An Efficiency Batch Authentication Scheme for Smart Grid Using Binary Authentication Tree

Lili Yan, Yan Chang, and Shibin Zhang
College of Information Security Engineering, Chengdu University of Information Technology, China

Abstract: *The Smart Grid (SG) is designed to replace traditional electric power infrastructure that manages electricity demand in a sustainable, reliable and economic manner. Advanced Metering Infrastructure (AMI) is proposed as a critical part of the smart grid. The gateway of AMI receives and verifies a mass of data from smart meters within a required interval. This paper focuses on the computation overhead of gateway, and proposes a batch authentication scheme based on binary tree. The proposed scheme enables the gateway to batch authenticate data. The computation cost to verify all messages only requires n multiplications and 2 pairing operations where n is the number of smart meters. That significantly reduces the computation cost of gateway, especially when the number of smart meters in the AMI gets large. We analyze security and performance of proposed scheme in detail to show that the proposed scheme is both secure and efficient for AMI in smart grid.*

Keywords: *Smart grid, smart meter, security, authentication.*

Received July 22, 2015; accepted January 1, 2017

1. Introduction

Recently, Smart Grid (SG) has attracted attentions from researchers in both electric power and communication sectors, which is considered as the next-generation power supply network. Smart grid is a modernized electrical grid that uses analogue or digital information and communications to gather and act on information. These information includes the behavior of supplier and consumer. According to these information, we improve the efficiency, reliability, economics, sustainability of production and distribution of electricity [23] in an automated fashion. Smart grid collects data from vast number of electronic household appliances, smart meters, distribution facilities and other devices. Compared with traditional communication network systems, smart grid has new goals, requirements and assumptions [29].

Figure 1 shows the communication architecture for smart grid, which includes Home Area Network (HAN), Building Area Network (BAN) and Neighborhood Area Network (NAN). There is a Control Center (CC) in each NAN which manages NAN. CC collects data from NAN gateway, sends real-time electricity bills to customers, and further sends the control information to customers. CC is also responsible for generating and assigning related parameters for NAN Gate Way (GW), BAN GW and smart meters. Advanced Metering Infrastructure (AMI) is a key element in smart grid which contains a component called Smart Meter (SM). AMI has two-way communication between smart meter and power appliances. SM is a rather limited resources with low memory and computational capacity.

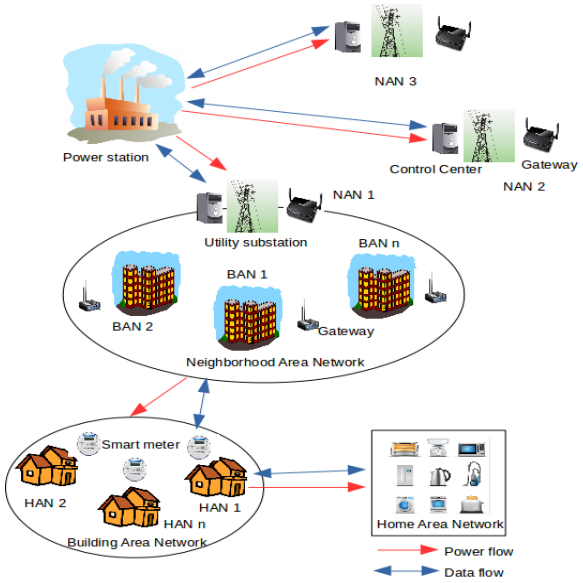

Figure 1. Communication architecture for smart grid.

The smart meters send various information of appliances to CC. In particular, one of information is the real-time power demands. CC sends the real-time statement to smart meter which allows customers to know how much electricity they use. Since these information may leak the daily life which should be private. Therefore, it is extremely important to propose an authentication scheme to provide communication security.

2. Related Work

Security and privacy face many challenges in smart grid. Researchers are working on the development of smart grid security requirements [3, 4, 6, 7, 10, 11, 12, 16, 24]. Many authentication schemes have been

proposed to achieve different security goals for smart grid [1, 5, 13, 14, 18, 19, 20, 21, 25, 26, 27, 28].

Fouda *et al*. [5] proposed a light weight message authentication scheme for smart grid based on Diffie-Hellman algorithm. This scheme solved the mutual authentication problem between HAN GW and BAN GW. Kamto *et al*. [12] proposed a key management which combined Needham-Schroeder authentication protocol and elliptic curve cryptography. The key management scheme relies on a trust anchor to establish session key. Xia and Wang [28] found that the Wu and Zhou [25] scheme is vulnerable to the man-in-the-middle attack.

Nabeel *et al*. [19] designed a key management scheme to achieve secure communication in the AMI based on the use of Physically Unclonable Function (PUF) devices. The scheme provides a hardware based strong authentication mechanism. However, the proposed scheme relies on a single centralized sever to store secrets for all smart meters, which makes the scheme unscalable [26].

A key management scheme is designed for AMI in [13]. The scheme is constructed based on a key graph [27] to achieve secure communication. Unfortunately, [26] found that the scheme has severe weakness which makes it susceptible to DoS attacks. Then Wan *et al*. [26] proposed a key management scheme which combined identity-based cryptosystem and efficient key tree technique. The scheme achieves secure communication between smart meters and meter data management systems.

Gave an authentication scheme for smart grid based on merkle hash tree [14]. The scheme considers the smart meters with computation-constrained resource and uses only simple hash computations. Although the scheme considers the computation overhead on smart meters, BAN gateway also needs to verify every smart meter's message separately, and smart meters need to store many data. The protocol also cannot resist the replay attack.

In order to achieve real-time electricity consumption report collection and allow customers to get real-time statement, smart meter should communicate with BAN gateway in a short time such as 15 minutes. Thus, BAN gateway needs to authenticate all messages which are sent by smart meters in the area. There are thousands of smart meters in each BAN. So, the computation overhead is heavy for BAN gateway which applies these authentication scheme [5, 12, 13, 18, 19, 21, 25, 26, 27, 28]. In this paper, we propose an efficiency batch authentication scheme based on binary tree which is a secure authentication and key agreement framework for smart grid. In the proposed scheme, BAN GW can batch authenticate all smart meters in one time. That noticeably reduces computation cost of BAN GW, especially there are a large number of smart meters.

3. Preliminaries

In this section, we first give the communication architecture of smart grid. Then the identity-based cryptography and bilinear pairings are given which are the foundation of the proposed scheme.

3.1. Smart Grid AMI Communication Architecture

AMI is one of the critical parts of a smart grid system. Figure 2 shows our considered SG communication architecture for AMI. It consists of the following components: a BAN GW, several smart meters and electronic household appliances. The BAN GW is responsible for gathering, analyzing and storing data such as real-time power demands which are sent from smart meters to NAN GW. Then it also receives instructions such as real-time statement which are sent from NAN GW to smart meters. To facilitation communication between smart meter and BAN GW, Wi-Fi will be adopted. Meantime, a smart meter comprises MSP430-F4270, Its memory size is up to 8KB Random Access Memory (RAM) and 120 KB Flash memory. The BAN GW is also a smart meter which is equipped with a high-power server, 160 MHz CPU, 128 KB RAM, and 1MB flash memory is considered [20].

Due to the limited computation and storage resources for smart meter, the computational efficiency should be considered. BAN GW needs to mange thousands of smart meters, the computational efficiency is also a challenging issue. In this paper, we focus on secure mutual communication between the BAN GW and smart meter in HAN.

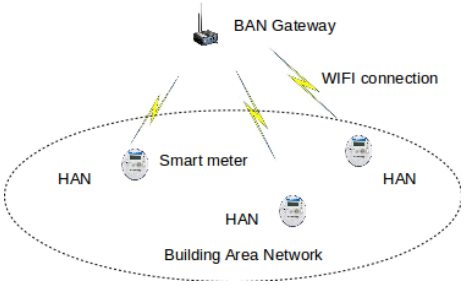

Figure 2. Smart grid architecture for AMI.

3.2. Identity-Based Cryptography and Bilinear Pairings

Identity-based cryptography can simplify certificate management. The public key of user is his unique identity information. The pairing-based scheme offers lower transmission cost which compares with the RSA based schemes. In this section, we briefly describe the definition and properties of the bilinear pairings.

Let G_1 be a cyclic additive group generated by P, whose order is prime q, and G_2 be a cyclic multiplicative group of the same order q. A bilinear

pairing is a map $\hat{e}: G_1 \times G_1 \to G_2$ with the following properties:

1. Bilinear: $\forall P, Q, R \in G_1$ and $\forall a, b \in Z$, $\hat{e}(Q, P+R) = \hat{e}(P+R, Q) = \hat{e}(P, Q) \cdot \hat{e}(R, Q)$. Especially, $\hat{e}(aP, bP) = \hat{e}(P, bP)^a = \hat{e}(aP, P)^b = \hat{e}(P, P)^{ab}$.
2. Non-degenerate: $\exists P, Q \in G_1$ such that $\hat{e}(P, Q) \neq 1$.
3. Computable: $\forall P, Q \in G_1$,there is an efficient algorithm to calculate $\hat{e}(P, Q)$.

Such a bilinear pairing can be constructed by the revised Weil pairing [1] or Tate pairing [17] with elliptic curves. With such a group G_1, the Computational Diffie-Hellman (CDH) problem is hard, but Decision Diffie-Hellman problem (DDH) is easy. They can be stated as follows.

The CDH problem: given $\forall a, b \in Z_P$ and $P, aP, bP \in G_1$, find the element abP.

The DDH problem: given $P, aP, bP, abP \in G_1$ for $\forall a, b, c \in Z_P$, decide whether $c = ab \pmod q$.

4. The Proposed Scheme

When BAN gateway receives data from smart meters, it needs to verify them. In this section, we propose a robust and efficient batch authentication scheme for smart grid. Firstly, a basic signature scheme is given.

4.1. Basic Authentication Scheme

Firstly, CC generates basic parameters. When smart meter joins a smart grid, it first registers with the CC. The proposed scheme based on [9, 22] which has four phases: Setup, Registration, Authentication phase and Key refreshment. The notations used throughout the paper are shown in Table 1.

Table 1. Notations used in the paper.

Symbol	Definition
ID_i	Unique identity of SM_i
DID_i	Dynamic identity of SM_i
h(),h_1()	The one-way hash function
⊕	The bitwise XOR operation
H( )	MapToPoint hash function such as H: $\{0,1\}^* \to G_1$

- *Setup phase*: CC sets up the following basic parameters. Let G_1 be a cyclic additive group generated by P, whose order is prime q, and G_2 be a cyclic multiplicative group of the same order q. A bilinear pairing is a map ê:$G_1 \times G_1 \to G_2$. The CC randomly selects $s \in Z_q^*$ as its secret master key, and computes $P_{pub}=sP$ as its public keys.
- *Registration*: BAN GW and smart meters register before they join the smart grid. BAN GW is preloaded with the public parameters $\{G_1, G_2, q, P, P_{\text{pub}}, h, h_1, H()\}$. Each smart meter obtains its system parameters as follows.

1) Smart meter SM_i sends its ID_i to the CC when it joins the network.
2) CC picks a secret random $x_i \in Z_q^*$, compute g^{xi}, $DID_i = h(h(g^{x_i}) \oplus ID_i)$ and $sk_i = sH(DID_i)$.
3) Lastly, the CC sends$\{G_1, G_2, q, P, P_{\text{pub}}, h, h_1, H()\}$and $\{DID_i, sk_i, h(g^{xi})\}$to SM_i through a secure channel [30].

The registration phase must be run before smart meters are deployed in the smart gird. It is the setup phase, runs offline which is done by an administrator.

- *Authentication Phase*:

1. In order to collect the real-time electricity consumption report, smart meter SM_i needs to send related information m_i to BAN GW. To sign this message, SM_i first selects a random $r_i \in Z_q^*$, computes $A_i=r_iP$ and where $M_i=Enc_{h(gxi)}(DID_i, m_i, T_i)$ and *Enc* is a symmetric encryption algorithm such as AES or DES. Finally, SM_i send the message $<DID_i, A_i, B_i, M_i, T_i, C_i>$ $B_i=sk_i+h(M_i, A_i)r_iP_{pub}$ where $C_i=h_1(A_i, B_i, M_i, T_i)$ to the BAN GW.
2. On receiving the message $< DID_i, A_i, B_i, M_i, T_i, C_i >$. Checks if $(T^*-T_i) \leq \Delta T$ then BAN GW proceeds to next step, else abort, where T^* is the current time, ΔT denotes the maximum allowed transmission delay.

Computes $\hat{e}(B_i,P)=\hat{e}(H(DID_i)+h(M_i,A_i)A_i,P_{pub})$, since it can be verified as follows,

$$\begin{aligned} \hat{e}(B_i, P) &= \hat{e}(sk_i + h(M_i, A_i) r_i P_{pub}, P) \\ &= \hat{e}(sH(DID_i), P) \cdot \hat{e}(h(M_i, A_i) r_i P_{pub}, P) \\ &= \hat{e}(H(DID_i), P_{pub}) \cdot \hat{e}(h(M_i, A_i) r_i sP, P) \\ &= \hat{e}(H(DID_i), P_{pub}) \cdot \hat{e}(h(M_i, A_i) r_i P, P_{pub}) \\ &= \hat{e}(H(DID_i) + h(M_i, A_i) A_i, P_{pub}) \end{aligned} \quad (1)$$

Clearly, the computation cost to verify a signature primarily consists of one multiplication and two pairing operations. Compared with multiplication operation, the computation cost of a pairing operation is much higher.

4.2. Batch Authentication Scheme

In order to collect real-time electricity consumption report, every t minutes, such as t=15 min, each SM_i sends electricity report to the BAN GW. In addition, they also need to send other information such as emergency information to BAN GW. In this paper, we just consider the real-time electricity consumption information. Each time, BAN GW verifies n multiplication and 2n pairing operations where n is the number of smart meters. This will become a performance bottleneck with the increasing number of smart meters. In order to solve the problem, a batch authentication scheme is proposed based on binary tree.

Suppose that there are $n=2^h$smart meters {SM_1, SM_2, ..., SM_n}, the binary tree is shown in Figure 3.

Each leaf-node <h, v> is a smart meter which associated with the signature messages C_{i+1}=<A_{i+1},B_{i+1}> of SM_{i+1}, (i=0, 1, 2, ..., n-1).

Each inner-node <l, v> ($I \le (h-1)$) is associate with an aggregate signature {S_{k1} ,...., S_{k2}}, where $k_1=2^{h-1}.v$ and $k_2=2^{h-1}.(v+1)-1$. The root node is an aggregate signature of all node.

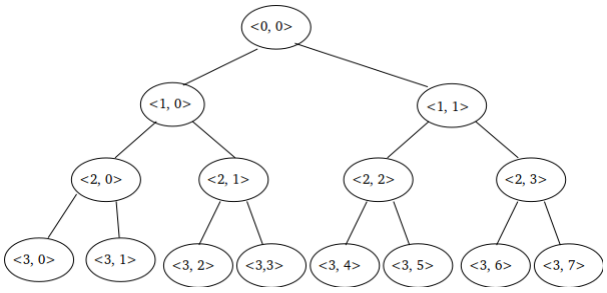

Figure 3. Binary authentication tree.

For instance, SM_1, SM_2, ..., SM_n send messages <DID_1, A_1, B_1, M_1, T_1, C_1> ,< DID_2, A_2, B_2, M_2, T_2, C_2>, ..., <DID_n, A_n, B_n, M_n, T_n,C_n> to BAN GW. Firstly, BAN GW checks if (T^*- T_j)$\le \Delta T$ where T^* is the current time of BAN GW (j=1, 2, ..., n), T_j is the time of SM_j. T_1, T_2,…, T_n maybe not the same time, but they must in the same time interval.

Then BAN GW can batch verify the messages by $\hat{e}(\sum_{i=k_1}^{k_2} B_i, P) = \hat{e}\{\sum_{i=k_1}^{k_2}[H(DID_i)+h(M_i,A_i)A_i], P_{pub}\}$ where $k_1 = 2^{h-l}\cdot v$ and $k_2=2^{h-1}.(v+1)-1$, since it can be proofed with the following steps.

$$\begin{aligned}
&\hat{e}(\sum_{i=k_1}^{k_2} B_i, P) = \hat{e}\{\sum_{i=k_1}^{k_2}[sk_i + h(M_i,A_i)r_iP_{pub}], P\} \\
&= \hat{e}(\sum_{i=k_1}^{k_2} sH(DID_i), P)\cdot \hat{e}(\sum_{i=k_1}^{k_2} h(M_i,A_i)r_iP_{pub}, P) \\
&= \hat{e}(\sum_{i=k_1}^{k_2} H(DID_i), sP)\cdot \hat{e}(\sum_{i=k_1}^{k_2} h(M_i,A_i)r_isP, P) \\
&= \hat{e}(\sum_{i=k_1}^{k_2} H(DID_i), P_{pub})\cdot \hat{e}(\sum_{i=k_1}^{k_2} h(M_i,A_i)r_iP, P_{pub}) \\
&= \hat{e}\{\sum_{i=k_1}^{k_2}[H(DID_i)+h(M_i,A_i)A_i], P_{pub}\}
\end{aligned} \quad (2)$$

If they are all leaf nodes, just smart meters SM_1, SM_2,…, SM_n, it can become $\hat{e}(\sum_{i=1}^{n} B_i, P) = \hat{e}\{\sum_{i=1}^{n}[H(DID_i)+h(M_i,A_i)A_i], P_{pub}\}$. Thus, BAN GW can verify all the smart meters SM_1,SM_2,…, SM_n with $\hat{e}(\sum_{i=1}^{n} B_i, P) = \hat{e}\{\sum_{i=1}^{n}[H(DID_i)+h(M_i,A_i)A_i], P_{pub}\}$, which just needs n multiplication and 2 pairing operations. That can noticeably reduce the computation cost.

If the verification holds, BAN GW authenticates smart meters and proves them legitimacy. In contrast, BAN GW has to compute $C_i^* = h_1(DID_i, A_i, B_i, M_i, T_i)$ and uses it to check whether it equals with the received value C_i (i = 1, 2, ..., n), thereby authenticating smart meters and finding malicious meters.

Because all smart meters are leaf nodes, BAN GW unaffected when smart meter adds or leaves the smart grid in the scheme.

In order to protect the session key, the scheme presents a key refreshment mechanism. Smart meters and BAN GW update their session key during the key change phase. The system sets the update interval which is saved in smart meters and BAN GW as a system parameter. When the refreshment process, the SM and CC separately re-compute a new session key g^{xi}=h(g^{xi}).

Moreover, user must input the ID and g^{xi} to the smart meter when user wants to obtain the data in smart meter. The smart meter verifies the validity of ID and g^{xi} with stored values DID and $h(g^{xi})$.

After authenticating smart meters, BAN GW decrypts $M_i = Enc_{h(g^{xi})}(DID_i, m_i, T_i)$ and gets the message m_i where T_i is a timestamps which is used to resist replay attack.

5. Security and Performance Evaluations

In this section, we present the security analysis and performance evaluation about our scheme. We also discuss and compare performance of the proposed scheme with RSA based authentication scheme.

5.1. Security Analysis

Following the threat model [14], we refer to the discussion about the most concerned attacks such as integrity, replay, impersonation and MIMT attack. The main security features of the protocol is given as follows:

1. Replay Attack: In the protocol, we add a timestamp in messages <DID_i, A_i, B_i, M_i, T_i, C_i> where $M_i = Enc_{h(g^{xi})}(DID_i, m_i, T_i)$. When BAN GW receives messages, they first validates the timestamp. The attacker cannot obtain the key g^{xi}. Hence, we conclude that a replay attack cannot work in the protocol.
2. Impersonation attack: If attacker wants to masquerade as a legal smart meter, he/she must intercept the message sent by smart meter and forge fake authentication messages < DID_i, A_i, B_i, M_i, T_i, C_i > to BAN GW. However, because $A_i=r_iP$, $B_i=sk_i+h(M_i,A_i)r_iP_{pub}$, $C_i=h_1$ (A_i, B_i, M_i, T_i, C_i) (where $M_i = Enc_{h(g^{xi})}(DID_i, m_i, T_i)$ in our scheme. The attacker cannot forge valid authentication messages without knowing P, sk_i, P_{pub}. The attacker needs to know ID and g^{xi} if he/she want to obtain P, sk_i, P_{pub}. Hence, our scheme can resist impersonation attack.
3. Integrity assurance: In the proposed scheme, BAN GW authenticates every smart meter

by $\hat{e}(B_i, P) = \hat{e}(H(DID_i) + h(M_i, A_i)A_i, P_{pub})$, and there is an authentication data $C_i=h_1 (A_i, B_i, M_i, T_i)$ in every message. If messages are changed, BAN GW can find that. So, these messages cannot be tampered in our scheme.

4. MIMT: The adversary may receive messages which transmit between smart meters and BAN GW. Each SM sends the encryption message M_i to BAN GW where $M_i = Enc_{h(g^{x_i})}(DID_i, m_i, T_i)$ is the cipher-text encrypted by the key $h(g^x)^i$. Although the adversary accesses the data M_i, he/she cannot decrypt them and inject new valid data during the communication.

By the informal analysis, our scheme has the ability to resist various possible known attacks and suitable for SG environment.

5.2. Performance Evaluations

In this section, we discuss the computation complexity of the proposed scheme. Clearly, the computation cost to verify signatures which consists of multiplication, pairing operation, hash operation. Compared with hash operation, the computation cost of multiplication operation and pairing operation is much higher. We mainly consider the cost of multiplication operation and pairing operation in the scheme. Let T_{mul} denotes the time cost to perform one point multiplication over an elliptic curve, T_{par} is the time of a pairing operation, and $B(h, t)$ and $C(h, t)$ denote the computation cost of bath authentication and basic authentication scheme respectively, where h is the height of tree and t is bogus signatures in its leaf node.

- *Lemma* 1: Given a smart grid which has $n = 2^h$ smart meters SM_1, $SM_{2,...}SM_n$ in a BAN, BAN GW needs to receive and authenticate n messages in one period. The smart meter can be constructed an authentication tree with height h and 0 forged signatures among them.

$B(h, 0) = nT_{mul} + 2T_{par}$, which the computation cost is minimized.

- *Lemma* 2: (Best and Worse Cases) Given a smart grid which has $n=2^h$ smart meters SM_1, $SM_{2,....}$ SM_n in a BAN, BAN GW needs to receive and authenticate n messages in one period. The smart meter can be constructed an authentication tree with height h and k forged signatures among them. BAN GW need to find the forge smart meters with binary search algorithm. BAN GW authenticates inner-node <1, 0> and <1, 1> where <1, 0> includes leaf-node <3, 0>, <3, 1>, <3, 2> , <3, 3> and <1, 1> includes leaf-node <3, 4>, <3, 5>, <3, 6> , <3, 7>. If the bath verification of inner-node <1, 0> holds, BAN GW has authenticated leaf-node <3, 4>, <3, 5>, <3, 6> , <3, 7> and proved them legitimacy. In contrast, BAN GW need verifies <2, 0> and <2, 1>. The binary tree is shown in Figure 3.

1) The best computation cost is:

$$k=1,\ B(h, 1) = nT_{mul} + 2(2h+1)\ T_{par} + \sum_{l=1}^{h} 2^{(1-l)} nT_{mul} \quad (3)$$

2) The worst computation cost is

$$k=n,\ B(h, n) = \sum_{l=0}^{h} 2^{(1+l)} T_{par} + (h+1)nT_{mul} \quad (4)$$

The average computation cost of bath authentication scheme is

$$\frac{B(h,1) + B(h,n)}{2} = \frac{\sum_{l=1}^{h} 2^{(1-l)} nT_{mul} + (h+1)nT_{mul}}{2} + (2h+1)T_{par} + \sum_{l=0}^{h} 2^{l} T_{par} \quad (5)$$

The computation cost of basic authentication scheme is $C(h, k)=2nT_{mul}+2(n+1)\ T_{par}$.

The computation cost of bath authentication scheme is very higher when it is used to find forge smart meters. Therefore, BAN GW can find forge smart meters by checking $C_i=h_1(A_i, B_i, M_i, T_i)$, if there are malicious smart meters in smart grid.

Recently, the RSA algorithm was suggested to secure smart grid [8], we compare our protocol with the RSA based authentication scheme. In computation complexity, we mainly consider RSA, pairing operations and point multiplication in these protocols. In RSA based scheme, the BAN GW needs to perform a RSA signature verification to verify every smart meter's signature. Experiments have been conducted to study the execution. We adopt the benchmarks of the pairing-based [15] and RSA based cryptography [2] as shown in Table 2. The implementation was executed on an Intel(R) Core(TM) i5-4300M 2.6-GHz machine.

Table 2. Benchmarks of cryptographic operation.

Description	Ececution Time
Pairing	2.275ms
Point Multiplication	0.004ms
RSA signature verification	0.284ms

With the benchmarks given in Table 2, we demonstrate computation overhead of BAN GW of our scheme and compare with the RSA based authentication scheme showed in Figure 4. Every 15 min, BAN GW should receive the electricity consumption reports from all smart meters in the BAN. On Figure 4 the smart grid which has n smart meters. BAN GW needs to verify n RSA signature in the RSA based authentication scheme. In our scheme, it needs to perform n T_{mul} and 2 T_{par} to verify whether or not there are forged signatures among the message. As shown in the table, the total computation cost significantly increases with the increasing number of smart meters in the RSA based scheme.

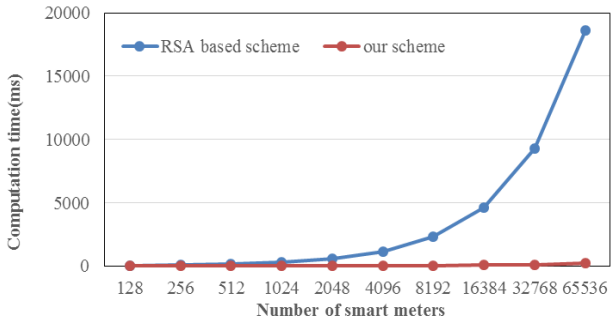

Figure 4. Computation cost of BAN gateway.

6. Conclusions

Secure and efficient authentication scheme is critical for ensuring security in smart grid. In this paper, we proposed a bath authentication scheme for the AMI system in smart grid. Detailed security analysis and performance evaluation show that the proposed scheme can meet the security require of smart grid. And the BAN GW has lower computation cost when they bath authenticate messages in our scheme. For our future work, we will explore new method to find out fake signatures.

References

[1] Boneh D. and Franklin M., "Identity-Based Encryption from the Weil Pairing," *in Proceedings of Annual International Cryptology Conference*, Santa Barbara, pp. 213-229, 2001.

[2] Dai W., Crypto++ 5.6.2 Benchmarks 2013. [Online]. Available: http://www.cryptopp.com/, Last Visited, 2013.

[3] Ericsson G., "Cyber Security and Power System Communication Essential Parts of A Smart Grid Infrastructure," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, pp. 1501-1507, 2010.

[4] Fang X., Misra S., Xue G., and Yang D., "Smart Grid-the New and Improved Power Grid: a Survey,"*IEEE Communications Surveys and Tuto rials*, vol. 14, no. 4, pp. 944-980, 2012.

[5] Fouda M., Fadlullah Z., Kato N., Lu R., and Shen X., "A Lightweight Message Authentication Scheme for Smart Grid Communications," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 675-685, 2011.

[6] Hamlyn A., Cheung H., Mander T., Wang L., Yang C., and Cheung R., "Network Security Management and Authentication of Actions for Smart Grids Operations," *in Proceedings of IEEE Canada Electrical Power Conference*, Que, pp. 417-422, 2007.

[7] Hammad M., Ibrahim M., and Hadhoud M., "A Novel Biometric Based on ECG Signals and Images for Human Authentication," *The International Arab Journal for Information Technology*, vol. 13, no. 6A, pp. 959-964, 2016.

[8] Harvey M., Long D., and Reinhard K., "Visualizing NISTIR 7628, Guidelines for Smart Grid Cyber Security," *in Proceedings of IEEE Power and Energy Conference*, Illinois, pp. 1-8, 2014.

[9] Jiang Y., Shi M., Shen X., and Lin C., "BAT: A Robust Signature Scheme For Vehicular Networks Using Binary Authentication Tree," *IEEE Transactions on Wireless Communications*, vol. 8, no. 4, pp. 1974-1983, 2009.

[10] Kursawe K., Danezis G., and Kohlweiss M., "Privacy-Friendly Aggregation for the Smart-Grid," *in Proceedings of International Symposium on Privacy Enhancing Technologies Symposium*, Berlin, pp. 175-191, 2011.

[11] Krishna E., Reddy T., Reddy M., Reddy G., Madhusudhan E., and Almuhteb S., "Securing Smart Grid Technology," *in Proceedings of International Conference on Graphic and Image Processing*, Singapore, 2012.

[12] Kamto J., Qian L., Fuller J., and Attia J., "Light-Weight Key Distribution and Management for Advanced Metering Infrastructure," *in Proceedings of IEEE GLOBECOM Workshops*, Houston, pp. 1216-1220, 2011.

[13] Liu N., Chen J., Zhu L., Zhang J., and He Y., "A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid" *IEEE Transactions on Industrial Electronics*, vol. 60, no. 10, pp. 4746-4756, 2013.

[14] Li H., Lu R., Zhou L., Yang B., and Shen X., "An Efficient Merkle-Tree-Based Authentication Scheme for Smart Grid," *IEEE Systems Journal*, vol. 8, no. 2, pp. 655-663, 2014.

[15] Lynn B., PBC Library Manual 0.514 Benchmarks 2013. [Online]. Available: http://crypto.stanford.edu/pbc/, Last Visited, 2013.

[16] Moslehi K. and Kumar R., "A Reliability Perspective of the Smart Grid," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 57-64, 2010.

[17] Miyaji A., Nakabayashi M., and Takano S., "New Explicit Conditions of Elliptic Curve Traces For FR-Reduction," *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, vol. E84-A, no. 5, pp. 1234-1243, 2001.

[18] Nicanfar H., Jokar P., Beznosov K., and Leung V., "Efficient Authentication and Key Management Mechanisms for Smart Grid Communications," *IEEE Systems Journal*, vol. 8, no. 2, pp. 629-640, 2014.

[19] Nabeel M., Kerr S., Ding X., and Bertino E., "Authentication and Key Management for Advanced Metering Infrastructures Utilizing Physically Unclonable Functions," Technical

Report, Purdue University, 2012.
[20] O'Connell D. and De Vries I., "Digital Energy Metering for Electrical System Management," *in Proceedings of the ACM Symposium on Applied Computing*, Sierre, pp. 516-520, 2010.
[21] Seo S., Ding X., and Bertino E., "Encryption Key Management For Secure Communication In Smart Advanced Metering Infrastructures," *in Proceedings of IEEE International Conference on Smart Grid Communications*, Vancouver, pp. 21-24, 2013.
[22] Shim K., "Reconstruction of a Secure Authentication Scheme for Vehicular Ad Hoc Networks Using a Binary Authentication Tree," *IEEE Transactions on Wireless Communications*, vol. 12, no. 11, pp. 5386-5393, 2013.
[23] Ton D., Wang W., and Wang W., "Smart Grid R&D by the U.S. Department of Energy to Optimize Distribution Grid Operations," *in Proceedings of IEEE Power and Energy Society General Meeting*, Detroit, pp. 1-5, 2011.
[24] Wang W. and Lu Z., "Cyber Security in Smart Grid: Survey and Challenges," *Computer Network*, vol. 57, no. 5, pp. 1344-1371, 2013.
[25] Wu D. and Zhou C., "Fault-Tolerant and Scalable Key Management for Smart Grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 371-378, 2011.
[26] Wan Z., Wang G., Yang Y., and Shi S., "SKM: Scalable Key Management for Advanced Metering Infrastructure in Smart Grid," *IEEE Transactions on Industrial Electronics*, vol. 61, no. 12, pp. 7055-7066, 2014.
[27] Wong C., Gouda M., and Lam S., "Secure Group Communication Using Key Graphs," *IEEE/ACM Transactions on Networking*, vol. 8, no. 1, pp. 16-30, 2000.
[28] Xia J. and Wang Y., "Secure Key Distribution for the Smart Grid," *IEEE Transactions on Smart Grid* , vol. 3, no. 3, pp. 1437-1443, 2012.
[29] Yan Y., Qian Y., Sharif H., and Tipper D., "A Survey on Cyber Security for Smart Grid Communications," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 4, pp. 998-1010, 2012.
[30] Yeh H., Chen T., Liu P., Kim T., and Wei H., "A Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography," *Sensors*, vol. 11, no. 5, pp. 4767-4779, 2011.

Lili Yan received her Ph.D. degree in information security from Southwest Jiaotong University, Sichuan, China, in 2011. She is currently an associate professor in Chengdu University of Information Technology. Her research interests include information security and secure communicatin.

Yan Chang received her Ph.D. degree in information security from University of Electronic Science and Technology of China in 2016. She is currently an associate professor in Chengdu University of Information Technology. Her research interests are quantum information, information security.

Shibin Zhang received his Ph.D. degree in traffic information engineering and control from Southwest Jiaotong University, Sichuan, China, in 2006. He is currently a professor in Chengdu University of Information Technology. His research interests include information security, and cryptography.