Lightweight Security and Privacy Preserving Scheme for Smart Grid Customer-Side Networks

Asmaa Abdallah and Xuemin Shen, *Fellow, IEEE*

***Abstract*—Information security and customers' privacy in smart grid are significant concerns. Existing security and privacy preserving schemes consider that the consumption reports for electricity consumption aggregation and billing purposes are sent periodically. These periodic messages increase the computation and communication burden on restricted-capabilities smart meters. In this paper, we propose a lightweight security and privacy preserving scheme that is based on forecasting the electricity demand for a cluster of houses in the same residential area; it limits the cluster's connection with electricity utility only when the cluster needs to adjust its total demand. The scheme efficiently satisfies the security and privacy requirements in customer-side networks, i.e., communication between customers and power utility. At the same time, it significantly reduces the communication and computation overhead. Moreover, the proposed scheme utilizes NTRU cryptosystem to further reduce the computation complexity.**

***Index Terms*—Building area networks (BANs), home area networks (HANs), lattice-based scheme NTRU.**

I. Introduction

SMART GRID is the incorporation between traditional power grid and communication and information technologies, where various networking techniques are utilized to exchange information about grid's conditions and customers' demands between different parties to improve power generation and distribution and reduce electricity losses. Through diverse networking technologies, three main networks are deployed in smart grid: the first type is the home area network (HAN), which is responsible for computing electricity consumption for customers. To perform its task, HAN consists of a smart meter that connects to house's smart appliances in order to aggregate their consumption readings. This aggregated value is forwarded to service provider to calculate the electricity bill. Two other networks are considered HANs: 1) building area networks (BANs); and 2) industrial area networks (IANs). BAN is a connection between several HANs within the same residential area while IAN connects HANs in the same industrial area. The second network is the neighbor area network (NAN) that connects HANs in a specific zone with the main control center (CC) for utility company. NAN forwards electricity consumption reports for the region to CC. The last network is the wide area network (WAN), which is utilized by NANs to forward the electricity reports to CC [2]–[5]. In this paper, we refer to HANs, BANs/IANs, and NANs networks as customer-side network.

The upgrade of power grid exposes it to the cyber security threats that communication networks suffer from, such as malicious attacks to forge the consumption reports, extract personal information, or establish denial of service (DoS) attacks. Security concerns in smart grid can be categorized into three major groups [2], [4], [6]–[8]: the first concern is the network availability. Malicious adversaries can launch availability attacks, DoS attacks, on network's resources. They attempt to block or corrupt network's resources and make them unavailable to legitimate parties. Second, data integrity is a significant concern. In integrity attacks, adversaries attempt to tamper or fabricate the exchanged messages in the grid, such as forging electricity consumption messages. Finally, information privacy is an essential concern especially for customers. Personal information and daily habits can be revealed to outsiders from the electricity consumption pattern for customers.

In this paper, we study the security and privacy threats for smart grid's customer-side networks, i.e., HANs, BANs/IANs, and NANs and propose a lightweight lattice-based security and privacy preserving scheme. Our scheme is based on forecasting the future electricity demand for a cluster of customers in the same residential area; it limits the whole cluster's connection with electricity utility only when the cluster needs to adjust its total electricity share. The proposed scheme guarantees security and privacy demands, i.e., customers privacy, data integrity, and network resources and information availability, for customer-side networks. It is also a lightweight and efficient in terms of communication and computation complexities so that it is suitable for limited-capabilities devices, i.e., smart meters.

The remaining of this paper is organized as follows. Section II discusses related works and existing solutions. Section III introduces our system model, security parameters, and design goals. Section IV reviews lattice-based NTRU scheme and its signing NTRU signature scheme (NSS) scheme. In Section V, we present our proposed scheme. Section VI gives security analysis, while Section VII evaluates the performance of our scheme. Finally, Section VIII concludes this paper.

Manuscript received April 18, 2015; revised May 3, 2015 and June 25, 2015; accepted July 23, 2015. Date of publication August 14, 2015; date of current version April 19, 2017. A preliminary version of this paper was presented at the 2014 IEEE GLOBECOM Conference [1]. Paper no. TSG-00441-2015.

The authors are with the Department of Electrical and Computer Engineering, University of Waterloo, ON N2L 3G1, Canada (e-mail: a3abdall@bbcr.uwaterloo.ca; xsheng@bbcr.uwaterloo.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2015.2463742

II. Related Work

Smart grid encounters new security challenges, which require powerful security schemes. Many studies propose solutions to confront these concerns; these studies can be divided into three categories. First one is connecting smart meters to hardware devices, such as temper-resistance devices or electrical batteries, to conceal the real electricity consumption [9]–[11]. These procedures alleviate the computation and communication load, but it is not practical to connect such expensive devices to each deployed smart meter besides the necessary maintenance operations. Second category is distorting the consumption value by adding noise to the message at smart meter and removing it at CC [12]–[14]. These methods conserve the computation abilities, but suffer from difficulties in reconstructing original data and billing accuracy. Final category utilizes cryptographic schemes to guarantee information security and customers' privacy, such as employing public key infrastructure [15] or key-policy attribute-based encryption [16], [17]. Other studies [18]–[20] utilize the homomorphic feature for certain public key schemes; these schemes aggregate the electricity consumption for a region without revealing the individual consumption values. However, applying public key schemes especially the homomorphic schemes increases the overheads. For instance, the privacy-preserving aggregation scheme based on homomorphic Paillier [19] requires from 100 to 220 ms computational costs as messages' number increased. The homomorphic schemes are not scalable, since their performances degrade as the meters' number increased [8].

Other works propose the authentication schemes [21]–[23] to guarantee information integrity and confidentiality, but the authentication operation increases the computation and communication burden. The lightweight Diffe–Hellman authentication scheme [21], for example, causes an average delay varied from 1 to 10 s as the meters' number increased. Also, the meter should previously have a secret value to create its authentication key. Other studies employ the anonymization techniques to conceal the link between the meter's real identity and its electricity consumption. These techniques are based on issuing two identities (real and pseudorandom) for each device, create binding factors, or attach credentials to prove messages' validity [24], [25]. These methods guarantee users' privacy but increase the overhead, as they perform several processes especially at the setup phase. Moreover, they depend on the presence of a third trusted party most of time.

In addition to aforementioned concerns, existing solutions are based on periodic consumption reports, which deplete devices' resources. Alternatively, in our proposed scheme, messages are only exchanged if total demand of the cluster should be adjusted. Thus, it can significantly reduce communication complexity, as messages are sent occasionally. Similarly, the computation burden is light because of the little number of exchanged messages. Moreover, exploiting lightweight NTRU cryptosystem further reduces computation overhead.

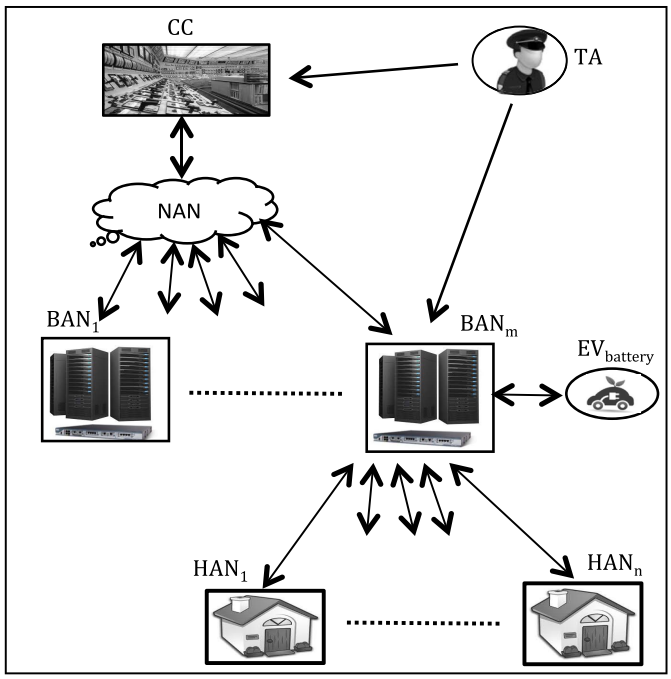

Fig. 1. System model.

III. System Model

A. Network Model

Our system model is shown in Fig. 1. Specifically, we consider a residential area that consists of a number of BANs $= \{\text{BAN}_1, \text{BAN}_2, \ldots, \text{BAN}_m\}$ connected with the main CC via NAN network, which only forwards the messages between BANs in the region and CC without performing any operations. CC is located in the main center for the utility company, and the communication between CC and NAN is through a secured wired connection.

Each BAN has a server with a reasonable memory, processing unit, and a gateway to connect to CC and involved HANs. BAN also connects to a storage unit, which could be the batteries of electric vehicles (EVs) for some of householders in the area. BAN consists of a cluster of HANs $= \{\text{HAN}_1, \text{HAN}_2, \ldots, \text{HAN}_n\}$; we assume that each BAN has up to 100 HANs to further reduce the overhead on BAN's server. HAN could be a house or a unit in a building; each HAN has a smart meter to estimate the electricity consumption of it. The communication between BAN gateways and their HANs is through the inexpensive WiFi technology. Both CC and BAN gateways have public keys provided by a trusted authority (TA). Each smart meter has a unique ID issued by TA and stored in a secured place in its memory. CC considers each BAN as one unit and does not know details about the involved HANs in each BAN.

B. Adversary Model and Security Requirements

We consider that both CC and BANs are honest but curious, i.e., they will not attempt to tamper HANs' data, but they are curious to know the detailed consumption pattern for each user. However, an adversary $\mathscr{A}$ in the region may

try to eavesdrop the exchanged messages between different parties or launch some active attacks, such as falsify the intercepted messages, or begin a replay attack. Moreover, $\mathscr{A}$ can launch a DoS attack to make the server unavailable to authorized users. To prevent $\mathscr{A}$'s malicious actions, the following security requirements should be satisfied.

1) *Customers Privacy:* Users' private information are not revealed to outsiders; $\mathscr{A}$ cannot gain any knowledge about individual consumers in the cluster. Also, CC does not need to know the details of individual user's consumption; it considers only total consumption and total bill for each BAN, as it deals with each cluster as a one unit.
2) *Confidentiality and Messages Integrity:* Users' electricity consumption and billing amounts are protected from any adversary. Even if $\mathscr{A}$ eavesdrops any message, he/she cannot extract any information from it. Additionally, integrity should be guaranteed. If $\mathscr{A}$ attempts to resend/modify a message, this malicious action should be detected. In addition, the BAN's database should be secured against any unauthorized access or modification so that any $\mathscr{A}$ cannot intrude or falsify its records.
3) *Availability:* BAN's server should be available to authorized parties all the time, i.e., DoS attacks are prevented.

C. Design Goals

The objective of the proposed scheme is to preserve the consumers' privacy and information confidentiality in addition to alleviate computation and communication overhead on limited-capabilities smart meters. These objectives can be divided into twofold.

1) The proposed scheme should guarantee security requirements for different parties in the network. Customers' privacy should be secured in addition to assure information integrity and confidentiality. Furthermore, the availability of network's resources should be preserved.
2) It also should be efficient and lightweight communication and computation overhead so that it is applicable for restricted-capabilities smart meters.

IV. Preliminaries

Our proposed scheme exploits NTRU cryptosystem [26], [27], which is a lattice-based alternative for RSA and Elliptic Curve Cryptography public key schemes. In NTRU scheme, encryption and decryption processes are simple polynomial multiplication operations so that NTRU is simple for implementation and very fast compared to other asymmetric schemes. In addition, NTRU scheme is efficiently secure against powerful attacks, such as lattice-basis reduction attacks and attacks through quantum computers.

A. NTRU Cryptographic Scheme

NTRU utilizes the hardness of shortest vector problem (SVP) [29] and learning with error (LWE) [30] problem. We utilize the revised version of NTRU [33] that exploits the worst-case lattice to define the secret key parameters.

1) NTRU Cryptosystem:

a) Notation: Let n be a power of 2, $\Phi = xn + 1$, $R = \mathbb{Z}[x]/\Phi, q$ is a prime number that Φ has n linear factors mod q $(q = 1 \bmod 2n) : \Phi = \prod_{i\le n} \Phi_i = \prod_{i\le n}(x - \Phi_i) \bmod q, R_q = R/qR = \mathbb{Z}[x]_q/\Phi$, and $R_q^{\times}$ is the set of invertible elements of R_q.

b) Key generation: Let $n, q \in \mathbb{Z}, p \in R_q^{\times}$, and $\sigma \in \mathbb{R}$. The pair $(\mathrm{sk}, \mathrm{pk}) \in R \times R_q^{\times}$ is generated by sampling value $\acute{f}$ from the discrete Gaussian distribution $D_{\mathbb{Z}^n,\sigma}$, where $\sigma > Poly(n) \cdot q^{1/2+\epsilon}$ for an arbitrary $\epsilon > 0$, compute the secret key f by

$$f = p \cdot \acute{f} + 1 \tag{1}$$

where $(f \bmod q) \in R_q^{\times}$, and $f = 1 \bmod p$, and sample secret value g from $D_{\mathbb{Z}^n,\sigma}$ where $(g \bmod q) \in R_q^{\times}$. Finally, return secret key $\mathrm{sk} = f$ and public key $\mathrm{pk} = h$, where

$$h = pg/f \in R_q^{\times}. \tag{2}$$

c) Encryption: To encrypt a message M, sender S generates two random values $s, e \leftarrow \overline{\Upsilon}_{\alpha}$ and computes ciphertext as

$$C = hs + pe + M \in R_q. \tag{3}$$

d) Decryption: Receiver R decrypts C by secret key f as

$$\acute{C} = f \cdot C \in R_q \tag{4}$$

$$M = \acute{C} \bmod p. \tag{5}$$

2) NTRU Signature Scheme: NSS [28] is a fast authentication and signature scheme; we utilize the new ring-signature NSS scheme [32].

a) Notations: Given a prime dimension N, a modulus q, a key size d, and a verification bound parameter NB, there are two polynomials f and g that are invertible modulo q and satisfy that $d + 1$ of their coefficients equal 1, d coefficients equal -1, and the remaining equal 0. These parameters are used to compute public key for all users

$$h = f^{-1} * g(\bmod q). \tag{6}$$

Then compute the small polynomials (F, G) satisfying

$$f * G - g * F = q. \tag{7}$$

b) Key generation: For user i, a random polynomial $r_i \in R_q$ is selected to set

$$f_i = f * r_i, \quad g_i = g * r_i \tag{8}$$

$$F_i = F * r_i^{-1} \tag{9}$$

$$G_i = G * r_i^{-1}. \tag{10}$$

Then the output $\mathrm{Sk}_i = (f_i, g_i, F_i, G_i)$.

c) Signing process: Signer S hashes the message M to create a random vector $(m_1, m_2)(\bmod q)$ and writes m_1, m_2 in

$$G_i * m_1 - F_i * m_2 = A_i + q * B_i \tag{11}$$

$$-g_i * m_1 + f_i * m_2 = a_i + q * b_i. \tag{12}$$

Then, the signature on M is the polynomial s_i given by

$$s_i = f_i * B_i + F_i * b_i(\bmod q). \tag{13}$$

d) Verification: The verifier V hashes the message M to create the random vector (m_1, m_2), and then computes the value

$$t_i = s_i * h(\text{mod } q). \tag{14}$$

Afterward, V verifies that if the following condition holds:

$$\| s_i - m_1 \|^2 + \| t_i - m_2 \|^2 \leq NB. \tag{15}$$

Then, the signature is valid. Two pairs of keys are used in our proposed scheme to provide higher security level; the first pair is used for encryption and the other one is utilized in signing process.

V. Proposed Scheme

Our proposed scheme is divided into two phases. The first phase is initialization phase, which is responsible for establishing the connection among different parties and initializing the electricity supply agreement. The second phase is message exchange phase, which organizes the electricity consumption operation in BAN's region.

A. Phase 1 (Initialization)

1) Key Generation: TA generates two pairs of keys for CC and BAN gateway as follows.

a) Encryption keys: TA computes CCs secret key f_{cc} as: $f_{cc} = p \cdot \acute{f}_{cc} + 1$, where $(f_{cc} \bmod q) \in R_q^{\times}$ and $f_{cc} = 1 \bmod p$ and samples g_{cc} from $D_{\mathbb{Z}^n,\sigma}$ so that $g_{cc} \bmod q \in R_q^{\times}$. Then, TA computes $h_{cc} = pg_{cc}/f_{cc} \in R_q^{\times}$. So, the pair (h_{cc}, f_{cc}) is CCs encryption public and private keys, respectively.

For BAN gateway, TA computes its secret key f_{ban} as: $f_{ban} = p \cdot \acute{f}_{ban} + 1$, where $(f_{ban} \bmod q) \in R_q^{\times}$ and $f_{ban} = 1 \bmod p$. Then, samples g_{ban} from $D_{\mathbb{Z}^n,\sigma}$ so that $g_{ban} \bmod q \in R_q^{\times}$. Next, TA computes $h_{ban} = p\, g_{ban}/f_{ban} \in R_q^{\times}$. Then, the pair (h_{ban}, f_{ban}) is BAN's public and private keys.

b) Signing keys: TA chooses polynomials f and g that are invertible modulo q. f and g satisfy that $d + 1$ of their coefficients equal 1, d coefficients equal -1, and the remaining equal 0. TA then computes public key for all users: $h = f^{-1} * g \,(\text{mod } q)$. TA computes small polynomials (F, G), where $f * G - g * F = q$.

To generate signing key for CC, TA selects a random polynomial $r_{cc} \in R_q$ and sets $f_{ccs} = f * r_{cc}$, $g_{ccs} = g * r_{cc}$. Then, TA computes $F_{cc} = F * r_{cc}^{-1}$ and $G_{cc} = G * r_{cc}^{-1}$. Therefore, CCs signing key is $\text{Sk}_{cc} = (f_{ccs}, g_{ccs}, F_{cc}, G_{cc})$.

To generate signing key for BAN gateway, TA selects a random polynomial $r_{ban} \in R_q$ and sets $f_{bans} = f * r_{ban}, g_{bans} = g * r_{ban}$. Then, TA computes $F_{ban} = F * r_{cc}^{-1}$ and $G_{cc} = G * r_{cc}^{-1}$. Therefore, BAN's signing key is $\text{Sk}_{ban} = (f_{bans}, g_{bans}, F_{ban}, G_{ban})$.

2) Demand Forecast: The approximate requirement of electricity for each HAN in the range is computed by a forecasting function, $g()$, from the historical consumption levels of the HAN during a specific time period. For example, $g()$ could be the average electricity consumption every month for the HAN in last five years. Applying $g()$, the average electricity consumption value is calculated for all HANs in BAN's cluster so that $\text{HAN}_1, \text{HAN}_2, \ldots, \text{HAN}_n$ have the amounts $x_1, x_2, \ldots, x_n$, respectively, where $x_i = g(\text{HAN}_i)$ and n is the number of HANs in BAN region. BAN is responsible for applying $g()$ to obtain the electricity share for each HAN. BAN stores the ID for each HAN and the corresponding pair of electricity demand and current price in its database, ID_i, x_i, pc. BAN then aggregates the total demand for all smart meters in the cluster and computes the total required energy amount for BAN during the billing period

$$x = \sum(x_1, x_2, \ldots, x_n) + \epsilon \tag{16}$$

where ϵ is an extra amount of electricity used as backup.

a) Backup value calculation: After applying $g()$, BAN needs to set a value for ϵ as: each BAN gateway connects to a fixed number of HANs m, which runs from 1 to 100 HANs. Also, BAN can predict the expected number of EVs in the area $N_{\text{EV}-\text{expected}}$. Assume that the available capacity for EV_i to store electricity is C_i, which is known for each EV. So, BAN can compute the total expected available capacity to store extra power as

$$C_{\text{EV}} = \sum_i C_i$$

where i run from 1 to $N_{\text{EV}-\text{expected}}$. Then, ϵ is calculated as a ratio of C_{EV}

$$\epsilon = r * C_{\text{EV}}$$

where $0 < r \leq 1$ is a scaling factor. The value of r increases when the number of involved HANs m increases, because more HANs in the cluster requires more backup value for emergency cases. So, as the number of HANs increases, ϵ increases.

During initialization phase, BAN needs to select the optimal number of EVs to work as a storage unit for the cluster. The optimal number of EVs to store ϵ can be computed by

$$\begin{aligned} &\min \quad N_{\text{EV}}(m) \\ &\text{subject to} \\ &\quad \epsilon(m) \leq \sum\nolimits_i C_i(m), i \in \{1, \ldots, N_{\text{current}}(m)\} \\ &\quad N_{\text{EV}}(m) \leq N_{\text{current}}(m), N_{\text{current}}(m) \in \{1, \ldots, N_{\text{Max}}(m)\}, \\ &\quad \text{and } m \in \{1, \ldots, 100\}. \end{aligned} \tag{17}$$

N_{EV} is the optimal number of EVs to store ϵ; $\epsilon(m)$ is the total required electricity backup value for the cluster when the number of HANs equals m, where m can run from 1 to 100 HANs within the same cluster; $C_i(m)$ is the available capacity storage for electricity in EV_i; $i = 1, \ldots, N_{\text{current}}$, where N_{current} is the number of EVs that are currently available in the cluster's region from the total number of EVs in the cluster N_{Max}. This optimization model computes the optimal (minimum) number of EVs to store ϵ for BAN's cluster in the case of different number of HANs. ϵ is stored in BAN's storage unit, i.e., number of EVs owned by householders, for emergency. If HANs require more electricity than the assigned share and BAN gateway cannot satisfy the extra share, it supplies the extra electricity from ϵ. However, these cases rarely happen, because the electricity share for each HAN is predefined via accurate forecasting function, and any increase/decrease in the demand is expected to be within a limited range. In certain situations, when one HAN asks for increasing its share,

another one may want to decrease the share; so, BAN transfers electricity between them without using ϵ. Generally, if all HANs want to increase their shares, the increase is expected to be within ϵ. But, if the total share's increase is beyond ϵ, a specific procedure is activated to satisfy it.

3) Electricity Agreement: BAN considers x as its fixed demand per month. BAN gateway is responsible now for accomplishing an agreement with CC to supply the connected HANs with their electrical needs per month. CC deals with BAN as a one unit; it has no information about individual HANs in BAN's range.

a) Agreement request message:

i) At BAN gateway: BAN gateway establishes the connection by sending an agreement request message m_a to CC; BAN signs the electricity amount x, and encrypts it by CCs public key to provide m_a. BAN hashes x to create $(x_1, x_2)(\text{mod } q)$ and write

$$G_{\text{ban}} * x_1 - F_{\text{ban}} * x_2 = A_{\text{ban1}} + q * B_{\text{ban1}}$$
$$-g_{\text{bans}} * x_1 + f_{\text{bans}} * x_2 = a_{\text{ban1}} + q * b_{\text{ban1}}.$$

The signature on x is the polynomial s_{ban_1} given by

$$s_{\text{ban}_1} = f_{\text{bans}} * B_{\text{ban1}} + F_{\text{ban}} * b_{\text{ban1}}(\text{mod } q).$$

The result is (x, s_{ban_1}). Then, BAN computes $m_1 = x\|s_{\text{ban}_1}\|T_{s1}\|k_1$, where T_{s1} is time stamp and k_1 is a random nonce; they are used to prevent replay attacks. Next, BAN encrypts the message m_1 by CCs public key. BAN sets two random values s_1 and $e_1 \leftarrow \overline{\Upsilon}_\alpha$, and uses h_{cc} to obtain the cipher text, $m_a = h_{\text{cc}}s_1 + pe_1 + m_1 \in R_q$. Subsequently, BAN gateway sends the agreement request message m_a to CC.

ii) At CC: CC decrypts the received message by its private key. First, CC calculates $\acute{m}_1 = f_{\text{cc}}\, m_a \in R_q$, then $m_1 = \acute{m}_1 \bmod p$. Second, CC verifies BAN's signature s_{ban_1} on the message $m_1 = x\|s_{\text{ban}_1}\|T_{s1}||k_1$; CC hashes the message x to create a random vector $(x_1, x_2)(\text{mod } q)$, computes $t_{\text{ban}_1} = s_{\text{ban}_1} * h(\text{mod } q)$, and verifies that $\| s_{\text{ban}_1} - x_1 \|^2 + \| t_{\text{ban}_1} - x_2 \|^2 \leq NB$. If this condition holds, then the signature is valid. Subsequently, CC checks the validity of timestamp T_{s1} and nonce k_1, and accepts the message if they are acceptable. CC receives many agreement requests from different BANs; it compares the expected total electricity demand for the area with the expected electricity supply and attempts to balance between them. CC should have enough power generation resources to satisfy the electricity requirement for all BANs in the region during the billing period, i.e., one month.

b) Agreement response message:

i) At CC: If CC accepts BAN's request, it encrypts the value y, $y = (x, p_e)$, which contains the assigned electricity amount x and the expected price p_e, to obtain the agreement response message m_r. Then, it sends m_r to BAN.

ii) At BAN: BAN receives m_r and decrypts it using its private key and verifies CCs signature. Then, BAN checks the timestamp and nonce validity. Now, BAN guarantees the electricity share x from CC during the whole billing period and knows approximately the expected bill.

B. Phase 2 (Exchange Message)

At the beginning, BAN gateway supplies each HAN by a specific electricity share based on the previously calculated amount. BAN computes the current payment b_i for each HAN_i by: $b_i = x_i * p * T_j$, where x_i is the electricity share for HAN_i, p is the current electricity price, and T_j is the time period that the HAN_i consumes its share x_i by the price p. BAN gateway encrypts b_i before storing it in the database, e.g., $b_i = E(b_i)$. Only the BAN's operator knows the exploited key and can decrypt the stored values.

1) Demand Change:

a) At HAN: If HAN wants to change (increase/decrease) the current share to a new share $x_{i-\text{new}}$, it sends a demand message m_d to BAN gateway. First, a timestamp T_{s3} and nonce k_3 are attached to m_d to prevent replay attacks; $m_3 = x_{i-\text{new}}\|\text{Id}_i\|T_{s3}\|_{k3}$. Next, HAN_i encrypts the message m_3 by BAN's public key. HAN_i sets two random values s_3 and $e_3 \leftarrow \overline{\Upsilon}_\alpha$; using h_{ban}, it obtains: $m_d = h_{\text{ban}}s_3 + pe_3 + m_3 \in R_q$. Subsequently, HAN_i sends demand message m_d to BAN.

b) At BAN: BAN gateway decrypts the message m_d. First, BAN calculates: $\acute{m}_3 = f_{\text{ban}} \cdot m_d \in R_q$, and then computes $m_3 = \acute{m}_3 \bmod p$. Note that the demand message sends only when the power demand for HAN is altered. Thus, the communication overhead is light. BAN supplies HAN with the new share and computes new payment for it: $b_{i-\text{new}} = x_{i-\text{new}} * p * T_j$. BAN encrypts $b_{i-\text{new}}$, and then stores it with pervious payment values in HANs record in BAN's database.

2) Price Change: When the electricity price changes, BAN receives a price message from CC with the new price p_{new}; this message is broadcasted to all connected BANs. $p_{\text{new}} = p_n\|T_{s3}\|k_3$, where p_n is the new price, T_{s3} is a timestamp and k_3 is a random nonce. The price message is sent in plaintext; it is only signed by CCs public key: CC hash p_{new} to create $(p_{\text{new1}}, p_{\text{new2}})(\text{mod } q)$, and write

$$G_{\text{cc}} * p_{\text{new1}} - F_{\text{cc}} * p_{\text{new2}} = A_{\text{cc2}} + q * B_{\text{cc2}}$$
$$-g_{\text{ccs}} * p_{\text{new1}} + f_{\text{ccs}} * p_{\text{new2}} = a_{\text{cc2}} + q * b_{\text{cc2}}.$$

The signature on p_{new} is the polynomial $s_{\text{cc}_2} = f_{\text{ccs}} * B_{\text{cc2}} + F_{\text{cc}} * b_{\text{cc2}}(\text{mod } q)$. The result is the pair $(p_{\text{new}}, s_{\text{cc}_2})$.

a) At BAN: When BAN receives $(p_{\text{new}}, s_{\text{cc}_2})$, it checks the validity of CCs signature s_{cc_2} on $p_{\text{new}} = p_n\|T_{s3}\|k_3$: BAN hashes the message p_{new} to create a random vector $(p_{\text{new1}}, p_{\text{new2}})(\text{mod } q)$, then computes $t_{\text{cc}_2} = s_{\text{cc}_2} * h(\text{mod } q)$, and verify that $\| s_{\text{cc}_2} - p_{\text{new1}} \|^2 + \| t_{\text{cc}_2} - p_{\text{new2}} \|^2 \leq NB$. If this condition holds, then the signature is valid. Next, BAN checks the validity of T_{s3} and k_3; if they are valid, BAN gateway ensures that the message is legitimate. But, HANs in BAN's range has no connection with CC; they only trust BAN gateway. So, BAN signs p_{new} by its signing key and then forwards the pair $(p_{\text{new}}, s_{\text{ban}_2})$ to the connected HANs.

b) At HAN: When HAN receives $(p_{\text{new}}, s_{\text{ban}_2})$, it checks BAN's signature s_{ban_2} validity: HAN hashes message p_{new} to create a random vector $(p_{\text{new1}}, p_{\text{new2}})(\text{mod } q)$, and compute the value $t_{\text{ban}_2} = s_{\text{ban}_2} * h(\text{mod } q)$. Verify that $\| s_{\text{ban}_2} - p_{\text{new1}} \|^2 + \| t_{\text{ban}_2} - p_{\text{new2}} \|^2 \leq NB$. If this condition holds, then the signature is valid. Next step, HAN checks the validity of T_{s4} and k_4;

if they are valid, HAN gateway ensures that the message is legitimate. Notice that the message is sent only when the electricity price changes. If any HAN needs to alter its electricity consumption considering the new price, then it sends a demand message m_d to BAN gateway asking for a new electricity share $x_{i-\text{new}}$. The demand message is sent only when HAN wants to update its electricity share, i.e., the consumed electricity in HAN increases/decreases. BAN gateway still supplies HAN by the last requested amount of electricity until HAN sends new m_d.

3) Billing Process: BAN gateway computes the payment values for each HAN by multiplying consumed amount by current electricity price and accumulates it with previous values, and saves the result in HANs record in the database. These records help in tracking the payment amounts for HANs during the billing period to assure accountability. At the end of billing period, BAN computes the total bill for each HAN $B_i (B_i = \sum_l b_l)$, and aggregates the region's total bill $S (S = \sum_i B_i)$. The billing message S is signed by BAN's private key and encrypted using CCs public key: BAN hash S to create $(S_1, S_2) (\text{mod}\, q)$ and writes

$$G_{\text{ban}} * S_1 - F_{\text{ban}} * S_2 = A_{\text{ban3}} + q * B_{\text{ban3}}$$
$$-g_{\text{bans}} * S_1 + f_{\text{bans}} * S_2 = a_{\text{ban3}} + q * b_{\text{ban3}}.$$

The signature on S is $s_{\text{ban}_3} = f_{\text{bans}} * B_{\text{ban3}} + F_{\text{ban}} * b_{\text{ban3}} (\text{mod}\, q)$. The result is (S, s_{ban_3}). Then, BAN computes $m_5 = S \| s_{\text{ban}_3} \| T_{s5} \| k_5$. Next, BAN encrypts m_5. BAN sets two random values s_5 and $e_5 \leftarrow \overline{\Upsilon}_\alpha$, and uses h_{cc} to obtain: $m_b = h_{\text{cc}} s_5 + p e_5 + m_5 \in R_q$. Subsequently, BAN gateway sends the billing message m_b to CC.

a) At CC: CC uses f_{cc} to decrypt m_b. CC then verifies BAN's signature s_{ban_3}, and checks the validity of timestamp and nonce, and accepts the message if they are acceptable.

C. Electricity Share Adjustment Procedure

Electricity share adjustment procedure is a procedure to handle the case when the fixed assigned share for BAN (x) does not fit the current electricity requirements (y). As in Algorithm 1, there are four different cases.

- Case 1: If x is slightly larger than y, then the extra electricity is stored in EVs' batteries.
- Case 2: If x is slightly smaller than y, then remaining demand of electricity is consumed from stored power in EVs.
- Case 3: If x is much smaller than y and EVs' batteries cannot cover the remaining demand, BAN gateway asks for more electricity from CC.
- Case 4: If x is much larger than y and EVs' batteries does not have a room for the remaining demand of electricity, BAN gateway sells the extra power to CC.

As the accuracy of employed forecasting function increases, the probability for cases 3 and 4 to occur decreases. However, if case 3 or 4 is repeated, BAN will ask CC to change its fixed value x in the agreement to y.

Algorithm 1 BAN Electricity Share Adjustment Procedure

```
BAN Electricity Share Adjustment Procedure
x: The fixed demand for BAN
y: The current actual demand for BAN
z: The EV remaining capacity
β:β = ‖x − y‖ The difference between x and y
if (x > y & β < z) then
    β → EV_battery
else if (x < y & β < z) then
    β ← EV_battery
else if (x < y & β > z) then
    β ← z ← CC
else if (x < y & β > z) then
    β → z → CC
end if
```

VI. Security Analysis

The proposed scheme is expected to preserve customers' privacy in the cluster. In addition, it guarantees the security requirements: confidentiality, integrity, availability, authenticity, and accountability. This section analyzes the security characteristics of our proposed scheme.

Customers Privacy is Preserved: Private information that clearly identifies the customers' habits or life style is preserved in the proposed scheme. CC does not know the electricity consumption for each customer in BAN; instead, it receives the bill for the whole BAN S as a one unit. In other words, the individual bills b_is are not exposed to any party outside BAN even the utility. Consequently, any outsider cannot obtain any information about each customer's bill. Moreover, the outsider adversaries cannot know the total bill S, because the billing message is encrypted by CCs public key and CC only can decrypt it. For the adversaries who attempt to compromise the exchanged messages between BAN gateway and different parties, they cannot reveal any information since the exchanged messages between BAN and CC are encrypted using BAN and CCs public keys. Similarly, the messages from HANs to BAN are encrypted by BAN's public key. As a result, no unauthorized party can decrypt these messages.

For instance, an adversary $\mathscr{A}$ intercepts the demand request sent from HAN_i to BAN, and tries to detect its share x_i, $\mathscr{A}$ cannot acquire any knowledge about x_i, because the demand message is encrypted by h_{ban}, and only BAN gateway has the decryption key f_{ban}. It is an NP-hard problem to extract f_{ban} from h_{ban}. Even if $\mathscr{A}$ has unlimited computation resources, more powerful than quantum computers, and could compromise f_{ban}, and detect x_i, then he/she also cannot extract any private information about HAN_i, because x_i is HAN_i's share in a relatively large time period and does not reveal the detailed user's consumption pattern. According to BAN's database, it is located in a secured place; no attacker can reach to it. However, if an attacker attempts to compromise the database, he/she needs to discover the applied encryption key to decrypt its contents. Suppose $\mathscr{A}$ succeed to obtain the record for a specific customer from the database, $\mathscr{A}$ knows only the electricity needs for this customer for a long period of time (from

one month to 6 h) and cannot acquire any detailed information about the real-time electricity consumption pattern for that consumer.

Messages' Confidentiality is Guaranteed: The confidentiality of exchanged messages is guaranteed in the proposed scheme; the agreement messages between CC and BAN are confidential because of using public keys for CC and BANs. Also, the messages from HANs to BAN are encrypted using BAN's public key. If $\mathscr{A}$ tries to impersonate a smart meter to compromise its messages, he/she fails because the smart meter's ID is stored in a secure place, and $\mathscr{A}$ cannot obtain it. As a result, no impersonation attacks succeed. According to price message, if $\mathscr{A}$ intercepts it, it is not a concern, because he/she can only know the current price of electricity, which is not secret, but cannot modify the message, as it is signed by BAN's private key. Moreover, the message cannot be resend again by $\mathscr{A}$ because of the involved timestamp and nonce values. No man in the middle (MITM) attacks success. If $\mathscr{A}$ only eavesdrops the messages as in passive MITM attack, he/she cannot decrypt the messages. While in active MITM attack, if $\mathscr{A}$ attempts to modify/falsify the message, the attack is detected, as $\mathscr{A}$ cannot mimic BAN's signature or discover the secret IDs for smart meters.

Messages' Integrity is Assured: The messages from CC/BAN are hashed and signed using its signing key. While the messages from smart meters contain the hashed value of their secret IDs; only BAN can check the validity of smart meter's ID by comparing it with the corresponding ID stored in its database. The integrity of the stored data in the database is assured too; if any attacker attempts to modify the stored data, BAN's operator will detect the attack, because the stored data are encrypted by a secret key known only to the operator.

Authenticity for Different Parties is Guaranteed: Both CC and BAN are authenticated by their public keys. Therefore, the messages encrypted/signed by them are authenticated. As well, the attached unique IDs authenticate smart meters' demand messages.

Availability of Resources is Confirmed: BAN gateway is always available and no DoS attacks succeed. DoS attack may be launched by a malicious node that sends a huge number of messages to the server until it goes down. In each BAN, there is a specific number of HANs that provides a limited number of messages, and BAN's server capabilities are prepared to deal with that number; this expected number of received messages cannot cause overflow or congestion. Consequently, if BAN notes that the number of messages is larger than expected or an individual HAN sends a huge number of messages, BAN does not respond to these requests and isolates the malicious HAN. For instance, consider a BAN's cluster with 80 HANs and the price is expected to change three times a day. Then, BAN gateway assumes that all HANs will send a demand change message for every price change (e.g., three demand messages per HAN per day). Therefore, the maximum number of demand messages that BAN gateway can receive when the price changes is 80, and the total number of demand messages during the day is around 240. Accordingly, if BAN gateway receives a large number of messages in a short period of time, it discards the messages and blocks the malicious HAN.

Accountability and Tracking Historical Processes are Guaranteed: If any householder wants to validate of the bill's value, he/she can check his/her monthly record in BAN's database. HANs record indicates the amount of consumed electricity and the corresponding price. These records assure the correctness of payment amount for each HAN in BAN.

The limited number of transmitted messages enhances security and customer's privacy and reduces adversary's chance to acquire any knowledge about the system. In addition, the deployed NTRU cryptosystem prevents attackers from extracting any knowledge about private keys from the corresponding public keys or any intercepted message. Suppose an $\mathscr{A}$ with reasonable computation capabilities captures a message exchanged between BAN gateway and CC or between BAN and one of the HANs, such as the billing message m_b sent from BAN to CC. $\mathscr{A}$ cannot extract any information from the message, because $\mathscr{A}$ needs to knows CCs private key f_{cc} to decrypt m_b and obtains $m_5 (m_5 = \acute{m}_5 \bmod p$ and $\acute{m}_5 = f_{\text{cc}} \cdot m_b \in R_q)$. In addition, $\mathscr{A}$ cannot modify the message, as he/she requires BAN's private signing key parameters $(f_{\text{bans}}, g_{\text{bans}})$ to forge its signature on the message. $\mathscr{A}$ also cannot resend the message, as it contains a timestamp and nonce number. CC and BANs' secret parameters $(f_{\text{cc}}, g_{\text{cc}}, f_{\text{ccs}}, g_{\text{ccs}}, f_{\text{ban}}, g_{\text{ban}}, f_{\text{bans}}, g_{\text{bans}})$ are designated exploiting the hardness of SVP and LWE problems. If $\mathscr{A}$ attempts to compromise CCs private key f_{cc}, he/she requires to check all the nonzero vectors in $R \times R_q$ field, and according to SVP, if a lattice L with norm $\mathscr{N}$ and a basis of a vector space V are given, it is an NP-hard problem to find the shortest nonzero vector υ in V, given that $\mathscr{N}(\upsilon) = \lambda(L)$, even by the powerful lattice basis reduction algorithms. Even if $\mathscr{A}$ manages to formulate a number of approximate equations n to determine f_{cc}, the problem will be converted to LWE problem as

$$\begin{aligned} \langle f_{\text{cc}}, a_1 \rangle &\approx_{\chi} b_1 (\bmod p) \\ \langle f_{\text{cc}}, a_2 \rangle &\approx_{\chi} b_2 (\bmod p) \\ &\cdots\cdots \\ \langle f_{\text{cc}}, a_n \rangle &\approx_{\chi} b_n (\bmod p). \end{aligned}$$

Then, $\mathscr{A}$ requires $2^{O(n)}$ equations/time using best known algorithm to solve LWE problem to obtain f_{cc} value, which is an NP-hard problem [31]. Consequently, $\mathscr{A}$ cannot compromise the secret key f_{cc} even via a quantum computer. As a result, the data confidentiality and integrity are guaranteed. In addition, the authenticity of different parties is confirmed.

In conclusion, our proposed scheme preserves customers' privacy and fulfills different security requirements for the involved parties in customer-side network.

VII. Performance Evaluation

This section studies communication and computation complexity for our scheme.

A. Communication Overhead

The number of exchanged messages between different parties (CC, BAN, and HANs) is very small. During initialization phase, CC and each BAN are exchanging two messages to

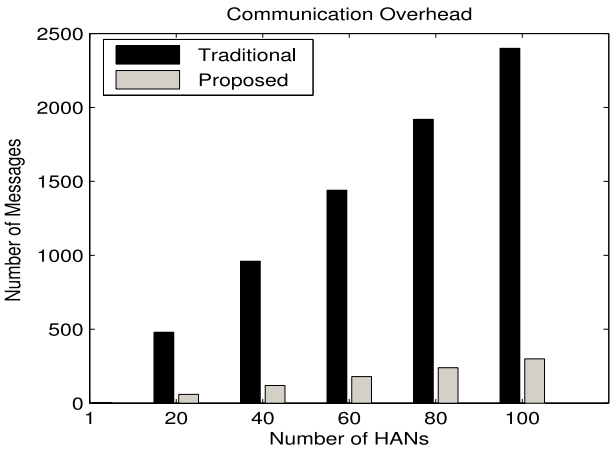

Fig. 2. Communication overhead traditional versus proposed scheme.

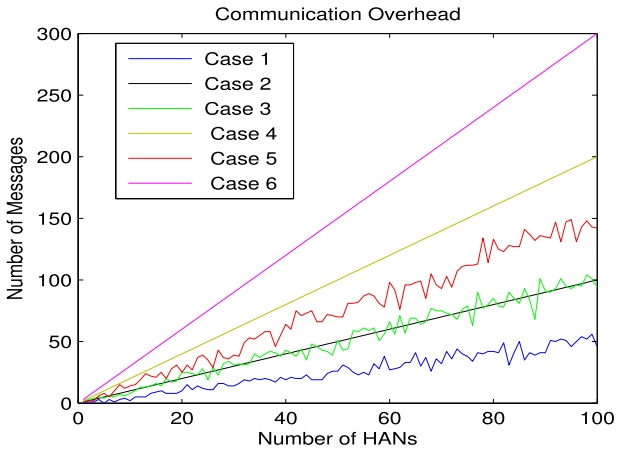

Fig. 3. Communication overhead for proposed scheme different cases.

setup the electricity-share agreement, but HANs do not participate in this phase. In second phase, HANs send demand messages only if they require altering their electricity share due to change in HANs' consumption or in electricity price. Note that HANs electricity share may remain the same during the whole billing period; therefore, no demand messages are sent. Furthermore, two price messages are disseminated only in case of price modification; first one is broadcasted from CC to connected BANs; and second message is forwarded from BAN to its HANs. In addition, BAN should send one billing message to CC indicating the payment amount for whole BAN. However, this message is sent once at the end of billing period, i.e., every month.

Consequently, the total number of messages is changed from three messages (two agreement messages and one billing message) to $d+3$ messages, where d is the number of demand messages during the month. Therefore, d is a small number as the electricity share for each HAN is not expected to change frequently. Since the electricity share is predefined for each HAN, we assume that HAN updates its share when electricity price changes only. If time-of-use pricing plan [34] is used, there are three different prices during the day known as off-peak, mid-peak, and on-peak prices. Therefore, we consider that the maximum number of demand messages is three demand messages per HAN every day. While in the traditional periodic-pattern schemes, each HAN sends its reading message every 1 h or 15 min. Fig. 2 shows communication overhead for our proposed scheme versus a periodic-pattern scheme in terms of different number of connected HANs. As shown, our proposed scheme saves a significant number of messages compared with the traditional periodic schemes. In a cluster of 100 HANs, our scheme requires at maximum 300 demand messages per day, while periodic schemes need 2400 messages (if demand messages are sent every hour).

Fig. 3 shows the variation in communication burden for our proposed scheme at different number of demand messages. Fig. 3 includes six different scenarios.

Case 1: Only portion of HANs send one demand message a day, while the remaining does not send any messages.

Case 2: All HANs send one demand message per day.

Case 3: Number of HANs send two messages, other group of HANs send one message, and the remaining does not send any.

Case 4: All HANs send two demand messages per day.

Case 5: Group of HANs send three messages, other number of HANs send two messages, some HANs send one message, and the remaining does not send any messages.

Case 6: All HANs send three demand messages every day.

Axiomatically, the communication complexity grows as number of demand messages increases but within a limited value. The number of messages rises from one message when the cluster has only one HAN to maximally 300 messages when the cluster has 100 HANs. Thus, the maximum number of messages is no more than 300 messages per month, which is a trivial communication overhead for the network.

B. Computation Complexity

Suppose that computation time for encryption, decryption, signing, and verification operations are T_e, T_d, T_s, and T_v, respectively. During initialization phase in our scheme, CC and each BAN exchange agreement request and agreement response messages. Thus, each of CC and BAN needs to perform one encryption, one decryption, one signing and one verification process. Accordingly, the computation time for this phase is $2*(T_e+T_d+T_s+T_v)$ units. In second phase, if HANs share changes, HAN preforms one encryption operation per each demand message, while BAN decrypts the message. Thus, we have (T_e+T_d) units per message. In case of modified price, two price messages are sent from CC to BANs and from each BAN to its connected HANs. As a consequent, both CC and BAN sign the price message once; as well, BAN and HAN verify the message once. Hence, the computation time for price message is $2*(T_s+T_v)$ units. So, the total computation operations in this phase equals $m*(T_e+T_d)+(2*T_s+(m+1)*T_v)$, where m is the number of HANs in the cluster. During payment process, only billing message is sent from BAN to CC; it requires one encryption, one decryption, one sign and one verification process. The computation time for this

TABLE I
TOTAL COMPUTATION OVERHEAD PER HAN PER MONTH TRADITIONAL VERSUS PROPOSED SCHEME

	Computation Overhead
Traditional	$810 * T_E + 810 * T_D + 810 * T_S + 810 * T_V$
Proposed	$90 * T_E + 90 * T_D + 90 * T_S + 90 * T_V$

message is $(T_e + T_d + T_s + T_v)$ units. While, the performed operations on BAN's database, i.e., computing electricity shares and bills, are trivial computation loads and can be neglected.

We exploits the moderate security mode for public key NTRU cryptosystem with private key = 530 bits, public key = 1169 bits, and plaintext size = 187 bits. For NSS signing parameters, the used private key = 502 bits, public key = 1757 bits, and signature size = 1757 bits. We expect three demand messages per HAN every day in our scenario; each demand message requires two operations: 1) one encryption and 2) one decryption. Also, three price messages are applied; each one requires two signing and two verification operations. BAN also requires three signing and three verification operations every day for the first send of the price message from CC to BAN. Moreover, the second price message from BAN to each HAN requires three signing and three verification operations per day. So, the operations for one HAN per day are three encryption, three decryption, three signing, and three verification operations.

On the other hand, each HAN sends its reading message every hour in the periodic-pattern schemes. Each reading message necessitates four processes: 1) one encryption; 2) one decryption; 3) one signing; and 4) one verification operation. In addition, CC should reply by control message; if we assume these control messages are sent as price changes. Thus, there are three control messages per day for each HAN. As result, each HAN needs 27 encryption, 27 decryption, 27 signing, and 27 verification operations per day. Table I demonstrates the total computation overhead for our proposed scheme versus a periodic-pattern scheme for each HAN per month. As the number of HANs in the cluster increases, the computation overhead increases. Consequently, the total computation operations for the whole cluster in our proposed scheme per month equal $[2 * (T_e + T_d + T_s + T_v)] + 30 * ([3 * m * (T_e + T_d)] + [6 * (T_s) + 3 * (m + 1) * (T_v)]) + [(T_e + T_d + T_s + T_v)] = [(90*m+3)*(T_e+T_d)]+183*T_s+[(90*m+93)*T_v]$ operations, where m is the number of HANs in the BAN cluster. While, the periodic-pattern scheme computes $810*n*(T_e+T_d+T_s+T_v)$ operations per month, where n is the number of connected HANs (we assume that m and n have the same value. However, n value could be much greater that m).

We evaluate the performance of our proposed scheme versus the traditional periodic scheme when both schemes exploit NTRU cryptosystem as encryption scheme and NSS as signing scheme. Fig. 4 compares the worst case of our proposed scheme, when all HANs in the cluster send their maximum number of demand messages, with the moderate case of the traditional scheme, when every HAN sends periodic demand message every hour. It can be seen that there is significant

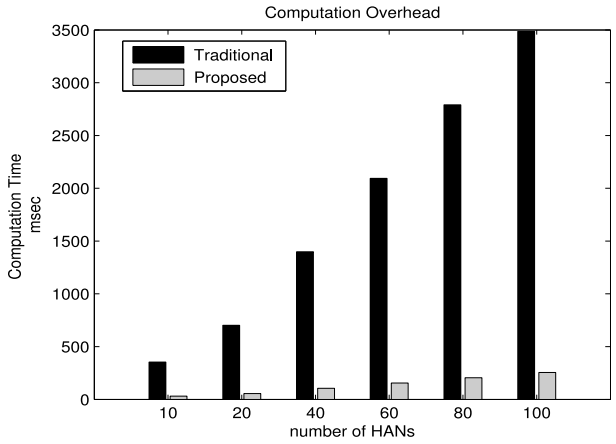

Fig. 4. Computation overhead traditional versus proposed scheme.

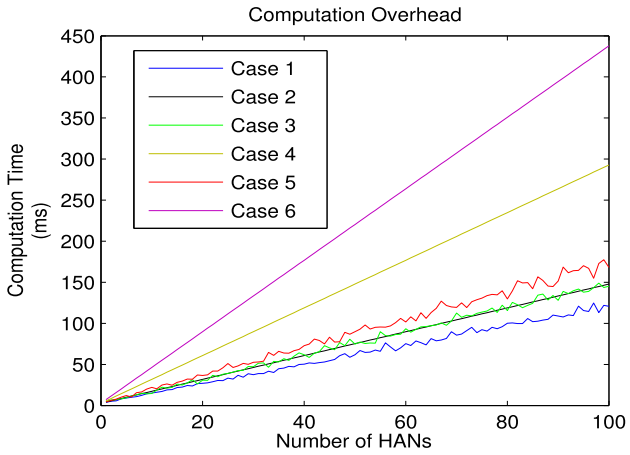

Fig. 5. Computation overhead for proposed scheme different cases.

difference in computation overhead between the two schemes; our proposed scheme consumes much less computation time than the traditional one, especially as the number of HANs increases. In the proposed scheme, the computation delay increases from 8.7 to 255.21 ms per day as the number of HANs increases from 1 to 100. While the traditional scheme computation time increases from 410 to 3486.2 ms per day. Consequently, our proposed scheme remarkably decreases the overall computation time.

If the number of demand messages varies from zero (when the HAN does not want to change its share during the day) to the maximum number of messages (e.g., three messages a day), the total computation operations for the whole cluster in our proposed scheme per month equals $[2 * (T_e + T_d + T_s + T_v)] + 30 * ([d * m * (T_e + T_d)] + [6 * (T_s) + 3 * (m + 1) * (T_v)]) + [(T_e + T_d + T_s + T_v)] = [(30 * d * m + 3) * (T_e + T_d)] + 183 * T_s + [(90 * m + 93) * T_v]$ operations, where m is the number of HANs in the BAN cluster, and d is the number of demand messages, $d \in \{0, 1, 2, 3\}$. Fig. 5 shows the impact of demand messages' number on the computation time in our proposed scheme (Fig. 5 includes the same six cases as in Fig. 3). Although computation complexity rises as number of demand messages increases, this increase is not a heavy computation

overhead on the network's resources. For instance, computation time per day increases from 7.14 ms when the cluster has only one HAN to 225.21 ms as maximum when the cluster has 100 HANs. In conclusion, our proposed scheme not only guarantees security and privacy requirements for customer-side network, but also ensures low communication and computation overhead.

VIII. Conclusion

Consumers privacy and information confidentiality are major concerns for customer-side networks in smart grid. In contrary to the existing solutions, we have proposed a lightweight security and privacy preserving scheme based on predicting the expected electricity demand for a cluster of HANs. The proposed scheme guarantees the electricity customers' privacy in addition to assuring the confidentiality and integrity of the exchanged electricity consumption messages. It also restricts the connection with the provider only when the total cluster's demand needs to be adjusted. Security analysis and simulation results demonstrate that the proposed scheme satisfies security and privacy requirements for householders, at the same time, guarantees light communication and computation burden. In the future work, we aim to study the impact of malicious BANs on the performance of customer-side networks.

References

[1] A. R. Abdallah and X. Shen, "A lightweight lattice-based security and privacy-preserving scheme for smart grid," in *Proc. IEEE GLOBECOM*, Austin, TX, USA, Dec. 2014, pp. 668–674.

[2] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 944–980, Dec. 2012.

[3] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Comput. Netw.*, vol. 55, no. 15, pp. 3604–3629, 2011.

[4] M. Kuzlu, M. Pipattanasomporn, and S. Rahman, "Communication network requirements for major smart grid applications in HAN, NAN and WAN," *Comput. Netw.*, vol. 67, pp. 74–88, Jul. 2014.

[5] Z. Fan *et al.*, "Smart grid communications: Overview of research challenges, solutions, and standardization activities," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 21–38, Mar. 2013.

[6] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 998–1010, Dec. 2012.

[7] J. Liu, Y. Xiao, S. Li, W. Liang, and C. Chen, "Cyber security and privacy issues in smart grids," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 981–997, Dec. 2012.

[8] Z. Erkin, J. Troncoso-Pastoriza, R. Lagendijk, and F. Perez-Gonzalez, "Privacy-preserving data aggregation in smart metering systems," *IEEE Signal Process. Mag.*, vol. 30, no. 2, pp. 75–86, Mar. 2013.

[9] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

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

[11] Z. Chen and L. Wu, "Residential appliance DR energy management with electric privacy protection by online stochastic optimization," *IEEE Trans. Smart Grid*, vol. 4, no. 4, pp. 1861–1869, Dec. 2013.

[12] X. He, X. Zhang, and C. Kuo, "A distortion-based approach to privacy-preserving metering in smart grids," *IEEE Access*, vol. 1, pp. 67–78, 2013.

[13] L. Sankar, S. Rajagopalan, S. Mohajer, and H. Poor, "Smart meter privacy: A theoretical framework," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 837–846, Jun. 2013.

[14] W. Jia, H. Zhu, Z. Cao, X. Dong, and C. Xiao, "Human-factor-aware privacy-preserving aggregation in smart grid," *IEEE Syst. J.*, vol. 8, no. 2, pp. 598–607, Jun. 2014.

[15] A. Metke and R. Ekl, "Security technology for smart grid networks," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 99–107, Jun. 2010.

[16] Z. Fadlullah, N. Kato, R. Lu, X. Shen, and Y. Nozaki, "Toward secure targeted broadcast in smart grid," *IEEE Commun. Mag.*, vol. 50, no. 5, pp. 150–156, May 2012.

[17] J. Liu, Y. Xiao, and J. Gao, "Achieving accountability in smart grid," *IEEE Syst. J.*, vol. 8, no. 2, pp. 493–508, Jun. 2014.

[18] H. Li *et al.*, "EPPDR: An efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 8, pp. 2053–2064, Aug. 2014.

[19] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1621–1631, Sep. 2012.

[20] X. Li *et al.*, "Securing smart grid cyber attacks, countermeasures, and challenges," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 38–45, Aug. 2012.

[21] M. Fouda, Z. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 675–685, Dec. 2011.

[22] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An efficient Merkle-tree-based authentication scheme for smart grid," *IEEE Syst. J.*, vol. 8, no. 2, pp. 655–663, Jun. 2014.

[23] H. Nicanfar, P. Jokar, K. Beznosov, and V. Leung, "Efficient authentication and key management mechanisms for smart grid communications," *IEEE Syst. J.*, vol. 8, no. 2, pp. 629–640, Jun. 2014.

[24] C. Rottondi, G. Verticale, and C. Krauss, "Distributed privacy-preserving aggregation of metering data in smart grids," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1342–1354, Jul. 2013.

[25] T. Chim, S. Yiu, L. Hui, and V. Li, "Privacy-preserving advance power reservation," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 18–23, Aug. 2012.

[26] J. Hoffstein, D. Lieman, J. Pipher, and J. Silverman, "NTRU: A public key cryptosystem," in *Proc. EUROCRYPT*, Innsbruck, Austria, 2001, pp. 211–225.

[27] A. Nitaj, "Cryptanalysis of NTRU with two public keys," *Int. J. Network Secur.*, vol. 16, no. 2, pp. 112–117, 2014.

[28] J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. Silverman, and W. Whyte, "NTRUSign: Digital signatures using the NTRU lattice," in *Proc. CT-RSA*, San Francisco, CA, USA, 2003, pp. 122–140.

[29] D. Micciancio, "Shortest vector problem," in *Encyclopedia of Cryptography and Security*. Berlin, Germany: Springer-Verlag, 2011, pp. 1196–1197.

[30] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *J. ACM*, vol. 56, no. 6, 2009, Art. ID 34.

[31] A. Blum, A. Kalai, and H. Wasserman, "Noise-tolerant learning, the parity problem, and the statistical query model," *J. ACM*, vol. 50, no. 4, pp. 506–519, 2003.

[32] C. Wang and H. Wang, "A new ring signature scheme from NTRU lattice," in *Proc. ICCIS*, Chongqing, China, 2012, pp. 353–356.

[33] D. Stehlé and R. Steinfeld, "Making NTRU as secure as worst-case problems over ideal lattices," in *Proc. EUROCRYPT*, Tallinn, Estonia, 2011, pp. 27–47.

[34] Ontario Hydro, [Online]. Available: http://www.ontario-hydro.com/index.php?page=current_rates, accessed Jul. 28, 2015.

Asmaa Abdallah received the B.Sc. degree in computer and control engineering, and the M.Sc. degree in mobile networks from Suez Canal University, Ismaïlia, Egypt, in 2003 and 2007, respectively. She is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, USA.

Her current research interests include security and privacy in smart grid, wireless network security, and mobile computing.

Xuemin (Sherman) Shen (M'97–SM'02–F'09) received the B.Sc. degree from Dalian Maritime University, Dalian, China, in 1982, and the M.Sc. and Ph.D. degrees from Rutgers University, New Brunswick, NJ, USA, in 1987 and 1990, respectively, all in electrical engineering.

He is a Professor and the University Research Chair of the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, where he was the Associate Chair for Graduate Studies from 2004 to 2008. His current research interests include resource management in interconnected wireless/wired networks, wireless network security, social networks, smart grid, and vehicular ad hoc and sensor networks.

Dr. Shen was a recipient of the Excellent Graduate Supervision Award in 2006 and the Outstanding Performance Award in 2004, 2007, 2010, and 2014 from the University of Waterloo; the Premier's Research Excellence Award in 2003 from the province of ON; and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. He served as the Technical Program Committee Chair/Co-Chair for IEEE INFOCOM'14 and IEEE VTC'10; the Symposia Chair for IEEE ICC'10; the Tutorial Chair for IEEE VTC'11 and IEEE ICC'08; the Technical Program Committee Chair for IEEE GLOBECOM'07; the General Co-Chair for ACM Mobihoc'15, Chinacom'07, and QShine'06; and the Chair for the IEEE Communications Society Technical Committee on Wireless Communications and P2P Communications and Networking. He also serves/served as the Editor-in-Chief for IEEE NETWORK, *Peer-to-Peer Networking and Application*, and *IET Communications*; a Founding Area Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS; an Associate Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, *Computer Networks*, and *ACM/Wireless Networks*; and a Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, IEEE WIRELESS COMMUNICATIONS, *IEEE Communications Magazine*, and *ACM Mobile Networks and Applications*. He is an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, and a Distinguished Lecturer of the IEEE Vehicular Technology Society and Communications Society. He is an elected member of the IEEE Computer Society Board of Governors, and the Chair of the Distinguished Lecturers Selection Committee. He is a Registered Professional Engineer of ON.