] Dong Zheng[ab] Ping Li[c] Yangguang Tian[d]

[a] National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, PR China
[b] Westone Cryptologic Research Center, Beijing 100070, PR China
[c] School of Computer Science, Guangzhou University, Guangzhou 510006, PR China
[d] School of Information Systems, Singapore Management University, Singapore 188065

Published in Journal of Network and Computer Applications, 15 November 2018, 122, Pages 50-60.
https://doi.org/10.1016/j.jnca.2018.07.017

Abstract

As an important combination of autonomous vehicle networks (AVNs) and smart grid, the vehicle-to-grid (V2G) network can facilitate the adoption of renewable resources. Based on V2G networks, parked electric vehicles (EVs) can charge during off-peak hours and inject excess power to the grid during peak hours for earnings. However, each EV's power injection bids in V2G are sensitive and vehicle-to-vehicle (V2V) communication may be eavesdropped, which has become an obstacle to the wide deployments of AVNs. Aiming to efficiently tackle these security and privacy issues in AVNs, we propose an efficient privacy-preserving communication and power injection (ePPCP) scheme without pairings, which is suitable for vehicle networks and 5G smart grid slice. In ePPCP, each EV calculates two secret keys shared respectively by the utility company and the gateway to blind power injection bids. A novel aggregation technique called hash-then-homomorphic is used to further aggregate the blinded bids of different time slots. Our security analysis indicates that individual bids are hidden and secure V2V communication is ensured. Furthermore, extensive performance comparisons show that ePPCP is efficient in terms of the computation cost and communication overhead.

Keywords

Vehicle networks, Smart grid, Power injection, Security privacy, Aggregation

1. Introduction

Recent developments in communication, control and information technologies have provided new chances to the Internet of Things (IoT), especially the vehicle network and smart grid. The urban vehicles are evolving from a collection of sensor platforms to an autonomous vehicle network (AVN) in which the human control is removed and autonomous vehicles could efficiently cooperate to optimize a well defined utility function. Smart grid is suggested to be a representative use case of the fifth generation of mobile technology (5G) in the Next Generation Mobile Network association's white paper (Alliance). 5G could be adaptively deployed to accommodate smart grid in a flexible and cost efficient manner. As an important combination of AVNs and smart grid, vehicle-to-grid (V2G) networks can facilitate the adoption of renewable sources like solar and wind (Kempton and Tomić, 2005). Based on V2G networks, parked electric vehicles (EVs) can store surplus power generated during off-peak hours and inject some power back to the grid during peak hours for benefits (Kempton and Tomić, 2005; Mahmoud et al., 2017; Zhang et al., 2017a). In addition, secure vehicle-to-vehicle (V2V) communication is indispensable for extensive deployments of AVNs.

Transactions are usually involved in power injection, and hence data security and user privacy are of significance. Security and privacy concerns have become main obstacles to the wide deployment of AVNs. During the communication process of power injection, each EV's individual power injection bids are sensitive which should be protected against various adversaries (Mahmoud et al., 2017; Zhang et al., 2017a). Although aggregation techniques have been used in existing schemes, the performance especially the computation and communication efficiency remains to be improved. For one thing, as power storage units, EVs usually don't aggregate power bids before sending them to the gateway. For another, expensive bilinear pairing operations are involved in computation. As far as the authors' knowledge, most existing power injection schemes either cannot protect users' privacy or suffer a bad efficiency.

1.1. Our contribution

In this paper, for the sake of security and privacy protection in power injection over vehicle networks, we enable secure communication, privacy-preserving power injection and efficient computation, simultaneously. The contributions of this paper can be summarized as follows.

- Firstly, we propose a system architecture of vehicle communication and power injection over vehicle networks and 5G smart gird slice. In addition, we present the adversary model and design goals in terms of security and efficiency. We propose an efficient privacy-preserving communication and power injection (ePPCP) scheme over vehicle networks and 5G smart grid slice. Both the computation cost and the communication overhead of ePPCP are very low due to the elimination of computationally expensive pairing operations and the adoption of data aggregation.
- Secondly, each EV calculates two secret keys shared respectively by the utility company and the gateway to blind power injection bids. A novel aggregation technique called *hash-then-homomorphic* is used to further aggregate the blinded bids of different time slots. Only the utility company can completely remove the blind factor to obtain the total amount of injected power at each time slot, and individual power bids are hidden to any adversaries.
- Finally, extensive security analysis and performance comparisons indicate that ePPCP is secure under the proposed adversary model and efficient in terms of computation and communication overheads.

1.2. Related work

Recently, a plenty of researches have been done to address security and privacy issues in V2V, V2G, smart grid, 5G, etc. Cost-effective storage units are very important for power grid especially the future 5G smart grid slice where large amount of renewable resources are expected to be adopted. A promising solution to this problem is EV-based AVNs, in which EVs can participate in the V2G network. To ensure adequate EVs can participate in the V2G network, well-designed incentive schemes are required (Yang et al., 2011; Wang et al., 2015). As for 5G solutions, the advanced cloud radio access network is a potential one (Peng et al., 2014). Nikaein et al. (2015) presented a slice-based 5G architecture which can efficiently manage network slices. Data aggregation is important to smart grid slice in terms of security and performance. Castelluccia et al. (2005) enabled efficient aggregation of encrypted data based on homomorphic encryption techniques, which can also be used to outsourced computation (Liu et al., 2016, 2018). Besides, homomorphic signature can be used to realize authentication in different network environment (Li et al., 2014a; Qun et al., 2018). In order to realize a multidimensional privacy-aware data aggregation in wireless sensor networks, Lin et al. (2010) integrated the super-increasing sequence and perturbation techniques into compressed data aggregation. Lu et al. (2012) proposed a data aggregation scheme under the public key infrastructure for better efficiency and high reliability. In addition, to improve the performance of power grid, coordinating power charging has been studied (Gan et al., 2013).

In V2G networks, the data of power consumption is closely related to users' activities and hence is sensitive. Tonyali et al. (2015) proposed a meter data obfuscation scheme to preserve consumer privacy from the utility company and any other eavesdropper. Furthermore, privacy-aware solutions with different security characteristics have been investigated for various network environment and applications including wireless authentication (Zhang et al., 2012; Liu et al., 2018; Han et al., 2012; Li et al., 2014b; Zhang et al., 2014), wireless relay security (Fan et al., 2016, 2017; Xie et al., 2018), smart vehicle and grid security (Mohit et al., 2017; Li et al., 2014c; Rahman et al., 2017), and wireless sensor network security (Zhang et al., 2018a; Bhuiyan et al., 2016, 2017). In order to improve efficiency in vehicle networks, cloud computing technologies are used to optimize resource allocation (Yu et al., 2018). In cloud computing, privacy protection should be considered because of the untrusted servers (Gao et al., 1109; Zhang et al., 2017b; Shen et al., 2018b; Yang et al., 2018a; Zhang et al., 2016). To protect the confidentiality of the outsourced data, the access control technology is also important to allow only the privileged users to access the outsourced data (Yang et al., 2018b; Cai et al., 2017; Wang et al., 2018). The attribute based encryption has been widely used to realize the access control because of its flexibility (Liang et al., 2014; Wang et al., 2017). Especially, blockchain technologies have been used to realize fair payment of outsourcing services in cloud computing (Zhang et al., 2018b, 2018c).

As the computation ability of mobile devices is limited, secure computation outsourcing has also been researched to outsource the computation overhead to cloud servers such as (Shen et al., 2018a; Li et al., 2014d). There are also many works which considered the data processing outsourcing to save the local computation, such as (Li et al., 2014e, 2018a; Chen et al., 2016; Xiang et al., 2016). Similar to the notion of outsourcing computation, offline computation (Li et al., 2018b) has been well studied, which allows the devices to perform the computation offline. However, these schemes are not focusing on the security and privacy issues of power injection. To fill this gap, Mahmoud et al. (2017) proposed a power injection scheme in smart grid. In (Mahmoud et al., 2017), a point addition aggregation and a homomorphic encryption aggregation are utilized to enable the local gateway to aggregate power storage units' bids. However, the scheme (Mahmoud et al., 2017) is found to be not privacy-aware and the aggregation method puts additional limitations on power bibs (Zhang et al., 2017a). In (Zhang et al., 2017a), an aggregation technique called hash-then-addition is proposed for power injection. Whereas, power storage units in this scheme don't aggregate power bids and hence the communication cost is high. In order to tackle this problem, Zhang et al. (2017c) proposed a privacy-aware data aggregation scheme with efficient communication suitable for power injection. Nevertheless, the above schemes involve many expensive bilinear pairing operations and the computation efficiency remains to be improved.

The remainder of this paper is organized as follows. Some preliminaries are reviewed in Section 2. Section 3 describes the system architecture and design goals of communication and power injection over AVNs and 5G smart grid slice. The proposed ePPCP scheme is presented in Section 4, followed by the security analysis in Section 5. Performance-related issues are discussed in Section 6. Finally, concluding remarks are given in Section 7.

2. Preliminaries

In this section, we briefly review some cryptographic background.

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 properties as below:*

1. *Bilinear: $\hat{e}(aP, bP) = \hat{e}(P, P)^{ab}$ for all $a, b \in \mathbb{Z}_q^*$.*
2. *Non-degenerate: There exists $P, Q \in \mathbb{G}$ such that $\hat{e}(P, Q) \neq 1$.*
3. *Computable: It is feasible to compute $\hat{e}(P, Q)$ for all $P, Q \in \mathbb{G}$.*

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

2.2. Discrete logarithm assumption

Definition 2. (Discrete Logarithm Problem). *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). *In group $\mathbb{G}$, it is computationally infeasible to determine x from P and $Q = xP$.*

2.3. Paillier cryptosystem

The Paillier Cryptosystem (Paillier, 1999) is used for aggregation and it consists of three algorithms: key generation, encryption and decryption.

- *KeyGen:* Given a security parameter κ, two large primes p_1, q_1 are chosen with $|p_1| = |q_1| = \kappa$. Then, compute the RSA modulus $N = p_1 q_1$ and $\lambda = \text{lcm}(p_1 - 1, q_1 - 1)$. Define a function $L(u) = \frac{u-1}{N}$ and compute $\mu = (L(g^\lambda \bmod N^2))^{-1} \bmod N$ where g is an element of order N in $\mathbb{Z}^*_{N^2}$. Finally, the public key is $pk = (N, g)$ and the corresponding private key is $sk = (\lambda, \mu)$.
- *Encryption:* Given a message $M \in \mathbb{Z}_N$, choose a random number $r \in \mathbb{Z}^*_N$ and the ciphertext can be calculated as $C = g^M r^N \bmod N^2$.
- *Decryption:* Given the ciphertext $C \in \mathbb{Z}^*_{N^2}$, the message is recovered as $M = L(C^{\lambda \bmod N^2}) \cdot \mu \bmod N$.

3. System architecture and design goals

3.1. System architecture

As shown in Fig. 1, the system architecture of communication and power injection over AVNs and 5G smart grid slice involves an administration center, a utility company, roadside units and different communities such as parking lots and residential districts. In a community covered by a gateway, a lot of power storage units, i.e., vehicles, communicate with the gateway. Each gateway connects the utility company through a smart grid 5G network slice. All the vehicles on the road, parking lots and residential districts and other units form an autonomous vehicle network. The details are given in the following.

- *Administration Center (AC)*: The administration center is responsible for the registration of other entities.
- *Power Storage Units*: Power storage units are vehicles at a parking lot or a residential district. They store power energy from the smart grid or other environment friendly energy sources. Each storage unit can buy power from the grid at a low-price period and inject excess power to the grid for earnings at a high-price period.
- *Gateway*: In the proposed system model, a gateway serves as an aggregator. As an interactive agent between power grid and vehicles, the gateway can directly collect power injection information, which is initially aggregated by corresponding smart meters. The gateway aggregates the data and sends the result to the utility company. Besides, a gateway is a roadside unit in AVNs and it can establish contracts with each vehicle owner and the grid operator (Han et al., 2010).
- *Smart Grid Slice in* 5G *Networks*: A 5G network slice consists of various 5G network functions and specific radio access technology settings that are combined together for particular use cases. For a 5G smart grid use case, security, privacy, reliability and latency are of paramount importance. In order to tailor the network functions to suit the smart gird slice, all the necessary functions are instantiated at the cloud edge node in 5G.
- *Utility Company*: During the peak hour of power consumption, if the energy supply falls short of the demand from communities, the utility company should contact electricity vendors to buy power or contact power storage units to collection power. Note that the utility company communicates with the power storage units via the AVN and 5G smart grid slice networks.

3.2. Adversary model and design goals

Assume that the administration center is trustworthy and other entities are "honest-but-curious". Each power storage unit is curious to know the other units' bids to judge whether it is more profitable to inject power currently. The attackers in the AVN are also interested in the other's private information, such as the amount and time of the power injection of each power storage unit. The utility company tries to obtain secret information of owners of the power storage units. We know that the utility company wants to collect power at a low price but the storage units want to increase revenues. Therefore, the utility company and the power storage units have conflicting interests and they will not collude with each other. The power storage units will inject the committed amount of power in bids because this is more profitable. In a secure power injection system, to prevent adversaries from learning power storage units' individual bid, the following security requirements

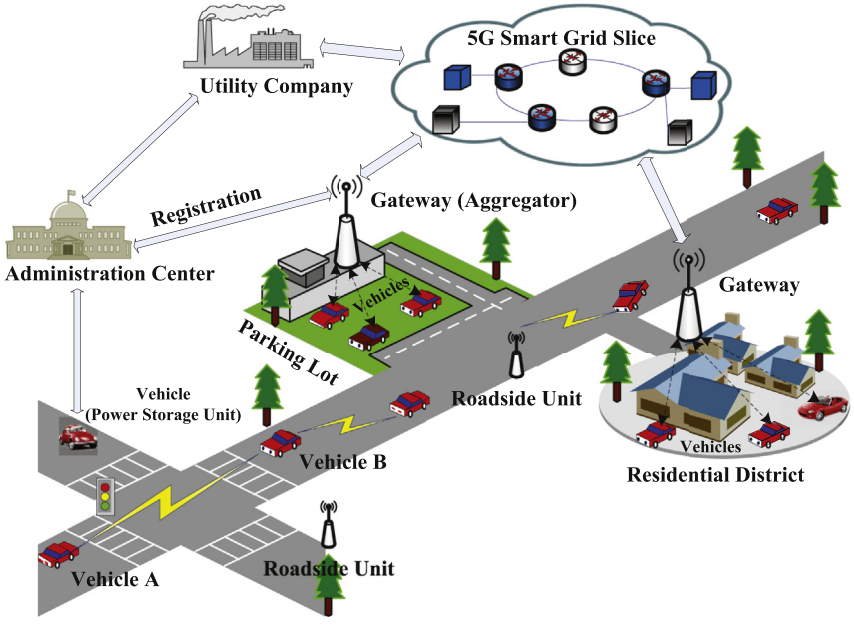


Fig. 1. System architecture of vehicle communication and power injection.

should be taken into account.

- *Privacy Protection*: Even if an adversary eavesdrops the communication on the AVN and 5G smart grid slice, it cannot achieve the total amount of power injected from the community. The utility fails to know the contents of individual power storage unit's bid. The aggregation at gateways is adopted to achieve these goals.
- *Authentication and Integrity*: The utility company can authenticate the received packets to ensure that the packets are really from particular power storage units and have not been modified during transmission. Besides, the adversary should not impersonate the utility company, the gateway or a storage unit. During communication, the vehicles can authenticate with each other.
- *Secure Communication*: Different vehicles can realize secure communication based on authenticated key agreement protocols. Other entities can also realize secure communication in the same way.

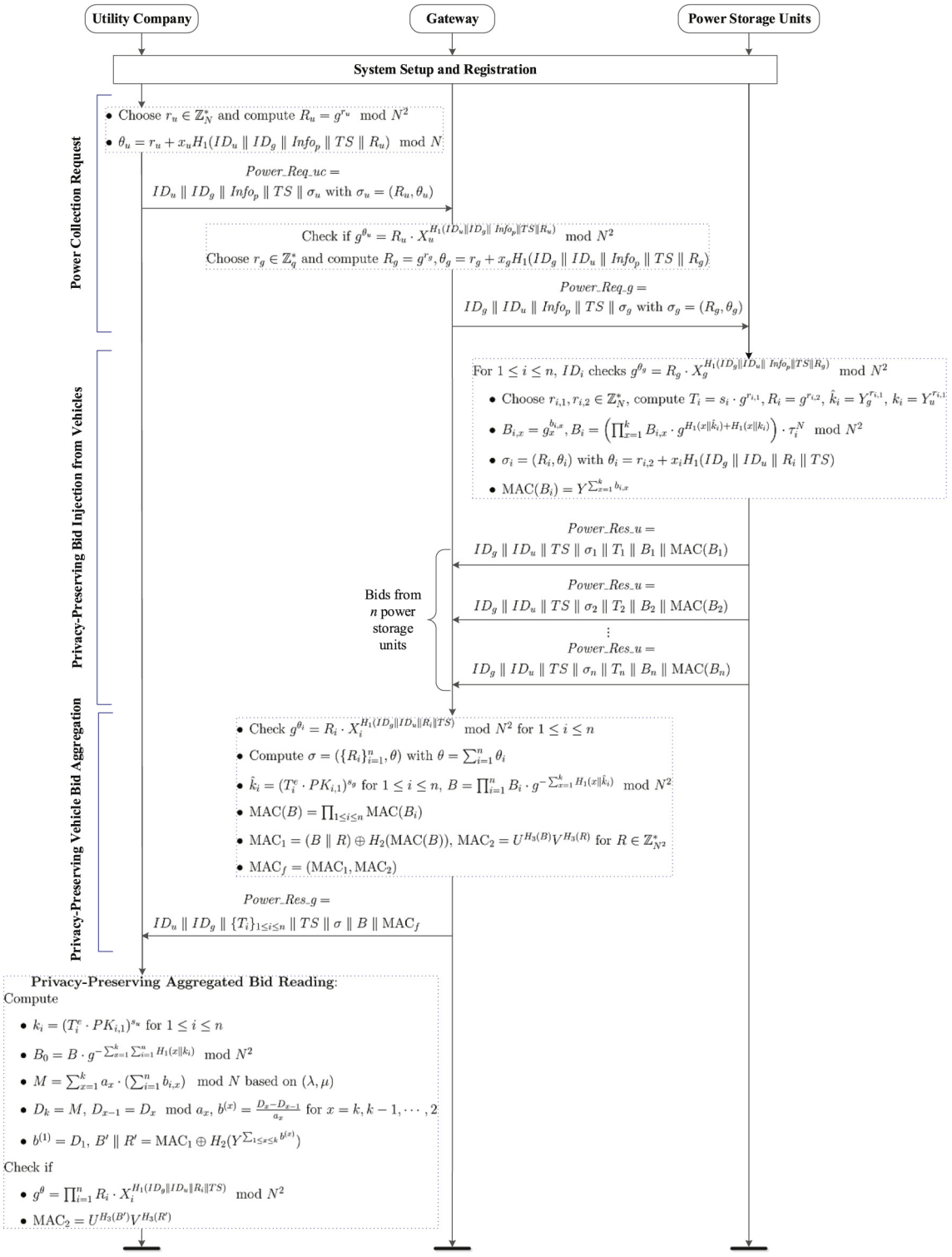


Fig. 2. Power injection of the proposed ePPCP system.

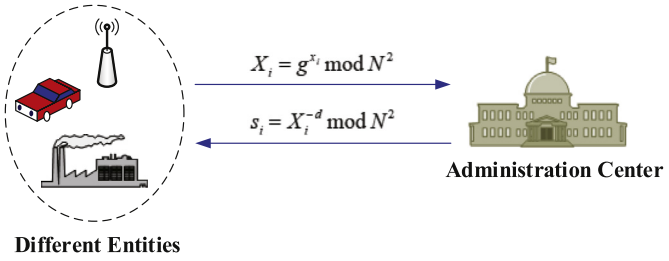


Fig. 3. The registration process.

In addition, the performance-related issue should be considered. In the proposed scheme, we achieve desirable communication performance by aggregating data before transmission. Particularly, in order to improve the computation efficiency, we eliminate the expensive pairing operations in each phase of communication and power injection.

4. ePPCP: efficient PPCP without pairing operations

In ePPCP, we simultaneously address security and efficiency issues which have not been successfully solved in previous work. The phases of power injection in ePPCP are shown in Fig. 2. More details are given as below.

4.1. System setup

Suppose the maximum number of power storage units covered by a gateway is n, and k time slots are used by the utility company during collecting power. Besides, assume that ω is an upper bound of each power bid injected by a power storage unit at a time slot. Then, given the security parameter κ, the utility company does the following:

1. The utility company calculates the Paillier Cryptosystem's public key (N, g) and the corresponding private key (λ, μ).
2. The administration center chooses a prime number e and an integer d satisfying $e \cdot d = 1 \bmod \varphi(N^2)$ where $\varphi(\cdot)$ means the Euler function.
3. For $1 \le x \le k$, the utility company computes $g_x = g^{a_x} \bmod N^2$ where $a_1 = 1$ and $a_2, \ldots, a_k$ are primes such that $(a_1, a_2, \ldots, a_k)$ is a superincreasing sequence satisfying $|a_x| \ge \kappa$, $\sum_{j=1}^{x-1} a_j n\omega < a_x$ for $2 \le x \le k$ and $\sum_{j=1}^{k} a_j n\omega < N$.
4. The utility company chooses two random elements $U, V \in \mathbb{Z}_{N^2}^*$ and three secure cryptographic hash functions H_1, H_2 and H_3, where $H_1 : \{0,1\}^* \to \mathbb{Z}_N^*$, $H_2 : \mathbb{Z}_{N^2}^* \to \{0,1\}^*$ and $H_3 : \mathbb{Z}_{N^2}^* \to \mathbb{Z}_N^*$.

Finally, the utility company keeps the master secret key $MSK = (\lambda, \mu, \{a_x\}_{1 \le x \le k})$ secretly and the administration center keeps d secret. The global public parameters are $GPK = (N, g, e, U, V, H_1, H_2, H_3, \{g_x\}_{1 \le x \le k})$.

4.2. Registration

The registration process is illustrated in Fig. 3, in which $X_i = X_u$ (resp. X_g) if the entity is the utility company (resp. the gateway). To be specific, in order to join the ePPCP system, the utility company with identification information ID_u chooses a random element $x_u \in \mathbb{Z}_N^*$, calculates $X_u = g^{x_u} \bmod N^2$ and gets $s_u = X_u^{-d} \bmod N^2$ from AC. Then the utility company computes $Y_u = g^{e \cdot s_u} \bmod N^2$ and sets $PK_u = (X_u, Y_u)$ as its public key and $sk_u = (x_u, s_u)$ as its secret key. Similarly, the gateway with identification information ID_g chooses a random element $x_g \in \mathbb{Z}_N^*$, calculates $X_g = g^{x_g} \bmod N^2$ and gets $s_g = X_g^{-d} \bmod N^2$ from AC. Then the gateway computes $Y_g = g^{e \cdot s_g} \bmod N^2$ and sets $PK_g = (X_g, Y_g)$ as its public key and $sk_g = (x_g, s_g)$ as its secret key. A power storage unit with identity ID_i chooses a random element $x_i \in \mathbb{Z}_N^*$, calculates $X_i = g^{x_i} \bmod N^2$ and gets $s_i = X_i^{-d} \bmod N^2$ from AC. Then the power storage unit computes $Y_i = g^{e \cdot s_i} \bmod N^2$ and sets $PK_i = (X_i, Y_i)$ as its public key and $sk_i = (x_i, s_i)$ as its secret key.

4.3. Power collection request

During peak hours of power consumption, the utility company sends power collection request (*Power_Req_uc*) packets to corresponding gateways for power collection. Suppose the utility company collects power in the community covered by the gateway ID_g. The packet $Power\_Req\_uc = ID_u \| ID_g \| Info_p \| TS \| \sigma_u$, where ID_u and ID_g are respectively the identities of the utility company and the gateway, and $Info_p = (p_1, p_2, \ldots, p_k)$ is the power collection price per unit at each time slot. Besides, TS is a timestamp and $\sigma_u = (R_u, \theta_u)$ is a signature, where $R_u = g^{r_u} \bmod N^2$, $\theta_u = r_u + x_u H_1(ID_u \| ID_g \| Info_p \| TS \| R_u) \bmod N$ with r_u randomly chosen from $\mathbb{Z}_N^*$. Both TS and σ_u will be used by the gateway in verification of the packet.

Upon receiving the packet *Power_Req_uc* from the utility company, the gateway ID_g first checks the freshness of *Power_Req_uc* based on the timestamp TS. Then, it checks if the following equation holds:

$$g^{\theta_u} = R_u \cdot X_u^{H_1(ID_u \| ID_g \| Info_p \| TS \| R_u)} \bmod N^2.$$

If and only if the equation holds, the gateway ID_g randomly chooses $r_g \in \mathbb{Z}_N^*$, computes $R_g = g^{r_g}$ and $\theta_g = r_g + x_g H_1(ID_g \| ID_u \| Info_p \| TS \| R_g)$. Then, the gateway broadcasts in its community the new packet $Power\_Req\_g = ID_g \| ID_u \| Info_p \| TS \| \sigma_g$, where $\sigma_g = (R_g, \theta_g)$. The power collection request is shown in Fig. 4.

4.4. Privacy-preserving bid injection from vehicles

Upon receiving a power collection request from the gateway ID_g, each power storage unit (i.e., a vehicle) first checks the freshness of *Power_Req_g* based on the timestamp TS. Then, it checks if the following equation holds:

$$g^{\theta_g} = R_g \cdot X_g^{H_1(ID_g \| ID_u \| Info_p \| TS \| R_g)} \bmod N^2.$$

If and only if the equation holds, each power storage unit prepares a bid as the power amount it can inject at each time slot. It sends a power request response *Power_Res_u* packet to ID_g.

In order to protect users' privacy and improve communication and computation efficiency, we adopt the *hash-then-homomorphic* aggregation method without needing pairing operations for each power storage unit to aggregate and protect his bids corresponding to time slots. 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 at the x-th time slot with price p_x for $1 \le x \le k$. To response a power collection request, the power storage unit ID_i does the following:

1. Randomly choose $r_{i,1}, r_{i,2} \in \mathbb{Z}_N^*$ and compute $T_i = s_i \cdot g^{r_{i,1}}, R_i = g^{r_{i,2}}$.

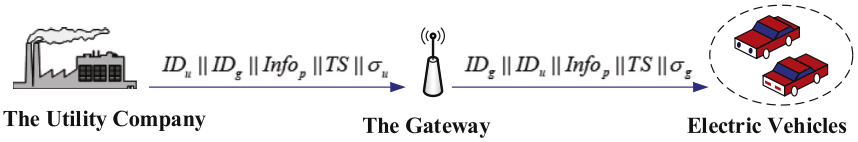


Fig. 4. The power collection request in ePPCP.

2. Compute two keys: $\widehat{k}_i = Y_g^{r_{i,1}}$, $k_i = Y_u^{r_{i,1}}$. which will be used to mask ID_i's bids.
3. *Hash-then-homomorphic*: randomly choose $\tau_i \in \mathbb{Z}_N^*$, aggregate and mask its injection bids corresponding to time slots as

$$B_i = \left(\prod_{x=1}^{k} B_{i,x} \cdot g^{H_1(x\|\widehat{k}_i)+H_1(x\|k_i)}\right) \cdot \tau_i^N \bmod N^2,$$

where $B_{i,x} = g_x^{b_{i,x}}$ for $1 \le x \le k$.

4. Calculate a signature $\sigma_i = (R_i, \theta_i)$ and a message authentication code $\mathrm{MAC}(B_i)$, where $\theta_i = r_{i,2} + x_i H_1(ID_g \| ID_u \| R_i \| TS)$, $\mathrm{MAC}(B_i) = Y^{\sum_{x=1}^{k} b_{i,x}}$.

Finally, the power storage unit ID_i sends $Power\_Res\_u = ID_g \| ID_u \| TS \| \sigma_i \| T_i \| B_i \| \mathrm{MAC}(B_i)$ to ID_g. The bid injection from vehicles is shown in Fig. 5.

4.5. Privacy-preserving vehicle bid aggregation

Upon receiving all the power request response packets from power storage units, the gateway ID_g first checks if the following equation holds:

$$g^{\theta_i} = R_i \cdot X_i^{H_1(ID_g\|ID_u\|R_i\|TS)} \bmod N^2.$$

If and only if the equation holds, the gateway ID_g further aggregates these packets in terms of storage units and sends an aggregated response packet to ID_u. In the following, the gateway ID_g aggregates the packets.

1. Aggregate the signatures to generate an aggregated signature $\sigma = (\{R_i\}_{i=1}^n, \theta)$, where $\theta = \sum_{i=1}^n \theta_i$.
2. For $1 \le i \le n$, compute $\widehat{k}_i = (T_i^e \cdot PK_{i,1})^{s_g}$ shared with the power storage unit ID_i. Note that $\widehat{k}_i = (T_i^e \cdot PK_{i,1})^{s_g} = (s_i^e \cdot g^{r_{i,1}e} \cdot PK_{i,1})^{s_g} = Y_g^{r_{i,1}}$, where $PK_{i,1} = X_i$.
3. Aggregate the masked bids to generate an aggregated masked bid

$$B = \prod_{i=1}^{n} B_i \cdot g^{-\sum_{x=1}^{k} H_1(x\|\widehat{k}_i)} \bmod N^2.$$

4. Aggregate the message authentication codes to generate an aggregated one $\mathrm{MAC}(B) = \prod_{i=1}^n \mathrm{MAC}(B_i)$.
5. Randomly choose $R \in \mathbb{Z}_{N^2}^*$, compute $\mathrm{MAC}_1 = (B \| R) \oplus H_2(\mathrm{MAC}(B))$ and $\mathrm{MAC}_2 = U^{H_3(B)} V^{H_3(R)}$. Then the final message authentication code is $\mathrm{MAC}_f = (\mathrm{MAC}_1, \mathrm{MAC}_2)$.

Finally, the aggregated response packet $Power\_Res\_g = ID_u \| ID_g \| \{T_i\}_{1\le i\le n} \| TS \| \sigma \| B \| \mathrm{MAC}_f$ is sent to the utility company ID_u. The vehicle bid aggregation process is shown in Fig. 6.

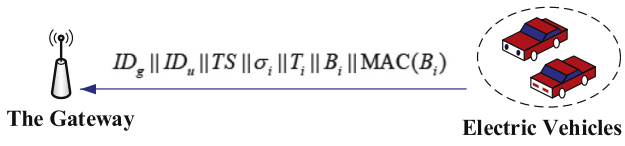


Fig. 5. The bid injection from vehicles.

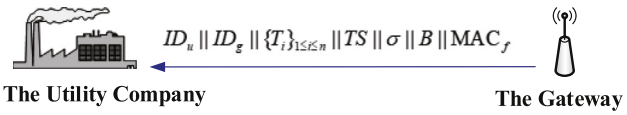


Fig. 6. The vehicle bid aggregation in ePPCP.

4.6. Privacy-preserving aggregated bid reading

After receiving the packet $Power\_Res\_g$ from the gateway ID_g, the utility company does the following to recover the bids of all power storage units at each time slot.

1. For $1 \le i \le n$, compute $k_i = (T_i^e \cdot PK_{i,1})^{s_u}$ shared with the power storage unit ID_i. Note that $k_i = (T_i^e \cdot PK_{i,1})^{s_u} = (s_i^e \cdot g^{r_{i,1}e} \cdot PK_{i,1})^{s_u} = Y_u^{r_{i,1}}$, where $PK_{i,1} = X_i$.
2. Compute $B_0 = B \cdot g^{-\sum_{x=1}^{k} \sum_{i=1}^{n} H_1(x\|k_i)} \bmod N^2$. It easily follows that

$$B_0 = \prod_{i=1}^{n}\left(\prod_{x=1}^{k} B_{i,x}\right) \cdot \tau_i^N = \left(\prod_{i=1}^{n}\prod_{x=1}^{k} g_x^{b_{i,x}}\right) \cdot \left(\prod_{i=1}^{n} \tau_i^N\right)$$
$$= g^{\prod_{x=1}^{k} a_x \cdot (\prod_{i=1}^{n} b_{i,x})} \cdot r^N \bmod N^2,$$

where $r = \prod_{i=1}^n \tau_i$.

3. Obviously, B_0 is a ciphertext of Paillier Cryptosystem and the utility company can use the master secret key (λ, μ) to recover

$$M = \sum_{x=1}^{k} a_x \cdot \left(\sum_{i=1}^{n} b_{i,x}\right) \bmod N.$$

Then, according to Algorithm 1, the utility company sets $D_k = M$, and for $x = k, k-1, \ldots, 2$, it sets $D_{x-1} = D_x \bmod a_x$. Based on the property of the superincreasing sequence, we have

$$b^{(x)} = \frac{D_x - D_{x-1}}{a_x} = \sum_{i=1}^{n} b_{i,x}, \tag{1}$$

where $b^{(x)}$ represents the amount of power collected at the x-th time slot from the community covered by ID_g. It's noted that $b^{(1)} = D_1 = \sum_{i=1}^n b_{i,1}$.

Finally, in order to ensure that the recovered aggregated bids stem from the particular community and they have not been modified in transition, the utility company computes $B' \| R' = \mathrm{MAC}_1 \oplus H_2(Y^{\sum_{x=1}^{k} b^{(x)}})$ and checks if

$$g^{\theta} = \prod_{i=1}^{n} R_i \cdot X_i^{H_1(ID_g\|ID_u\|R_i\|TS)} \bmod N^2,$$

$$\mathrm{MAC}_2 = U^{H_3(B')} V^{H_3(R')}.$$

Only if the equations hold, the recovered bids are valid.

4.7. Secure communication between vehicles

As we know, the urban vehicles are evolving from a collection of sensor platforms to AVN, in which the human control is removed and autonomous vehicles could efficiently cooperate to optimize a well defined utility function. Obviously, secure communication between vehicles is a basic requirement for the practical deployment of AVNs, which can ensure the vehicle safety and users' privacy. In the following, we use a key distribution scheme (Okamoto and Tanaka, 1989) to achieve this goal, in which no expensive bilinear pairing operations are involved and vehicles need not to apply for new secret keys from the administration center.

Suppose vehicle A and vehicle B on the road aim to communicate with each other. As shown in Fig. 7, vehicle A randomly chooses $r_a \in \mathbb{Z}_N^*$, computes $U_a = g^{e \cdot r_a}$, $h_a = H_1(U_a \| ID_a)$, $V_a = s_a \cdot g^{h_a \cdot r_a}$ and sends (U_a, V_a, ID_a) to vehicle B. Similarly, vehicle B randomly chooses $r_b \in \mathbb{Z}_N^*$, computes $U_b = g^{e \cdot r_b}$, $h_b = H_1(U_b \| ID_b)$, $V_b = s_b \cdot g^{h_b \cdot r_b}$ and sends (U_b, V_b, ID_b) to vehicle A. Vehicle B can authenticate A by checking if $PK_{a,1} \cdot V_a^e = U_a^{h'_a}$ holds, where $PK_{a,1} = g^{x_a}$ and $h'_a = H_1(U_a \| ID_a)$. The

Algorithm 1 Aggregated Bid Recovery.

Input: A superincreasing sequence $(a_1, a_2, \ldots, a_k)$ with $a_1 = 1$ and the plaintext M of the Paillier Cryptosystem ciphertext B_0.

Output: The amount of power collected at different time slots: $(b^{(1)}, b^{(2)}, \cdots, b^{(k)})$.

$D_k = M$;
for $x = k, k-1, \cdots, 2$ **do**
  $D_{x-1} = D_x \mod a_x$, $b^{(x)} = \frac{D_x - D_{x-1}}{a_x}$;
$b^{(1)} = D_1$;
final;
return $(b^{(1)}, b^{(2)}, \cdots, b^{(k)})$.

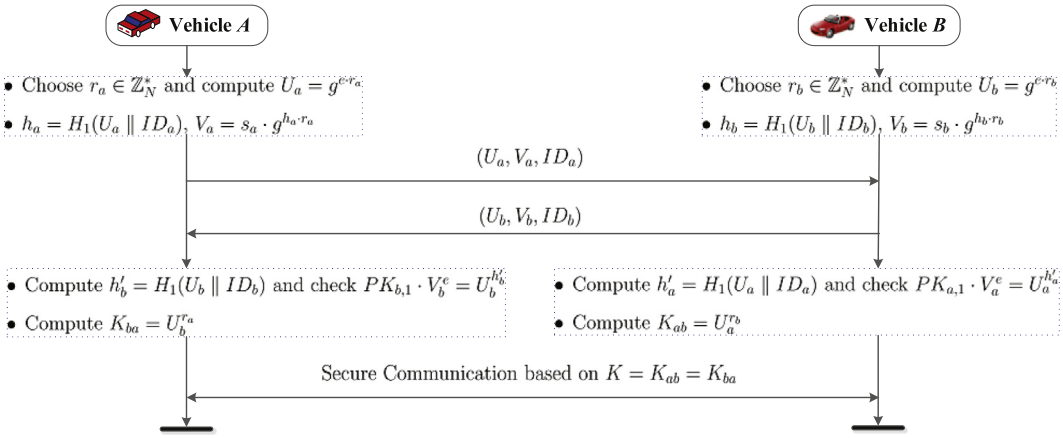


Fig. 7. Secure communication between vehicles in ePPCP.

correctness is shown as follows.

$PK_{a,1} \cdot V_a^e = X_a \cdot (s_a g^{h_a r_a})^e = g^{e h_a r_a} = U_a^{h'_a}$.

Then, vehicle B obtains a session key $K_{ab} = U_a^{r_b}$. Vehicle A can authenticate B and get a session key $K_{ba} = U_b^{r_a}$ in the same way. Note that $K_{ab} = K_{ba} = g^{e \cdot r_a \cdot r_b}$, which will be used to realize secure communication between vehicles A and B on the road.

5. Security analysis of ePPCP

In this section, we show ePPCP can achieve the expected security and privacy goals under the proposed adversary model.

5.1. Confidentiality

In the privacy-preserving aggregated bid reading phase, based on B_0 and M, the utility company computes $b^{(x)} = \prod_{i=1}^{n} b_{i,x}$ for $1 \leq x \leq k$, which is the power amount the utility company can collect from the community of ID_g at the x-th time slot with price p_x. Then the utility company gets the total amount of power $\sum_{x=1}^{k} b^{(x)}$ injected from the community covered by ID_g. Note that the secret keys $\{k_i = (T_i^e \cdot PK_{i,1})^{s_u}\}_{1 \leq i \leq n}$ are necessary for the computation of B_0 and s_u is private. Therefore, any adversary fails to know the total amount of power. In addition, based on the discrete logarithm assumption, it is infeasible for attackers to calculate $\sum_{x=1}^{k} b_{i,x}$ from $\mathrm{MAC}(B_i) = Y^{\sum_{x=1}^{k} b_{i,x}}$. In the secure communication between vehicles, $K_{ab} = K_{ba} = g^{e r_a r_b}$ is the final session key and it will be used to realize confidentiality.

5.2. Privacy protection

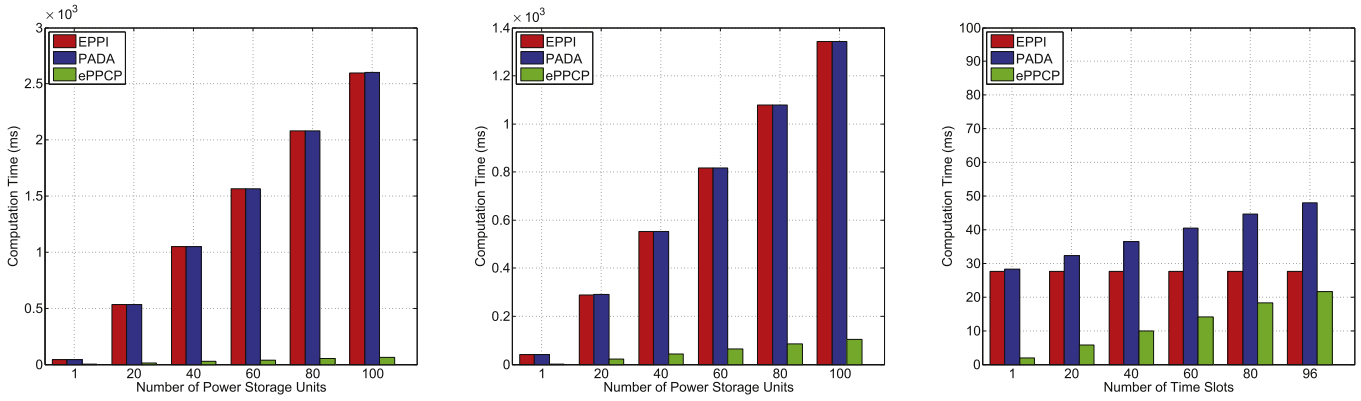
In this section, we first show that ePPCP enables privacy protection. To reflect the advantage of ePPCP over a previous scheme called EPPI (Zhang et al., 2017a), possible privacy issues are further analyzed and the performance issue is discussed. In ePPCP, we show that any adversaries including the utility company and the gateway cannot know the individual power bid at each time slot. In the privacy-preserving bid injection from vehicles phase, the power storage unit ID_i computes its own masked bid as $B_i = \left(\prod_{x=1}^{k} B_{i,x} \cdot g^{H_1(x \| \hat{k}_i) + H_1(x \| k_i)}\right) \cdot \tau_i^N \bmod N^2$, where $B_{i,x} = g_x^{b_{i,x}}$ for $1 \leq x \leq k$. In the privacy-preserving vehicle bid aggregation phase, the gateway further aggregates the masked bids as $B = \prod_{i=1}^{n} B_i \cdot g^{-\sum_{x=1}^{k} H_1(x \| \hat{k}_i)} \bmod N^2$. Obviously, it is impossible for the gateway to recover original power bids because $k_i = (T_i^e \cdot PK_{i,1})^{s_u}$ and the Paillier Cryptosystem's private key cannot be obtained by the gateway. Even if the utility company has the Paillier Cryptosystem's private key (λ, μ), it does not know $\hat{k}_i = (T_i^e \cdot PK_{i,1})^{s_g}$ and can only calculate $\sum_{i=1}^{n} \sum_{x=1}^{k} a_x b_{i,x}$ based on $k_i = (T_i^e \cdot PK_{i,1})^{s_u}$. Then, it further recovers $b^{(x)} = \sum_{i=1}^{n} b_{i,x}$. Therefore, the individual bid privacy of the power storage unit is preserved.

In EPPI, the power storage unit ID_i computes its masked bid as $B_i = (B_{i,1}, B_{i,2}, \ldots, B_{i,k})$, where $B_{i,x}$ is obtained by blinding $b_{i,x}$ based on two shared secret keys. Although the utility company has one of the shared secret keys, it fails to recover $b_{i,x}$ from $B_{i,x}$ in that the secret key shared by the power storage unit and the gateway cannot be removed from $B_{i,x}$. As a result, the utility company can only get the aggregated value $B^{(x)} = \sum_{1 \leq i \leq n} (B_{i,x} - H(x \| \hat{k}_i))$ from the gateway, where H is a hash function. Finally, it obtains the sum $\sum_{1 \leq i \leq n} b_{i,x}$ by removing $\sum_{1 \leq i \leq n} H(x \| k_i)$ from $B^{(x)}$. In this case, the individual bid privacy is still preserved.

Based on the above analysis, we know that ePPCP is different from EPPI in that all the k power bids of a power storage unit are blinded and encrypted based on the Paillier Cryptosystem. In particular, the k blinded bids are locally aggregated by the power storage unit along with the encryption process. Based on this observation, we show that ePPCP has advantages over EPPI in the following. On one hand, if the same shared key is reused in the blinding process, the attacker can calculate the difference between the bids at the same time slot. Thus, in EPPI, if one bid is exposed, all the bids that use the same shared key at the same time slot can also be exposed as well. In ePPCP, this possible

Table 1
Computation complexity.

	EPPI (Zhang et al., 2017a)	PADA (Zhang et al., 2017c)	Our ePPCP
UC	$(2n + 1)C_p + (n + 4)C_e + C_{et}$	$(2n + 1)C_p + (n + 4)C_e + C_{et} + 2C_{ez}$	$(3n + 7)C_{ez}$
GW	$(n + 2)C_p + (n + 3)C_e$	$(n + 2)C_p + (n + 3)C_e + C_{ez}$	$(5n + 5)C_{ez}$
PSU	$2C_p + 4C_e + C_{et}$	$2C_p + 4C_e + C_{et} + (k + 2)C_{ez}$	$(k + 8)C_{ez}$



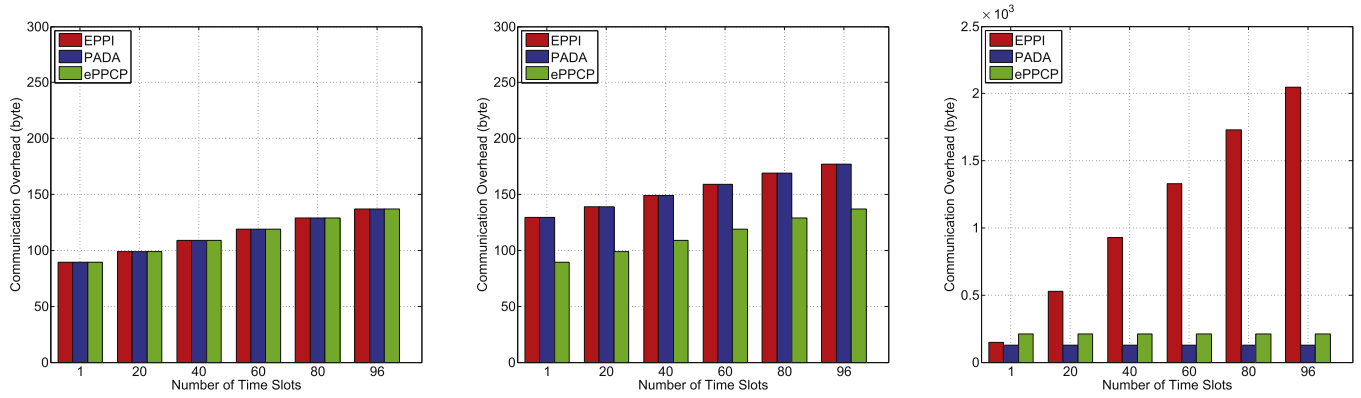
(a) Computation cost of UC. (b) Computation cost of GW. (c) Computation cost of PSU.

Fig. 8. Computation cost comparison.

privacy violation is resisted by the encryption process based on the Paillier Cryptosystem. On the other hand, in ePPCP, the blinded power bids are used as an exponent to perform an exponentiation operation and are further encrypted based on the Paillier Cryptosystem. Therefore, even if the secret key or the shared keys of a power storage unit are leaked to an adversary, the adversary cannot recover the original power bids due to the lack of the decryption secret key. Obviously, this robustness of privacy protection cannot be achieved in EPPI. Last but not least, compared with EPPI, besides the satisfactory privacy protection mentioned above, the aggregation of power bids based on time slots in ePPCP improves the communication efficiency and the elimination of bilinear pairing operations reduces the computation cost.

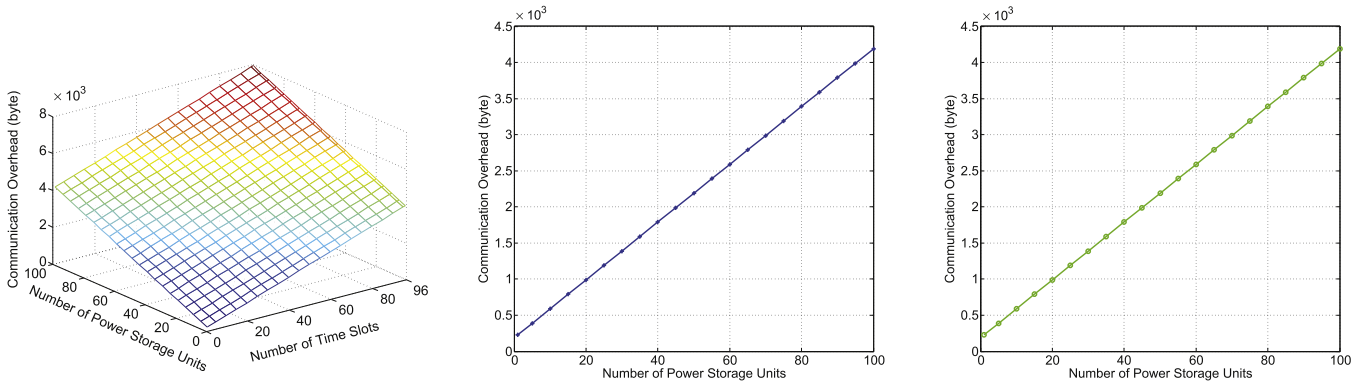
5.3. Authentication and integrity

In the privacy-preserving aggregated bid reading phase of the ePPCP system, the utility company ensures the authenticity and integrity of the recovered data by checking if $g^{\theta} = \prod_{i=1}^{n} R_i \cdot X_i^{H_1(ID_g \| ID_u \| R_i \| TS)} \bmod N^2$ and $\text{MAC}_2 = U^{H_3(B')} V^{H_3(R')}$ hold simultaneously. Any modification to packet contents will be found during the signature verification. Because a valid signature is generated based on a secret key, the attackers cannot impersonate the utility, the gateway or a power storage unit. Based on the discrete logarithm assumption, it is infeasible to get the secret key (x_i, s_i) from the corresponding public key $(X_i = g^{x_i} \bmod N^2, Y_i = g^{e \cdot s_i} \bmod N^2)$. In addition, it cannot get x_i from the signature $\theta_i = r_{i,2} + x_i H_1(ID_g \| ID_u \| R_i \| TS)$ because $r_{i,2}$ is a random value. The final message authentication code MAC_f is used by the utility company to ensure that the aggregated bid at each time slot has not been modified in transmission and it is collected from the intended power storage units. In the secure communication between vehicles on the road, $K_{ab} = K_{ba} = g^{er_a r_b}$ is the final session key. If U_a is changed to another value by unauthorized users, h'_a is not equal to h_a and hence $PK_{a,1} \cdot V_a^e = U_a^{h'_a}$ does not hold. In the same way, both vehicles can authenticate each other.



(a) UC-to-GW communication. (b) GW-to-PSU communication. (c) PSU-to-GW communication.

Fig. 9. Communication cost comparison.



(a) EPPI. (b) PADA. (c) ePPCP.

Fig. 10. GW-to-UC communication overhead comparison.

5.4. Man-in-the-middle attacks

In the proposed ePPCP system, suppose an attacker resides between the utility company ID_u and a power storage unit ID_i. It tries to establish two secret keys to fool ID_u and ID_i to believe that they communicate directly, where one key is shared with ID_u and the other is shared with ID_i. The secret key agreement mechanism is resilient to this attack because $\theta_u = r_u + x_u H_1(ID_u \parallel ID_g \parallel Info_p \parallel TS \parallel R_u)$ and $\theta_i = r_{i,2} + x_i H_1(ID_g \parallel ID_u \parallel R_i \parallel TS)$. That is, R_u and R_i are signed by the utility company and the power storage unit, respectively. In the secure communication between vehicles on the road, the session key agreement is resilient to this attack because $V_a = s_a \cdot g^{H_1(U_a \| ID_a) \cdot r_a}$ and $V_b = s_b \cdot g^{H_1(U_b \| ID_b) \cdot r_b}$. That is, U_a and U_b are signed by vehicle A and vehicle B, respectively.

5.5. Replay attacks

In the proposed ePPCP system, if adversaries record valid packets and replay them in a different time slot, these replayed packets will be found and dropped. Firstly, time stamps are adopted to resist replay attacks. Upon receiving the packets, the utility company or the storage unit first check the freshness of the packets based on the timestamps. Secondly, if an attacker replays packets associated with old secret keys, MAC_f cannot pass the verification. Finally, even if the gateway and some power storage units collude, they cannot achieve the shared secret key between a victim and the utility company in that the secret key computation is controlled jointly by the power storage unit and the utility company.

6. Performance comparisons

In this section, we compare the performance of the proposed scheme with previous power injection schemes based on the computation cost and the communication overhead. We denote the computation cost of a bilinear pairing operation, an exponentiation operation in $\mathbb{G}$, an exponentiation operation in $\mathbb{G}_T$ and an exponentiation operation in $\mathbb{Z}^*_{N^2}$ by C_p, C_e, C_{et} and C_{ez}, respectively. In the PADA scheme (Zhang et al., 2017c), in order to generate a power collection request *Power_Req_uc*, the utility company needs $2C_e$ computation cost. In ePPCP, it needs C_{ez} computation cost. In the privacy-preserving aggregated bid reading phase, the computation cost for the utility company is $(2n + 1)C_p + (n + 2)C_e + C_{et} + 2C_{ez}$, where n is the maximum number of power storage units covered by a gateway. In ePPCP, the computation cost is $(3n + 6)C_{ez}$. After receiving the packet *Power_Req_uc*, the gateway verifies the signature and computes $r_g P_0$, which needs $2C_p + C_e$ in PADA. The computation cost in ePPCP is $3C_{ez}$. In the privacy-preserving vehicle bid aggregation phase, the computation cost for the gateway is $nC_p + (n + 2)C_e + C_{ez}$ in PADA and $(5n + 2)C_{ez}$ in ePPCP. The computation cost for each power storage units is $2C_p + 4C_e + C_{et} + (k + 2)C_{ez}$ in PADA and $(k + 8)C_{ez}$ in ePPCP, where k is the number of time slots used by the utility company during collecting power. In EPPI (Zhang et al., 2017a), the computation cost for the utility company, the gateway and a power storage unit is $(2n + 1)C_p + (n + 4)C_e + C_{et}$, $(n + 2)C_p + (n + 3)C_e$ and $2C_p + 4C_e + C_{et}$, respectively. The computation complexity is presented in Table 1. In Fig. 8, the computation comparison is made. The time cost of primitive cryptography operations is evaluated on a PC with Intel IV 3 GHz processor based on the MIRACL library (Choi and Jung, 2010). The computation comparisons of UC (utility company), GW (gateway) and PSU (power storage unit) are shown in Fig. 8(a), (b) and (c), respectively. Note that, n usually has a large value in AVNs, and the maximum value of k is 96 if the time interval of power injection is 15 min. It easily follows from Fig. 8 that the proposed scheme ePPCP is most efficient because it does not need pairing operations.

The communication is divided into four phases: UC-to-GW, GW-to-PSU, PSU-to-GW and GW-to-UC. We assign two bytes for each identity, four bits for each price p_i, five bytes for TS, 20 bytes for q, 40 bytes for each group element in $\mathbb{G}$, $\mathbb{G}_T$ and $\mathbb{Z}^*_{N^2}$. In the UC-to-GW communication, the utility company generates a power collection request *Power_Req_uc* and delivers it to the gateway. In the GW-to-PSU communication, the *Power_Req_g* packet is sent. In the PSU-to-GW communication, the power request response *Power_Res_u* packet is sent. In this phase, the communication cost in PADA (Zhang et al., 2017c) and our ePPCP is smaller than the one in EPPI (Zhang et al., 2017a) because B_i is aggregated. In the GW-to-UC communication, the response message *Power_Res_g* is sent. In this phase, the response message size of PADA and ePPCP is smaller than that in EPPI based on B and MAC_f. The communication cost comparison is presented in Figs. 9 and 10. The communication overhead comparisons of UC-to-GW, GW-to-PSU and PSU-to-GW are given in Fig. 9(a), (b) and (c), respectively. Here, the communication overhead is related to the number of time slots. The GW-to-UC communication cost comparison is shown in Fig. 10, where the computation cost of EPPI is affected by the number of power storage units and time slots. In general, it easily follows that the proposed scheme is efficient in terms of communication cost.

7. Conclusions and future work

In this paper, in order to solve the security and privacy issues in AVNs and smart grid, we introduce ePPCP, an efficient privacy-preserving communication and power injection scheme without pairings. In ePPCP, the utility company can only recover the total amount of power injected by power storage units and individual power bids

are hidden. As a power storage unit, each electric vehicle blinds and aggregates its power injection bids associated with time slots based on a novel hash-then-homomorphic technique and the Paillier Cryptosystem. An extensive analysis indicates that the proposed scheme is secure under the proposed adversary model and efficient in terms of the computation and communication cost.

It would be interesting to design secure communication and power injection schemes without introducing trusted third parties in the future research.

Acknowledgment

We are grateful to the anonymous referees for their invaluable suggestions. This work is supported by National Key R&D Program of China (No. 2017YFB0802000), Natural Science Foundation of Guangdong Province for Distinguished Young Scholars (2014A030306020), National Natural Science Foundation of China (No. 61772418, 61472091, 61702126, 61402366), National Natural Science Foundation for Outstanding Youth Foundation (No. 61722203), Science and Technology Planning Project of Guangdong Province, China (2015B010129015), and Natural Science Basic Research Plan in Shaanxi Province of China (2018JZ6001, 2015JQ6236). Yinghui Zhang is supported by New Star Team of Xi'an University of Posts and Telecommunications (No. 2016-02).

References

N. Alliance, 5g White Paper, Next Generation Mobile Networks, White paper.

Bhuiyan, M.Z.A., Wu, J., Wang, G., Cao, J., 2016. Sensing and decision making in cyber-physical systems: the case of structural event monitoring. IEEE Trans. Ind. Inform. 12 (6), 2103–2114.

Bhuiyan, M.Z.A., Wu, J., Wang, G., Chen, Z., Chen, J., Wang, T., 2017. Quality-guaranteed event-sensitive data collection and monitoring in vibration sensor networks. IEEE Trans. Ind. Inform. 13 (2), 572–583.

Cai, Z., Yan, H., Li, P., Huang, Z.-a., Gao, C., 2017. Towards secure and flexible ehr sharing in mobile health cloud under static assumptions. Cluster Comput. 20 (3), 2415–2422.

Castelluccia, C., Mykletun, E., Tsudik, G., 2005. Efficient aggregation of encrypted data in wireless sensor networks. In: The Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services. IEEE, pp. 109–117.

Chen, X., Li, J., Weng, J., Ma, J., Lou, W., 2016. Verifiable computation over large database with incremental updates. IEEE Trans. Comput. 65 (10), 3184–3195.

Choi, J., Jung, S., 2010. A handover authentication using credentials based on chameleon hashing. IEEE Commun. Lett. 14 (1), 54–56.

Fan, L., Lei, X., Yang, N., Duong, T.Q., Karagiannidis, G.K., 2016. Secure multiple amplify-and-forward relaying with cochannel interference. IEEE J. Select. Top. Sig. Process. 10 (8), 1494–1505.

Fan, L., Lei, X., Yang, N., Duong, T.Q., Karagiannidis, G.K., 2017. Secrecy cooperative networks with outdated relay selection over correlated fading channels. IEEE Trans. Veh. Technol. 66 (8), 7599–7603.

Gan, L., Topcu, U., Low, S.H., 2013. Optimal decentralized protocol for electric vehicle charging. IEEE Trans. Power Syst. 28 (2), 940–951.

C. Gao, S. Lv, Y. Wei, Z. Wang, Z. Liu, X. Cheng, M-sse: An effective searchable symmetric encryption with enhanced security for mobile devices, IEEE Access https://doi.org/10.1109/ACCESS.2018.2852329.

Han, S., Han, S., Sezaki, K., 2010. Development of an optimal vehicle-to-grid aggregator for frequency regulation. IEEE Trans. Smart Grid 1 (1), 65–72.

Han, Q., Zhang, Y., Chen, X., Li, H., Quan, J., 2012. Efficient and robust identity-based handoff authentication in wireless networks. In: International Conference on Network and System Security. Springer, pp. 180–191.

Kempton, W., Tomić, J., 2005. Vehicle-to-grid power implementation: from stabilizing the grid to supporting large-scale renewable energy. J. Power Sources 144 (1), 280–294.

Li, J., Chen, X., Li, M., Li, J., Lee, P.P., Lou, W., 2014. Secure deduplication with efficient and reliable convergent key management. IEEE Trans. Parallel Distr. Syst. 25 (6), 1615–1625.

Li, H., Lin, X., Yang, H., Liang, X., Lu, R., Shen, X., 2014. Eppdr: an efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid. IEEE Trans. Parallel Distr. Syst. 25 (8), 2053–2064.

Li, H., Lin, X., Yang, H., Liang, X., Lu, R., Shen, X., 2014. Eppdr: an efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid. IEEE Trans. Parallel Distr. Syst. 25 (8), 2053–2064.

Li, H., Lu, R., Zhou, L., Yang, B., Shen, X., 2014. An efficient merkle-tree-based authentication scheme for smart grid. IEEE Syst. J. 8 (2), 655–663.

Li, J., Huang, X., Li, J., Chen, X., Xiang, Y., 2014. Securely outsourcing attribute-based encryption with checkability. IEEE Trans. Parallel Distr. Syst. 25 (8), 2201–2210, https://doi.org/10.1109/TPDS.2013.271.

Li, T., Li, J., Liu, Z., Li, P., Jia, C., 2018. Differentially private naive bayes learning over multiple data sources. Inf. Sci. 444, 89–104.

Li, T., Chen, W., Tang, Y., Yan, H., 2018. A Homomorphic Network Coding Signature Scheme for Multiple Sources and its Application in Iot, Security and Communication Networks 2018, pp. 1–6, https://doi.org/10.1155/2018/9641273.

Liang, K., Chu, C.-K., Tan, X., Wong, D.S., Tang, C., Zhou, J., 2014. Chosen-ciphertext secure multi-hop identity-based conditional proxy re-encryption with constant-size ciphertexts. Theor. Comput. Sci. 539, 87–105.

Lin, X., Lu, R., Shen, X.S., 2010. Mdpa: multidimensional privacy-preserving aggregation scheme for wireless sensor networks. Wireless Commun. Mobile Comput. 10 (6), 843–856.

Liu, Z., Wu, Z., Li, T., Li, J., Shen, C., 2018. Gmm and cnn hybrid method for short utterance speaker recognition. IEEE Trans. Ind. Inform. 14 (7), https://doi.org/10.1109/TII.2018.2799928.

Liu, X., Deng, R.H., Choo, K.-K.R., Weng, J., 2016. An efficient privacy-preserving outsourced calculation toolkit with multiple keys. IEEE Trans. Inf. Forensics Secur. 11 (11), 2401–2414.

Liu, X., Choo, R., Deng, R., Lu, R., Weng, J., 2018. Efficient and privacy-preserving outsourced calculation of rational numbers. IEEE Trans. Dependable Secure Comput. 15 (1), 27–39.

Lu, R., Liang, X., Li, X., Lin, X., Shen, X., 2012. Eppa: an efficient and privacy-preserving aggregation scheme for secure smart grid communications. IEEE Trans. Parallel Distr. Syst. 23 (9), 1621–1631.

Mahmoud, M.M., Saputro, N., Akula, P.K., Akkaya, K., 2017. Privacy-preserving power injection over a hybrid ami/lte smart grid network. IEEE Internet Things J. 4 (4), 870–880.

Mohit, P., Amin, R., Biswas, G., 2017. Design of authentication protocol for wireless sensor network-based smart vehicular system. Veh. Commun. 9, 64–71.

Nikaein, N., Schiller, E., Favraud, R., Katsalis, K., Stavropoulos, D., Alyafawi, I., Zhao, Z., Braun, T., Korakis, T., 2015. Network store: exploring slicing in future 5g networks. In: Proceedings of the 10th International Workshop on Mobility in the Evolving Internet Architecture. ACM, pp. 8–13.

Okamoto, E., Tanaka, K., 1989. Key distribution system based on identification information. IEEE J. Sel. Area. Commun. 7 (4), 481–485.

Paillier, P., 1999. Public-key cryptosystems based on composite degree residuosity classes. In: International Conference on the Theory and Applications of Cryptographic Techniques. Springer, pp. 223–238.

Peng, M., Yan, S., Poor, H.V., 2014. Ergodic capacity analysis of remote radio head associations in cloud radio access networks. IEEE Wirel. Commun. Lett. 3 (4), 365–368.

Qun, L., Hongyang, Y., Zhengan, H., Wenbin, C., Jian, S., Yi, T., 2018. An id-based linearly homomorphic signature scheme and its application in blockchain. IEEE Access, https://doi.org/10.1109/ACCESS.2018.2809426.

Rahman, M.S., Basu, A., Kiyomoto, S., Bhuiyan, M.A., 2017. Privacy-friendly secure bidding for smart grid demand-response. Inf. Sci. 379, 229–240.

Shen, J., Wang, C., Li, T., Chen, X., Huang, X., Zhan, Z.-H., 2018a. Secure data uploading scheme for a smart home system. Inf. Sci. 453, 186–197, https://doi.org/10.1016/j.ins.2018.04.048.

Shen, J., Gui, Z., Ji, S., Shen, J., Tan, H., Tang, Y., 2018b. Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. J. Netw. Comput. Appl.

Tonyali, S., Cakmak, O., akkaya, K., Mahmoud, M., Guvenc, I., 2015. Secure data obfuscation scheme to enable privacy-preserving state estimation in smart grid ami networks. IEEE Internet Things J. PP 99, https://doi.org/10.1109/JIOT.2015.2510504 1–1.

Wang, H., Qin, B., Wu, Q., Xu, L., Domingo-Ferrer, J., 2015. Tpp: traceable privacy-preserving communication and precise reward for vehicle-to-grid networks in smart grids. IEEE Trans. Inf. Forensics Secur. 10 (11), 2340–2351.

Wang, H., Zheng, Z., Wu, L., Li, P., 2017. New directly revocable attribute-based encryption scheme and its application in cloud storage environment. Cluster Comput. 20 (3), 2385–2392.

Wang, X., Zhang, Y., Zhu, H., Jiang, L., 2018. An identity-based signcryption on lattice without trapdoor. J. Univers. Comput. Sci.

Xiang, C., Tang, C., Cai, Y., Xu, Q., 2016. Privacy-preserving face recognition with outsourced computation. Soft Comput. 20 (9), 3735–3744.

Xie, D., Lai, X., Lei, X., Fan, L., 2018. Cognitive multiuser energy harvesting decode-and-forward relaying system with direct links. IEEE Access 6, 5596–5606.

Yang, Y., Liu, R., Chen, Y., Li, T., Tang, Y., 2018a. Normal cloud model-based algorithm for multi-attribute trusted cloud service selection. IEEE Access, https://doi.org/10.1109/ACCESS.2018.2850050.

Yang, Z., Yu, S., Lou, W., Liu, C., 2011. Privacy-preserving communication and precise reward architecture for v2g networks in smart grid. IEEE Trans. Smart Grid 2 (4), 697–706.

Yang, L., Han, Z., Huang, Z., Ma, J., 2018b. A remotely keyed file encryption scheme under mobile cloud computing. J. Netw. Comput. Appl. 106, 90–99.

Yu, Z., Gao, C.-z., Jing, Z., Gupta, B.B., Cai, Q., 2018. A practical public key encryption scheme based on learning parity with noise. IEEE Access 6, 31918–31923, https://doi.org/10.1109/ACCESS.2018.2840119.

Zhang, Y., Chen, X., Li, H., Cao, J., 2012. Identity-based construction for secure and efficient handoff authentication schemes in wireless networks. Secur. Commun. Network. 5 (10), 1121–1130.

Zhang, Y., Chen, X., Li, J., Li, H., 2014. Generic construction for secure and efficient handoff authentication schemes in eap-based wireless networks. Comput. Network. 75, 192–211.

Zhang, Y., Li, J., Chen, X., Li, H., 2016. Anonymous attribute-based proxy re-encryption for access control in cloud computing. Secur. Commun. Network. 9 (14), 2397–2411, https://doi.org/10.1002/sec.1509.
Zhang, Y., Zhao, J., Zheng, D., 2017. Efficient and privacy-aware power injection over ami and smart grid slice in future 5g networks. Mobile Inf. Syst. 2017, 1–12, https://doi.org/10.1155/2017/3680671.
Zhang, Y., Chen, X., Li, J., Wong, D.S., Li, H., You, I., 2017. Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. Inf. Sci. 379, 42–61, https://doi.org/10.1016/j.ins.2016.04.015.
Zhang, Y., Zheng, D., Zhao, Q., Lai, C., Ren, F., 2017. Pada: privacy-aware data aggregation with efficient communication for power injection in 5g smart grid slice. In: 2017 International Conference on Networking and Network Applications (NaNA). IEEE, pp. 11–16.
Zhang, Y., Zheng, D., Deng, R.H., 2018. Security and privacy in smart health: efficient policy-hiding attribute-based access control. IEEE Internet Things J. 5 (3), 2130–2145.
Zhang, Y., Deng, R.H., Liu, X., Zheng, D., 2018. Blockchain based efficient and robust fair payment for outsourcing services in cloud computing. Inf. Sci. 462, 262–277.
Zhang, Y., Deng, R.H., Shu, J., Yang, K., Zheng, D., 2018. Tkse: trustworthy keyword search over encrypted data with two-side verifiability via blockchain. IEEE Access 6, 31077–31087.

Yinghui Zhang received his Ph.D degree in Cryptography from Xidian University, China, in 2013. He is an associate professor at National Engineering Laboratory for Wireless Security (NELWS), Xi'an University of Posts & Telecommunications. Currently, he is also a research fellow at Singapore Management University. He has published over 50 research articles including ASIACCS, ACISP, Computer Networks, IEEE Internet of Things Journal, Computers & Security. His research interests include cloud security and wireless network security.

Jin Li received the BS degree in mathematics from Southwest University, Chongqing, China, in 2002. He recieved the PhD degree in information security from Sun Yat-sen University, Guangdong, China, in 2007. Currently, he works at Guangzhou University, China. His research interests include applied cryptography and security in cloud computing.

Dong Zheng received his Ph.D. degree in communication engineering from Xidian University, China, in 1999. He was a Professor at the School of Information Security Engineering, Shanghai Jiao Tong University. He is currently a Professor at National Engineering Laboratory for Wireless Security (NELWS), Xi'an University of Posts & Telecommunications. He has published over 100 research articles including CTRSA, IEEE Transactions on Industrial Electronics, Information Sciences. His research interests include cloud computing security, public key cryptography, and wireless network security.

Ping Li received the M.S. and Ph.D. degree in mathematics from Sun Yat-sen University in 2010 and 2016, respectively. Currently, she works at Guangzhou University as a postdoctor. And her main research interests include cryptography, privacy-preserving and cloud computing.

Yangguang Tian received his Ph.D degree in Cryptography from University of Wollongong, Australia, in 2017. He is a research fellow at Singapore Management University. His research interests include Applied Cryptography, Network Security, Privacy Enhancing Technologies.