Telecommun Syst (2017) 66:671–688
DOI 10.1007/s11235-017-0315-2

EPEC: an efficient privacy-preserving energy consumption scheme for smart grid communications

Mohamed Amine Ferrag[1]

Published online: 21 April 2017

Abstract In this paper, we propose an efficient privacy-preserving energy consumption scheme with updating certificates, called EPEC, for secure smart grid communications. Specifically, the proposed EPEC scheme consists of four phases: gateways initialization, party registration, privacy-preserving energy consumption, and updating certificates. Based on the bilinear pairing, the identity-based encryption, and the strategy of updating certificates, EPEC can achieve data privacy, gateway privacy, and is robust to data replay attack, availability attack, modification attack, man-in-the-middle attack, and Sybil attack. Through extensive performance evaluations, we demonstrate the effectiveness of EPEC in terms of transmission delay performance at the HAN gateway and average delivery ratio, by implementing three types of curves including, the Barreto–Naehrig curve with modulus 256 bits, the Kachisa–Schaefer–Scott curve with modulus 512 bits, and the Barreto–Lynn–Scott curve with modulus 640 bits.

Keywords Smart grid · Data privacy · Privacy-preserving · Energy consumption · Updating certificates

1 Introduction

The International Energy Agency (IEA) estimated in 2014 that the share of global final consumption of electricity energy is 22.3% [1]. This consumption is increasing every year by 3% (due, on the one hand to the increase in population and also by the development of different electronic technologies in the world, i.e., 5G, Cloud Computing, Vehicle Electric, Internet of Things, Smart Device…etc.). With this increase in consumption, how can we manage electricity without loss or damage? How do we improve the environmental protection? How can we make life easier for people by giving the opportunity to control its intelligent devices that consume a lot of electrical energy? The idea of placing a new generation of intelligent networks to control electrical power has recently come as an answer to these questions. This type of network is called the "Smart Grid". Today, the smart grid is among the objects of technological innovation in the topic of research "Energy and Networks" [2]. Since 2008, the developed countries that consume a lot of electrical energy have already invested billions of dollars in research on smart grids, like the United States, Canada, China, UK, Germany, Australia, and others. In the United States, cities that adopt smart grid technology already exist; namely Austin in Texas, Boulder and Fort Collins in Colorado, Sacramento and San Diego in California, and other cities in progress [3].

The smart grid is defined by the Department of Energy of the United States as a smart digital technology that allows two-way communication between the utility and its customers, the detection of long transmission and distribution lines. Traditionally, the smart grid consists of a set of computers, controllers, automation, and new communication technologies such as 4G. These components work together permanently, connected on the Internet, in order to digitally meet our rapid consumption of electricity demand within the smart grid [4]. Through the adaptation of a smart grid in a city, it is desirable not only to improve the security and transmission of electricity but also to increase the integration of renewable energy systems to large scales such as solar panels and windmills [5]. Moreover, some research projects have recently initiated for the adoption of a smart grid for large countries, i.e., in Europe with the project named "European

✉ Mohamed Amine Ferrag
mohamed.amine.ferrag@gmail.com

[1] Department of Computer Science, Guelma University, BP 401, 24000 Guelma, Algeria

Technology Platform (ETP) for the Electricity Networks of the Future", and in the United States with the project named "Unified National Smart Grid" [6].

With the innovation of electric vehicles, a vehicular ad hoc network (VANET) [7] can be integrated and controlled by the smart grid [8]. Recently, smart grids interconnection with VANETs has attracted much attention of researchers and engineers in both field's of energy and communication [9,10]. In [11], Cheng et al. proposed a method for transmitting data through the vanet in order to unload the cellular network that can stifle the cellular network. However, the method ignores some modern features of a smart grid such as advanced control of electricity transmission and distribution. Minimizing energy losses and improving voltage profile are studied in [12] by the collaboration of multiple plug-in electric vehicles (PEVs) in a smart grid system. The optimization of power distribution via V2G systems based on stochastic inventory theory is studied in [13]. In [14], Wang et al. proposed a coordinated strategy by loading the mobility of electric vehicles to improve the energy overall use while avoiding electrical system overload. Le et al. [15] proposed a scheme called DCD, which is based on enabling the integration of renewable energy sources (RESs) for reducing its characteristics negative impact. Zhang et al. [16] interested in controlling the local energy in a wireless mesh network powered by green energy through the formalization of the energy-trading problem as a Stackelberg game [17], in order to find the optimal trading price and the amount of the green power purchase. Security over cognitive radio sensor networks in smart grid is always desired and is discussed in [18].

With the development of a smart grid, the control center can ensure the proper management of electrical energy. The main problem in the development of a smart grid is not located at the physical support but mainly in reassuring both reliability and security [19]. With the adoption of smart grids, an adversary may find more ways to penetrate into the system, rising new security issues and asking for more secure communications in both systems [20]. In [21], Li et al. presented four basic attacks in smart grid communication, namely, equipment attack, data attack, privacy attack, and availability attack. Therefore, security requirements, including, anonymization [22], authentication [23], accountability [24], integrity [25], non-repudiation [26], access control [27], traceability [28], and confidentiality [29] should be paid more attention in the smart grid.

In this paper, in order to achieve privacy-preserving energy consumption inside a smart grid, we propose an efficient privacy-preserving energy consumption scheme with updating certificates. The main contributions of this work are summarized as follows:

- Firstly, we propose the EPEC scheme that employs the identity-based encryption to achieve privacy-preserving energy consumption. Then, we propose two types of updates of certificates, namely, one for the HAN network and another for the vehicle-to-grid network.
- Secondly, we conduct an extensive security analysis and prove that EPEC can achieve data privacy, gateway privacy, and can resist to five attacks, namely, data replay attack, availability attack, modification attack, man-in-the-middle attack, and Sybil attack.
- Finally, based on the M/D/1 queue, we demonstrate via simulation the effectiveness of the EPEC scheme with three performance metrics, namely, transmission delay, delivery ratio, and waiting time.

The remainder of this paper is organized as follows. We review related works in Sect. 2. Section 3 introduces the system model, the threat model, and identifies the design goals. In Sect. 4, we review the bilinear pairing, the identity-based encryption, and complexity assumptions. Our proposed EPEC scheme is presented in Sect. 5, followed by security analysis and performance evaluation in Sects. 6 and 7, respectively. Finally, we draw our conclusions in Sect. 8.

2 Related work

Recently, many research on security and privacy-preserving in smart grids have been appeared in literature [30–44]. Based on the classification of privacy preserving schemes for smart grid communications in our recent survey [45], these schemes can be classified according to several criteria, namely, networks models, countermeasures, and privacy models.

Balli et al. [46] proposed a novel system to provide a distributed, privacy-guaranteeing bidding protocol, which is secure against honest but curious adversaries. The most important feature of this protocol is that it does not rely on any kind of trusted third party. However, Zhang et al. [47] proposed a privacy-aware power injection scheme, called EPPI, for AMI and 5G smart grid network slice. EPPI scheme is based on a novel data aggregation technique, which 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.

Wen et al. [30] proposed the SESA scheme for auction in smart grids. Based on the public key encryption with keyword search, SESA scheme can achieve data privacy, bid integrity, keyword privacy, and trapdoor unforgeability. However, the availability, which is critical in smart electrical systems, is not supported in SESA. EPPDR scheme in [31] also does not support availability. Jiang et al. [32] proposed the LiSH+ scheme, which is an improvement of the LiSH scheme in [33]. The Lish+ scheme uses a polynomial with two variables in order to achieve the availability in SCADA communications, and

minimizes the cost of calculation, memory, communication, and energy, but the remote terminals ceases to operate during the key change phase. Choi et al. [34] proposed an architecture based on the hybrid key management in order to achieve the availability, but can be less effective during the process of communication between SCADA systems against internal attacks such as the ASKMA scheme in [35] and the scheme ASKMA+ in [48]. Another similar work to [34] is presented by Tsai and Lo [36], which secure anonymous key distribution.

Chen et al. [37] proposed the PDAFT scheme to prevent a strong opponent threatening user privacy while supporting tolerance in the smart grids. Based on the privacy report aggregation phase and the treatment phase of fault tolerance, PDAFT can protect the consumption privacy of electricity users against eavesdropping, and also can preserve user privacy without compromise, but the cost of communication increases from the first aggregation to N aggregations. Similar to the PDAFT scheme, Chen et al. [38] proposed the MuDA scheme for privacy-preservation in smart grid communications. Additionally to the objectives achieved in PDAFT scheme, the Muda scheme can also provide differential confidentiality for data users. Lu et al. [39] proposed the EPPA scheme to secure smart grid communications that preserves privacy by aggregating data. Based on the secure report (read and reply), the EPPA supports authentication and data integrity, but it is more computationally expensive related to both PDAFT and MuDA schemes. Li et al. [40] proposed an approach based on the routing tree aggregation. The privacy-preservation in this tree is based on homomorphic encryption, but it can not detect opponents that manipulate the aggregation results. Another security scheme for smart grids based on homomorphic encryption proposed in [41], which ensures especially the privacy by reporting the consumption of a neighbourhood of n smart meters. By exploiting the homomorphic properties, Cristina et al. [42] proposed the PPNs framework, which follows the honest-but-curious model. Garcia and Jacobs [43] proposed privacy schemes with aggregation for a single smart meter with the consideration of three different types, namely, spatial aggregation, temporal aggregation, and spatio-temporal data aggregation.

The public-key certificate revocation [44] can be applied for securing a smart grid against internal attackers and restore the operation of a grid, if some devices are compromised, with the preservation of the identity revocation. Similar to the work [44], the authors in [49] proposed a certificate revocation scheme for pseudonymous public key infrastructure. Rottondi and Verticale [50] proposed the coordination of energy consumption to ensure the privacy of the users. Yanmin et al. proposed a scheme in [51] for incentive-based demand response that guarantees privacy, integrity, and availability. In [52], Hyo Jin et al. proposed a scheme for suppressing compromise attacks. Using a distributed verification method, the scheme in [52] authenticate the demand response messages. Based on Camenisch–Lysyanskaya signature, the authors in [53] proposed a linkable anonymous credential protocol for privacy protection, message authentication, and traceability. In the context of anonymity, the authors in [54] proposed a scheme using the high-frequent metring data in the smart grid. The authentication schemes based on chaotic maps with privacy protection are always desired and are discussed in [55,56].

3 System model, threat model, and design goals

In this section, we formalize the system model, including threat model, and design goals.

3.1 System model

As shown in Fig. 1, the system model of the EPEC scheme consists of three types of network architecture (i.e., NAN, BAN, and HAN), including a control center (CC) and some cloud servers $CS = \{CS_1, CS_2, CS_3, \ldots, CS_n\}$. The cloud servers could benefit from variable energy prices in smart grids [57].

- **Home area network (HAN)** The HAN home network uses two types of digital networks, namely, Local Area Network (LAN) and Wide Area Network (WAN). LAN is a collection of computers, peripherals, and mobile devices that share a common communications line (e.g. Ethernet Cables) or wireless connection (e.g. Wifi, Bluetooth Low Energy, ZigBee and IEEE 802.15.4) in a small area geographical such as at home in order to share resources. The WAN is a geographically wider telecommunications network from a LAN (e.g. Internet). Previous power management solutions have been proposed for HAN networks [58,59]. Han et al. [58] proposed the SHEMS system based on IEEE 802.15.4 and ZigBee. Hwang et al. [59] proposed the design and development of a remote control for smart home based on the Zigbee protocol.
- **Building area network (BAN)** The BAN network connects various departmental networks within a single building, where the rates should be very high. It can accommodate the computer machines, which serve globally the company. The BAN is characterized by capacity 100 Mbps and ability to support synchronous flow. Within this category, two technologies stand out, namely, FDDI technology (Fiber Distributed Data Interface) and DQDB technology (Distributed Queue Dual Bus) which aims to build a computer network Local Area Network (LAN) or Metropolitan Area Network (MAN).

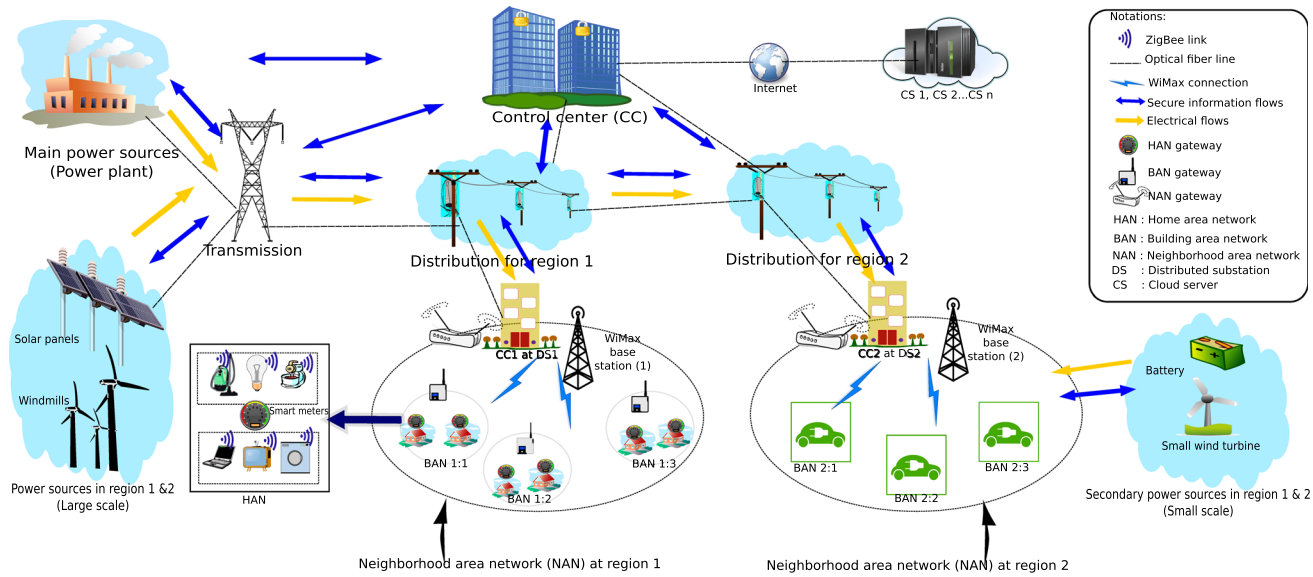


Fig. 1 Smart grid architecture

– **Neighborhood area network (NAN)** The NAN network provides secure access between the power company and independent users (a power generator) and the different types management of connected meters (water, gas, electric) [60].
– **Gateways** We propose a type of gateway for each type of network architecture, i.e., the HAN_x gateway for the HAN network, the BAN_x gateway for the BAN network, and the NAN_x gateway for the NAN network. These gateways are responsible for registration of different parties and for passing the information about energy consumption between smart grid systems. In addition, the BAN_x gateway is responsible for updating the certificates.

3.2 Threat model

The attacks of leaking privacy in smart grid communications can be classified into four categories according to our recent survey in [45], including, (1) key-based attacks, (2) data-based attacks, (3) impersonation-based attacks, and (4) physical-based attacks. However, we assume that the CC is fully trusted while the gateways are honest-but-curious. In our threat model, we consider an adversary $\mathcal{A}$ which can launch the following malicious attacks:

– Data replay attack: at any moment in the smart grid communications, an adversary $\mathcal{A}$ can inject a control input for replay sessions to change the place or the time of information transmission packets regarding the required energy. In addition, $\mathcal{A}$ can modify one or more information packets on the energy required before retransmitting it.
– Availability attack: using some attacks such as holes attacks, i.e., wormhole attack, black hole attack, and grey hole attack, an adversary $\mathcal{A}$ can disrupt the routing service in order to make it unavailable. The black hole attack is one kind of Denial of Service (DoS) attack where the adversary $\mathcal{A}$ first lures packets sent by the HAN_x gateway in order to claim that it is a real BAN_x gateway. However, all packets sent by the HAN_x gateway are dropped by the adversary $\mathcal{A}$.
– Modification attack: this attack is performed by the HAN_x where it inserts forged complimentary reviews or modifies/deletes negative reviews in a review collection of the required energy. Such attacks aim at false advertising by breaking the integrity of information transmission packets about the required energy.
– Man-in-the-middle attack: at any moment in the smart grid communications, an adversary $\mathcal{A}$ can intercept the data that passes between a HAN Node and a HAN_x gateway or a HAN_x gateway and a BAN_x gateway. This allows to spy exchanges and thus to recover passwords, certificates or even to modify the data that passes through, without the victims being aware of it.
– Sybil attack: when an adversary node has multiple identities, a Sybil attack can be launched in a smart grid environment. The major goal of the adversary in this attack is to be a favorable destination repeatedly for HAN_x gateway or BAN_x gateway. Once the packets are routed to the adversary, then he can realize other types of attacks such as the selective forwarding attack.

3.3 Design goals

Under the above system model with gateways architecture, our design goal is to develop a novel scheme to achieve energy consumption for smart grid communications. Specifically, the following three desirable objectives should be achieved.

- The proposed scheme should achieve data privacy and gateway privacy.
- The proposed scheme should be resilience to attacks as mentioned in the threat model, that is, data replay attack, availability attack, modification attack, man-in-the-middle attack, and Sybil attack.
- The proposed scheme should achieve computation efficiency under three type of curves, i.e., the Barreto–Naehrig curve, the Kachisa–Schaefer–Scott curve, and the Barreto–Lynn–Scott curve.

4 Preliminaries

In this section, we briefly recall the ideas of the bilinear pairing [61], the identity-based encryption [62], and the complexity assumptions [63], which will serve as the basis of the proposed EPEC scheme.

4.1 Bilinear pairing

Let G_1, G_2, and G_3 be three multiplicative cyclic groups of prime order q. A bilinear pairing is a mapping $e : G_1 \times G_2 \rightarrow G_3$ which satisfies the following properties:

- Bilinear: $e\left({g_1}^a, {g_2}^b\right) = e(g_1, g_2)^{ab}$ for any $g_1 \in G_1$, $g_2 \in G_2$ and for all $a, b \in Z_q^*$.
- Non-degenerate: $e(g_1, g_2) \neq 1_{G_3}$ whenever $g_1 \neq 1_{G_1}$ and $g_2 \neq 1_{G_2}$.
- Computable: there is an efficient algorithm to compute: $e(g_1, g_2)$ for all $g_1 \in G_1$ and $g_2 \in G_2$.

Definition 1 (*Bilinear generator*) A bilinear parameter generator Bsetup is a probability algorithm that takes on input the security parameter λ and outputs a 7-tuple $(q, g_1, g_2, G_1, G_2, G_3, e)$ where G_1, G_2, and G_3 are three multiplicative cyclic groups of prime order q, q is a k-bit prime number, $g_1 \in G_1$ and $g_2 \in G_2$ are generators, and $e : G_1 \times G_2 \rightarrow G_3$ is an admissible bilinear map.

4.2 Identity-based encryption

The EPEC scheme uses an identity-based encryption scheme (IBE) proposed by Boneh et al. [62]. This IBE scheme is based on the following four algorithms:

- **Setup** It takes as input 1^λ, $\alpha \in Z_q^*$, and $h = {g_1}^\alpha$. It then outputs the public parameters the master secret key msk $= \alpha$ and PubParam $= \{H, g_1, h\}$ where H is a hash function.
- **Key generation** It takes as input msk and an identity ID. It then computes $H(ID) = (h_1, \ldots, h_l)$ and samples $\{s_1, \ldots, s_l\} \in Z_q$. In the end, it outputs the secret key $SK_{ID} = \left(s_1, \ldots, s_l, \left(\prod_{j=1}^{l} h_j^{s_j}\right)^\alpha\right)$.
- **Encryption** It takes as input PubParam, an identity ID, and a message $m \in G_2$. It then computes $H(ID) = (h_1, \ldots, h_l)$ and samples $r \in Z_q$. In the end, it outputs the ciphertext $c = (c_0, \ldots, c_l)$, where $c_0 = {g_1}^r$ and for every $i \in [l]$, $c_i = \hat{e}(h, h_i)^r \cdot m$.
- **Decryption** It takes as input PubParam, c, and $SK = (s_1, \ldots, s_l, z)$. It then computes $dec = \left(\prod_{i \in [l]} c_i^{s_i}\right) / \hat{e}(c_0, z)$. In the end, it outputs $m = dec^{(s_1 + \cdots + s_l)^{-1}}$.

4.3 Complexity assumptions

Let G_1, G_2, and G_3 be the groups defined above and let g_1, g_2 be the generator of G_1, G_2, respectively. The security of our proposed scheme in Sect. 6 is based on the following two assumptions: BDH assumption and DBDH assumption.

Definition 2 (*BDH assumption*) We say that an algorithm $\mathcal{A}$ has advantages $\epsilon(\lambda)$ in solving the BDH problem for Bsetup. The Bsetup satisfies the BDH assumption if for any polynomial time algorithm $\mathcal{A}$, $\mathrm{Adv}_{\mathrm{Bsetup},\mathcal{A}}(\lambda)$ is negligible function, where:

$$\begin{aligned} &\mathrm{Adv}_{\mathrm{Bsetup},\mathcal{A}}(\lambda) \\ &\quad = \Pr[\mathcal{A}(q, g_1, g_2, G_1, G_2, G_3, e, ag_1, g_1 b, cg_1) \\ &\quad = e(g_1, g_1)^{abc} \geq \epsilon(\lambda) \end{aligned} \tag{1}$$

BDH problem: given $g_1, ag_1, bg_1, cg_1 \in G_1$ for unknown $a, b, c \in Z_q^*$, compute $e(g_1, g_1)^{abc} \in G_3$.

Definition 3 (*DBDH assumption*) We say that an algorithm $\mathcal{A}$ has advantages $\epsilon(\lambda)$ in solving the DBDH problem for Bsetup. The Bsetup satisfies the DBDH assumption if for any randomized polynomial time algorithm $\mathcal{A}$, it distinguishes the two tuples (g_1, ag_1, bg_1, cg_1) (g_1, ag_1, bg_1, abg_1) with a negligible probability.

DBDH problem: given g_1, ag_1, bg_1, cg_1, T for unknown $a, b, c \in Z_q^*$ and $\in G_3$, decide whether $T = ?e(g_1, g_1)^{abc}$.

5 Proposed EPEC scheme

The EPEC scheme consists of four phases: gateways initialization, party registration, privacy-preserving energy consumption, and updating certificates.

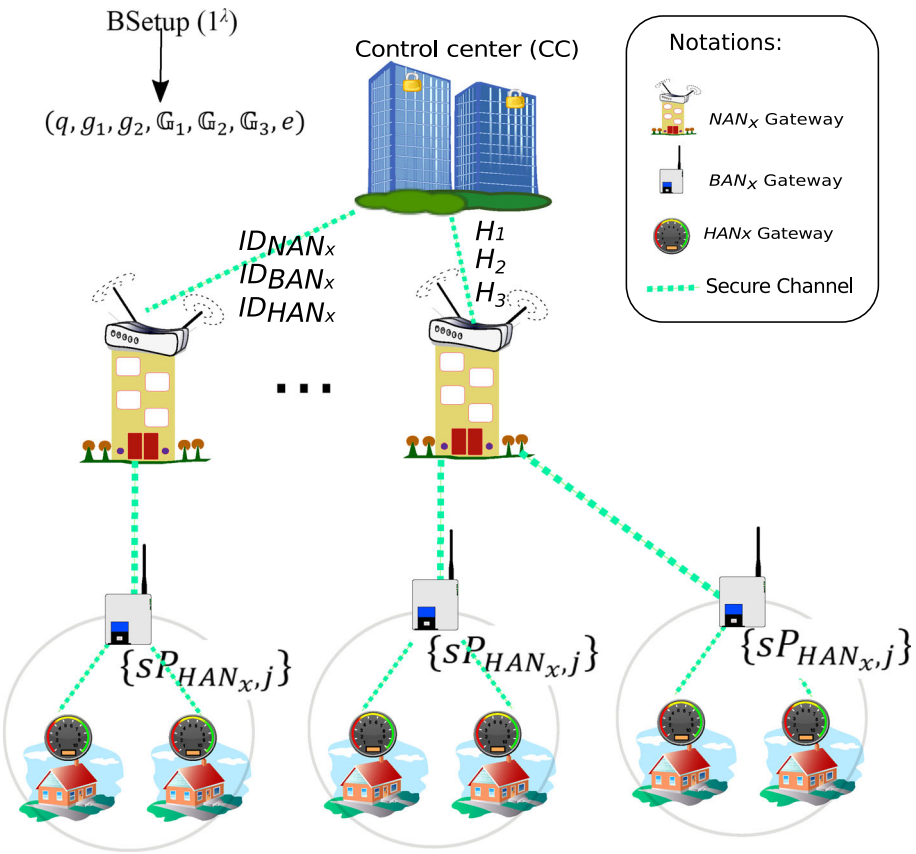


Fig. 2 An illustration of gateways initialization phase

5.1 Gateways initialization

Given the bilinear parameters $(q, g_1, g_2, \mathrm{G}_1, \mathrm{G}_2, \mathrm{G}_3, e)$ generated by BSetup(1^{λ}) where λ is the security parameter. The CC initializes the three gateway by running the following steps as shown in Fig. 2.

- **Step 1** The CC chooses three cryptographic hash function H_1, H_2, and H_3, where H_1 $\{0,1\}^* \rightarrow \mathrm{G}_1$, H_2 $\{0,1\}^* \rightarrow \mathrm{G}_2$, H_3 $\{0,1\}^* \rightarrow \mathrm{Z}_q^*$.
- **Step 2** The NAN_x gateway chooses three random number r_{NAN_x}, r_{BAN_x}, and r_{HAN_x} in Z_q^* and computes three private keys $sP_{NAN_x,j}$, $sP_{BAN_x,j}$, and $sP_{HAN_x,j}$ for $j \in \{0,1\}$, where $P_{NAN_x,j} = H_1(ID_{NAN_x}, j) \in \mathrm{G}_1$, $P_{BAN_x,j} = H_2(ID_{BAN_x}, j) \in \mathrm{G}_2$, and $P_{HAN_x,j} = H_3(ID_{HAN_x}, j) \in \mathrm{Z}_q^*$. ID_{NAN_x}, ID_{BAN_x}, and ID_{HAN_x} are the identity string of NAN_x gateway, BAN_x gateway, and HAN_x gateway, respectively.
- **Step 3** The NAN_x gateway sends $\{sP_{BAN_x,j}, sP_{HAN_x,j}\}$ through a secure channel to BAN_x gateway. Then it keeps the master key $(s, P_{NAN_x,j})$ and a set of public parameters as

$$\mathrm{PubParam}_{NAN_x}=\{(q, \mathrm{G}_1, e, r_{NAN_x}, H_1)\} \quad (2)$$

- **Step 4** The BAN_x gateway sends $\{sP_{HAN_x,j}\}$ through a secure channel to HAN_x gateway. Then it keeps the master key $(s, P_{BAN_x,j})$ and a set of public parameters as

$$\mathrm{PubParam}_{BAN_x}=\{(q, \mathrm{G}_2, e, r_{BAN_x}, H_2)\} \quad (3)$$

- **Step 5** The HAN_x gateway keeps the master key $(s, P_{BAN_x,j})$ and a set of public parameters as

$$\mathrm{PubParam}_{HAN_x}=\{(q, \mathrm{G}_1, \mathrm{G}_2, e, r_{HAN_x}, H_3)\} \quad (4)$$

5.2 Party registration

The NAN_x, BAN_x, and HAN_x gateways, once they have obtained the master key, can execute party registration sessions on the following three levels.

Algorithm 1.

Procedure: HAN Node Registration
Input: $Sess_{HAN_x}$ = {accepted}.
Output: a family of IDs $PID = \{pid_0, pid_1, \ldots\}$, the corresponding private key SK_{HAN_x,pid_j}, the public key PK_{HAN_x,pid_j}, and certificate $\text{Cert}_{HAN_x,pid_j}$.
Chooses a family of unlinkable pseudo-IDs $PID = \{pid_0, pid_1, \ldots\}$
Chooses a random $b_i \in Z_q^*$
Computes $X_{pid_0} = {g_1}^{b_i}$
For pseudo-ID $pid_j \in PID$, $j \geq 0$ **do**
Computes the public key $PK_{HAN_x,pid_j} = pid_j \bigoplus H_3\left(X_{pid_j} \| T_s\right)$
Computes the private key $SK_{HAN_x,pid_j} = b_i \bigoplus H_3\left(PK_{HAN_x,pid_j} \| T_s\right)$
Computes the corresponding certificate $\text{Cert}_{HAN_x,pid_j} = b_i \bigoplus H_3\left(SK_{HAN_x,pid_j} \| T_s\right)$
End for
Keeps the certificate ($\text{Cert}_{HAN_x,pid_j}$) secretly
Return all tuples (pid_j, SK_{HAN_x,pid_j}, PK_{HAN_x,pid_j}) to pid_j
End procedure

- **Level 1** After system's setup, the NAN_x gateway create a session $S_{BAN_x}(\text{Cert}_{BAN_x}, i_{BAN_x})$, where Cert_{BAN_x} denotes the certificate used by the BAN_x gateway in that session, and i_{BAN_x} is a counter. The $Sess_{BAN_x}$ session has two status, namely, active or inactive.
- **Level 2** When the status of $Sess_{BAN_x}$ is active, the BAN_x gateway create a session $Sess_{HAN_x}$ ($\text{Cert}_{HAN_x}, i_{HAN_x}$), where Cert_{HAN_x} denotes the certificate used by the HAN_x gateway in that session, and $\imath_{HAN_x}$ is a counter. The $Sess_{BAN_x}$ session has three status, namely, active, accepted, or rejected.
- **Level 3** When the status of $Sess_{HAN_x}$ is accepted, the HAN_x gateway issues a family of pseudo-IDs $PID = \{pid_0, pid_1, \ldots\}$, the corresponding private key SK_{HAN_x,pid_j}, the public key PK_{HAN_x,pid_j}, and certificate $\text{Cert}_{HAN_x,pid_j}$ by invoking Algorithm 1.

5.3 Privacy-preserving energy consumption

When a node N_{pid_j} with its energy consumption EC_{pid_j} in the HAN_x network, and wants to share with the HAN_x gateway, as shown in Fig. 3, they will run the following steps to establish a shared session key $SessK_{EN_\alpha}$ regarding the energy needs EN_α.

- **Step 1** N_{pid_j} first sets an energy need EN_α. Then, N_{pid_j} select random elements $\{x_1, x_2, \ldots, x_m\} \in Z_q^*$, computes $\chi = x_m \bigoplus H_3\left(PK_{HAN_x,pid_j} \| EC_{pid_j}\right)$ and uses the encryption algorithm to make a signature $\sigma_{pid_j} = \text{Enc}(EN_\alpha \| \chi)$ with regard to the private key SK_{HAN_x,pid_j} and the certificate $\text{Cert}_{HAN_x,pid_j}$. In the end, N_{pid_j} sends $EN_\alpha \| \chi \| \text{Cert}_{HAN_x,pid_j} \| SK_{HAN_x,pid_j} \| \sigma_{pid_j}$ to the HAN_x gateway.
- **Step 2** Upon receiving $EN_\alpha \| \chi \| \text{Cert}_{HAN_x,pid_j} \| SK_{HAN_x,pid_j} \| \sigma_{pid_j}$, the HAN_x gateway checks the existence of pid_j in the database. If it exists, HAN_x gateway requests a fresh identity; otherwise, it ignores directly. Then, the HAN_x gateway checks the validity of σ_{pid_j} with $\text{Cert}_{HAN_x,pid_j} \| SK_{HAN_x,pid_j}$. If it is valid, the HAN_x gateway select random elements $\{y_1, y_2, \ldots, y_m\} \in Z_q^*$, computes $Y = y_m \bigoplus H_3\left(P_{HAN_x,j} \| EC_{pid_j}\right)$ and $\sigma_{HAN_x} = \text{Enc}(EN \| Y)$ with regard to the private key SK_{HAN_x,pid_j} and the certificate $\text{Cert}_{HAN_x,pid_j}$. In the end, the HAN_x gateway sends the response $EN_\alpha \| Y \| \text{Cert}_{HAN_x,pid_j} \| SK_{HAN_x,pid_j} \| \sigma_{HAN_x}$ back to N_{pid_j} and the $EN_\alpha$to the BAN gateway.
- **Step 3** When N_{pid_j} receives $EN_\alpha \| Y \| \text{Cert}_{HAN_x,pid_j} \| SK_{HAN_x,pid_j} \| \sigma_{HAN_x}$, he checks the validity of σ_{HAN_x} with $\text{Cert}_{HAN_x,pid_j} \| SK_{HAN_x,pid_j}$. If it is invalid, it ignores the request. Otherwise, N_{pid_j} calculates the session key $SessK_{EN_\alpha} = H_3(Y \| \text{Cert}_{HAN_x,pid_j})$. Then, N_{pid_j} sends $SessK_{EN_\alpha}$ to the HAN_x gateway.
- **Step 4** When the HAN_x gateway receives $SessK_{EN_\alpha}$, he forward it to the BAN gateway.

The correctness of verification signature is shown as follows. Consider an energy consumption EC_{pid_j}, an encryption $\sigma_{pid_j} = (c_0, \ldots, c_l)$ of EC_{pid_j} under identity pid_j, and a secret key χ with $\{x_1, x_2, \ldots, x_m\} \in Z_q^*$. Then, we have:

$$dec = \sigma_{pid_j} / \hat{e}\,(c_0, z) \tag{5}$$

$$= \prod_{i \in [l]} c_i^{s_i} / \hat{e}\,(c_0, z) \tag{6}$$

$$= \prod_{i \in [l]} \hat{e}\,(h, h_i) \cdot {EC_{pid_j}}^{s_i} / \hat{e}\left(g^r, \prod_{i \in [l]} h_i^{\alpha \cdot s_i}\right) \tag{7}$$

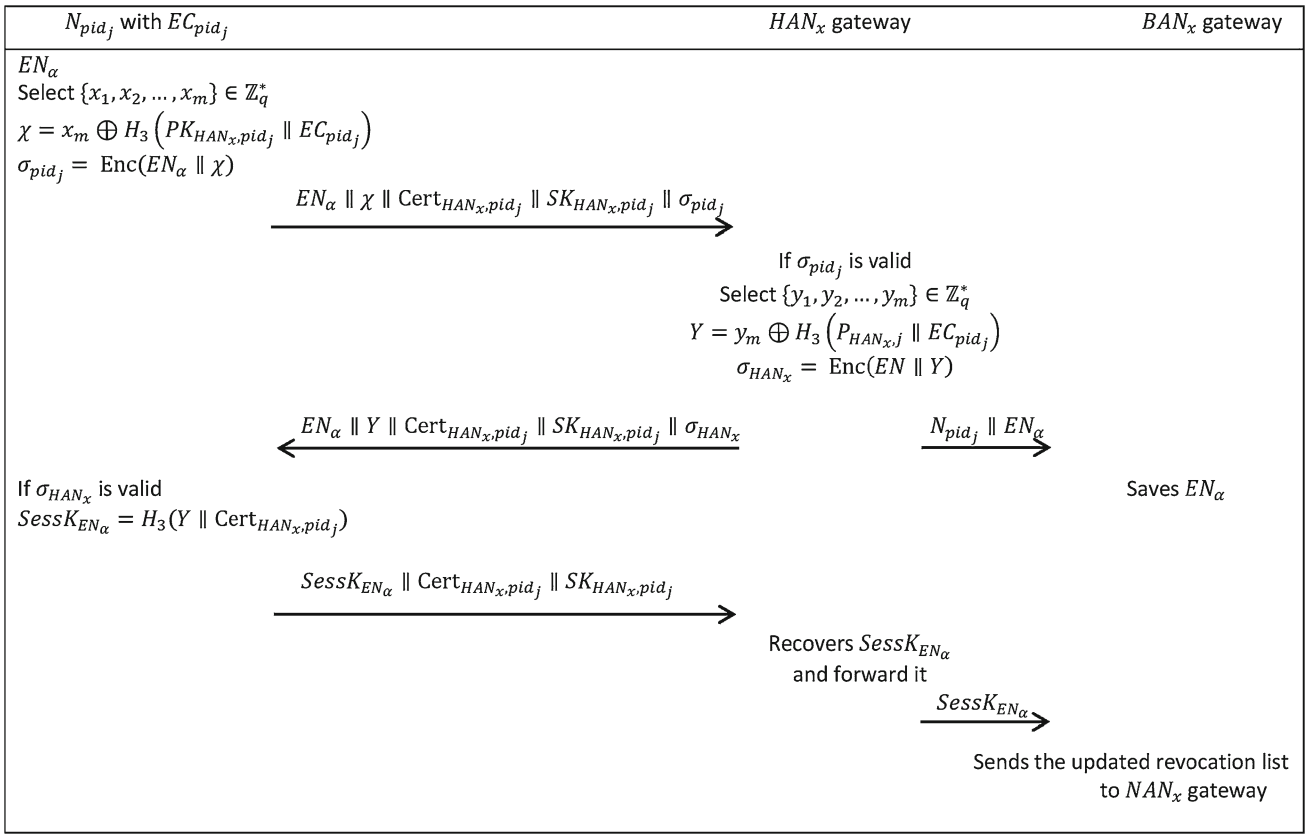


Fig. 3 Proposed privacy-preserving energy consumption scheme

$$= \prod_{i\in[l]} \hat{e}\left(g, h_i\right)^{r\alpha\cdot s_i} \cdot EC_{pid_j}{}^{s_i} / \prod_{i\in[l]} \hat{e}\left(g^r, h_i\right)^{\alpha\cdot s_i} \quad (8)$$

$$= EC_{pid_j}^{s_i} \quad (9)$$

5.4 Updating certificates

The EPEC scheme uses a revocation list for updating certificates. The certificates issued by the BAN_x gateway have a limited time frame. The lifetime of certificates should be short such that an adversary cannot link a new certificate to previous ones in the BAN network. As presented in our system model, we have two types of nodes in the BAN network, i.e., a smart home or an electric car. In this vision, we propose two types of updates, as shown in Fig. 4, one for the HAN network and another for the vehicle-to-grid network. For the HAN network, updating certificates is done when a family member enters or leaves the house. For the vehicle-to-grid network, updating certificates is done when a vehicle is plugged into a specialist firm of electric cars in order to recharge its energy. Note that each gateway (HAN_x, BAN_x, and NAN_x) should record the certificates in the user list and the recording in NAN level takes place in order to transmit the certificates to CC. The BAN_x gateway runs the following steps for updating certificates:

Type 1—Updating certificates for the HAN network:

- **Step 1** BAN_x sets a time $T \in \mathcal{T}$ and the revocation list $RevoList$. Then, BAN_x defines the revoked set R at T from $RevoList$.
- **Step 2** BAN_x sends T to the HAN_x gateway. HAN_x chooses a random $Ub_i \in Z_q^*$. Then, HAN_x computes the update of private key $USK_{HAN_x,pid_j} = Ub_i \bigoplus H_3\left(PK_{HAN_x,pid_j} \| T\right)$ and the update of the corresponding certificate $\text{UCert}_{HAN_x,pid_j} = Ub_i \bigoplus H_3\left(SK_{HAN_x,pid_j} \| T\right)$.
- **Step 3** HAN_x sends $UPK_{HAN_x,pid_j} \| USK_{HAN_x,pid_j} \| \text{UCert}_{HAN_x,pid_j}$ to pid_j. In the end, HAN_x sends the updated revocation list to NAN_x via BAN_x.
- **Step 4** Once an accepted message EC_{pid_j} about the energy consumption under the certificate $\text{UCert}_{HAN_x,pid_j}$, is disputed, the BAN_x gateway can efficiently trace the real identity by looking up in the updated revocation list.

Type 2—Updating certificates for the vehicle-to-grid network:

- **Step 1** It is the same step 1 of type 1.

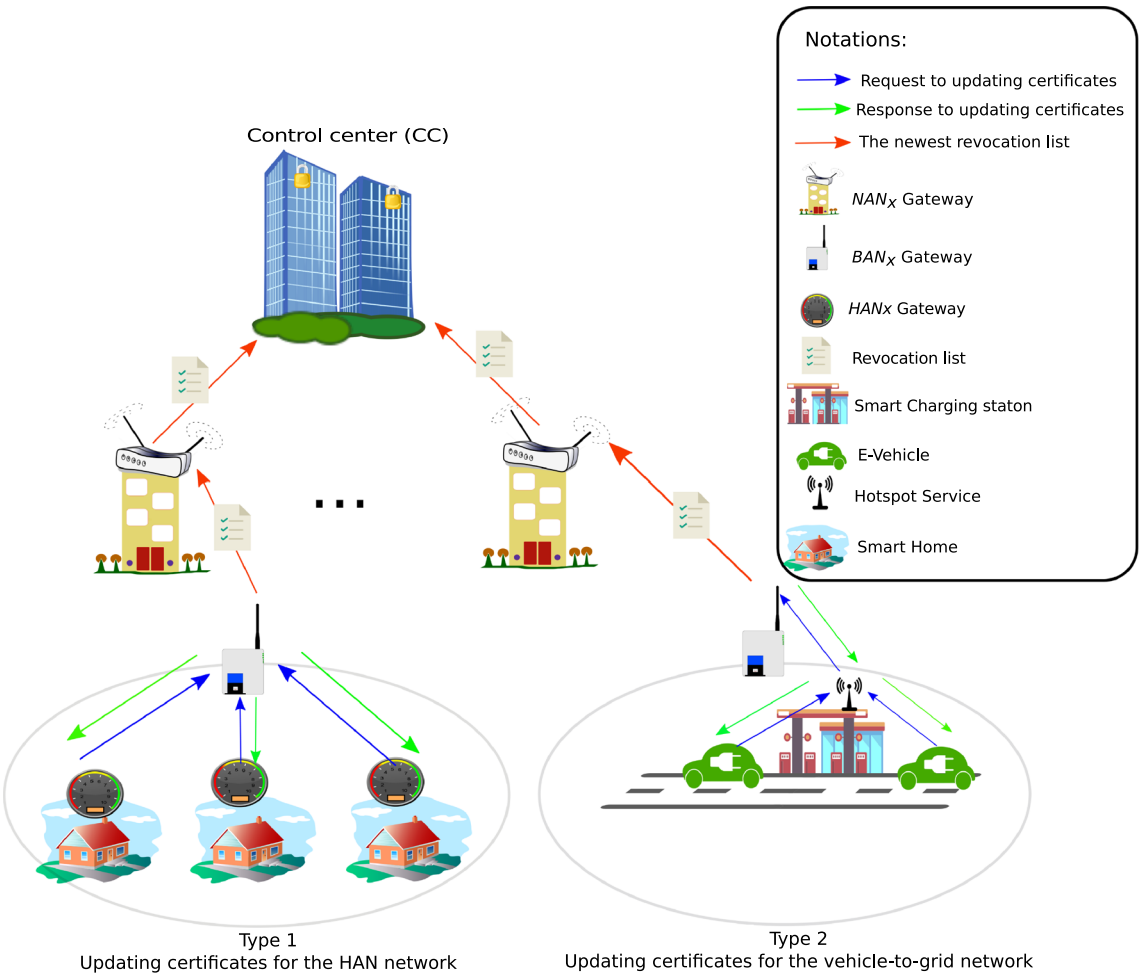


Fig. 4 Updating certificates phase

- **Step 2** BAN_x chooses a random $Ua_i \in Z_q^*$ and computes the update of private key $USK_{VG_i} = Ua_i \bigoplus H_3\left(PK_{VG_i} \| T\right)$ and the update of the corresponding certificate $\text{UCert}_{VG_i} = Ub_i \bigoplus H_3\left(SK_{VG_i} \| T\right)$.
- **Step 3** BAN_x sends $UPK_{VG_i} \| USK_{VG_i} \| \text{UCert}_{VG_i}$ to VG_i and the updated revocation list to NAN_x.
- **Step 4** Once an accepted message EC_{VG_i} about the energy consumption under the certificate UCert_{VG_i}, is disputed, the BAN_x gateway can efficiently trace the vehicle's real identity by looking up in the updated revocation list.

6 Security analysis

In this section, we analyze the security properties of our proposed EPEC. Specifically, our analysis focuses on data privacy and gateway privacy. Then, we study the resilience of EPEC against data replay attack, availability attack, modification attack, man-in-the-middle attack, and Sybil attack.

6.1 Data privacy

It is easy to verify that our proposed scheme satisfies data privacy by using Theorem 1.

Theorem 1 *Suppose the DBDH assumption holds in* G_1, *then our proposed EPEC scheme holds the data privacy.*

Proof Let $\mathcal{A}$ be a probabilistic polynomial time adversary. Suppose $\mathcal{A}$ has advantages $\epsilon(\lambda)$ in attacking the proposed EPEC scheme under the IND-ID-CCA game [61]. Suppose an algorithm $\mathcal{B}$ makes H-queries with a list of tuples $L = (ID_j, h_j, \alpha_j)$ for $j \in \{1, \ldots, Q_H\}$ where $h_j = (h_1^{(j)}, \ldots, h_l^{(j)}) \in G_1$ and $\alpha_j = (\alpha_1^{(j)}, \ldots, \alpha_l^{(j)}) \in Z_p$ are two vectors of elements. The result in [61,62] has shown that IBE scheme is semantically secure against an adaptive chosen ciphertext attack and is data private based on the DBDH assumption. In the proposed EPEC scheme, on one hand, the energy consumption EC_{pid_j} is protected by a hash function and a validated certificate. Anyone, including the neighbor node in the HAN_x network, cannot recover the EC_{pid_j} with

$EN_\alpha \| \chi \| \text{Cert}_{HAN_x, pid_j} \| SK_{HAN_x, pid_j} \| \sigma_{pid_j}$. On other hand, by using σ_{pid_j}, the HAN_x can easily check whether two signatures on the same packet are generated by the same signer or not. □

6.2 Gateway privacy

It is easy to verify that our proposed scheme satisfies gateways privacy. Since the three cryptographic hash function H_1, H_2, and H_3 are employed, the adversary cannot identify the identity string of NAN_x gateway, BAN_x gateway, and HAN_x gateway. Hence, our scheme satisfies gateways privacy.

6.3 Resilience to data replay attack

One possible severe attack launched by one or more eavesdropping attackers on the HAN_x network is the data replay attack, which refers to the adversary maliciously recording packets and injecting them using eavesdropped security materials. However, the HAN_x network accepts only data packets that contain a valid certificate. Without knowing the status of $Sess_{HAN_x}$, the adversary of data replay attack during party registration phase cannot recover the certificate. In addition, because the revocation list for updating certificates is adopted, malicious Trojan horse programs running in the BAN_x network can be detected. Therefore, EPEC can resist the data replay attack.

6.4 Resilience to availability attack

In an availability attack, after eavesdropping the routing packet, the suspicious e-vehicle nodes disrupt the routing service to make it not available. In updating certificates phase for the vehicle-to-grid network, when a vehicle VG_i request the BAN_x gateway to update its certificates, the BAN_x gateway checks the validity of certificate with the NAN_x gateway based on revocation list. If valid, it computes the update of private key $USK_{VG_i} = Ua_i \bigoplus H_3\left(PK_{VG_i} \| T\right)$ and the update of the corresponding certificate $\text{UCert}_{VG_i} = Ub_i \bigoplus H_3\left(SK_{VG_i} \| T\right)$, then, it sends $UPK_{VG_i} \| USK_{VG_i} \| \text{UCert}_{VG_i}$ to VG_i and the updated revocation list to NAN_x. Thus, if the certificate is not valid, it becomes suspicious, as shown in Fig. 5. As a result, the availability attack can be prevented by EPEC.

6.5 Resilience to modification attack

In the proposed EPEC scheme, after the authentication phase, when N_{pid_j} receives $EN_\alpha \| Y \| \text{Cert}_{HAN_x, pid_j} \| SK_{HAN_x, pid_j} \| \sigma_{HAN_x}$, it checks the validity of σ_{HAN_x} with $\text{Cert}_{HAN_x, pid_j} \| SK_{HAN_x, pid_j}$. If it is invalid, it ignores the request. Without knowing the private key SK_{HAN_x, pid_j} and the certificate $\text{Cert}_{HAN_x, pid_j}$, the adversary cannot break the integrity of information transmission packets about the required energy. As result, the modification attack can be prevented by EPEC.

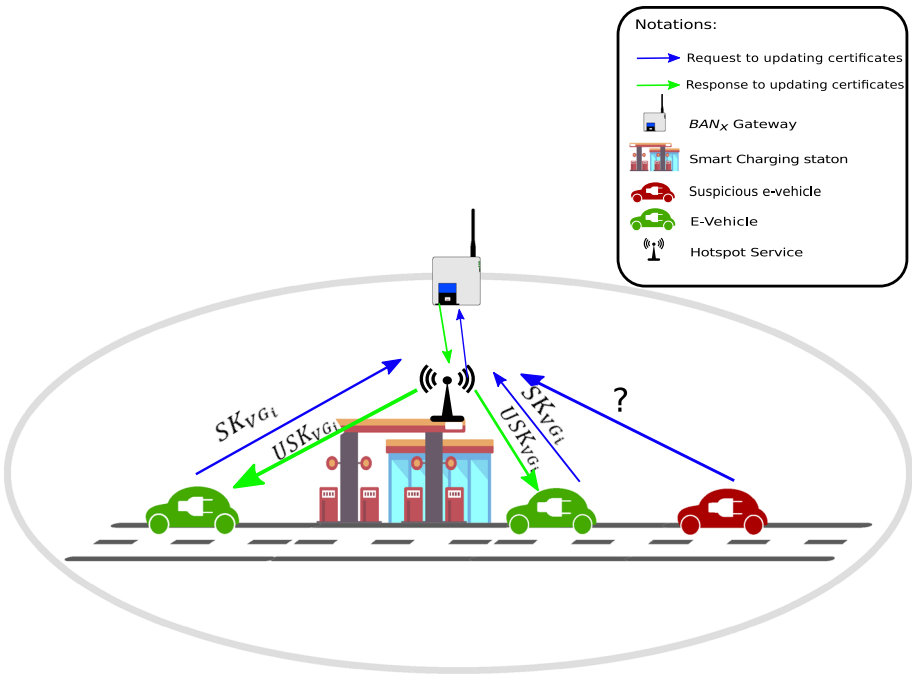


Fig. 5 Detect the suspicious e-vehicle nodes with updating certificates

Table 1 Comparison of security properties

Properties	Scheme EPEC	Scheme [29]	Scheme [40]	Scheme [54]
Data privacy	Yes	Yes	Partial	Partial
Gateway privacy	Yes	Partial	Partial	Partial
Resilience to data replay attack	Yes	No	No	No
Resilience to availability attack	Yes	No	No	No
Resilience to modification attack	Yes	Partial	No	Partial
Resilience to man-in-the-middle attack	Yes	No	Partial	No
Resilience to Sybil attack	Yes	No	No	No
Resilience to collusion attack	Partial	Yes	No	No
Resilience dictionary attack	Partial	Yes	No	No

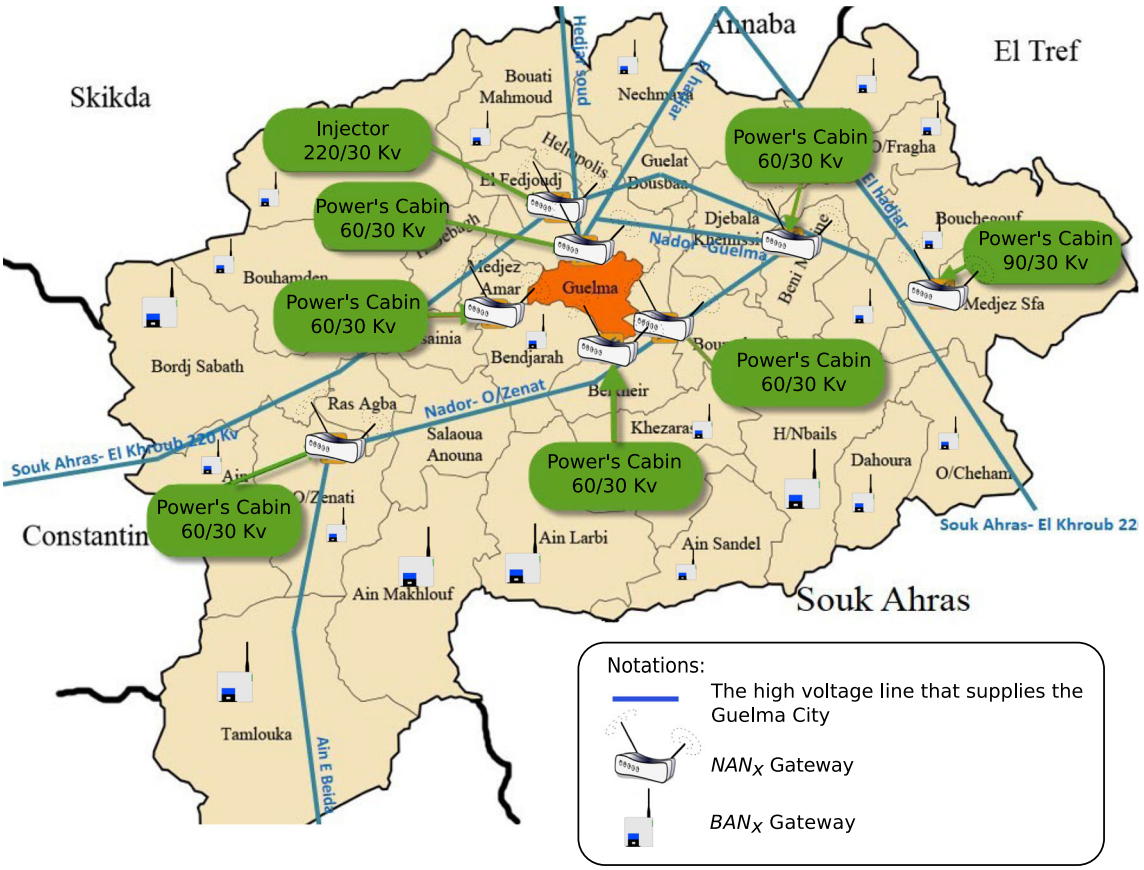


Fig. 6 High-voltage lines and power sources of the Guelma City considered for simulation

6.6 Resilience to man-in-the-middle attack

Similarly to the data replay attack, another attack that could be launched by an adversary is the man-in-the-middle attack. In a man-in-the-middle attack, when an adversary $\mathcal{A}$ intercepts the data that passes between a HAN Node and a HAN_x gateway or a HAN_x gateway and a BAN_x gateway, the destination information is disclosed to the adversary. However, the HAN Node N_{pid_j} selects random elements $\{x_1, x_2, \ldots, x_m\} \in Z_q^*$, computes $\chi = x_m \bigoplus H_3\left(PK_{HAN_x, pid_j} \| EC_{pid_j}\right)$ and uses the encryption algorithm to make a signature $\sigma_{pid_j} = \text{Enc}(EN_\alpha \| \chi)$ with regard to the private key SK_{HAN_x, pid_j} and the certificate $\text{Cert}_{HAN_x, pid_j}$. Since a signature is protected by the hash chain and the numbers that are randomly chosen from $\in Z_q^*$, the adversary cannot modify the data that passes through. As result, the man-in-the-middle attack can be prevented by EPEC. In addition, the man-in-the-middle attack doesn't affect the proposed EPEC for the vehicle-

Table 2 Notations used in overheads evaluation

Symbol	Notation
P	Pairing in the bilinear group
$\|G_1\|$	The length of any element in G_1
$\|G_2\|$	The length of any element in G_2
$\|Cert\|$	The length of the certificate
$\|UCert\|$	The length of the update certificate
$\|SC\|$	The length of the ciphertext $c = (c_0, \ldots, c_l)$
Dec	Decryption of the encryption scheme
$\|Z_q\|$	The length of any element in Z_q^*

to-grid network because timestamp is used for updating certificates.

6.7 Resilience to Sybil attack

One possible severe attack launched by one adversary that has multiple identities is the Sybil attack, which refers to an adversary to be a destination repeatedly for HAN_x gateway or BAN_x gateway. In the proposed EPEC scheme, upon receiving $EN_\alpha \| \chi \| \text{Cert}_{HAN_x, pid_j} \| SK_{HAN_x, pid_j} \| \sigma_{pid_j}$, the HAN_x gateway checks the existence of pid_j in the database. If it exists, HAN_x gateway requests a fresh identity; otherwise, it ignores directly. As result, the Sybil attack can be prevented by EPEC.

From the above security analysis and comparison in Table 1, our EPEC can achieve all of the data privacy and gateway privacy, and can resist to data replay attack, availability attack, modification attack, man-in-the-middle attack, and Sybil attack compared with the scheme [40] and the scheme [54].

Table 4 Computational cost on the BAN_x gateway side-timings in milliseconds

	BN-128	KSS-192	BLS-256
Initialization			
In theory	$1P$	$2P$	$3P$
In simulation	105	192	301
Registration			
In theory	$1\|Z_q\|+3\|G_2\|$	$1\|Z_q\|+6\|G_2\|$	$1\|Z_q\|+9\|G_2\|$
In simulation	300	310	322
Update			
In theory	$2\|Z_q\|+4\|G_1\|$	$3\|Z_q\|+7\|G_1\|$	$4\|Z_q\|+10\|G_1\|$
In simulation	301	356	404

7 Performance evaluation

An important performance metric in smart grids communication is how long it takes for the HAN_x gateway to send the energy consumption EC_{pid_j} and the energy need EN_α to reach the control center through the BAN_x gateway and the NAN_x gateway. In this section, we study the transmission delay performance (T_d) at the HAN_x gateway and the average delivery ratio (ADR), which is defined as the average ratio of EC_{pid_j} successfully delivered to the control center. Our simulation is based on a discrete event simulator coded in java.

7.1 Simulation settings

To simulate a smart grid communication, 8 NAN_x gateways are first deployed to cover the Guelma City region of 44, 74 km^2, as shown in Fig. 6. Specifically, we place a NAN_x

Table 3 Computational cost on the HAN_x gateway side-timings in milliseconds

	BN-128	KSS-192	BLS-256
Initialization			
In theory	$1P$	$2P$	$3P$
In simulation	110	186	302
Registration			
In theory	$1\|Z_q\|+3\|G_1\|+\|Cert\|$	$2\|Z_q\|+6\|G_1\|+\|Cert\|$	$3\|Z_q\|+9\|G_1\|+\|Cert\|$
In simulation	407	466	510
Encrypt ($\mathbf{T}_{enc}$)			
In theory	$6\|G_1\|+3\|G_2\|+\|SC\|$	$8\|G_1\|+5\|G_2\|+\|SC\|$	$10\|G_1\|+7\|G_2\|+\|SC\|$
In simulation	600	623	702
Decrypt ($\mathbf{T}_{dec}$)			
In theory	$8\|G_1\|+3\|G_2\|+\|Dec\|$	$10\|G_1\|+5\|G_2\|+\|Dec\|$	$12\|G_1\|+9\|G_2\|+\|Dec\|$
In simulation	832	901	1241
Update ($\mathbf{T}_{upd}$)			
In theory	$2\|Z_q\|+4\|G_1\|+\|UCert\|$	$3\|Z_q\|+7\|G_1\|+\|UCert\|$	$4\|Z_q\|+10\|G_1\|+\|UCert\|$
In simulation	507	555	593

Table 5 Computational cost on the NAN_x gateway side-timings in milliseconds

	BN-128	KSS-192	BLS-256
Initialization			
In theory	$2P$	$3P$	$4P$
In simulation	201	293	356
Registration			
In theory	$1\|Z_q\|+1\|G_2\|$	$1\|Z_q\|+2\|G_2\|$	$1\|Z_q\|+3\|G_2\|$
In simulation	111	145	197

gateway in each Power's Cabin. In addition, 30 BAN_x gateways deployed to cover all districts of the city.

The computation costs of EPEC include, gateways initialization, party registration, detection attack, and updating certificates, which mainly involve the following cryptographic operations: *genk*, *encrypt*, *decrypt*, multiplication in Z_q^* and hash operations. We implement three types of curves [64] include, the Barreto–Naehrig curve (BN-128), the Kachisa–Schaefer–Scott curve (KSS-192), and the Barreto–Lynn–Scott curve (BLS-256). The BN-128 is over F_{p^2} with

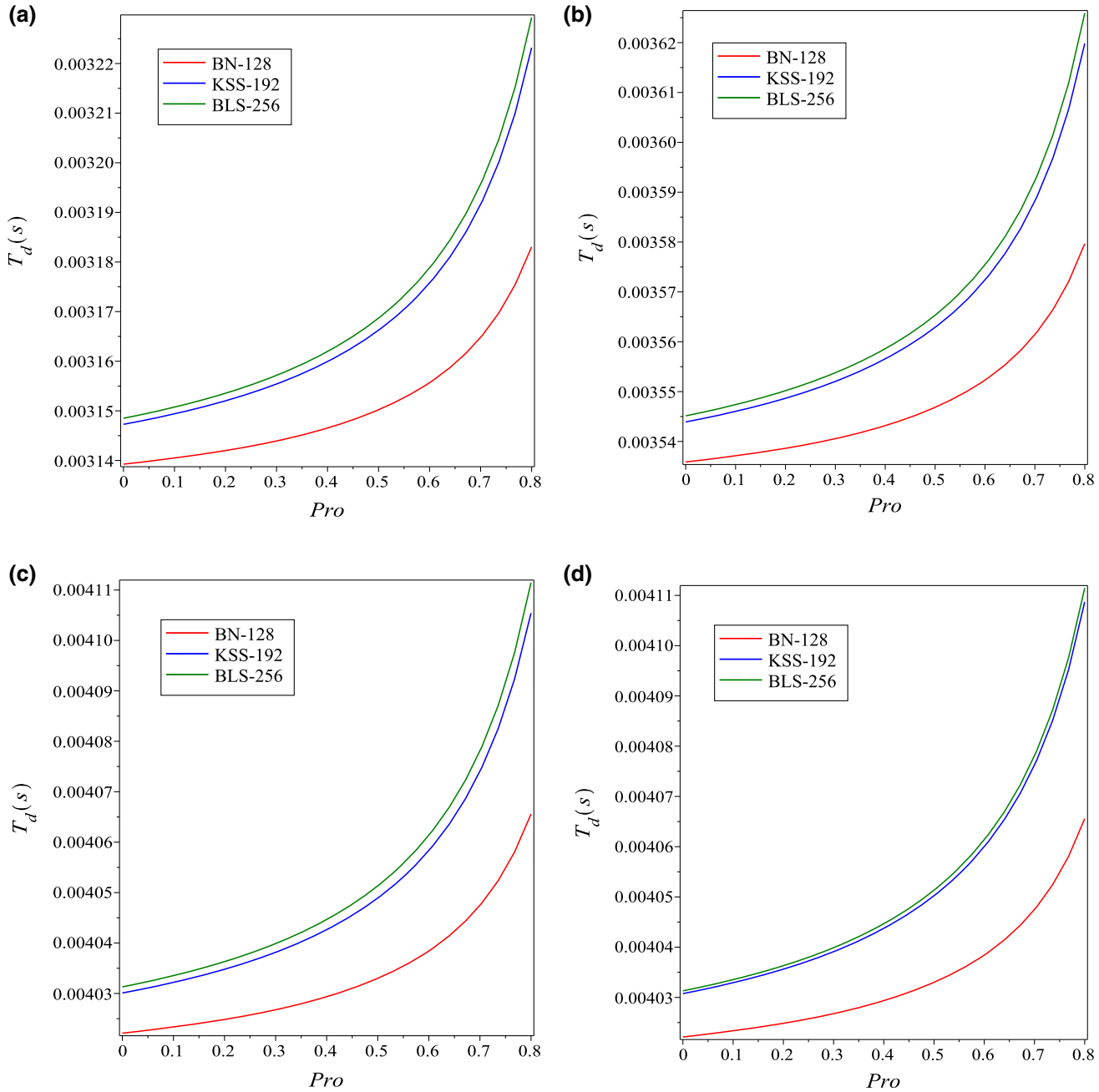


Fig. 7 Average transmission delay T_d at the HAN_x gateway varies with the invalid probability of an energy consumption EC_{pid_j}, where $0\% \leq Pro \leq 80\%$: **a** T_d versus Pro with $\lambda = 30$; **b** T_d versus Pro with $\lambda = 60$; **c** T_d versus Pro with $\lambda = 80$; **d** T_d versus Pro with $\lambda = 100$

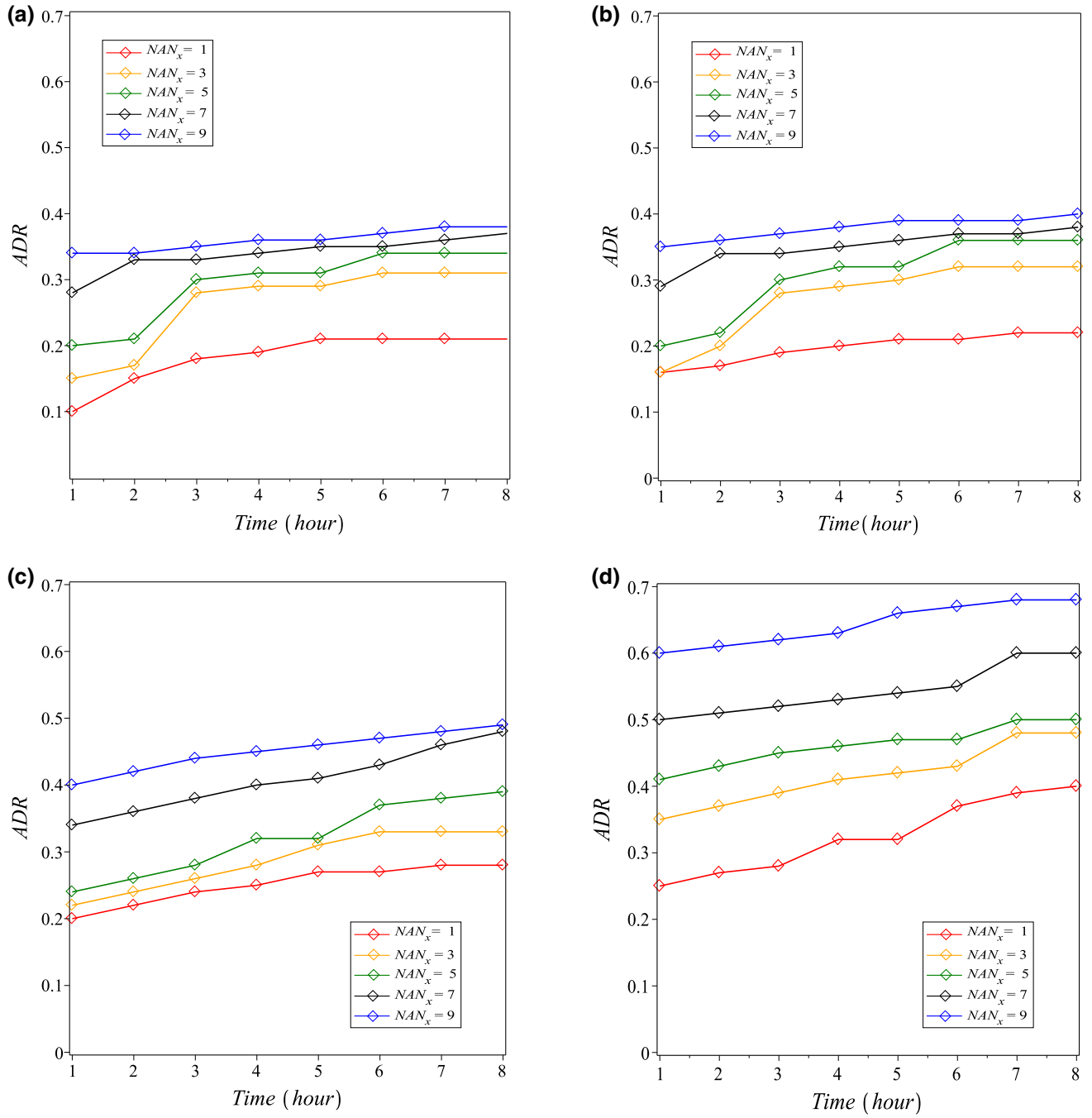


Fig. 8 Average delivery ratio of EC_{pid_j} with $NAN_x = \{1, 3, 5, 7, 9\}$: **a** *ADR* versus $Time$ with $\lambda = 30$; **b** *ADR* versus $Time$ with $\lambda = 60$; **c** *ADR* versus $Time$ with $\lambda = 80$; **d** *ADR* versus $Time$ with $\lambda = 100$

modulus 256 bits. The KSS-192 is over F_{p^3} with modulus 512 bits. The BLS-256 is over F_{p^4} with modulus 640 bits. Benchmarks (with the PBC library [65]) for the selected pairing were running on a modern workstation, where the processor is 2.6 GHz Intel i5 PC with 4 GB of RAM. The notations used in overheads evaluation in the simulation are summarized in Table 2. In addition, Tables 3, 4, and 5 give the detailed numbers of computational cost on the HAN_x gateway, the BAN_x gateway, and the NAN_x gateway, respectively.

Based on the M/D/1 queue [66], we consider the average arrival of an energy consumption EC_{pid_j} in the HAN_x network according to a Poisson process ($\lambda > 0$) with arrival Rate λ and departure rate μ. The service in the HAN_x network is provided by a single gateway. The duration between two consecutive arrivals and service times are mutually independent. Let *Pro* be the invalid probability of an energy consumption EC_{pid_j} arriving at the HAN_x gateway. The transmission delay T_d of EPEC at the HAN_x gateway depends on three factors

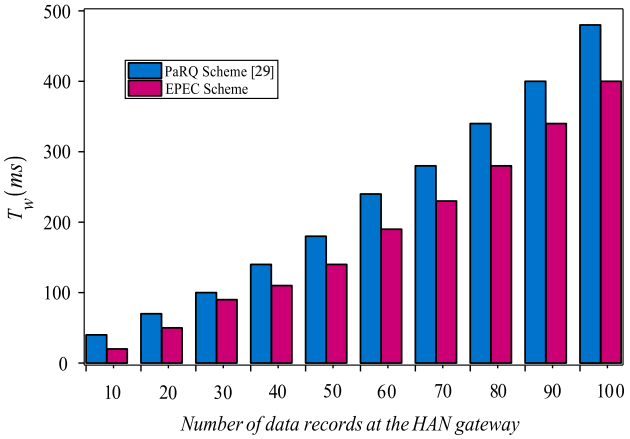


Fig. 9 Average waiting time in the HAN_x gateway varies with number of data records

namely, the average number of EC_{pid_j}, the average waiting time in the HAN_x gateway, and the computational cost of the encryption and decryption scheme.

– The average number of EC_{pid_j} in the HAN_x gateway, T_n is given by:

$$T_n = \rho + \frac{1}{2}\left(\frac{\rho^2}{1-\rho}\right), \quad \rho = \frac{\lambda}{\mu} < 1 \tag{10}$$

– The average waiting time in the HAN_x gateway, T_w is given by:

$$T_w = \frac{1}{\mu} + \frac{\rho}{2\mu(1-\rho)} + T_{enc} + T_{dec} + T_{upd}, \quad \rho = \frac{\lambda}{\mu} < 1 \tag{11}$$

– The transmission delay of EPEC at the HAN_x gateway, T_d is given by:

$$T_d = T_w + \frac{1}{2\mu(1-Pro)}. \tag{12}$$

7.2 Simulation results

Figure 7 shows that the average transmission delay T_d at the HAN_x gateway varies with the invalid probability of an energy consumption EC_{pid_j}, where $0\% \leq Pro \leq 80\%$. From the figure, we can see that T_d with the BN-128 curve is less than T_d with the KSS-192 curve and with the BLS-256 curve. The reason is due to the embedding degree k over a prime field, i.e., BN-128 curve uses $k = 12$, KSS-192 curve uses $k = 18$, and BLS-256 curve uses $k = 24$. It can also been seen that T_d increases with increasing the percentage of Pro, and that due to decryption time T_{dec}. In addition, when the arrival Rate λ increases from 10 to 100, the time costs of required operations in EPEC at the HAN_x gateway is increased in all three types of curves. This indicates that the arrival Rate λ may impose a significant impact on the proposed scheme in terms of the average transmission delay at the HAN_x gateway, especially when EC_{pid_j} is large.

Figure 8 shows the average delivery ratio of EC_{pid_j} within 8 h with $NAN_x = \{1, 3, 5, 7, 9\}$. We can see that increasing number of NAN_x gateway increases the average delivery ratio. This observation validates that the NAN_x gateway in each Power's Cabin is more reliable than the smart grid with one NAN_x gateway for the Guelma City. In addition, Fig. 8 also shows that, when the arrival Rate λ increases, the average delivery ratio will visibly increase. The performance of the scheme is significant especially when NAN_x and λ are large.

In Fig. 9, it can be seen that the average waiting time in the HAN_x gateway of the scheme EPEC is less than the scheme PaRQ [29] because more queries need to be sent to the gateway to obtain the corresponding data ciphertext. In addition, the more the number of data records at the HAN gateway increases, the more the average waiting time increases also.

8 Conclusion

In this paper, we have proposed an efficient privacy-preserving energy consumption (EPEC) scheme with updating certificates. It realizes secure and efficient energy consumption demand and response based on the identity-based encryption and the strategy of updating certificates. Security analysis has demonstrated that EPEC can achieve privacy of data and gateway, and can resist to data replay attack, availability attack, modification attack, man-in-the-middle attack, and Sybil attack. Performance evaluation further demonstrates its efficiency in terms of computation overhead. In our future work, we will study how selfish gateways affect the performance of our scheme. We will also study the robustness against other types of attacks such as injecting false data attack. In addition, we will propose a model based on social network analysis for the better coordination of energy consumption in a smart grid.

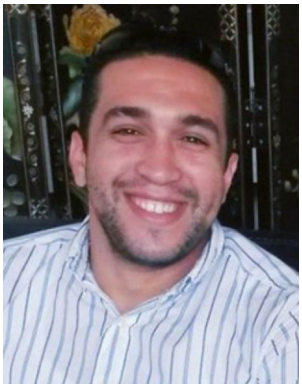
Acknowledgements This work was partly supported by the Guelma University and the Networks and Systems Laboratory (LRS). The corresponding author would also thank the support of National Society for Electricity and Gas at the Guelma City (http://www.sonelgaz.dz/).

References

1. Ferrag, M. A., & Ahmim, A. (2017). *Security solutions and applied cryptography in Smart Grid Communications*. IGI Global. doi:10.4018/978-1-5225-1829-7. http://www.igi-global.com/book/security-solutions-applied-cryptography-smart/166368.
2. Farhangi, H. (2010). The path of the smart grid. *IEEE Power and Energy Magazine*, *8*(1), 18–28. doi:10.1109/MPE.2009.934876.

3. Kingsbury, A. (2010). 10 Cities adopting smart grid technology. Tech. rep., U.S. News & World Report.
4. https://www.smartgrid.gov/.
5. Fadlullah, Z. M., Fouda, M. M., Kato, N., Takeuchi, A., Iwasaki, N., & Nozaki, Y. (2011). Toward intelligent machine-to-machine communications in smart grid. *IEEE Communications Magazine*, *49*(4), 60–65. doi:10.1109/MCOM.2011.5741147.
6. Simões, M. G., Roche, R., Kyriakides, E., Miraoui, A., Blunier, B., McBee, K., et al. (2011). Smart-grid technologies and progress in Europe and the USA. In *IEEE energy conversion congress and exposition: Energy conversion innovation for a clean energy future, ECCE 2011, proceedings* (pp. 383–390). doi:10.1109/ECCE.2011.6063795.
7. Ferrag, M. A., & Ahmim, A. (2017). ESSPR: An efficient secure routing scheme based on searchable encryption with vehicle proxy re-encryption for vehicular peer-to-peer social network. *Telecommunication Systems*. doi:10.1007/s11235-017-0299-y.
8. Su, W., Eichi, H., Zeng, W., & Chow, M. Y. (2012). A survey on the electrification of transportation in a smart grid environment. *IEEE Transactions on Industrial Informatics*, *8*(1), 1–10. doi:10.1109/TII.2011.2172454.
9. Han, W., & Xiao, Y. (2016). Privacy preservation for V2G networks in smart grid: A survey. *Computer Communications*, *91*, 17–28. doi:10.1016/j.comcom.2016.06.006.
10. Maglaras, L. A., Topalis, F. V., & Maglaras, A. L. (2014). Cooperative approaches for dymanic wireless charging of electric vehicles in a smart city. In *2014 IEEE international on energy conference (ENERGYCON)*. IEEE.
11. Cheng, N., Lu, N., Zhang, N., Shen, X. S., Mark, J. W. (2013). Vehicle-assisted data delivery for smart grid: An optimal stopping approach. In *2013 IEEE international conference on communications (ICC)* (pp. 6184–6188). IEEE. doi:10.1109/ICC.2013.6655595.
12. Deilami, S., Masoum, A. S., Moses, P. S., & Masoum, M. A. S. (2011). Real-time coordination of plug-in electric vehicle charging in smart grids to minimize power losses and improve voltage profile. *IEEE Transactions on Smart Grid*, *2*(3), 456–467. doi:10.1109/TSG.2011.2159816.
13. Liang, H., Choi, B. J., Zhuang, W., & Shen, X. (2013). Optimizing the energy delivery via V2G systems based on stochastic inventory theory. *IEEE Transactions on Smart Grid*, *4*(4), 2230–2243. doi:10.1109/TSG.2013.2272894.
14. Wang, M., Liang, H., Zhang, R., Deng, R., & Shen, X. (2014). Mobility-aware coordinated charging for electric vehicles in VANET-enhanced smart grid. *IEEE Journal on Selected Areas in Communications*, *32*(7), 1344–1360. doi:10.1109/JSAC.2014.2332078.
15. Le, T. N., Choi, B. J., Liang, H., Li, H., & Shen, X. S. (2015). DCD: Distributed charging and discharging scheme for EVs in microgrids. In *2014 IEEE international conference on smart grid communications, SmartGridComm 2014* (pp. 704–709). doi:10.1109/SmartGridComm.2014.7007730.
16. Zheng, Z., Cai, L. X., Zhang, N., Zhang, R., & Shen, X. S. (2014). A game theoretical approach for energy trading in wireless networks powered by green energy. In *Global communications conference (GLOBECOM)* (pp. 2562–2567). IEEE. doi:10.1109/GLOCOM.2014.7037193.
17. Wang, B., Han, Z., & Liu, K. J. R. (2009). Distributed relay selection and power control for multiuser cooperative communication networks using stackelberg game. *IEEE Transactions on Mobile Computing*, *8*(7), 975–990. doi:10.1109/TMC.2008.153.
18. Premarathne, U. S., Khalil, I., & Atiquzzaman, M. (2015). Secure and reliable surveillance over cognitive radio sensor networks in smart grid. *Pervasive and Mobile Computing*, *22*, 3–15. doi:10.1016/j.pmcj.2015.05.001. http://www.sciencedirect.com/science/article/pii/S1574119215000887.
19. Khurana, H., Hadley, M., Lu, N., & Frincke, D. A. (2010). Smart-grid security issues. *IEEE Security and Privacy*, *8*(1), 81–85. doi:10.1109/MSP.2010.49.
20. Maglaras, L. A. (2015). A novel distributed intrusion detection system for vehicular ad hoc networks. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *6*(4), 101–106.
21. Li, X., Liang, X., Lu, R., Shen, X., Lin, X., & Zhu, H. (2012). Securing smart grid: Cyber attacks, countermeasures, and challenges. *IEEE Communications Magazine*, *50*(8), 38–45. doi:10.1109/MCOM.2012.6257525.
22. Efthymiou, C., & Kalogridis, G. (2010). Smart grid privacy via anonymization of smart metering data. In *2010 1st IEEE international conference on smart grid communications (SmartGridComm)* (pp. 238–243). doi:10.1109/SMARTGRID.2010.5622050.
23. Fouda, M. M., Fadlullah, Z. M., Kato, N., Lu, R., & Shen, X. S. (2011). A lightweight message authentication scheme for smart grid communications. *IEEE Transactions on Smart Grid*, *2*(4), 675–685. doi:10.1109/TSG.2011.2160661.
24. Liu, J., Xiao, Y., & Gao, J. (2014). Achieving accountability in smart grid. *IEEE Systems Journal*, *8*(2), 493–508. doi:10.1109/JSYST.2013.2260697.
25. Ferrag, M. A., Nafa, M., & Ghanemi, S. (2014). SDPP: An intelligent secure detection scheme with strong privacy-preserving for mobile peer-to-peer social network. *International Journal of Information and Computer Security*, *6*(3), 241–269. doi:10.1504/IJICS.2014.066650.
26. Ferrag, M. A., Nafa, M., & Ghanemi, S. (2013). ECPDR: An efficient conditional privacy-preservation scheme with demand response for secure ad hoc social communications. *International Journal of Embedded and Real-Time Communication Systems (IJERTCS)*, *4*(3), 43–71. doi:10.4018/ijertcs.2013070103.
27. Ferrag, M. A., Nafa, M., & Ghanemi, S. (2016). EPSA: An efficient and privacy preserving scheme against wormhole attack on reactive routing for mobile ad hoc social networks. *International Journal of Security and Networks*, *11*(3), 107–125. doi:10.1504/IJSN.2016.10000172.
28. Wen, M., Zhang, K., Lei, J., Liang, X., Deng, R., & Shen, X. S. (2013). CIT: A credit-based incentive tariff scheme with fraud-traceability for smart grid. *Security and Communication Networks*. doi:10.1002/sec.895.
29. Wen, M., Lu, R., Zhang, K., Lei, J., Liang, X., & Shen, X. (2013). PaRQ: A privacy-preserving range query scheme over encrypted metering data for smart grid. *IEEE Transactions on Emerging Topics in Computing*, *1*(1), 178–191. doi:10.1109/TETC.2013.2273889.
30. Wen, M., Lu, R., Lei, J., Li, H., Liang, X., & Shen, X. S. (2014). SESA: An efficient searchable encryption scheme for auction in emerging smart grid marketing. *Security and Communication Networks*, *7*(1), 234–244. doi:10.1002/sec.699.
31. 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 Transactions on Parallel and Distributed Systems*, *25*(8), 2053–2064. doi:10.1109/TPDS.2013.124.
32. Jiang, R., Lu, R., Luo, J., Lai, C., & Shen, X. S. (2015). Efficient self-healing group key management with dynamic revocation and collusion resistance for SCADA in smart grid. *Security and Communication Networks*, *8*(6), 1026–1039. doi:10.1002/sec.1057.
33. Jiang, R., Lu, R., Lai, C., Luo, J., & Shen, X. (2013). Robust group key management with revocation and collusion resistance for SCADA in smart grid. In GLOBECOM—IEEE global telecommunications conference (pp. 802–807). doi:10.1109/GLOCOM.2013.6831171.

34. Choi, D., Jeong, H., Won, D., & Kim, S. (2013). Hybrid key management architecture for robust SCADA systems. *Journal of Information Science and Engineering*, *29*(2), 281–298.
35. Choi, D., Kim, H., Won, D., & Kim, S. (2009). Advanced key-management architecture for secure SCADA communications. *IEEE Transactions on Power Delivery*, *24*(3), 1154–1163. doi:10.1109/TPWRD.2008.2005683.
36. Tsai, J. L., & Lo, N. W. (2016). Secure anonymous key distribution scheme for smart grid. *IEEE Transactions on Smart Grid*, *7*(2), 906–914. doi:10.1109/TSG.2015.2440658.
37. Chen, L., Lu, R., Cao, Z., Chen, L., Cao, Z., & Lu, R. (2015). PDAFT: A privacy-preserving data aggregation scheme with fault tolerance for smart grid communications. *Peer-to-Peer Networking and Applications*, *8*(6), 1122–1132. doi:10.1007/s12083-014-0255-5.
38. Chen, L., Lu, R., Cao, Z., AlHarbi, K., & Lin, X. (2014). MuDA: Multifunctional data aggregation in privacy-preserving smart grid communications. *Peer-to-Peer Networking and Applications*, *8*(5), 777–792. doi:10.1007/s12083-014-0292-0.
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 Transactions on Parallel and Distributed Systems*, *23*(9), 1621–1632. doi:10.1109/TPDS.2012.86.
40. Li, F. F., Luo, B., & Liu, P. (2010). Secure information aggregation for smart grids using Homomorphic encryption. In IEEE SmartGridComm (pp. 327–332). doi:10.1109/SMARTGRID.2010.5622064. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5622064.
41. Busom, N., Petrlic, R., Sebé, F., Sorge, C., & Valls, M. (2015). Efficient smart metering based on homomorphic encryption. *Computer Communications*. doi:10.1016/j.comcom.2015.08.016. http://www.sciencedirect.com/science/article/pii/S0140366415003151.
42. Rottondi, C., Verticale, G., & Capone, A. (2013). Privacy-preserving smart metering with multiple data Consumers. *Computer Networks*, *57*(7), 1699–1713. doi:10.1016/j.comnet.2013.02.018.
43. Garcia, F. D., & Jacobs, B. (2011). Privacy-friendly energy-metering via homomorphic encryption. In *Lecture notes in computer science* (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics), vol. 6710 LNCS (pp. 226–238). doi:10.1007/978-3-642-22444-7_15.
44. Mahmoud, M. M. E. A., Misic, J., Akkaya, K., & Shen, X. (2015). Investigating public-key certificate revocation in smart grid. *IEEE Internet of Things Journal*, *2*(6), 490–503. doi:10.1109/JIOT.2015.2408597.
45. Ferrag, M. A., Maglaras, L. A., Janicke, H., & Jiang, J. (2016). A survey on privacy-preserving schemes for smart grid communications. Preprint. arXiv:1611.07722.
46. Balli, M., Uludag, S., Selcuk, A., & Tavli, B. (2017). Distributed multi-unit privacy assured bidding (PAB) for smart grid demand response programs. *IEEE Transactions on Smart Grid*. doi:10.1109/TSG.2017.2651029.
47. Zhang, Y., Zhao, J., & Zheng, D. (2017). Efficient and privacy-aware power injection over AMI and smart grid slice in future 5G networks. *Mobile Information Systems*. doi:10.1155/2017/3680671.
48. Choi, D., Lee, S., Won, D., & Kim, S. (2010). Efficient secure group communications for SCADA. *IEEE Transactions on Power Delivery*, *25*(2), 714–722. doi:10.1109/TPWRD.2009.2036181.
49. Mahmoud, M. M. E. A., Misic, J., & Shen, X. (2013). Efficient public-key certificate revocation schemes for smart grid. In *GLOBECOM—IEEE global telecommunications conference* (pp. 778–783). doi:10.1109/GLOCOM.2013.6831167.
50. Rottondi, C., & Verticale, G. (2015). Privacy-friendly load scheduling of deferrable and interruptible domestic appliances in smart grids. *Computer Communications*, *58*, 29–39. doi:10.1016/j.comcom.2014.08.003.
51. Gong, Y., Cai, Y., Guo, Y., & Fang, Y. (2015). A privacy-preserving scheme for incentive-based demand response in the smart grid. *IEEE Transactions on Smart Grid* 1. doi:10.1109/TSG.2015.2412091. http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=7069275.
52. Jo, H. J., Kim, I. S., & Lee, D. H. (2016). Efficient and privacy-preserving metering protocols for smart grid systems. *IEEE Transactions on Smart Grid*, *7*(3), 1732–1742. doi:10.1109/TSG.2015.2449278.
53. Diao, F., Zhang, F., & Cheng, X. (2015). A privacy-preserving smart metering scheme using linkable anonymous credential. *IEEE Transactions on Smart Grid*, *6*(1), 461–467. doi:10.1109/TSG.2014.2358225.
54. Tan, X., Zheng, J., Zou, C., & Niu, Y. (2016). Pseudonym-based privacy-preserving scheme for data collection in smart grid. *International Journal of Ad Hoc and Ubiquitous Computing*, *22*(2), 120–127. doi:10.1504/IJAHUC.2016.077203.
55. Sun, Y. (2016). An improved password authentication scheme for telecare medical information systems based on chaotic maps with privacy protection. *Journal of Information Hiding and Multimedia Signal Processing*, *7*(5), 1006–1019.
56. Zhu, H., Zhu, D., & Zhang, Y. (2016). A multi-server authenticated key agreement protocol with privacy preserving based on chaotic maps in random oracle model. *Journal of Information Hiding and Multimedia Signal Processing*, *7*(1), 59–71.
57. Bera, S., Misra, S., & Rodrigues, J. J. (2015). Cloud computing applications for smart grid: A survey. *IEEE Transactions on Parallel and Distributed Systems*, *26*(5), 1477–1494. doi:10.1109/TPDS.2014.2321378. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6809180.
58. Han, D.-M., & Lim, J.-H. (2010). Smart home energy management system using IEEE 802.15.4 and ZigBee. *IEEE Transactions on Consumer Electronics*, *56*(3), 1403–1410. doi:10.1109/TCE.2010.5606276.
59. Hwang, I. K., Lee, D. S., & Baek, J. W. (2009). Home network configuring scheme for all electric appliances using ZigBee-based integrated remote controller. *IEEE Transactions on Consumer Electronics*, *55*(3), 1300–1307. doi:10.1109/TCE.2009.5277992.
60. Du, D. H.-C., & For, E. (2013). Non-repudiation in neighborhood area networks for smart grid. *IEEE Communications Magazine*, *51*(1), 18–26. doi:10.1109/MCOM.2013.6400434. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6400434.
61. Boneh, D., & Franklin, M. (2003). Identity-based encryption from the Weil pairing. *SIAM Journal on Computing*, *32*(3), 586–615. doi:10.1137/S0097539701398521.
62. Boneh, D., Raghunathan, A., & Segev, G. (2013). Function-private identity-based encryption: Hiding the function in functional encryption. In *Lecture notes in computer science* (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics), vol. 8043 LNCS (pp. 461–478). doi:10.1007/978-3-642-40084-1_26.
63. Joye, M., & Neven, G. (2009). *Identity-based cryptography* (Vol. 2). Amsterdam: IOS Press.
64. Scott, M. (2011). On the efficient implementation of pairing-based protocols. In *Lecture notes in computer science* (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics), Vol. 7089 LNCS (pp. 296–308). doi:10.1007/978-3-642-25516-8_18.
65. Lynn, B. (2006) The pairing-based cryptography library. https://crypto.stanford.edu/pbc/.
66. Bose, S. K. (2002). *An introduction to queueing systems*. Berlin: Springer Science & Business Media. doi:10.1007/978-1-4615-0001-8.



Mohamed Amine Ferrag received the Bachelor's degree (June, 2008), Master's degree (June, 2010) and Ph.D. degree (June, 2014) from Badji Mokhtar-Annaba University, Algeria, all in Computer Science. Since October 2014, he is an assistant professor at the Department of Computer Science, Guelma University, Algeria. He is also affiliated as a Researcher member (Since October 2010) with Networks and Systems Laboratory—LRS, Badji Mokhtar—Annaba University, Algeria. His research interests include wireless network security, network coding security, and applied cryptography. He is currently serving on various editorial positions such as Editorial Board Member in Computer Security Journals like *International Journal of Information Security and Privacy (IGI Global), International Journal of Internet Technology and Secured Transactions (Inderscience Publishers)*, and *EAI Endorsed Transactions on Security and Safety (EAI)*. He has served as an Organizing Committee Member (Track Chair, Co-Chair, Publicity Chair, Proceedings Editor, Web Chair) in numerous international conferences like ICNAS'13, ICNAS'15, ASD'16, EUSPN 2017, (AINIS) Symposium, ANT 2017, SEIT-17, and IEEE ICCE'118. Dr. Ferrag is Editor of the book "*Security Solutions and Applied Cryptography in Smart Grid Communications*". He has served as Technical Program Committee (TPC) Member in ANT'15, IEEE GlobeCom'15, CyberSec'16, IEEE ANTS'16'17, IEEE ICEMIS'16, ANT'17, IEEE INFOCOM SCAN-2017, etc. He is a member of the IEEE Technical Committee on Security & Privacy and a member of the IEEE Cyber Security Community. He received some awards for his reviewing activities like Awarded Elsevier Outstanding Reviewer.