ISSN: 2710-0588 DOI: 10.29556/FSE.202105_1(2).0008

Research on Privacy Protection of Smart Meter Users under Mandatory Incentive Demand Response

Shaomin Zhang*, Zhiyuan Wu, Baoyi Wang

North China Electirc Power University, Hebei Baoding 071000, China.

Abstract

The implementation of demand response requires real-time, fine-grained two-way interaction of power information between grid side and user side. The real-time electricity information contains the user's privacy, such as living habits, interests, etc. the power supplier or attacker can mine and analyze the fine-grained electricity data uploaded by the smart meter, and obtain the user's living habits and work and rest rules, so as to steal the user's privacy. Under the mandatory incentive demand response, power suppliers are faced with the need to identify the power users who do not comply with the demand response plan and protect the privacy of the users who comply with the demand response plan. To solve the above problems, based on fair blind signature and power consumption threshold overload audit, this paper proposes an anonymous user privacy protection scheme under mandatory incentive demand response, designs an anonymous identification algorithm based on fair blind signature and power consumption overload denial proof, and introduces one-way hash chain technology to update smart meter key. This paper presents the implementation process of the scheme. It is proved that the scheme satisfies strong anonymity, unlinkability, unforgeability, recognizability and integrity. Through the example analysis, compared with other schemes, this scheme has lower computational overhead and better communication efficiency.

Keywords

Demand Response; Condition Anonymity; Privacy Protection; Smart Meter; Identification.

1. Introduction

Energy Internet uses advanced information and management technology to combine various energy forms, such as wind energy, electric energy, solar energy, etc., and supports the access of large-scale distributed generation system and distributed energy storage system, which provides a feasible technical solution to solve the problem of renewable energy utilization. However, due to the influence of season, climate and other factors, new energy power generation has the characteristics of randomness, intermittence and unstable power generation, which also leads to the problem of "abandoning light", "abandoning wind" and other energy can not be fully utilized, which brings great challenges to the dispatching work of power grid. Demand response (DR) is an effective means to solve the above problems [1-2]. Demand response is demand side response, which means that when the price of electricity rises or the reliability of the system is threatened, after receiving the signal from the power supplier to reduce the power consumption or increase the price of electricity, the power users reduce or shift the power consumption of a certain period of time, so as to ensure the stability of the power grid and restrain the rise of the price of electricity, It is a kind of power adjustment means provided by power supply department to power users. The international federal energy mediation commission (FERC) also divides demand response into two categories: price based demand response (PDR) project and incentive based demand response (IDR) project [3]. Price based demand response (PDR) refers to that power users adjust their power demand according to the received price signal. The common ones are ladder price, time of use price and peak price. Based on Incentive demand response (IDR), compensation or discount is directly used to motivate and guide users to participate in various load reduction projects needed by the system. Users who participate in the IDR mechanism usually have to sign a contract with the Dr implementation agency, and users adjust their own electricity consumption according to the contract signed. Incentive based demand response in smart grid can be realized by two fundamentally different schemes: voluntary and mandatory.

At present, many scholars have carried out research on privacy protection based on voluntary incentive demand response, but there are few researches on privacy protection in mandatory incentive demand response mechanism. However, literature [4] shows that the threat of power shortage to power infrastructure is greater than that of oversupply, They will broadcast demand response instructions to their users, requiring them to adjust power consumption to ensure the security and stability of the power grid, while mandatory demand response requires that once consumers choose to participate, they must comply with the instructions issued by power suppliers during the period of power shortage, otherwise they will be punished. Therefore, in the case of power shortage, the mandatory demand response plan has better effect than the voluntary demand response plan. During the implementation of incentive demand response plan, smart meters need to upload users' fine-grained electricity data to power suppliers frequently. Power suppliers or attackers can mine and analyze users' fine-grained electricity data through non intrusive appliance load monitoring (nalm) technology to infer the status of various types of users' appliances, So as to steal the user's personal privacy. The status analysis of electrical appliances by nalm technology is shown in Figure 1 [5]. At the same time, power suppliers are faced with the problem of identifying the power users who do not comply with the demand response plan. The scheme proposed in this paper properly solves the above two problems, which not only ensures the user privacy during the mandatory demand response planning, but also brings convenience to the demand side management of power grid. Therefore, this paper has important research significance.

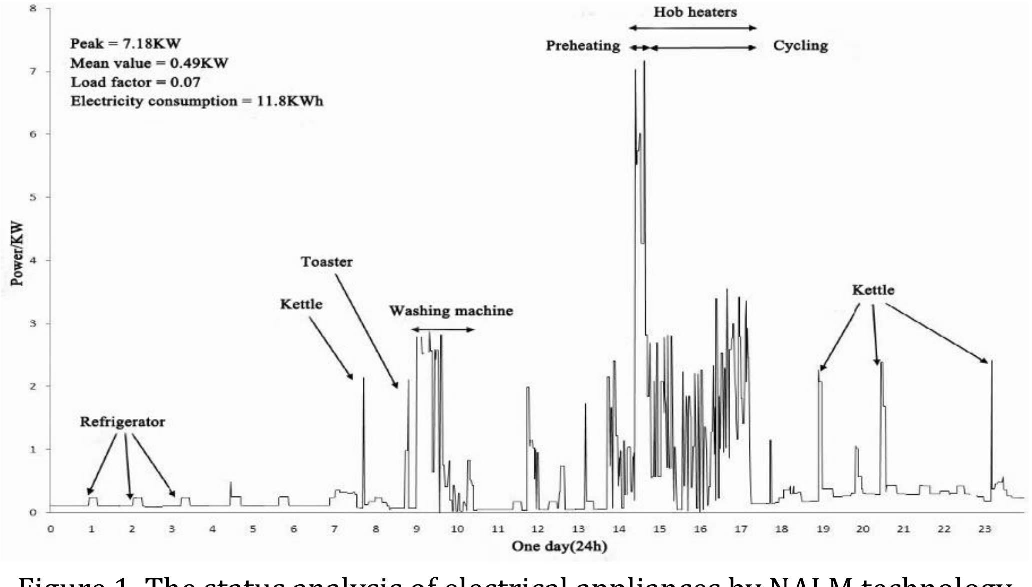

Figure 1. The status analysis of electrical appliances by NALM technology

Data aggregation scheme hides the privacy of consumers by hiding the fine-grained data of users, which are needed by power suppliers to identify the sources of users who do not obey users in smart grid. In order to achieve this, the scheme of voucher is usually used to introduce trusted third parties to ensure that the communication between power suppliers and consumers is reliable. The certificate can be a pseudonym or a blind certificate [13]. At present, there is a lot of work on the research of multi -kana technology. Efthmiou [6] proposed using pseudonym technology to protect the privacy of users, using different identities when sending high-frequency data and low-frequency data. Liu et al. Proposed an authentication scheme to ensure the identification of users in the smart grid, so as to support the guaranteed audit of consumers for billing purposes [7, 8].

In order to realize identity recognition, these schemes need more complete information of users, so the problem of user privacy leakage is not fully considered. Gong et al. [9] proposed using pseudonym to protect the user's identity. Finally, the verifier confirms the validity of the pseudonym according to the ring signature. This partially blind signature verifies the pseudonym of the consumer in the incentive based demand response plan, and the real identity of the consumer is hidden by the BBS + signature. However, aliasing can't completely protect users' private information. Reference [10] points out that Gong et al's method is vulnerable to the threat of de aliasing attack. The user's personal data contains important information, through which the user's source can be linked. Therefore, meeting the unlinkability is the key indicator in the process of identification. The above defects in the current solution promote the necessity of studying new and better solutions. The new solution provides an effective authentication scheme, which can not only identify the disobedient consumers, but also protect the privacy of the compliant consumers, without bringing the trusted third party into the computationally complex system.

2. Methodology

2.1. Preliminaries

2.1.1. Basic content of Fair Blind Signature

Blind signature is a kind of digital signature technology in which the signer is not allowed to know the content of the signature. The information owner first blinds the information to be signed and submits it to the signer for signature. After signing, the blind factor is removed from the signature to obtain the signer’s signature of the original information [11]. According to the nature of blind digital signature, we can know that the information security of users is guaranteed. But this completely anonymous feature is also easy to use by the lawbreakers. In view of this problem, the concept of fair blind signature is proposed in literature [12]. In view of the existing problems, the adjudicator is added on the basis of blind digital signature. The signer can, in a specific case, rely on the help of the adjudicator to find out the actual owner of the signed blind content [12]. Therefore, the idea of fair blind signature provides the dual characteristics of protecting information privacy and suppressing unconditional anonymous abuse. The fair blind signature is shown in Figure 2.

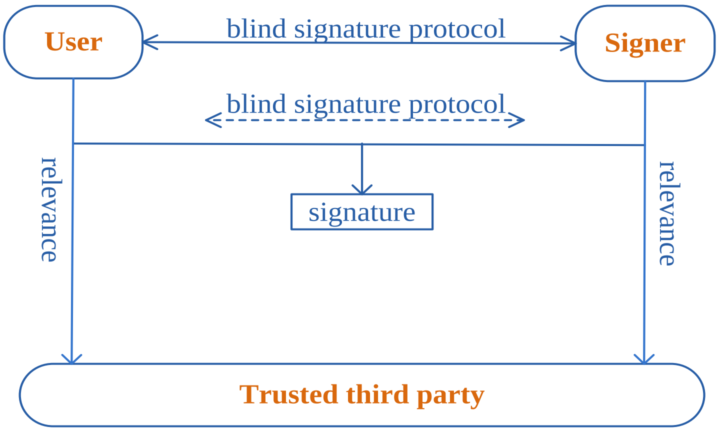

Figure 2. Fair Blind Signature Schematics

2.1.2. Fair Blind Signature Protocol

The user registers with a trusted third party:The user selects a random number $r, 1 < r < n$, to calculate $T = r^e h(m) \, mod \, n$, m represents the message to be signed by the signer, m, r, ID and User signature $S_u(T)$ Transmit to TP through public channel.

TP verify signature: TP calculate $T^{'} = r^e h(m) \, mod \, n$, The algorithm $S_u(T)$ of searching users' signature by users, Then verify $(T^{'}, S_u(T))$, if true $T = T^{'}$, register r, m, t, Then send the signature $S_{TP}(T)$ to the user.

Users calculate T verify $(T, S_{TP}(T))$, If verified, the message has not been modified and is then sent to signer S. Signer verify $(T, S_{TP}(T))$, If validated, then calculate $S' = T_d \, mod \, n$. And send it to the user, At the same time to save $(T, S_{TP}(T))$. Users calculate $s = s'/r \, mod \, n$, S is the signer's signature on the message M, verified by $s^e = h(m)$.

2.1.3. Bilinear Map

Bilinear pairing associates the elements of two groups to a third group, assuming that p is a prime number and G, G_T is an addition and multiplicative group of order p. Mapping relation $G \times G \to G_T$, and the mapping function should also meet the following properties:

1) *Bilinearity:* $e(aP_1, bP_2) = e(P_1, P_2)^{ab}, a, b \in \mathbb{Z}_p^*, P_1, P_2 \in G$;

2) Generality: $e(P, P) \neq 1$, 1 represents the unit element in G_T;

3) *Computability:* $\forall P, Q \in G$, $e(P, Q)$ can be computed by a valid algorithm;

2.1.4. Diffe-Hellman Assumptions

(*Decisional Diffifie-Hellman (DDH) Assumption*): *for* $a, b, c \in Z_q^*$, given P, aP, bP, cP Determine whether $c = ab \bmod q$.

(*Gap-Discrete Logarithm (Gap-DL) Assumption*): *For a given tuple* $(xP, P), P \in \mathbb{Q}, x \in \mathbb{Z}_P^*$, solve the x.

(*q-Strong Diffifie-Hellman (q-SDH) Assumption*): *given* $(P, xP, x^2P, \cdots, x^qP) \in G_1^{q+1}$, calculate $(c, \frac{1}{x+c}P) \in Z_q^* \times G_1$.

2.1.5. Non-interactive proof of zero knowledge

Through zero-knowledge proof technology, the prover can prove that he knows the content of a secret without showing the secret content he knows to the verifier. For example, a proof to the verifier that he knows the value of x can be abbreviated to the form of Eq. 1:

$$PK\{(x): C = xP\} \quad (1)$$

2.2. Assumptions and Security Requirements

This paper found in the literature [13] TAI solutions exist the following problems, excessive use of zero knowledge proof and double line for operation, increase the computational overhead of the system, and the second on the anonymous user identification after there is no will identify to the anonymous user after problems. Therefore, an anonymous recognition scheme based on fair blind signature and electricity threshold is designed to improve the TAI scheme in reference [13]. The concrete implementation process of this scheme is given in this chapter. The security of the scheme is proved by theory. Compared with TAI scheme, CRS scheme and DRS scheme, it is proved that the proposed scheme has lower computing cost and better communication efficiency.

2.2.1. Assumptions

(1) SMS (Smart Meters) features secure storage and autonomous encryption.

(2) Assume that the communication channel between the Service Provider (SP) and the SM does not provide the SM's identity information or the household's location information.

ISSN: 2710-0588 DOI: 10.29556/FSE.202105_1(2).0008

(3) During peak hours, the load of users is greater than the amount of electricity generated by the power generation company.

2.2.2. Security Requirements

Since electricity providers track non-compliant consumers based on their consumption reports, some consumers may try to send false consumption reports to mislead the electricity providers. There is a need for a scheme to ensure the security of power infrastructure while ensuring the anonymity of compliant consumers.

(1) Unlinkability: no one can link different consumption reports from the same consumer.

(2) Strong anonymity: no one can associate the consumption data of compliant consumers with its source

(3) non-forgery: no one can produce illegal signatures to frame legitimate consumers. The unstructured nature of demand response instructions from power suppliers cannot be modified.

(4) Identifiability: Consumption that does not meet the requirements must be identified according to consumption data.

(5) Integrity: the power supplier can check whether the electricity consumption data really comes from legitimate users without authorization.

2.3. Scheme model

2.3.1. System architecture

In this paper, a three-layer communication architecture is designed, which consists of the smart meter SM, the trusted center TP and the power service provider SP. It involves three entities: the power service provider SP, the smart meter SM and the trusted center TP. The trusted center TP consists of the identity authentication center AC, the pseudonym publishing center PAC and the tracking center TC. The overall architecture of the scheme is shown in Figure 3.

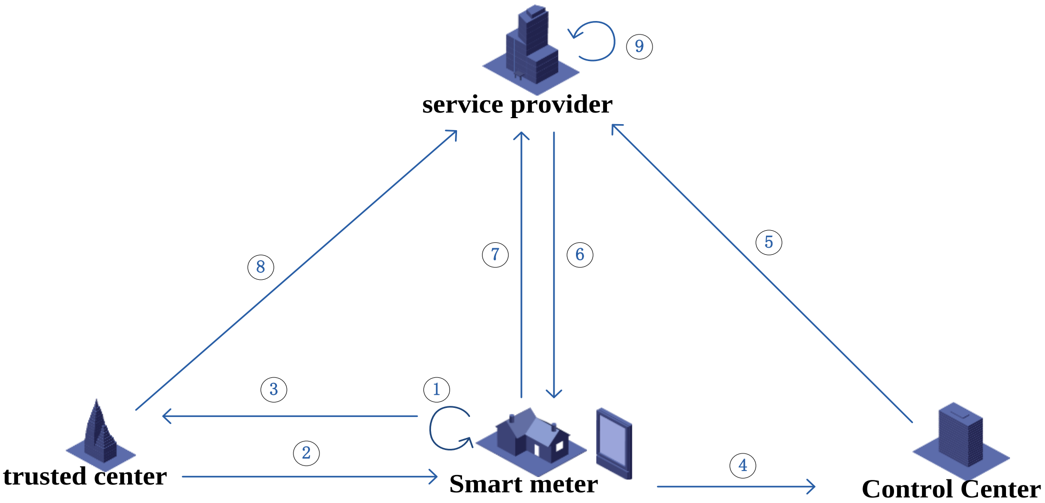

Figure 3. System architecture

Three types of entities in the solution architecture

1) The trusted center TP is firstly generated into the public and private keys corresponding to the certification center AC, the pseudo issuing center PAC and the tracking center TC through the system initialization. The trusted center needs to publish their public keys to the smart meter SM and the power service provider SP. The Trusted Center issues pseudonym certificates to smart meters, which are pseudonym authenticated and tracked for smart meters that communicate with power service provider SP through pseudonyms.

2) Smart meter SM generates its internal public key and private key through system initialization, and preload AC, PAC and TC public keys for each smart meter at the same time. Smart meters record fine-grained electricity consumption data of users.

3) power service provider SP, and smart meters to interact with users fine-grained electricity report collection, and to verify the identity of the smart meter, when need power users demand response to electricity users to send demand response command, when users of electricity is greater than the power threshold method, to the users to send instructions. Identify users who do not comply with requirements response instructions.

The implementation process of the scheme is described as follows:

① nitialize the smart meter;

② The smart meter SM is registered at AC and applies for a pseudonym certificate from PAC;

③ AC verifies and signs SM, PAC verifies SM's identity information and issues a pseudonym certificate to SM;

④ SM sends the user's electricity consumption report to CC and signs it;

⑤ CC sends the power consumption report corresponding to the false name information of the user to SP;

⑥ SP sends demand response instructions to users;

⑦ SM sends proof of denial report;

⑧ PAC sends user pseudonym certificate;

⑨ SP identifies users who do not comply with demand response instructions;

2.3.2. Generation and authentication process of pseudonyms

The interaction and recognition between SM and SP need to be authenticated through the trusted center TP. The interaction process between the three parties is shown in Figure 4.

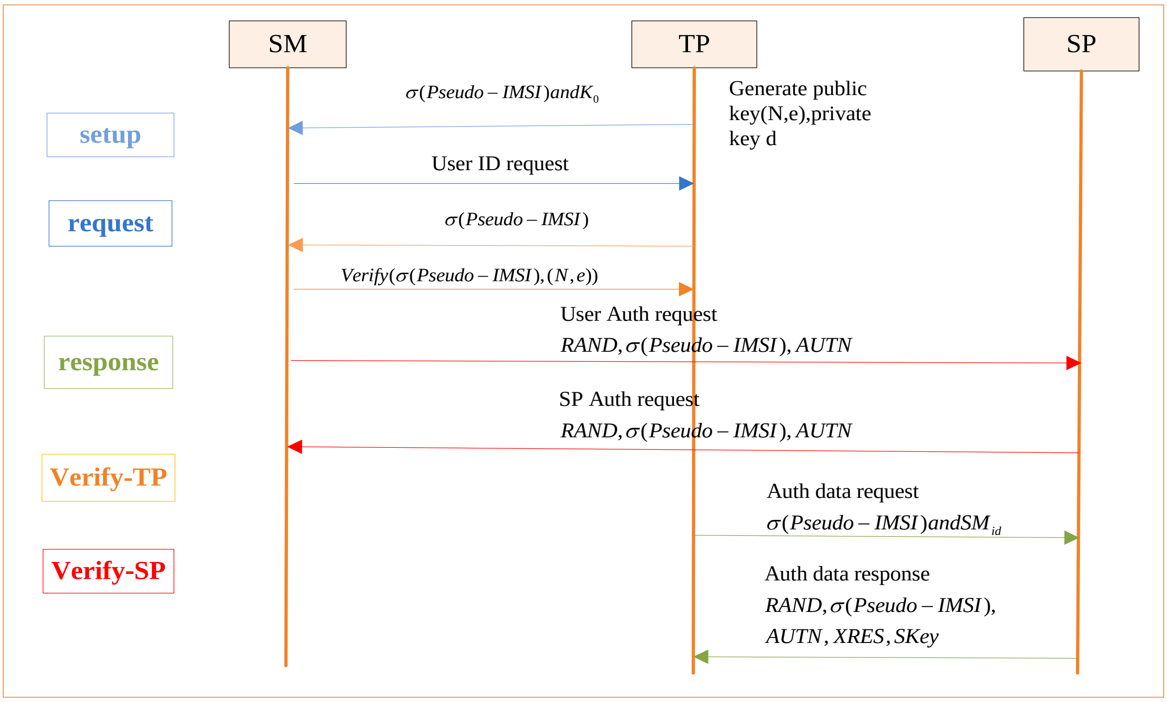
SM
TP
SP
$\sigma(Pseudo-IMSI) and K_0$
Generate public key(N,e),private key d
setup
User ID request
request
$\sigma(Pseudo-IMSI)$
$Verify(\sigma(Pseudo-IMSI),(N,e))$
User Auth request
$RAND,\sigma(Pseudo-IMSI),AUTN$
response
SP Auth request
$RAND,\sigma(Pseudo-IMSI),AUTN$
Verify-TP
Auth data request
$\sigma(Pseudo-IMSI) and SM_{id}$
Verify-SP
Auth data response
$RAND,\sigma(Pseudo-IMSI),$
$AUTN, XRES, SKey$

Figure 4. Authentication interaction process

2.3.3. The realization process of anonymous recognition

In this paper, the anonymous identification process of smart electricity meters is divided into two stages: anonymous report stage and demand response stage.

the smart electricity meter needs to generate false names through the authentication of AC and PAC, and then send the electricity consumption report to the power supplier in an anonymous way, and the power supplier can test the validity of the report, In the anonymous reporting stage. In demand response phase, power supply party is expected to power consumption value is greater than the original power generation, power supply party defined threshold, the threshold instruction contains (threshold, the corresponding timestamp), each user must reduce electricity consumption, make oneself in the corresponding moment of power consumption is less than the threshold, if the user in the corresponding period of the power consumption is greater than the threshold, electricity power supply direction user radio instruction. The smart meter verifies the validity of the signage instruction, the instruction is valid, and the smart meter checks whether it violates the initial power consumption reduction instruction. In case of violation, send proof of refusal to the supplier; No violation. Refuse to execute the flag instruction. This can identify non-compliant users while maintaining the anonymity of compliant consumers.

2.4. Scheme implementation

The implementation process of the scheme proposed in this paper is shown in Figure 5. Through six processes of setting, joining, report generation, report reading, instruction generation and identification, the privacy protection of users who comply with demand response instruction and anonymous identification of users who do not comply with demand response instruction under mandatory incentive demand response are realized.

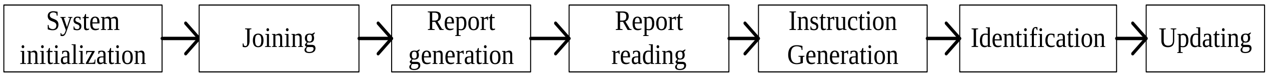

Figure 5. Scheme implementation process

2.4.1. System initialization

1) Select RSA algorithm mod $n = p_0 q_0$, $p_0 = 2p' + 1, q_0 = 2q' + 1$ where p' and $q'$are both large prime numbers;

2) A generator g_0 in the quadratic residue group QR_n is randomly selected;

3) Choose appropriate safety parameters α, k_1, k_2, k_3;

4) Two constant integers X and Y, and $Y > 2^{\alpha(k_1+k_3)+1}, X > 2Y + 2^{\alpha(k_1+k_2)+2}$;

5) Two safe hash functions: $H_1: \{0,1\}^* \to Z_n^*, H_2: \{0,1\}^* \to \{0,1\}^{k_1}$;

6) The public key (N_{AC}, e_{AC}) and private key d_{AC} generated by initialization of AC. The generated PAC public key is (N_{PAC}, e_{PAC}), and the PAC private key d_{PAC} needs to be updated frequently. TC generates public key (N_{TC}, e_{TC}) and private key d_{TC}, and the trusted center discloses its public key;

7) The public and private keys of the smart electricity meter are: $(h_1{}^x, x)$;

2.4.2. Joining

When the new smart meter is added, its interaction with AC is as follows:

① SM uses internal seeds to randomly generate integers $x \in Z_p^*$ as its secret key, selects a random number v' and sends $h_1^{v'}, h_2^x$ to AC, and then SM users use non-interactive zero-knowledge proof to prove that they have x, v'.

② AC verifies the proof, and then selects the random number. AC generates credentials (A, e) that satisfy $A^e h_1^v h_2^x = h_0 \in QR_N$ (e is an initial number), here $v = v'' + v'$. After AC send v' and (A, e) to SM, AC will be sent $(id, (h_1^x, h_2^v), (A, e))$ to SP as part of the parameter.

2.4.3. Report Generation

In order to ensure the real-time performance of electricity report and the privacy of smart electricity meter, SM runs the report generation algorithm to generate legal signatures. First of all, using the knowledge of the secret key X, SM will consume data M and the timestamp T bound to the element T. In order to protect the privacy of valid SM, the signature of honest SM should be independent at different time intervals. To solve this problem, we update each discrete logarithmic basis H2(T) time interval, where T is the timestamp. SM displays its credentials to AC, which is actually a non-interactive zero-knowledge signature on M.

$$PK\{(A,e,x,v):A^{e}\,h_1^{v}\,h_2^{x}=h_0\wedge T_2=H_2(T)^{x}\}(M) \tag{2}$$

The details are as follows:

SM randomly selects $s_0\in\{0,1\}^{k_1},r_1\in\{0,1\}^{2k_1+k_2+1}$, and then calculates:

$$T_0=h_0^{s_0},T_1=Ah_3^{s_0},h\ _0=T_1^{e}h_1^{x}h_2^{v}h_3^{-s_1}(s_1=es_0)$$
$$T_2=H_1(T)^{x},D_0=h_0^{r_0},D_1=T_1^{r_e}h_1^{r_x}h_2^{v}h_3^{-r_1};D_2=H_1(T)^{r_x} \tag{3}$$

Questioning C is:

$$c=H_2(M,T,T_0,T_1,T_2,D_{0,},D_1,D_2) \tag{4}$$

The reply is:

$$z_e=r_e-ce\,;z_i=r_i-cs_i,i=0{,}1;z_x=r_x-cx,z_v=r_v-cv \tag{5}$$

The final signature of the output of the smart meter is as follows:

$$\sigma=(M,T,T_0,T_1,T_2,c,z_e.z_0,z_1,z_x,z_y) \tag{6}$$

2.4.4. Report Reading

In the anonymous report part, the smart meter sends the consumption report to the public utility in an anonymous way regularly, and the public utility verifies and reads the report sent by SM. After receiving all signatures from SM, SP first checks to see if the T2 of these signatures are all different. If so, the following validation algorithm is performed; otherwise, the following tracing algorithm is performed.

$$\widetilde{D}_0=h_0^{z_0}T_0^{c},\widetilde{D}_1=T_1^{z_e}h_1^{z_x}h_2^{z_v}h_3^{-z_1}h_0^{c},\widetilde{D}_2=H_1(T)^{z_x}T_2^{c},\tilde{c}=H_2(M,T,T_0,T_1,T_2,\widetilde{D}_0,\widetilde{D}_1,\widetilde{D}_2) \tag{7}$$

SP verification, if equal, accept the electricity report sent by the SM, otherwise reject. The correctness of the verification is proved as follows:

$$\widetilde{D}_0=h_0^{z_0}T_0^{c}=h_0^{z_0}h_0^{cs_0}=h_0{}^{z_0+cs_0}=h_0^{r_0}=D_0$$
$$\widetilde{D}_1=T_1^{z_e}h_1^{z_x}h_2^{z_v}h_3^{-z_1}h_0^{c}=T_1^{z_e}h_1^{z_x}h_2^{z_v}h_3^{-z_1}*T_1^{ce}h_1^{cx}h_2^{cv}h_3^{-cs_1}$$
$$=T_1^{z_e+ce}h_1^{z_x+cx}h_2^{z_v+cv}h_3^{-(z_1+cs_1)}=T_1^{r_e}h_1^{r_x}h_2^{r_v}h_3^{-r_1}=D_1$$
$$\widetilde{D}_2=H_1(T)^{z_x}T_2^{c}=H_1(T)^{z_x}H_1(T)^{c_x}=H_1(T)^{z_x+c_x}=D_2$$
$$\tilde{c}=H_2(M,T,T_0,T_1,T_2,\widetilde{D}_0,\widetilde{D}_1,\widetilde{D}_2)=H_2(M,T,T_0,T_1,T_2,D_0,D_1,D_2)=c \tag{8}$$

When SP finds that the expected power consumption is greater than the amount of power generated at this time, it will execute the instruction generation protocol, which requires the users who sign the demand response agreement to reduce their power consumption. The power service provider first defines the instruction (D_n,T_n). If the consumer's power consumption is higher than the threshold $d_i\in D_n$ defined by SP, then the power consumption must be reduced below d_i at $t_i\in T_n$, and then the SP needs to prove its iden tity with a valid signature. The SP can be linked to the corresponding user through the SM ID information. The SP performs the setup algorithm to generate its long-term key pair (γ,p_{pub}), there $P_{pub}=\gamma P$.

SP selects a random number $k_5\in Z_p^{*}$, $W=k_5P,f=H_1(D_n||T_n||W||t),s_5=k_5-f\gamma$. The SP then broadcasts the demand response instruction and its signature (D_n,T_n,s_5,f,t) to all smart meters. When a smart meter receives a power cut instruction, the smart meter checks whether the timestamp and instruction are valid and whether its electricity consumption within the timestamp meets the instruction. The smart meter calculates $W'=fP_{pub}+s_5P$, checks and calculates $f\underline{?}H_1(D_n||T_n||W'||t)$ the electricity consumption at this time $m > d_i$. If the electricity consumption is greater than the power threshold value, the smart meter reduces the electricity usage. Otherwise, the instruction and signature are ignored.

2.4.5. Identification

After the demand response instruction is generated, SP receives all signatures from SM and checks from AC whether the TN in these signatures is consistent. If so, the validation algorithm is executed; otherwise, the following tracing algorithm is executed. When all SM's signatures are authenticated, if SP still finds a valid consumption (m^*, t^*), where $m^* > d_i$ and $t^* = t_i$, it will execute the recognition protocol to identify the non-compliant consumer.

The SP generates a valid identification command that includes the noncompliant consumer's consumption data, timestamp, and proof from the SP. SP selects a random number $k_6 \in Z_p^*$, and calculates $X = k_6P, l = H_2(m^*||X||t^*||t), s_6 = k_5 - l\gamma$. SP broadcasts identification commands (m^*, t^*, l, s_5, t) to all smart meters. After receiving the recognition command, the smart meter calculates $X^{'} = lp_{pub} + s_6P$ and checks $l\,? = H_2(m^*||X^{'}||t^*||t), m^* > d_i, t^* = t_i$. If the above conditions are not true, the smart meter ignores the identification command; Otherwise, SM generates a proof of denial.

2.4.6. Updating

One-way hash chain technology can guarantee the freshness and forward and backward security of the key, and it has very little computation and communication overhead. In the anonymous update scheme of this paper, AC updates the secret keys of smart electricity meters after each punishment through one-way hash chain technology. At the same time, smart electricity meters rejoin with the updated secret keys, so that the rejoining of smart electricity meters after punishment can be realized. The basic process of updating is shown in Figure 6:

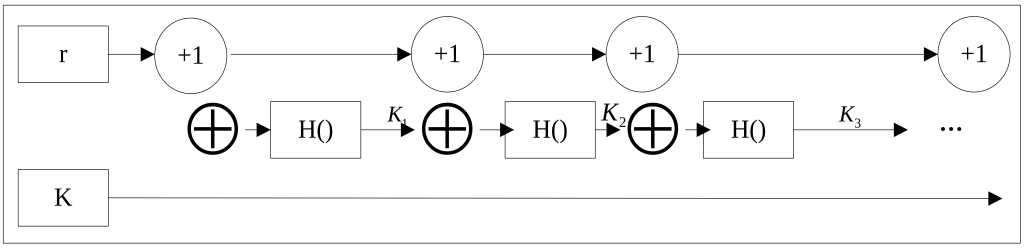

Figure 6. Key updating process

The specific steps are as follows:

SM generate a random number u, Then send $M_1 = \{B_1, B_2, B_3, K_{SM_j}\}$ to AC.

$$u \in z_p^*, B_1 = up, B_2 = H_3(uK_{AC}) \oplus ID_{SM_j}, B_3 = H_3(B_1||K_{SM_j}||K_{AC}||ID_{SM_j}) \qquad (9)$$

2) AC calculate $ID_{SM_j} = B_2 \oplus H_3(s_{AC}B_1)$, check $B_3? = H_3(B_1||K_{SM_j}||ID_{SM_j}||K_{AC})$. If this equation is true, select a random number $v \in Z_p^*$ and calculate:

$$B_4 = vp, SK_{AC} = H_3\big(B_1\big|\big|B_4\big|\big|vB_1\big),$$
$$B_5 = H_3(vK_{SM_j} + vH_1(K_{SM_j}||ID_{SM_j})P_{pub}) \oplus ID_{AC}$$
$$B_6 = H_3(ID_{SM_j}||ID_{AC}||B_1||B_4||SK_{AC}) \qquad (10)$$

3) SM calculate $SK_{SM_j} = H_3(B_1||B_4||vB_4), ID_{AC} = H_3(s_{SM_j}B_4) \oplus B_5$, Check

$B_6? = H_3(ID_{SM_j}||ID_{AC}||B_1||B_4||SK_{SM_j})$. If the equation is equal, AC updates the smart meter with its own secret key.

Through the improved one-way hash chain technology, the secret key $K_i = H(K_i - 1 \oplus K_0 \oplus r_i)$ updated each time is obtained.

3. Results and discussion

3.1. Security analysis

3.1.1. Unlinkability

In the process of communicating with the trusted third party TP, the authentication center is unable to determine the correspondence between the pseudonym and the real identity of the smart meter from the information obtained from the communication with the smart meter. As a result, there is no way to establish contact with the real identity of the smart meter, and the tracking center no longer communicates with the smart meter after the signing process is completed. The power supplier is only required to authenticate the pseudonym issued by the smart meter, but does not know the actual sender. For the certification authority AC, because the parameters A_i and B_i are randomly generated and uniquely saved by the smart meter, it is impossible to calculate the parameter A_i even if AC has obtained relevant information $ID_{SM}, B_i^{e_{AC}}A_i, C_i, D_i, ts$. Thus, the corresponding relationship between the pseudonym ID and the real identity cannot be obtained.

3.1.2. Strong Anonymity

The strong anonymity of this scheme is based on the unlinkability analysis of the scheme, according to which no party can link two different consumption reports from the same SM. Without the necessary parameter information, AC and PAC could not obtain the real identity of the smart meter through the only parameters, nor could they obtain the relationship between the pseudonym ID and the real identity of the smart meter. For the power supplier, it is necessary to obtain the real identity information of the smart meter and need to decrypt $A_i^{e_{TC}}$, which is computationally impossible. As a result, this paper fulfills a strong anonymity requirement.

3.1.3. Certification security

This scheme also has strong security in the authentication process, and it also needs to attach signature when using pseudonym to communicate and interact, and messages without signature will not be accepted, so as to ensure the validity of authentication. SM, AC or other attackers trying to forge signatures or fake names are as difficult as factoring large numbers. In the process of authentication by SM at AC, the information sent by SM to AC will not be tampered with by AC. If AC adds false identity information to the blind signature, SM can also determine whether the information has been tampered with through the return $D_i^{e_{AC}} = (i||ID_{SM}||ts)^{e_{TC}}$ of AC at the verification stage.

When SM sends parameter $(ID_{AC}||\{ID_{PSM_i}||E_{i,1}||E_{i,2}||e_{PSM_i}||N_{PSM_i}||S_{PSM_i}\})^{e_{PAC}}$ to PAC, SM cannot modify the signature. Therefore, the scheme in this paper is tamper-proof. The validity of authentication. In the process of applying for a pseudonym, it is necessary to first authenticate and sign at the place, and then obtain the pseudonym certificate from the place with the signature at the place of passing. In the whole process, SM and SP can carry out two-way authentication.

3.1.4. Identifification

The scheme identification in this paper is based on GAP-DL hypothesis and Q-SDH hypothesis. Non-compliant power users can have the following two cases of non-compliance with the marking order. the supplier verifies SM's promise by BBS+ signature. In other words, the use of BBS+ signature means that an attacker can destroy and control a polynomial number of key pairs held by the corresponding SM, but he cannot forge a new key pair without the help of AC. It also means that smart meters are safe to install. The signature and denial of the electricity data report are both signed by the same key. From the previous analysis of unforgeability we can see that a disobedient SM cannot masquerade as a obedient SM. This means that an attacker cannot generate false proof to get past the identity protocol.

3.1.5. Integrity

In the scheme of this paper, the certification process of smart electricity meters at AC and PAC and TC are separate. The Trusted Center is unable to track the real identity of the user throughout the process. So even if the trusted center is attacked, the real identity of the user will not be revealed. Based on the above analysis, in this paper, the improved scheme not only have not link, anonymity and authentication security, response instruction does not comply with the requirements of smart meters can identification, at the same time also with smart meters after the punishment to join a new renewable, AC hash to chain mechanism of smart meters after each punishment the secret key is updated, At the same time, the smart electricity meter uses the updated secret key to rejoin, so that the smart electricity meter can be rejoined after punishment. To sum up, this scheme has a good integrity.

3.2. Performance analysis

3.2.1. Computing performance

In this paper, the main communication and computing costs of the scheme come from the report generation stage and the report reading stage. This paper considers three time-consuming operations, namely bilinear pair operation, scalar multiplication operation and power exponential operation, and compares other conditional anonymity protection schemes [13,14,15]. Table 1 shows the comparison of the calculation amount of the scheme in the report generation stage and the report reading stage. Where, Gp, Ge and Gm respectively represent the time required for a bilinear pair operation, exponential operation and scalar multiplication operation, and n represents the number of smart meters.

Table 1. Comparison of computational performance

scheme	Report generation	Report reading
References [13]	Gp+3Ge+8Gm	2Gp+4Ge+8Gm
References [14]	Gp+4Ge+nGm	(4q-1)Ge
References [15]	2Gp+3Ge+qGm	4nGe
This paper	3Ge+nGm	(2d+2)Ge+5Gm

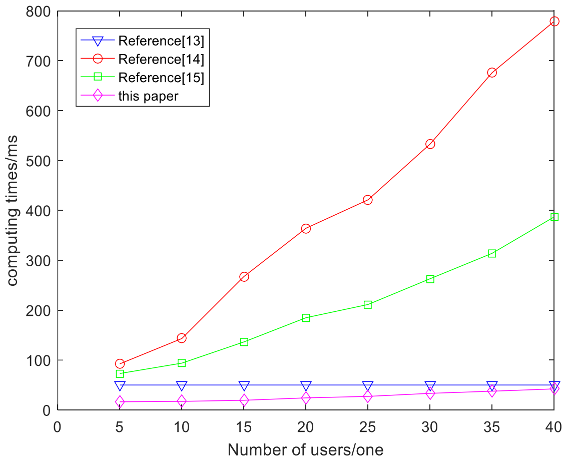

Figure 7. Report generation phase

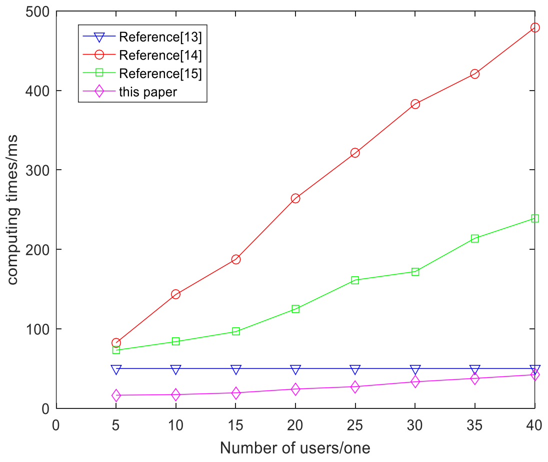

Figure 8. Report reading phase

Due to the computational cost, the proposed scheme is simulated on Ubuntu12.04 virtual operating system, which uses IntelCorei5-8250U @1.60GHz CPU, four cores and 1GB RAM. The communication process between 40 smart meters SM and power service provider SP is simulated, and the communication overhead and delay between SP and SMS are ignored in the simulation. PBC (Pairing-Based Cryptography) is used in the emulation of encryption. PBC (Pairing-Based Cryptography) is a library for bilinear Pairing. The simulation results of this scheme are compared with threshold based anonymous demand response identification scheme (TAI), conditional anonymous ring signature (CRS) [15] and deniable ring signature (DRS) [14].

The simulation results are shown in Fig. 7 and Fig. 8 respectively. The abscissa represents the number of smart electricity meters, and the ordinate represents the calculation time used. By comparing the schemes in Fig. 7 and Fig. 8, it can be seen that this scheme has lower computing cost.

3.2.2. Communication performance

Next, we compare the signature sizes between the proposed scheme, the TAI scheme, the CRS and the DRS. The number of bits used in their signature is 114N +167, 161N +804 and 481N +161, respectively, where N is the number of SMS. The more bits in the signature, the greater the communication overhead. The simulation results of the communication overhead between the smart electricity meter SM and the power service provider SP are shown in Fig. 9.

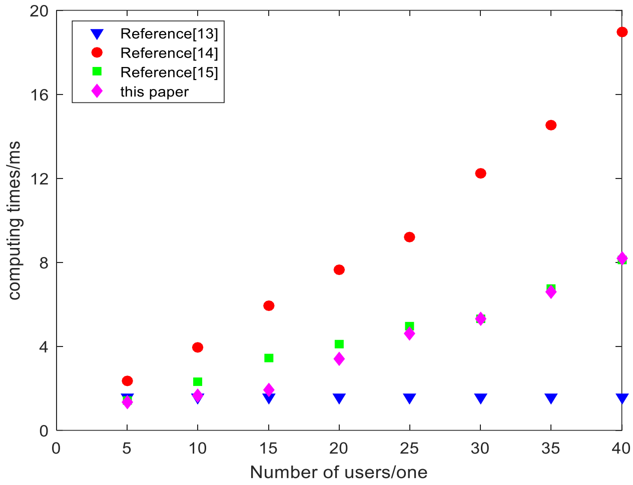

Figure 9. Communication overhead comparison

4. Conclusion

Based on fair blind signature and electricity threshold overload audit, this paper proposes an anonymous user privacy protection scheme under mandatory incentive demand response. In this scheme, the privacy protection of users depends on the real-time electricity consumption of users when the power center makes demand response. When the real-time electricity consumption of users exceeds the real-time electricity consumption threshold value, the electricity users will be identified. The realization process of the scheme is given in this paper. Theoretically, it is proved that the scheme satisfies strong anonymity, unlinkability, unforgability, identifiability and integrity. Compared with TAI scheme, CRS scheme and DRS scheme, this scheme has lower computational overhead and improves communication efficiency to some extent.

References

[1] J. Y. Hwang, L. Chen, H. S. Cho and D. Nyang, "Short Dynamic GroSP Signature Scheme SSPporting Controllable Linkability," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1109-1124, June 2015.

[2] Li Xiang. Research on Privacy Protection in Energy Internet Incentive Demand Response [D].North China Electric Power University (Beijing),2018.

[3] Research Reports International. Advanced Metering Infrastructure. Research Reports International, June 2007.pp.109-131.

[4] P. O. Leu and D. Peter, "Case study: Information flflow resilience of a retail company with regard to the electricity scenarios of the sicherheitsverbundsübung schweiz (Swiss security network exercise) SVU 2014," in Proc. Int. Conf. Critical Inf. Infrastruct. Security, Berlin, Germany, 2015, pp. 159–170.

[5] Xingze He, Man-On Pun and C. -. J. Kuo, "Secure and efficient cryptosystem for smart grid using homomorphic encryption," 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), 2012, pp. 1-8, doi: 10.1109/ISGT.2012.6175676.

[6] C. Efthymiou and G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," 2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, 2010, pp. 68-243.

[7] J. Liu and Y. Xiao, "An accountable neighborhood area network in smart grids," in Proc. Int. Conf. Embedded Multimedia Comput., Gwangju, South Korea, Sep. 2012, pp. 171–178.

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

[9] Y. Gong, Y. Cai, Y. Guo and Y. Fang, "A Privacy-Preserving Scheme for Incentive-Based Demand Response in the Smart Grid," in IEEE Transactions on Smart Grid, vol. 7, no. 3, pp. 1304-1313, May 2016.

[10] Zhang, S., K. Wang and B. Wang, {A user-transparent pseudonym renewal scheme for smart meters in incentive-based demand response programs}. {INTERNATIONAL JOURNAL OF ELECTRICAL POWER \& ENERGY SYSTEMS}, 2019. {109}: p. {49-56}.

[11] Du Hongzhen.Research on several problems of digital signature technology [D]. Beijing University of Posts and Telecommunications,2009.

[12] Zhang Jinquan, Liu Huanping.A Fair Blind Signature Scheme Based on RSA [J]. Journal of Suihua University,2005(02):166-167.

[13] Z. Sui, M. Niedermeier and H. de meer, "TAI: A Threshold-Based Anonymous Identification Scheme for Demand-Response in Smart Grids," in IEEE Transactions on Smart Grid, vol. 9, no. 4, pp. 3496-3506, July 2018.

[14] S. Zeng, S. Jiang, and Z. Qin, "An efficient conditionally anonymous ring signature in the random oracle model," Theor. Comput. Sci., vol. 461, pp. 106–114, Nov. 2012.

[15] Y. Komano, K. Ohta, A. Shimbo, and S. Kawamura, "Toward the fair anonymous signatures: Deniable ring signatures," in Proc. CrypgologyCT_RSA, San Jose, CA, USA, Feb. 2006, pp. 174–191.