An Efficient Merkle-Tree-Based Authentication Scheme for Smart Grid

Hongwei Li, *Member, IEEE*, Rongxing Lu, *Member, IEEE*, Liang Zhou, *Member, IEEE*, Bo Yang, *Member, IEEE*, and Xuemin (Sherman) Shen, *Fellow, IEEE*

***Abstract*—Smart grid has emerged as the next generation of power grid, due to its reliability, flexibility, and efficiency. However, smart grid faces some critical security challenges such as the message injection attack and the replay attack. If these challenges cannot be properly addressed, an adversary can maliciously launch the injected or replayed message attacks to degrade the performance of smart grid. To cope with these challenging issues, in this paper, we propose an efficient authentication scheme that employs the Merkle hash tree technique to secure smart gird communication. Specifically, the proposed authentication scheme considers the smart meters with computation-constrained resources and puts the minimum computation overhead on them. Detailed security analysis indicates its security strength, namely, resilience to the replay attack, the message injection attack, the message analysis attack, and the message modification attack. In addition, extensive performance evaluation demonstrates its efficiency in terms of computation complexity and communication overhead.**

***Index Terms*—Authentication, Merkle hash tree, smart grid.**

I. Introduction

DUE TO the lack of effective real-time diagnosis and healing, the traditional power grid is sporadically suffering from failures and blackouts. For example, on August 14, 2003, power system outage affected large portions of the Northeastern U.S. and Canada, which ultimately caused a $6 billion loss in economic revenue [1]. Recently, smart grid has attracted increasing attention [2]–[5]. Compared with the traditional power grid, smart grid is featured with many attractive characteristics, e.g., self-monitoring, self-healing, remote check, pervasive control, and more customer choices [6]–[9]. Smart grid is expected to be the next generation of power system.

In the traditional power grid, the architecture is featured with the one-way electrical flows, i.e., electricity utility only delivers power to the consumers. In addition to the one-way electrical flows, smart grid also provides an attractive feature, i.e., two-way information flow communication. As depicted in Fig. 1, parallel to the one-way power flows, two-way information flow sharing is also implemented. In the two-way information flow sharing, the neighborhood gateway can collect electricity consumption reports from the customers via a wireless connection. Then, the neighborhood gateway sends the electricity reports to the control center via a wired link with high bandwidth and low delay. Based on the statistics and analysis of the aforementioned electricity reports, the control center can further respond the real-time pricing information to the customers for their lower electricity bills, or send the control information to flatten the demand peak [10], [11].

The consumption-reporting device at the customer side is called the smart meter, which is vulnerable to malicious operations, e.g., the meter's reading modification [12]. Currently, in the U.S., such reading modifications have resulted in a $6 billion loss [13]. It is indispensable for electricity utility to prevent the malicious operations. Furthermore, with a mass of smart meters being deployed in the smart grid, the malicious operations become more sophisticated. For instance, a large number of replayed/injected electricity consumption reports might maliciously be sent to the control center. If the attacks cannot be detected, the control center will be misled and make incorrect decisions, such as send a false pricing information to the customers. Therefore, it is extremely important to develop an authentication scheme to detect the replayed/injected messages. In addition, a smart meter is only equipped with limited resources, i.e., a computation-constrained microprocessor, a small memory, a low computational capacity, etc. However, the computation overhead is heavy for the smart meter. For example, the initial deployments of the advanced metering infrastructure in Ontario, Canada, support meter readings at 5–60-min intervals [14]. The next generation of smart meters is planning to reduce these time intervals to 1 min or even less. Thus, the developed authentication scheme should minimize computation overhead on the smart meters.

In this paper, we address the aforementioned challenging issues by proposing an efficient authentication scheme for securing communication between the customers and the

Manuscript received April 15, 2012; revised October 3, 2012; accepted January 23, 2013. This work was supported by the National Natural Science Foundation of China under Grants 61103207, U1233108, 61272525, 61073106, and 61003232 by the Fundamental Research Funds for Chinese Central Universities under Grant ZYGX2011J059, and by the Natural Sciences and Engineering Research Council of Canada .

H. Li and B. Yang are with the School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: hongwei.uestc@gmail.com; boyang.uestc@gmail.com).

R. Lu is with the School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore (e-mail: rxlu@ntu.edu.sg).

L. Zhou is with the National Key Laboratory of Science and Technology on Communication, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: lzhou@uestc.edu.cn).

X. Shen is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: sshen@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/JSYST.2013.2271537

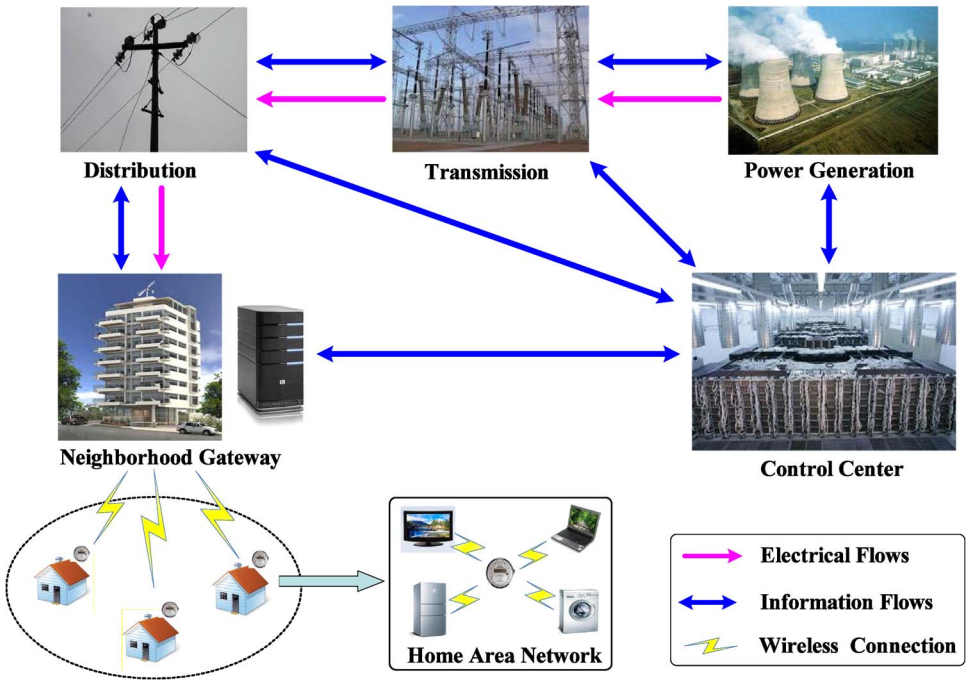


Fig. 1. Communication architecture for smart grid.

neighborhood gateway. Specifically, the contributions of this paper are twofold.

1) First, we propose a novel authentication scheme, where the Merkle hash tree technique is leveraged to facilitate the authentication implementation. The security analysis indicates that the proposed scheme can resist the replay attack, the message injection attack, the message analysis attack, and the message modification attack.
2) Second, extensive performance evaluation demonstrates that the proposed authentication scheme can achieve less communication overhead and dramatically reduce computation cost compared with the traditional authentication scheme, e.g., Rivest–Shamir–Adleman (RSA)-based authentication [15].

The remainder of the paper is organized as follows: In Section II, we present the system model, the threat model, and the design goal. Then, we propose the authentication scheme in Section III, followed by the security analysis and performance evaluation in Sections IV and V, respectively. We also present related works in Section VI. Finally, we draw our conclusions in Section VII.

II. Models and Design Goal

Here, we present the system model, the threat model, and the design goal.

A. System Model

In our system model, we focus on how the neighborhood gateway detects the replay attack, authenticates the source of electricity consumption reports, and ensures the reports' confidentiality and integrity. Specifically, as shown in Fig. 2, we consider a neighborhood area that covers a

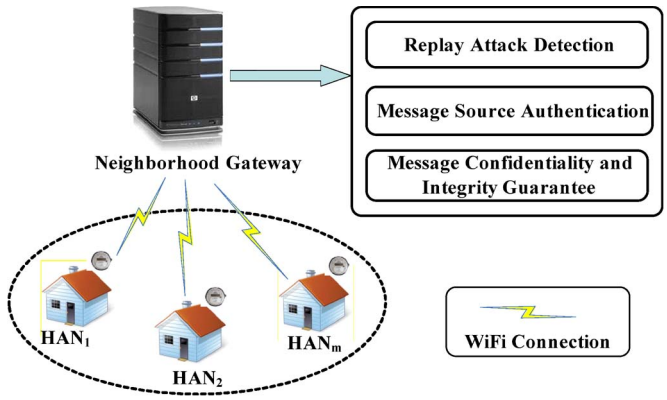


Fig. 2. System model.

neighborhood gateway connected with m home area networks (HANs).

1) The neighborhood gateway is equipped with a database for storing the detection and authentication information. The main functions of the neighborhood gateway are the replay attack detection, the message source authentication, and the message confidentiality and integrity guarantee.
2) Each HAN is equipped with a smart meter, which contains a processor, nonvolatile storage, and communication facilities. The smart meter can collect the electricity consumption report at small timescales, e.g., every 15 min [14], and send the report to the neighborhood gateway. Note that the sent report is featured with a certain format. We assume that the neighborhood gateway knows the certain format, which can help the neighborhood gateway detect the reports' integrity.

Communication between the HAN and the neighborhood gateway is through relatively inexpensive WiFi technology.

Within the WiFi coverage of the neighborhood gateway, each HAN user can directly communicate with the neighborhood gateway. Meantime, the neighborhood gateway is equipped with a high-power server, e.g., with the Inter Core i7 CPU and 6-GB random access memory (RAM). The smart meter has limited resource, e.g., MSP430-F4270, 8-KB RAM, and 120-KB Flash memory [16].

For the smart meter, the computational efficiency should be considered, due to the limited computation resources. In addition, for the neighborhood gateway, since hundreds of electricity consumption reports will be synchronously collected, the computational efficiency is also a challenging issue.

B. Threat Model

In our threat model, we assume that both the neighborhood gateway and the HAN users cannot be compromised. We consider a global external adversary$\mathcal{A}$ as follows.

1) *Global* indicates that the adversary $\mathcal{A}$ has full communication information of the whole smart grid.
2) *External* indicates that the adversary $\mathcal{A}$ can capture the communication messages between the neighborhood gateway and the HAN users, but not compromise the database of any HAN user.

Specifically, we consider that the adversary $\mathcal{A}$ can launch the following attacks.

1) *Replay attack:* The external adversary $\mathcal{A}$ captures the previous message and replays the out-of-date messages to the neighborhood gateway.
2) *Message injection attack:* The external adversary $\mathcal{A}$ sends fabricated messages to the neighborhood gateway. If the messages cannot be filtered, the control center might ultimately be misled and make incorrect decisions. It is essential to develop an efficient authentication technique to identify the illegitimate message source.
3) *Message analysis attack:* After eavesdropping a message from a HAN user, the external adversary $\mathcal{A}$ makes an attempt to recover the electricity consumer report. In this way, the privacy of the HAN user can be compromised.
4) *Message modification attack:* The external adversary $\mathcal{A}$ captures a message from a HAN user and attempts to tamper the message.

C. Design Goal

Under the aforementioned models, our design goal is to develop an efficient authentication scheme for smart grid. Specifically, the following two desirable objectives should be achieved.

1) The proposed scheme should be secure in the threat model. As previously stated, if the threats cannot be detected and excluded in the smart grid, the performance of smart grid will be degraded. Thus, the proposed scheme should resist the replay attack, the message injection attack, the message analysis attack, and the message modification attack.

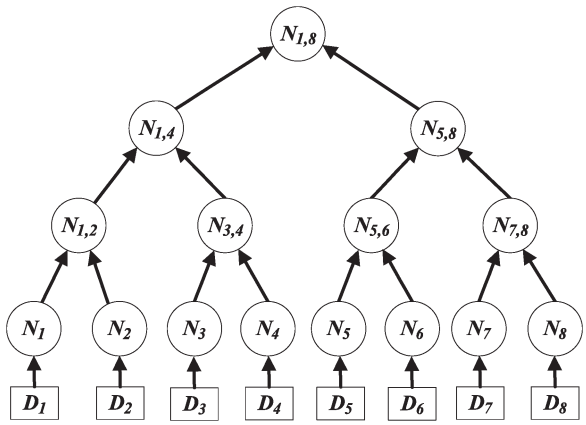


Fig. 3. Merkle hash tree.

2) The proposed scheme should achieve computation effectiveness. The smart meter is equipped with a limited computation resource. Therefore, the computation overhead of the neighborhood gateway is also a challenging issue, since hundreds of HAN user electricity consumption reports will be synchronously collected to the neighborhood gateway. Therefore, the proposed scheme should consider the computation effectiveness in both the smart meter and the neighborhood gateway.

III. Proposed Authentication Scheme

Here, we will propose our efficient authentication scheme, which consists of three phases: system initialization, report generation, neighborhood gateway authentication. Before describing them, we first review the Merkle hash tree technique [17], which will serve as the basis of the proposed authentication scheme.

A. Merkle Hash Tree Technique

The main idea of Merkle hash tree is to construct a tree based on a one-way cryptographic hash function $h(.)$ [18]. Then, each leaf node can be verified through its authentication path information (API). Since only the hash functions are computed, the computation cost of verification is very low. We illustrate the construction and application of the Merkle hash tree through an example. As shown in Fig. 3, the values of the eight leaf nodes are the message hashes, i.e., $h_i = h(D_i)(i = 1, \ldots, 8)$, respectively. The values of internal nodes are derived from their child nodes. For instance, the value of the node $N_{3,4}$ is $h_{3,4} = h(h_3|h_4)$, and the value of the root node $N_{1,8}$ is $h_{1,8} = h(h_{1,4}|h_{5,8})$. Each leaf node can be verified with $h_{1,8}$ and the corresponding API. For instance, the node N_1 can be authenticated by the server who stores $h_{1,8}$ as follows: N_1 sends D_1 and the corresponding API $= \langle h_2, h_{3,4}, h_{5,8}\rangle$ to the server. Then, the server can check the authenticity of node N_1 by first computing h_1, $h_{1,2} = h(h_1|h_2)$, $h_{1,4} = h(h_{1,2}|h_{3,4})$, $h_{1,8} = h(h_{1,4}|h_{5,8})$. And then, the server checks whether the computed $h_{1,8}$ is the same as the existing $h_{1,8}$. The server accepts N_1, only if the two values are equal.

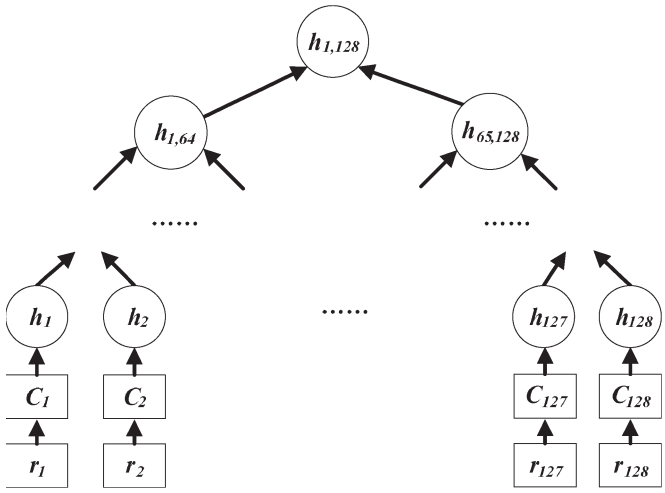


Fig. 4. System initialization.

TABLE I
HAN USER ELECTRICITY REPORT COLLECTION

TS	r	C	API
0:00	r_1	C_1	$h_2, h_{3,4}, h_{5,8}, h_{9,16}, h_{17,32}, h_{33,64}, h_{65,128}$
0:15	r_2	C_2	$h_1, h_{3,4}, h_{5,8}, h_{9,16}, h_{17,32}, h_{33,64}, h_{65,128}$
0:30	r_3	C_3	$h_4, h_{1,2}, h_{5,8}, h_{9,16}, h_{17,32}, h_{33,64}, h_{65,128}$
$\cdots$	$\cdots$	$\cdots$	$\cdots$
23:45	r_{96}	C_{96}	$h_{95}, h_{93,94}, \cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$
$\cdots$	r_{128}	C_{128}	$\cdots$

TABLE II
HAN USER AUTHENTICATION INFORMATION

ID	Root Value	Set of Hash (C_j)
U_1	$(h_{1,128})_{U_1}$	Null
U_2	$(h_{1,128})_{U_2}$	Null
U_3	$(h_{1,128})_{U_3}$	Null
$\cdots$	$\cdots$	$\cdots$
U_m	$(h_{1,128})_{U_m}$	Null

B. Description of the Authentication Scheme

1) System Initialization: Based on the system model in Section II-A, the following steps are performed to initialize the system.

Step 1: For each HAN user $U_i(i = 1, \ldots, m)$, U_i securely communicates with the neighborhood gateway by running the Diffie–Hellman key establishment protocol [19]. Subsequently, a shared session key K_i is generated between U_i and the neighborhood gateway. Meantime, the symmetric encryption and decryption algorithms, e.g., Advanced Encryption Standard (AES) [20], are shared by U_i and the neighborhood gateway. Let Enc and Dec denote the encryption and decryption algorithms, respectively.

Step 2: As depicted in Fig. 4, each HAN user $U_i(i = 1, \ldots, m)$ constructs a Merkle hash tree with 128 leaf nodes in the following manner:

1) U_i randomly chooses 128 numbers $r_j \in \mathbb{Z}_q^*(j = 1, \ldots, 128)$, where r_j has the same size as the electricity consumption report. Then, U_i picks 128 predefined timestamps $TS_j(j = 1, \ldots, 128)$. How to predefine the timestamps will be described in *Step 3*.
2) U_i generates the AES ciphertexts C_j with the session key K_i, where $C_j = Enc_{K_i}(r_j \| TS_j)$ [20]. Then, U_i computes the value of 128 leaf nodes, which are the cryptographic message hashes, i.e., $h_j = h(C_j)(j = 1, \ldots, 128)$, respectively.
3) U_i computes the value of internal nodes, which are derived from their child nodes. For example, the value of node $N_{1,2}$ is $h_{1,2} = h(h_1|h_2)$, and $h_{127,128} = h(h_{127}|h_{128})$. Thus, U_i can recursively compute the values of the tree from the leaf nodes to the root node. Finally, the value of the root node is computed, i.e., $h_{1,128} = h(h_{1,64}|h_{65,128})$.

Step 3: In order to achieve the real-time electricity consumption report collection, every t minutes, e.g., $t = 15$ min, each HAN user U_i should collect the electricity report and send it to the neighborhood gateway. Thus, there are 96 electricity report collections every day. Therefore, among the 128 leaf nodes, 96 leaf nodes are used as U_i's electricity report collection for every 15-min interval. The other 32 leaf nodes are stored for other purposes, such as urgent electricity report collections. As shown in Table I, U_i creates a table in its local database. The table's data structure is in the form of (TS, r, C, API), where TS, r, and C denote the collection time of electricity report, the corresponding random number, and the corresponding ciphertext of r, respectively, and API is the authentication path information. For example, at 0:00, r, C, and API are r_1, C_1, and $\langle h_2, h_{3,4}, h_{5,8}, h_{9,16}, h_{17,32}, h_{33,64}, h_{65,128}\rangle$, respectively.

Step 4: U_i generates the ciphertext C of the root node value $h_{1,128}$ with the session key K_i [20], where $C = Enc_{K_i}(h_{1,128})$. Then, U_i securely sends C to the neighborhood gateway.

Step 5: After receiving C from U_i, the neighborhood gateway first decrypts C with the session key K_i to get the root value $h_{1,128}$, where $h_{1,128} = Dec_{K_i}(C)$. Then, the neighborhood gateway creates a table in its local database. As shown in Table II, the table's data structure is in the form of (ID, Root Value, Set of Hash(C_j)), where ID and Root Value are the identity of U_i and the hash tree's root value of U_i, respectively, and Set of Hash(C_j) is the hash set of previously received C_j. The initialized set of Hash(C_j) is null.

Report Generation: In order to achieve the real-time electricity consumption collection, as shown in Fig. 5, every 15 min, HAN user $U_i(i = 1, \ldots, m)$ performs the following steps:

Step 1: According to the current time TS_j, U_i searches Table I to get r_j, C_j, and API_j. Then, U_i uses the smart meters to collect the electricity consumption report D_j and computes $S_j = r_j \oplus D_j$.

Step 2: U_i sends the encrypted electricity consumption report $U_i \| C_j \| S_j \| API_j$ to the neighborhood gateway.

Neighborhood Gateway Authentication: Upon receiving the encrypted electricity consumption report $U_i \| C_j \| S_j \| API_j$, the neighborhood gateway performs the following steps:

Step 1: Replay attack detection. With the detecting process in Algorithm 1, the neighborhood gateway can identify the replay attack.

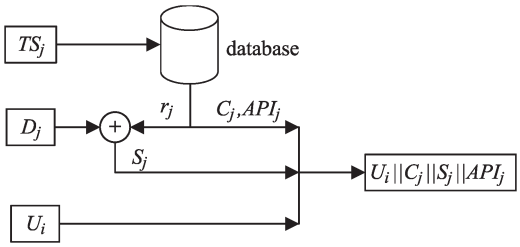


Fig. 5. Report generation.

Algorithm 1 Replay attack detection

1: **procedure** REPLAY ATTACK DETECTION
2: According to ID $= U_i$, the neighborhood gateway searches Table II in the local database.
3: **if** the returned result is Null **then**
4: This message is damaged and the algorithm terminates. Then the neighborhood discards the message.
5: **else**
6: The corresponding set of Hash(C_j) is returned. Then the neighborhood gateway computes $h(C_j)$.
7: **end if**
8: **if** the returned set of Hash(C_j) is Null **then**
9: The corresponding root value is returned and the algorithm terminates.
10: **else if** $h(C_j)$ is the element of the returned set of Hash(C_j) **then**
11: The replay attack is detected and the algorithm terminates.
12: **else**
13: Then the corresponding root value is returned and the algorithm terminates.
14: **end if**
15: **end procedure**

An illustration example of Algorithm 1 is presented in Table III. Let ID $= U_2$ and $h(C_j) = e$. First, according to ID $= U_2$, the neighborhood gateway searches Table III, and a matching ID can be found in Table III. Then, the corresponding set of Hash(C_j) is returned. Because the returned set of Hash(C_j) is $\langle d, e, f, g\rangle$ which is not null, the elements of $\langle d, e, f, g\rangle$ will be compared with $h(C_j)$ one by one. Since e is already in the set of Hash(C_j), the report is a replayed one and will be discarded.

Step 2: Message source authentication. On receiving the returned root value, the neighborhood gateway can authenticate the message source in conjunction with $h(C_j)$ and API_j. For example, the neighborhood gateway, which has stored the value of the root node $h_{1,128}$, needs to authenticate U_1 in conjunction with $h(C_1)$ and API_1, where $API_1 = \langle h_2, h_{3,4}, h_{5,8}, h_{9,16}, h_{17,32}, h_{33,64}, h_{65,128}\rangle$. The neighborhood gateway can authenticate U_1 by, in turn, computing

$$\begin{aligned} h_{1,2} &= h\left(h(C_1)|h_2\right) \\ h_{1,4} &= h(h_{1,2}|h_{3,4}) \\ h_{1,8} &= h(h_{1,4}|h_{5,8}) \\ h_{1,16} &= h(h_{1,8}|h_{9,16}) \\ h_{1,32} &= h(h_{1,16}|h_{17,32}) \\ h_{1,64} &= h(h_{1,32}|h_{33,64}) \\ h_{1,128} &=, h(h_{1,64}|h_{65,128}). \end{aligned} \tag{1}$$

Then, the neighborhood gateway checks whether the computed $h_{1,128}$ is the same as the existing $h_{1,128}$. The neighborhood gateway accepts the report, only if the two values are equal. Finally, the neighborhood gateway inserts $h(C_j)$ into the set of $Hash(C_j)$ of Table II.

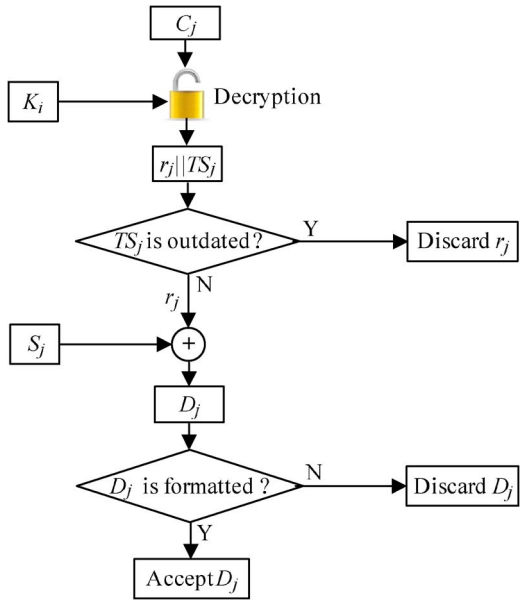


Fig. 6. Message confidentiality and integrity guarantee.

Step 3: Message confidentiality and *integrity guarantee.* As depicted in Fig. 6, the neighborhood gateway performs the following operations:

1) The neighborhood gateway runs AES decryption algorithm Dec to decrypt the received ciphertext C_j. With the session key K_i, the plaintext can be recovered by computing $Dec_{K_i}(C_j)$ [20]. The plaintext is in the form of $r_j \| TS_j$.
2) The neighborhood gateway checks the current local time TS' to detect whether the received message is fresh or not. We assume that θ is the predefined time limit. Then, the neighborhood gateway checks whether $TS' - TS_j \leq \theta$; if it holds, the neighborhood gateway accepts the fresh r_j; else, discards r_j.
3) The neighborhood gateway computes U_i's electricity consumption report $D_j = r_j \oplus S_j$. It is easily verified that $D_j = r_j \oplus S_j = r_j \oplus (r_j \oplus D_j) = D_j$. As described in Section II-A, the electricity report is featured with a certain format, which is also known by

TABLE III
EXAMPLE OF DETECTING REPLAY ATTACK

ID	Root Value	Set of Hash (C_j)
U_1	$(h_{1,128})_{U_1}$	Null
U_2	$(h_{1,128})_{U_2}$	d, e, f, g
U_3	$(h_{1,128})_{U_3}$	Null
$\cdots$	$\cdots$	$\cdots$
U_m	$(h_{1,128})_{U_m}$	Null

the neighborhood gateway. Thus, the neighborhood gateway can compare D_j's format with the existing one. If the comparison result is positive, the neighborhood gateway accepts the message; otherwise, it discards it.

IV. SECURITY ANALYSIS

Here, we analyze the security properties of the proposed authentication scheme. In particular, following the threat model discussed earlier, we are most concerned with how the proposed authentication scheme can resist the replay attack, the message injection attack, the message analysis attack, and the message modification attack.

A. Proposed Authentication Scheme can Resist the Replay Attack

In the proposed authentication scheme, after receiving the message $U_i\|C_j\|S_j\|API_j$, the neighborhood gateway runs Algorithm 1 to detect the replay attack. First, the neighborhood gateway computes $h(C_j)$. Then, according to the ID $= U_i$, the neighborhood gateway searches Table II and compares $h(C_j)$ with the elements of the returned set of Hash(C_j) one by one; if an equal value has been existing in the set of Hash(C_j), the replay attack is detected. Because the set of Hash(C_j) covers all previously received $h(C_j)$, a message is considered as a replayed one if it is equal to any one of the set of Hash(C_j). Therefore, the proposed authentication scheme can resist the replay attack.

B. Proposed Authentication Scheme can Resist the Message Injection Attack

In the proposed authentication scheme, after the replay attack detection, the neighborhood gateway will authenticate the message source. As described in Section III-A, With $h(C_j)$, API_j, and $h_{1,128}$, the neighborhood gateway can, in turn, compute hash values along the path from the leaf node to the root node. In the end, $h_{1,128}$ can be computed. Then, the computed $h_{1,128}$ is compared with the existing $h_{1,128}$. If the two values are equal, the message source is considered to be a legitimate HAN user; otherwise, a message injection attack is detected. Since the external adversary $\mathcal{A}$ cannot compromise the database of the HAN user to steal the secret information and the Merkle hash tree authentication is proved to be secure [17], $\mathcal{A}$ cannot pass the authentication process.

Note that, if an external adversary $\mathcal{A}$ compromises the communications between U_i and the neighborhood gateway and captures the message $U_i\|C_j\|S_j\|API_j$, $\mathcal{A}$ can fabricate a message, denoted by C'_j so that $h(C'_j) = h(C_j)$, which is called a collision, then sends the fabricated message in the form of $U_i\|C'_j\|S_j\|API_j$. As state above, this type of attack cannot be detected. In the following, we will prove the probability of $h(C'_j) = h(C_j)$ is negligible.

In the proposed authentication scheme, the hash function $h(.)$ adopts a 128-bit cryptographic hash function [21]. Therefore, for a random message m, there are 2^{128} possible values for $h(m)$. Here, we demonstrate how many fabricated messages have been delivered to the neighborhood gateway when the collision, i.e., $h(C'_j) = h(C_j)$, occurs. We assume that $P(n)$ is the probability that more than one collision occurs after n fabricated messages were sent to the neighborhood gateway. Let E_j denote the event that the jth fabricated message collides with $h(C_j)$. Then, $Pr[E_j] = (j-1)/2^{128}$, and

$$\begin{aligned} P(n) &= Pr[E_1 \vee E_2 \vee \cdots \vee E_n] \\ &\leq Pr[E_1] \vee Pr[E_2] \vee \cdots \vee Pr[E_n] \\ &\leq \frac{0}{2^{128}} + \frac{1}{2^{128}} + \cdots + \frac{n-1}{2^{128}} \\ &= \frac{n(n-1)}{2^{129}}. \end{aligned} \tag{2}$$

As shown in (2), the upper bound of the collision probability $P(n)$ grows with $O(2^{-129}n^2)$. When $P(n) \to 1/2$, $n^2 \approx 2^{128}$. Thus, $n \approx 2^{64}$. Therefore, after at least 2^{64} fabricated messages were launched to the neighborhood gateway, a collision might occur with 50% chance. Note that C_j varies every 15 min. As a result, in the limited time period, the collision probability is negligible.

In summary, the proposed authentication scheme can resist the message injection attack.

C. Proposed Authentication Scheme can Resist the Message Analysis Attack

In the proposed authentication scheme, each HAN user U_i sends the encryption message C_j to the neighborhood gateway, where $C_j = Enc_{K_i}(r_j\|TS_j)$ is the AES ciphertext encrypted by the session key K_j [20]. Since AES encryption algorithm is secure, the external adversary $\mathcal{A}$ cannot recover the plaintext $r_j\|TS_j$ without the session key K_j. Thus, $\mathcal{A}$ cannot recover the electricity consumption report by computing $D_j = r_j \oplus S_j$. Therefore, the proposed authentication scheme can resist the message analysis attack.

D. Proposed Authentication Scheme can Resist the Message Modification Attack

In the proposed authentication scheme, each HAN user U_i sends a message to the neighborhood gateway in the form of $U_i\|C_j\|S_j\|API_j$. After receiving the message, the neighborhood gateway first decrypts C_j with the session key K_i to recover the plaintext $r_j\|TS_j$, and then, the neighborhood gateway computes the electricity consumption report $D_j = r_j \oplus S_j$. Furthermore, the neighborhood gateway checks D_j's format. Because the format is certain, unless C_j and/or S_j were

TABLE IV
EXECUTION TIME OF CRYPTOGRAPHIC OPERATIONS

	Descriptions	Execution Time
T_s	The time of one RSA signature	2.25 ms
T_v	The time of one RSA signature verification	0.10 ms
T_h	The time of one cryptographic hash	0.000092 ms

tampered by the external adversary $\mathcal{A}$, the format check will be positive. Therefore, by the format check, the proposed authentication scheme can resist the message modification attack.

V. PERFORMANCE EVALUATION

The proposed authentication scheme provides three functions, i.e., the replay attack detection, the message source authentication, and the message confidentiality and integrity guarantee. Here, we focus on investigating the authentication performance. Since the RSA algorithm was suggested to secure smart grid [15], we compare the proposed authentication scheme with the RSA-based authentication scheme, in terms of the computation complexity of the HAN user and the neighborhood gateway, and the communication overhead between the HAN user and the neighborhood gateway.

A. Computation Complexity

For the proposed authentication scheme and the RSA-based scheme, since the RSA signing, RSA signature verifying, and the cryptographic hash computations dominate the computation complexity, we only count the number of these operations in the assessment of computation performance.

In the proposed authentication scheme, since the HAN user only performs the electricity consumption report collection and EXCLUSIVE-OR operation, the computation complexity is negligible. On the other hand, for the neighborhood gateway, it costs seven hashes to compute the hash value of the root node. However, in the RSA-based authentication scheme, the HAN user needs to perform an RSA signature to sign the electricity consumption. For the neighborhood gateway, it performs an RSA signature verification to verify the signature.

Experiments have been conducted to study the execution time. Table IV gives the observed processing time. The implementation was executed on an Intel Pentium IV 3.0-GHz machine [22].

Fig. 7 shows the computation costs of the HAN users. As we can see, in the RSA-based authentication scheme, with the increasing number of HAN users, the total computation cost significantly increases. On the contrary, in the proposed scheme, the computation cost is constantly low. For instance, when the number of HAN users hits 4000, the computation cost of the RSA-based scheme is relatively high (9000 ms) in contrast with a significantly low value (near to zero) for the proposed scheme. The RSA-based scheme experiences higher computation cost due to the time-consuming RSA signature computation. Therefore, the proposed scheme enables the resource-restrained HAN user more lightweight.

Fig. 8 shows the computation cost of the neighborhood gateway for different number of HAN users. It can be easily seen that the proposed scheme achieves lower computation cost.

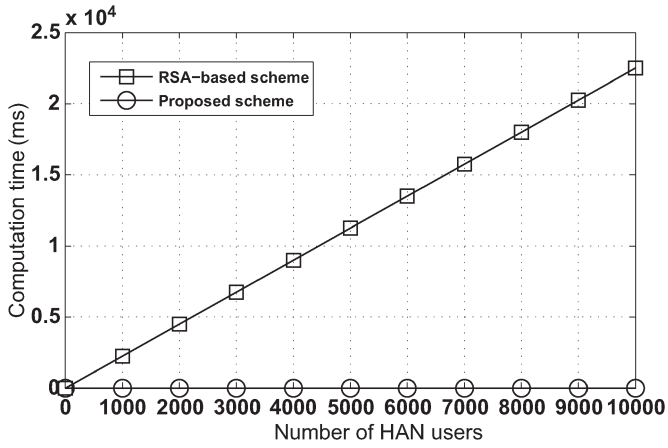


Fig. 7. Computation cost of the HAN users.

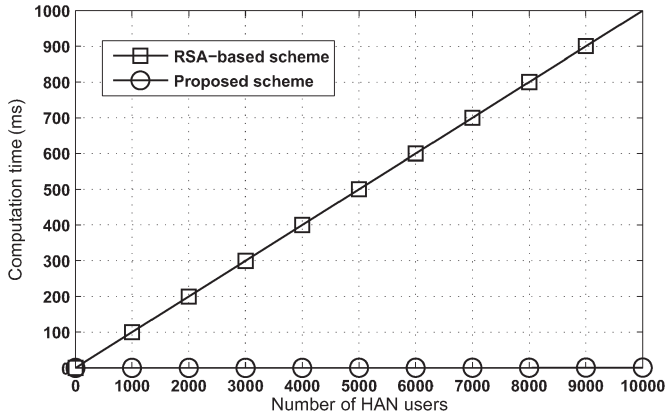


Fig. 8. Computation cost of the neighborhood gateway.

For example, when the number of HAN users reaches 4000, the computation cost of the proposed scheme is only 0.36 ms, but 400 ms in the RSA-based scheme. The proposed scheme experiences lower computation cost due to the efficient Merkle hash tree authentication. Thus, the proposed scheme achieves more computation-efficient neighborhood gateway than the RSA-based scheme.

B. Communication Overhead

In the proposed authentication scheme, the HAN user sends the message to the neighborhood gateway in the form of $U_i \| C_j \| S_j \| API_j$. Note that $U_i \| C_j \| S_j$ is served for detecting the replay attack and assuring message confidentiality and integrity and only API_j is served for authenticating the message source. As stated in Table I, API_j includes seven 128-bit cryptographic hash values. Thus the total communication overhead is $128 \times 7 = 896$ bits. In comparison, in the RSA-based authentication scheme, the HAN user sends an RSA signature to the neighborhood gateway. Considering the popular security, we choose 1024 bits as the size of RSA signature.

Fig. 9 depicts the communication overhead at a given neighborhood gateway for different number of HAN users. When the number of HAN users is small, the communication overhead is low in both the proposed scheme and the RSA-based scheme.

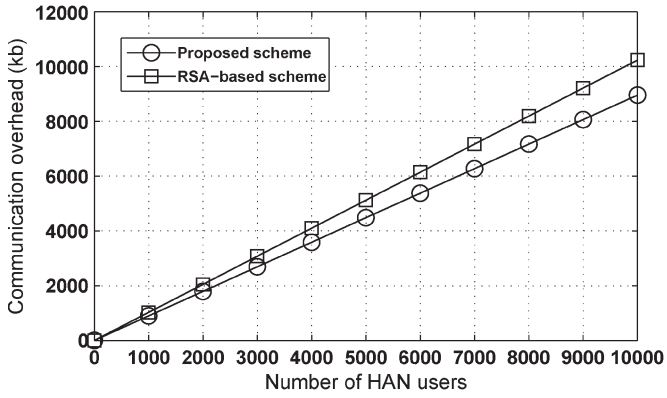


Fig. 9. Comparison of communication overhead.

Then, the communication overhead increases with the increased HAN users. However, it should be noted that the increase is much faster in the case of the RSA-based scheme. For example, when 2000 HAN users are considered for the given neighborhood gateway, the communication overhead of the RSA-based scheme is 2000 Kb, but only 1750 Kb in the proposed scheme. The RSA-based scheme bears a higher communication overhead because of the RSA signature included in the message.

VI. Related Works

Merkle hash tree [17] is well known for achieving secure and computation-efficient verification. It has been applied in many research works [23]–[25]. These works have led the following authentication schemes [26], [27]. Xu *et al.* [26] proposed a hash-tree-based authentication scheme in Session Initiation Protocol (SIP). The scheme can be used in SIP entities, which have less computation power and limited memory. Lin and Sung [27] developed an efficient source authentication scheme for multicast based on Merkle hash tree. The scheme can reduce both communication and computation costs, comparing with other source authentication schemes.

On the other hand, authentication is also essential for smart grid. Because not all the entities in the smart grid are trusted, for a secure smart grid communication, it is indispensable to verify whether the parties involved in communication are the exact entities they appear to be. Therefore, an authentication technique should be developed, so that the attackers cannot impersonate legitimate entities in the smart grid. Hamlyn *et al.* [28] proposed a new utility computer network security management and authentication, which can be used for actions or commands requests in smart grid operations. Ayday and Rajagopal [29] proposed three secure, intuitive, and low-cost device authentication mechanisms for the HAN part of the smart grid networks. These mechanisms are resilient to adversarial behavior, including man-in-the-middle and impersonation attacks. Li and Cao [30] developed a multicast authentication in the smart grid with a one-time signature. The scheme can reduce the storage cost and the signature size and flexibly allocate the computations between the sender and the receiver based on their computing resources. Fouda *et al.* [31] proposed a message authentication scheme for smart grid communications. Based on the Diffie–Hellman key establishment protocol, the scheme allows smart meters to make mutual authentication and achieve message authentication with low latency and a few signal messages exchanging.

Different from the aforementioned authentication schemes in smart grid, in this paper, we have considered extra security requirements, i.e., the replay attack detection, the message source authentication, and the message confidentiality and integrity guarantee. Furthermore, we have focused on reducing the computation cost on the resource-restrained smart meters and proposed an efficient authentication scheme where the neighborhood gateway can authenticate the message source through the Merkle hash tree technique. The proposed authentication technique is more lightweight than the RSA-based authentication.

VII. Conclusion

In this paper, we have proposed an efficient authentication scheme tailored for the requirements of secure smart grid. Detailed security analysis shows that the proposed authentication scheme can resist the replay attack, the message injection attack, the message analysis attack, and the message modification attack. Extensive performance evaluation further demonstrates its efficiency in terms of computation complexity and communication overhead. For our future work, we will explore other challenging security issues in smart grid, such as the denial of service attack.

References

[1] *Blackout*, Independent Electricity System Operator, Toronto, ON, Canada, 2003.

[2] R. Deng, J. Chen, X. Cao, Y. Zhang, S. Maharjan, and S. Gjessing, "Sensing-performance tradeoff in cognitive radio enabled smart grid," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 302–310, Mar. 2013.

[3] H. Liang, B. Choi, W. Zhuang, and X. Shen, "Towards optimal energy store-carry-and-deliver for PHEVs via V2G system," in *Proc. IEEE INFOCOM*, 2012, pp. 1674–1682.

[4] 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.

[5] X. Li, X. Liang, R. Lu, H. Zhu, X. Lin, and X. Shen, "Securing smart grid: Cyber attacks, countermeasures and challenges," *IEEE Commun. Mag.*, vol. 58, no. 8, pp. 38–45, Aug. 2012.

[6] H. Liang, B. Choi, A. Abdrabou, W. Zhuang, and X. Shen, "Decentralized economic dispatch in microgrids via heterogeneous wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 6, pp. 1061–1074, Jul. 2012.

[7] D. He, C. Chen, J. Bu, S. Chan, Y. Zhang, and M. Guizani, "Secure service provision in smart grid communications," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 53–61, Aug. 2012.

[8] 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.

[9] M. Wen, R. Lu, J. Lei, H. Li, X. Liang, and X. Shen, "SESA: An efficient searchable encryption scheme for auction in emerging smart grid marketing," in *Security and Communication Networks*. Hoboken, NJ, USA: Wiley, 2012.

[10] H. Liu, H. Ning, Y. Zhang, and L. Yang, "Aggregated-proofs based privacy-preserving authentication for V2G networks in the smart grid," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1722–1733, Dec. 2012.

[11] H. Li, X. Liang, R. Lu, X. Lin, and X. Shen, "EDR: An efficient demand response scheme for achieving forward secrecy in smart grid," in *Proc. IEEE GLOBECOM*, 2012, pp. 929–934.

[12] D. Nordell, "Terms of protection: The many faces of smart grid security," *IEEE Power Energy Mag.*, vol. 10, no. 1, pp. 18–23, Jan./Feb. 2012.

[13] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy*, vol. 7, no. 3, pp. 75–77, May/Jun. 2009.
[14] A. Cavoukian, "Privacy by design," Information and Privacy Commissioner of Ontario, Canada 2009.
[15] *Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security*, Nat. Inst. of Standards and Technol., Gaithersburg, MD, USA, 2010.
[16] D. O'Connell and I. De Vries, "Digital energy metering for electrical system management," in *Proc. ACM Symp. Appl. Comput.*, 2010, pp. 516–520.
[17] R. Merkle, "Protocols for public key cryptosystems," in *Proc. IEEE Symp. Security and Privacy*, 1980, pp. 122–134.
[18] R. Rivest, "RFC 1321: The MD5 message-digest algorithm," in *Internet Activities Board*. Gaithersburg, MD, USA: National Institute of Standards and Technology, 1992.
[19] D. Stinson, *Cryptography: Theory and Practice*. Boca Raton, FL, USA: CRC Press, 2006.
[20] N. Ferguson, R. Schroeppel, and D. Whiting, "A simple algebraic representation of Rijndael," in *Proc. Sel. Areas Cryptogr.*, 2001, pp. 103–111.
[21] R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen, "A novel anonymous mutual authentication protocol with provable link-layer location privacy," *IEEE Trans. Veh. Technol.*, vol. 58, no. 3, pp. 1454–1466, Mar. 2009.
[22] W. Dai, Crypto++ 5.6.2 Benchmarks 2013. [Online]. Available: http://www.cryptopp.com/
[23] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure information aggregation in sensor networks," in *Proc. ACM Conf. Embedded Netw. Sensor Syst.*, 2003, pp. 255–265.
[24] H. Chan, A. Perrig, and D. Song, "Secure hierarchical in-network aggregation in sensor networks," in *Proc. 13th ACM Conf. Comput. Commun. Sec.*, 2006, pp. 278–287.
[25] K. Ren, W. Lou, K. Zeng, and P. Moran, "On broadcast authentication in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 11, pp. 4136–4144, Nov. 2007.
[26] K. Xu, X. Ma, and C. Liu, "A hash tree based authentication scheme in SIP applications," in *Proc. IEEE Int. Conf. Commun.*, 2008, pp. 1510–1514.
[27] I. Lin and C. Sung, "An efficient source authentication for multicast based on Merkle hash tree," in *Proc. 6th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, 2010, pp. 5–8.
[28] A. Hamlyn, H. Cheung, T. Mander, L. Wang, C. Yang, and R. Cheung, "Network security management and authentication of actions for smart grids operations," in *Proc. IEEE Canada Elect. Power Conf.*, 2007, pp. 31–36.
[29] E. Ayday and S. Rajagopal, "Secure, intuitive and low-cost device authentication for smart grid networks," in *Proc. IEEE CCNC*, 2011, pp. 1161–1165.
[30] Q. Li and G. Cao, "Multicast authentication in the smart grid with one-time signature," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 686–696, Dec. 2011.
[31] 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.

Hongwei Li (M'12) received the Ph.D. degree in computer software and theory from the University of Electronic Science and Technology of China, Chengdu, China, in 2008.

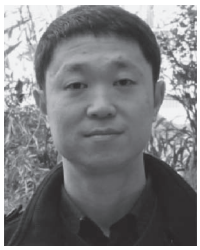
He is currently an Associate Professor with the School of Computer Science and Engineering, University of Electronic Science and Technology of China. He also serves as the Editor of *International Journal of Research and Reviews in Wireless Sensor Networks*. His research interests include network security, applied cryptography, and trusted computing.

Dr. Li is a member of the China Computer Federation and the China Association for Cryptologic Research. He served as a Program Committee Member of the 7th International Conference on Body Area Networks (BODYNETS 2012) and the 8th IEEE International Conference on Dependable, Autonomic and Secure Computing (IEEE DASC 2009).

Rongxing Lu (S'09–M'11) received the Ph.D. degree in computer science from Shanghai Jiao Tong University, Shanghai, China in 2006 and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2012.

He is currently an assistant professor, School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore. His research interests include wireless network security, applied cryptography, and trusted computing.

Liang Zhou (M'11) is a Professor with the National Key Laboratory of Science and Technology on Communication, University of Electronic Science and Technology of China, Chengdu, China. His current research interests include error control coding, secure communication, and cryptography.



Bo Yang (M'06) received the B.Eng. and M.Eng. degrees from the Xi'an Jiaotong University, Xi'an, China, and the Ph.D. from the National University of Singapore, Singapore.

He is a Professor with the University of Electronic Science and Technology of China, Chengdu, China. He has published over 50 research papers in refereed academic journals and conferences. He is on the editorial board of six international academic journals. He has given three invited talks. His research interests include software and system reliability, distributed computing, and cloud computing system.

Dr. Yang has been a Senior Member of the Chinese Institute of Electronics since 2005 and a Member of the China Computer Federation Technical Committee on Collaborative Computing since 2011. He served as the General Chair of the 2010 International Workshop on Knowledge and Data Engineering in Web-based Learning (IWKDEWL'10), the Program Chair of the 2011 International Conference on Cloud and Service Computing (CSC 2011) and the 8th IEEE International Conference on Dependable, Autonomic and Secure Computing (IEEE DASC 2009), the Program Vice-Chair of the 12th IEEE International Conference on High Performance Computing and Communications (IEEE HPCC 2010), as well as a Program Committee Member of over 20 international conferences/workshops.

Xuemin (Sherman) Shen (M'97–SM'02–F'09) is currently a Professor and University Research Chair with 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 research focuses on resource management in interconnected wireless/wired networks, wireless network security, and vehicular ad hoc and sensor networks.

Dr. Shen is a Fellow of the Engineering Institute of Canada and the Canadian Academy of Engineering. He is a Registered Professional Engineer of Ontario, Canada. He is also a Distinguished Lecturer of the IEEE Vehicular Technology Society and Communications Society. He served as the Technical Program Committee Chair for the 2010 IEEE 72nd Vehicular Technology Conference (IEEE VTC'10 Fall) and the 2007 IEEE International Conference on Global Communications (IEEE Globecom'07). 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 IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS; and an Associate Editor for IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and *Computer Networks*.