Secure Three-factor User Authentication Scheme for Renewable Energy Based Smart Grid Environment

Mohammad Wazid, *Student Member, IEEE,* Ashok Kumar Das, *Member, IEEE,* Neeraj Kumar, *Member, IEEE,* and Joel J. P. C. Rodrigues, *Senior Member, IEEE*

***Abstract*—Smart grid (SG) technology has recently received significant attention for providing intelligent and distributed electric power transmission systems. In SG, electric vehicles (EVs) charging becomes one of the emerging applications. However, authentication between a vehicle user and a smart meter is required so that both of them can securely communicate among each other for managing demand response during peak hours. To address the above mentioned issues, in this paper, we propose a new efficient Three-factor User Authentication Scheme for a Renewable Energy based Smart Grid environment (TUAS-RESG), which uses the lightweight cryptographic computations such as one-way hash functions, bitwise XOR operations and elliptic curve cryptography (ECC). The detailed security analysis shows the robustness of TUAS-RESG against various well-known attacks. Moreover, TUAS-RESG provides superior security with additional features, such as dynamic smart meter addition, flexibility for password and biometric update, user and smart meter anonymity, and untraceability as compared to other related existing schemes. The practical demonstration of TUAS-RESG is also proved using the widely-accepted NS2 simulation.**

***Index Terms*—Renewable energy, smart grid, user authentication, key agreement, security, NS2 Simulation.**

I. Introduction

Internet of Things (IoT) is an emerging concept of computing in which different physical objects are connected to the Internet to form a network. The connected physical objects can access, interpret and exchange information among each other. It has revolutionized the communication technologies by empowering advanced applications such as Smart Grid (SG). SG becomes the buzz word as it attracts the attentions from engineers and researchers in both electric power and communication sectors [1], [2]. It is also sometimes referred as the intelligent grid or grid of the future. The objective of the SG is to provide power to end users in a more stable and reliable manner. SG incorporates a two-way communication between the provider and consumers of electric power. Sensing devices, smart meters and control systems are expected to be between the provider and end users to facilitate this two-way communication system in SG. Electric vehicle charging becomes one of the emerging applications of SG. A detailed survey on the smart grid environment is provided in [3], [4], [5], [6], [7], [8], [9].

In this paper, we propose a new remote user authentication scheme for a renewable energy based smart grid environment (TUAS-RESG), which is very efficient as it only uses the lightweight cryptographic computations. In TUAS-RESG, a vehicle user can remotely authenticate to a smart meter. After mutual authentication between user and smart meter, they establish a session key for their future secure communication. The rigorous security analysis shows the robustness of TUAS-RESG against the existing attacks. The practical demonstration of TUAS-RESG using the widely-accepted NS2 simulation is also provided.

The paper is organized as follows. We provide the literature survey of the related existing schemes of smart grid environment in Section II. After that, we discuss the network and threat models which are used in TUAS-RESG in Section III. We present a new remote user authentication and session key agreement scheme for a renewable energy based smart grid environment in Section IV. In Section V, we provide the detailed security analysis of TUAS-RESG. We compare the performance among TUAS-RESG and other related existing schemes in Section VI. The practical demonstration of TUAS-RESG using the widely-accepted NS2 simulation is provided in Section VII. We finally conclude the paper in Section VIII.

II. Related Work

Gazdar *et al.* [10] presented a dynamic and distributed trust model, which establishes a trust relationship between vehicles and filters out malicious and selfish vehicles in Vehicular Adhoc Networks (VANETs). Their model is flexible and also robust as it can detect various malicious behaviors in the network. Haddadou *et al.* [11] proposed a distributed trust model for VANETs, which is adapted from the job market signaling model. Their model increases the cooperation of selfish nodes by maintaining a high reception ratio. Gazdar *et al.* [12] also proposed a distributed and dynamic public key infrastructure for VANETs, which achieves authentication, confidentiality as well as a reliable vehicle-to-vehicle data exchange. Rachedi and Benslimane [13] designed an anonymous scheme to secure nodes which have important roles in the network. They further considered the clustering approach to secure the mobile adhoc networks. In addition, Alnasser and Rikli [14] developed a trust security model for smart meters in an urban power grid network. Their trust model works at two

M. Wazid is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India (e-mail: mohammad.wazid@research.iiit.ac.in).

A. K. Das is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India (e-mail: iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in).

N. Kumar is with the Department of Computer Science and Engineering, Thapar University, Patiala 147 004, India (e-mail: neeraj.kumar@thapar.edu).

J. J. P. C. Rodrigues is with National Institute of Telecommunications (Inatel), Brazil; Instituto de Telecomunicações, Universidade da Beira Interior, Portugal; ITMO University, Russia; University of Fortaleza (UNIFOR), Brazil (email: joeljr@ieee.org). *(Corresponding author: Joel J. P. C. Rodrigues.)*

different levels. At the first level, called the smart meter level, the nodes need to gather the information from its neighbor nodes. At the second level, called the collecting node level, the malicious nodes in the network are detected and isolated. This is done by requesting the nodes to stop communications with the malicious nodes.

Fouda *et al.* [2] proposed a message authentication scheme for securing communication among various smart meters at different points of the smart grid. Their scheme uses the Diffie-Hellman key establishment protocol and hash-based message authentication code for mutual authentication. Later, Mahmood *et al.* [1] proposed a hybrid Diffie-Hellman based authentication scheme, which achieves authentication between smart meter gateway located in home area network and smart meter gateway located in building area network. Their scheme provides less communication and computation costs as compared to the scheme of Fouda *et al.* [2].

Nicanfar *et al.* [15] presented an authentication scheme that mutually authenticates a smart meter of a home area network and an authentication server in smart grid. Li *et al.* [16] proposed another authentication scheme that employs the Merkle hash tree technique to secure communication in smart gird. Chim *et al.* [17] discussed the hierarchical structure of smart grid and also proposed a privacy-preserving recording and gateway-assisted authentication of power usage information for smart grid environment. Chan *et al.* [18] also proposed a two-factor cyber-physical device authentication scheme to provide protection against coordinated cyber-physical attacks in a smart grid environment.

Tsai and Lo [19] applied an identity-based signature and identity-based encryption to propose an anonymous key distribution scheme for smart grid in which smart meter and service provider mutually authenticate with each other, and then establish a session key between them for secure communication. It was shown that Tsai-Lo's authentication scheme is insecure against the ephemeral secret leakage attack, and also it fails to provide the strong credentials' privacy of the smart meter [20]. Odelu *et al.* [20] then proposed a secure authenticated key agreement scheme for smart grid, which overcomes the security weaknesses of Tsai-Lo's scheme.

Jo *et al.* [21] proposed a privacy-preserving authentication scheme for smart grid environment. They designed two protocols, namely protocol I and protocol II. Protocol II is a modified version of protocol I. Both protocols are executed by processing intial setup and registration phases. The public parameters and certificates are initialized during the initial setup phase. The registration phase contains two parts, namely, a basic part and an additional part. The basic part is needed for both the protocols, whereas the additional part is only required for the protocol II.

Doh *et al.* [22] also proposed a scheme to provide authentication between the utility system and the smart meters. Saxena *et al.* [23] proposed an authentication and authorization scheme for smart grid environment. Their scheme provides protection against outsider and insider threats in the smart grid by verifying the user authorization and performing user authentication together. He *et al.* [24] proposed an ECC based anonymous key distribution scheme for the smart grid, which provides less communication and computation costs as compared to the scheme of Tsai and Lo [19].

In the schemes of Tsai and Lo [19] and Odelu *et al.* [20], there is authentication between smart meter and service provider. In the scheme of Jo *et al.* [21], there are two protocols for authentication between smart meter and data collection unit as well as data collection unit and advanced metering infrastructure. In the scheme of Wu and Zhou [25], the key management is done for smart sensor and data collector. Xia and Wang [26] identified that the scheme of Wu and Zhou [25] is vulnerable to man-in-the-middle attack, and presented an improved scheme for key distribution in smart grid in which the key establishment between a smart meter and a service provider is executed with the help of a trusted anchor.

The scheme of Wu and Zhou [25], Xia and Wang [26], and Jo *et al.* [21] do not provide some functionality and security features, such as perfect secrecy, strong smart meter credentials' privacy, session key (SK) security, offline password guessing attack protection, password and biometric update phases and dynamic smart meter addition. The scheme of Tsai and Lo [19] is vulnerable to privileged-insider attack and does not provide functionality and security features such as strong smart meter credentials' privacy, SK-security, offline password guessing attack protection, password and biometric update phase and dynamic smart meter addition phase, whereas the scheme of Odelu *et al.* [20] does not support password and biometric update phase and dynamic smart meter addition phase. Therefore, to overcome these drawbacks and limitations in the existing schemes, we propose a new three-factor user authentication scheme for SG environment.

III. System Models

In this section, we consider the following two models to discuss and analyze the proposed TUAS-RESG.

A. Network Model

Figure 1 show the network model for a renewable energy based smart grid environment. The solar arrays (renewable energy producers) produce electricity, and then the electricity is distributed by some utility company. The utility company further provides electricity to various charging stations. Suppose there is a vehicle, which requires some electricity to charge its battery. In this model, there are two types of flows: 1) one is energy flow, which is represented by green arrowed line, and 2) other one is data flow which is represented by red arrowed line. Before sharing information, entities (user and smart meter) need to authenticate themselves. Due to wireless communication in the SG environment, there is a possibility of various attacks, such as replay, man-in-the middle and impersonation attacks. The smart meter privacy is also another important issue in SG. Smart meter reading can be modified by an attacker, which can affect various required tasks, such as billing of vehicle user. It may also provide different billing information to the users. Thus, there is a great need of a remote user authenticated key agreement scheme by which user and smart meter can authenticate each other.

Assume that there is a car user U_i who has mobile device MD_i with the Internet connectivity. At the charging station, there is a smart meter SM_j which is connected to the utility company (service provider). Both MD_i and SM_j are then connected through the Internet. If U_i wants to charge its car's battery, first of all he/she needs to authenticate with SM_j. After mutual authentication between U_i and SM_j, a session key is established between them. U_i can then provide his/her battery charging requirement to SM_j. After battery charging, U_i can pay to the service provider for charging (energy) with the help of maintained secure session with SM_j [27], [28].

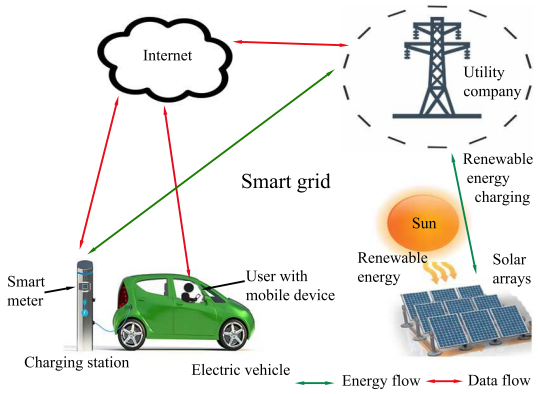

Fig. 1. Renewable energy based smart grid environment

B. Threat Model

We follow the well-known Dolev-Yao threat model (DY model) [29] in TUAS-RESG. According to this model, any two nodes communicate over an insecure channel [30], in which the end-point communicating parties, such as U_i and SM_j, are not in general trustworthy. An attacker $\mathcal{A}$ can then eavesdrop, modify or delete the exchanged messages during transmission. Furthermore, if MD_i of U_i is lost or stolen, $\mathcal{A}$ can extract all the sensitive information stored in MD_i using the power analysis attacks [31], [32]. The current *de facto* standard model in modeling key-exchange protocols is the CK-adversary model [33], [34], where $\mathcal{A}$ is responsible for delivering messages (as in the DY model), and can further compromise private keys, session keys and session state. Thus, the security of an authenticated key-exchange protocol should guarantee that the leakage of some forms of secret information, such as session ephemeral secrets, session key, or long-term private keys, will have the least possible effect on the security of other secret credentials and session keys of the communicated parties [20].

IV. TUAS-RESG: Three-factor User Authentication for Renewable Energy based Smart Grid environment

In this section, we describe a new three-factor lightweight authentication protocol for renewable energy based smart grid environment (TUAS-RESG), where a user U_i and a smart meter SM_j authenticate each other in the network. After successful mutual authentication between U_i and SM_j, both entities will establish a session key SK_{ij} for their future secure communications. The three factors used in TUAS-RESG are: 1) mobile device MD_i of a user U_i; 2) password PW_i of U_i; and 3) biometrics BIO_i of U_i. TUAS-RESG contains the six phases: 1) pre-deployment; 2) offline user registration; 3) login; 4) authentication and key agreement; 5) password and biometric update; and 6) dynamic smart meter addition. The notations listed in Table I are used for describing and analyzing TUAS-RESG. To provide strong replay attack protection, we aim to use both random nonces and current timestamps. For this purpose, it is assumed that all the network entities are synchronized with their clocks.

TABLE I
Notations used in this paper

Notation	Description
TA	Trusted authority
ID_{TA}	Identity of TA
U_i, SM_j	i^{th} user and j^{th} smart meter
ID_{SM_j}	Identity of SM_j
MD_i, ID_i, PW_i	U_i's mobile device, identity and password
RID_i, RID_{SM_j}	Pseudo identities of U_i and SM_j
n_i, r_i	Random secrets of U_i and TA
ru_i, rs_j	Random nonces of U_i and SM_j
R_i	Public key of U_i
Pub_{TA}	Public key of TA
$E_p(a,b)$	Elliptic curve: $y^2 = x^3 + ax + b \pmod p$, where p is prime and $a, b \in Z_p$ are constants such that $4a^3 + 27b^2 \neq 0 \pmod p$
P	A base point on $E_p(a,b)$
$k.P$	$P + P + \cdots + P(k$ times), an elliptic curve point (scalar) multiplication
$P + Q$	Elliptic curve point addition, $P, Q \in E_p(a,b)$
σ_i	Biometric secret key of U_i
τ_i	Public reproduction parameter of U_i
t	Error tolerance threshold used in fuzzy extractor
T_1, T_2, T_3	Current timestamps
ΔT	Maximum transmission delay
Gen	Fuzzy extractor probabilistic generation procedure
Rep	Fuzzy extractor deterministic reproduction procedure
$h(\cdot)$	Collision-resistant cryptographic hash function
$\|\|, \oplus$	Concatenation and bitwise XOR operations

A. Pre-deployment Phase

In this phase, the trusted authority (TA) registers each smart meter SM_j before their deployment in the network. The TA first selects a non-singular elliptic curve $E_p(a,b)$: $y^2 = x^3 + ax + b \pmod p$ having a large prime p and two constants $a, b \in Z_p = \{0, 1, \ldots, p-1\}$ such that the necessary and sufficient condition $4a^3 + 27b^2 \neq 0 \pmod p$ is satisfied. After that, the TA selects a base point P on $E_p(a,b)$ whose order is as large as p, and a master secret key k which is only known to the TA. The TA then computes its public key $Pub_{TA} = k.P$, where $k.P = P + P + \cdots + P(k$ times) is the elliptic curve point (scalar) multiplication, and also a pseudo identity $RID_{TA} = h(ID_{TA}||k)$. Further, the TA chooses a unique identity ID_{SM_j} for each SM_j, and computes its corresponding pseudo identity $RID_{SM_j} = h(ID_{SM_j}||k)$. Finally, the TA stores the credentials $\{RID_{SM_j}, Pub_{TA}, RID_{TA}\}$ in the memory of SM_j prior to its deployment in the network.

B. User Registration Phase

To access SM_j, U_i needs to register at the TA securely either in person or via a secure channel. This phase is executed in the offline mode by the TA and U_i. The steps of this phase are given below.

Step REG1. U_i first chooses a unique identity ID_i and a secure collision resistant hash function $h(\cdot)$ (for example, SHA-1 hash function [35]), and sends the registration request $\langle ID_i, h(\cdot)\rangle$ to the TA through a secure channel.

Step REG2. After receiving the registration request $\langle ID_i, h(\cdot)\rangle$ from U_i, the TA chooses an 160-bit random secret r_i and computes public key of U_i as $R_i = r_i.P$. The TA then computes the pseudo identity of U_i as $RID_i = h(ID_i||k)$, $c_i = h(R_i||Pub_{TA})$, and also the ElGamal-type ECC signature on r_i as $s_i = r_i + c_i k \pmod p$. The TA then sends the registration reply with the information $\{RID_i, s_i, R_i, RID_{TA}\}$ to U_i securely.

Step REG3. After receiving securely the registration reply $\{RID_i, s_i, R_i, RID_{TA}\}$ from the TA, the mobile device MD_i asks U_i to input his/her credentials. U_i then selects a password PW_i as per his/her own choice and also imprints personal biometrics BIO_i at the sensor of MD_i. MD_i generates an 160-bit random secret n_i and computes masked password $RPW_i = h(PW_i||n_i)$.

Step REG4. MD_i applies the fuzzy extractor probabilistic generation function $Gen(\cdot)$ to generate the secret biometric key σ_i and the corresponding public parameter τ_i as $Gen(BIO_i) = (\sigma_i, \tau_i)$ as done in [36], [37], [38]. The detailed description of the fuzzy extractor functions $Gen(\cdot)$ and $Rep(\cdot)$ can be found in [38]. MD_i further computes $BI_i = h(ID_i \ ||\sigma_i) \oplus n_i$, $CI_i = h(ID_i \ ||RPW_i \ ||\sigma_i)$, $RID'_{TA} = RID_{TA} \oplus h(ID_i \ ||\sigma_i)$, and $s_i^* = s_i \oplus h(n_i \ ||ID_i \ ||\sigma_i)$, and replaces RID_{TA} by RID'_{TA} and s_i with s_i^* in its memory. Finally, MD_i stores the information $\{RID_i, R_i, BI_i, CI_i, RID'_{TA}, s_i^*, \tau_i, Gen(\cdot), Rep(\cdot), h(\cdot), t\}$ in its memory, where t is the error tolerance threshold value used in $Rep(\cdot)$ to recover the original biometric key σ_i. Note that the TA also stores the information RID_i corresponding to ID_i of U_i in its database.

C. Login Phase

The following steps are executed in the login phase by U_i:

Step L1. U_i first provides his/her identity ID_i and inputs password PW_i^* into the interface of MD_i, and also imprints his/her biometrics BIO_i^* at the sensor of MD_i. MD_i extracts biometric key $\sigma_i^* = Rep(BIO_i^*, \tau_i)$ provided that the Hamming distance between the original biometrics BIO_i at the time of registration and the entered BIO_i^* is less than the error tolerance threshold value t. Then, MD_i retrieves $n_i^* = BI_i \oplus h(ID_i \ ||\sigma_i^*)$, $RPW_i^* = h(PW_i^* \ ||n_i^*)$ and $CI_i^* = h(ID_i \ ||RPW_i^* \ ||\sigma_i^*)$. After these computations, MD_i checks whether the condition $CI_i^* = CI_i$ holds or not. If it holds, U_i passes both password and biometric verification. Otherwise, the session is terminated immediately.

Step L2. MD_i further computes $RID_{TA}^* = RID'_{TA} \oplus h(ID_i \ ||\sigma_i^*)$, $s'_i = s_i^* \oplus h(n_i^* \ ||ID_i \ ||\sigma_i^*) = r_i + c_i k \pmod p$. In addition, MD_i chooses a random nonce ru_i and generates the current timestamp T_1, where $ru_i \in Z_p^* = \{1, 2, \ldots, p-1\}$. MD_i calculates $x = h(RID_i \ ||RID_{TA}^* \ ||ru_i \ ||RWP_i^* \ ||\sigma_i^* \ ||T_1)$, $X_i = x.P$, $R_i^* = R_i \oplus h(RID_{TA}^* \ ||T_1)$ and $A_i = x + s'_i \pmod p$. Finally, MD_i sends the login request $\langle X_i, R_i^*, A_i, T_1\rangle$ to SM_j via a public channel.

User (U_i)/Mobile device (MD_i)	Smart meter (SM_j)
Input ID_i, PW_i^*, BIO_i^*.	
Compute $\sigma_i^* = Rep(BIO_i^*, \tau_i)$,	
$n_i^* = BI_i \oplus h(ID_i \|\|\sigma_i^*)$,	
$RPW_i^* = h(PW_i^* \|\|n_i^*)$,	
$CI_i^* = h(ID_i \|\|RPW_i^* \|\|\sigma_i^*)$.	
Check if $CI_i^* = CI_i$? If so, compute	
$RID_{TA}^* = RID'_{TA} \oplus h(ID_i \|\|\sigma_i^*)$,	Check if $\|T_1 - T_1^*\| < \Delta T$? If so,
$s'_i = s_i^* \oplus h(n_i^* \|\|ID_i \|\|\sigma_i^*)$	compute $R_i = R_i^* \oplus h(RID_{TA} \ ||T_1)$,
$= r_i + c_i k \pmod p$,	$c_i = h(R_i \ ||Pub_{TA})$,
$x = h(RID_i \ ||RID_{TA}^* \ ||ru_i$	and verify if
$\|\|RWP_i^* \ ||\sigma_i^* \ ||T_1)$, $X_i = x.P$,	$A_i.P = X_i + (R_i + c_i.Pub_{TA})$?
$R_i^* = R_i \oplus h(RID_{TA}^* \ ||T_1)$,	If verification holds,
$A_i = x + s'_i \pmod p$.	compute $y = h(RID_{SM_j}$
$\langle X_i, R_i^*, A_i, T_1\rangle$ $\xrightarrow{}$	$\|\|RID_{TA} \ ||rs_j \ ||A_i \ ||T_2)$,
(via public channel)	$Y_j = y.P$, $Z_j = y.X_i = xy.P$,
	$SK_{ij} = h(RID_{TA} \ ||T_1$
	$\|\|T_2 \ ||A_i \ ||Z_j)$,
	$V_j = h(SK_{ij} \ ||T_1 \ ||T_2)$.
	$\langle Y_j, V_j, T_2\rangle$ $\xleftarrow{}$
Check if $\|T_2 - T_2^*\| < \Delta T$?	(via public channel)
If so, compute	
$Z_i = x.Y_j = x.(y.P) = xy.P$,	
$SK'_{ij} = h(RID_{TA}^* \ ||T_1$	
$\|\|T_2 \ ||A_i \ ||Z_i)$,	
$V_i = h(SK'_{ij} \ ||T_1 \ ||T_2)$.	
Check if $V_i = V_j$? If so,	Check if $\|T_3 - T_3^*\| < \Delta T$?
compute $ACK_i = h(SK'_{ij} \ ||T_3)$.	If so, compute
$\langle ACK_i, T_3\rangle$ $\xrightarrow{}$	$ACK_j = h(SK_{ij}||T_3)$.
(via public channel)	Check if $ACK_j = ACK_i$?
Both U_i and SM_j store session key SK_{ij} $(= SK'_{ij})$.	

Fig. 2. Summary of login, and authentication and key agreement phase

D. Authentication and Key Agreement Phase

This phase helps the session key establishment between a user U_i and an accessed smart meter SM_j after their mutual authentication. After receiving the login request $\langle X_i, R_i, A_i, T_1\rangle$ by SM_j, the following steps are executed. The login, and authentication and key agreement phases of TUAS-RESG is further summarized in Figure 2.

Step AKE1. SM_j first checks the timeliness of T_1 by the condition $|T_1 - T_1^*| < \Delta T$, where ΔT is the maximum transmission delay and T_1^* is the time when the message $\langle X_i, R_i, A_i, T_1\rangle$ was received by SM_j. If it holds, SM_j computes $R_i = R_i^* \oplus h(RID_{TA} \ ||T_1)$, $c_i = h(R_i \ ||Pub_{TA})$ and then verifies the condition $A_i.P = X_i + (R_i + c_i.Pub_{TA})$. Note that $A_i.P = (x + s'_i).P = x.P + (r_i + c_i k).P = X_i + (r_i.P + c_i(k.P)) = X_i + (R_i + c_i.Pub_{TA})$. If verification holds, it ensures that U_i is authenticated by SM_j. Otherwise, the session is terminated immediately.

Step AKE2. SM_j generates a random nonce $rs_j \in Z_p^*$ and the current timestamp T_2, and calculates $y = h(RID_{SM_j} \ ||RID_{TA} \ ||rs_j \ ||A_i \ ||T_2)$, $Y_j = y.P$, $Z_j = y.X_i = xy.P$. By using all these computed values, SM_j computes the session key shared with U_i as $SK_{ij} = h(RID_{TA} \ ||T_1 \ ||T_2 \ ||A_i \ ||Z_j)$ and $V_j = h(SK_{ij} \ ||T_1 \ ||T_2)$. Then, SM_j sends the authentication reply $\langle Y_j, V_j, T_2\rangle$ to U_i via a public channel.

Step AKE3. After receiving the authentication reply $\langle Y_j, V_j, T_2\rangle$ from SM_j, U_i checks the timeliness of T_2 by the

verification condition $|T_2 - T_2^*| < \Delta T$, where T_2^* is the time when the message $\langle Y_j, V_j, T_2\rangle$ was received by MD_i of U_i. If this condition holds, U_i computes $Z_i = x.Y_j = x.(y.P) = xy.P$ and the session key shared with SM_j as $SK'_{ij} = h(RID^*_{TA} ||T_1 ||T_2 ||A_i ||Z_i)$. It further computes $V_i = h(SK'_{ij} ||T_1 ||T_2)$ and checks if the condition $V_i = V_j$ holds. If this condition holds, it also ensures that SM_j is authenticated by U_i. U_i then chooses the current timestamp T_3 and calculates $ACK_i = h(SK'_{ij} ||T_3)$ and sends acknowledgment message $\langle ACK_i, T_3\rangle$ to SM_j via a public channel.

Step AKE4. After receiving the message $\langle ACK_i, T_3\rangle$ from U_i, SM_j checks the timeliness of T_3 by checking the condition $|T_3 - T_3^*| < \Delta T$, where T_3^* is the time when the message $\langle ACK_i, T_3\rangle$ was received. If this condition holds, SM_j computes $ACK_j = h(SK_{ij} ||T_3)$ and checks if the condition $ACK_j = ACK_i$ holds. If the condition does not hold, it terminates the connection immediately. Otherwise, it assures that the computed session key by U_i is correct, and both U_i and SM_j establish the same common session key SK_{ij} $(= SK'_{ij})$ for future secure communication.

E. Password and Biometric Update Phase

TUAS-RESG provides password and biometric update facility by which a legitimate user U_i can change his/her password as well as biometrics for security reasons at any time after user registration phase without involving the TA. The biometric information of a given user U_i is unique and unchanged as compared to a chosen password by that user U_i. However, we suggest U_i should update his/her biometric information as well in TUAS-RESG, if he/she desires to do so. This is necessary to protect strongly the offline password guessing attack by an adversary. The following steps are necessary for this purpose:

Step PB1. U_i first inputs his/her identity ID_i, old password PW_i^{old} to interface of MD_i, and also imprints his/her old biometrics BIO_i^{old} to the sensor of MD_i. MD_i then calculates $\sigma_i^{old} = Rep(BIO_i^{old}, \tau_i)$, $n_i^* = BI_i \oplus h(ID_i ||\sigma_i^{old})$, $RPW_i^{old} = h(PW_i^{old} ||n_i^*)$, $CI_i^{old} = h(ID_i ||RPW_i^{old} ||\sigma_i^{old})$, and proceeds to check whether the condition $CI_i^{old} = CI_i$ holds. If it matches, U_i is considered as genuine user; otherwise, this phase is terminated immediately.

Step PB2. MD_i asks U_i to enter a new password PW_i^{new}, and also to imprint new biometrics BIO_i^{new}, if U_i is desired to change BIO_i^{old}. Note that if U_i does not want to change his/her biometrics, he/she still can keep the same old biometrics BIO_i^{old}, and in this case, BIO_i^{new} is treated as BIO_i^{old}. However, U_i must provide a new password PW_i^{new} which needs to be different from PW_i^{old}. MD_i then computes $Gen(BIO_i^{new}) = (\sigma_i^{new}, \tau_i^{new})$, $BI_i^{new} = h(ID_i|| \sigma_i^{new}) \oplus n_i^*$, $RPW_i^{new} = h(PW_i^{new} ||n_i^*)$, $CI_i^{new} = h(ID_i|| RPW_i^{new} ||\sigma_i^{new})$, $RID''_{TA} = (RID'_{TA} \oplus h(ID_i ||\sigma_i^{old})) \oplus h(ID_i ||\sigma_i^{new}) = RID_{TA} \oplus h(ID_i ||\sigma_i^{new})$, and $s_i^{**} = (s_i^* \oplus h(n_i^* ||ID_i|| \sigma_i^{old})) \oplus h(n_i^* ||ID_i ||\sigma_i^{new}) = s_i \oplus h(n_i^*|| ID_i||\sigma_i^{new})$.

Step PB3. MD_i replaces BI_i, CI_i, RID'_{TA}, s_i^* and τ_i with BI_i^{new}, CI_i^{new}, RID''_{TA}, s_i^{**} and τ_i^{new} in its memory, respectively. Finally, MD_i contains the information $\{RID_i, R_i, BI_i^{new}, CI_i^{new}, RID''_{TA}, s_i^{**}, \tau_i^{new}, h(\cdot), Gen(\cdot), Rep(\cdot), t\}$.

F. Dynamic Smart Meter Addition Phase

To deploy a new smart meter, say SM_j^{new} in the existing network, the TA performs the following steps in offline mode:

Step SMA1. The TA first assigns a new unique identity $ID_{SM_j}^{new}$, which is different from the identities of the already deployed smart meters. The TA then computes the pseudo identity for SM_j^{new} as $RID_{SM_j}^{new} = h(ID_{SM_j}^{new} ||k)$ using its master secret key k.

Step SMA2. The TA stores the credentials $\{RID_{SM_j}^{new}, Pub_{TA}, RID_{TA}\}$ into the memory of SM_j^{new} prior to its deployment in the network.

V. Security Analysis of TUAS-RESG

This section shows the ability of TUAS-RESG to resist various well-known attacks. For this, we provide following definitions and then discussion on various attacks.

Definition 1. *A one-way collision-resistant hash function h: $\{0,1\}^* \rightarrow \{0,1\}^l$ is a deterministic function. It takes an arbitrary length binary string $u \in \{0,1\}^*$ as an input, and then outputs a binary string $h(u) \in \{0,1\}^l$ of fixed-length l, called message digest or hash value. An adversary $\mathcal{A}$'s advantage in finding collision [39] is given by $Adv_{\mathcal{A}}^{HASH}(t) = Pr[(u,v) \leftarrow_R \mathcal{A}: u \neq v$ and $h(u) = h(v)]$, where $Pr[E]$ is the probability of an event E, and $(u,v) \leftarrow_R \mathcal{A}$ denotes the pair (u,v) is randomly chosen by $\mathcal{A}$. $\mathcal{A}$ is allowed to be probabilistic and the probability in the advantage is computed over the random choices made by $\mathcal{A}$ with the execution time t. By an (η, t)-adversary $\mathcal{A}$ attacking the collision resistance of $h(\cdot)$, it means that the runtime of $\mathcal{A}$ is at most t and that $Adv_{\mathcal{A}}^{HASH}(t) \leq \eta$.*

Definition 2. *Let $E_p(a,b)$ be an elliptic curve and $P \in E_p(a,b)$ be a base point. The elliptic curve discrete logarithm problem (ECDLP) is defined as follows. Given two points P and $x.P$ in $E_p(a,b)$, to find the discrete logarithm x.*

Definition 3. *Let $E_p(a,b)$ be an elliptic curve and $P \in E_p(a,b)$ be a base point. The elliptic curve decisional Diffie-Hellman problem (ECDDHP) is defined as follows. Given four points P, $x.P$, $y.P$ and $z.P$ in $E_p(a,b)$, to decide whether $z = x.y$ or a uniform value.*

Replay attack: Suppose an adversary $\mathcal{A}$ intercepts the messages $Msg_1 = \langle X_i, R_i^*, A_i, T_1\rangle$, $Msg_2 = \langle Y_j, V_j, T_2\rangle$ and $Msg_3 = \langle ACK_i, T_3\rangle$ during the login, and authentication and key agreement phases, and then tries to send these messages again after some time. Since all these messages include the timestamps T_1, T_2 and T_3, validity of the timestamps will fail by SM_j, MD_i and SM_j, respectively. Hence, TUAS-RESG provides the replay attack protection.

Man-in-the-middle attack: Let an adversary $\mathcal{A}$ intercept the message $Msg_1 = \langle X_i, R_i^*, A_i, T_1\rangle$ sent to SM_j by the user U_i during the login phase. Suppose $\mathcal{A}$ generates a new timestamp T_1' and a random nonce ru_i', and tries to compute $x = h(RID_i ||RID_{TA} ||ru_i' ||RPW_i ||\sigma_i ||T_1')$, $X_i = x.P$ and $A_i = x + s_i \pmod p$. However, $\mathcal{A}$ does not know secret credentials RID_i, RID_{TA} and signature s_i on r_i, where $R_i = r_i.P$. Without these, it is not possible for $\mathcal{A}$

to calculate x, and as a result, modification of Msg_1 is not also possible. Similarly, $\mathcal{A}$ can not also modify other messages $Msg_2 = \langle Y_j, V_j, T_2 \rangle$ and $Msg_3 = \langle ACK_i, T_3 \rangle$ during the authentication and key agreement phase. Thus, TUAS-RESG is resilient against the man-in-the-middle attack.

Privileged-insider attack: Suppose a privileged-insider user of the TA, being an adversary $\mathcal{A}$, knows the registration information $\{ID_i, h(\cdot)\}$ during the user registration phase, which were sent by U_i to the TA. We further assume that $\mathcal{A}$ has lost/stolen mobile device MD_i of the registered user U_i after the registration phase is completed. $\mathcal{A}$ can then extract the important information $\{RID_i, R_i, BI_i, CI_i, RID'_{TA}, s_i^*, \tau_i, Gen(\cdot), Rep(\cdot), h(\cdot), t\}$ stored in MD_i's memory by applying the power analysis attacks [31], [32]. Without having the biometric key σ_i of U_i, $\mathcal{A}$ can not derive $n_i = BI_i \oplus h(ID_i \,||\, \sigma_i)$ and hence, $\mathcal{A}$ can not also verify a guessed password with the help of CI_i through the offline password guessing attack. Moreover, without σ_i and n_i, it is also hard for $\mathcal{A}$ to derive RID_{TA} and s_i. As compared to low-entropy passwords, the biometric keys have several other advantages, which include 1) biometric keys cannot be lost or forgotten, 2) biometric keys are hard to forge or distribute, 3) biometric keys are difficult to copy or share. Therefore, guessing the biometric keys becomes a hard problem [38]. Thus, TUAS-RESG protects the privileged-insider attack.

User impersonation attack: Suppose an adversary $\mathcal{A}$ tries to impersonate the user U_i (mobile device MD_i) in order to send valid login request and authentication acknowledgment messages to the smart meter SM_j. In order to create a valid login request message $\langle X_i, R_i^*, A_i, T_1' \rangle$ on behalf of U_i, $\mathcal{A}$ can generate current timestamp T_1' and random nonce ru_i'. However, without having the secret credentials RID_i, RID_{TA}, PW_i, σ_i and signature s_i on r_i, it is difficult task for $\mathcal{A}$ to calculate $x = h(RID_i \,||RID_{TA} \,||ru_i' \,||RPW_i \,||\sigma_i \,||T_1')$, $X_i = x.P$ and $A_i = x + s_i \pmod p$. Furthermore, computation of session key $SK_{ij} = h(RID_{TA} \,||T_1' \,||T_2 \,||A_i \,||Z_j)$ requires the secret credentials x, y, s_i and RID_{TA}, where $Z_j = y.X_i = xy.P = x.Y_j = Z_i$. Given X_i and Y_j, it is hard to calculate Z_j or Z_i due to difficulty of solving ECDDHP (see Definition 3). Without computing SK_{ij}, $\mathcal{A}$ can not calculate $ACK_i = h(SK_{ij}||T_3')$, where T_3' is the current timestamp generated by $\mathcal{A}$. It is then clear that TUAS-RESG is resilient against the user impersonation attack.

Smart meter impersonation attack: In this case, assume that an adversary $\mathcal{A}$ tries to impersonate the smart meter SM_j in order to send valid authentication request message $\langle Y_j, V_j, T_2' \rangle$ by generating a random nonce rs_j' and current timestamp T_2'. Without having the secret credentials RID_{SM_j} and RID_{TA}, $\mathcal{A}$ can not calculate $y = h(RID_{SM_j} \,||RID_{TA} \,||rs_j' \,||A_i \,||T_2')$, $Y_j = y.P$, $Z_j = y.X_i = xy.P$. Also, deriving x from X_i and y from Y_j are computationally infeasible due to difficulty of solving ECDLP (see Definition 2). As a result, $\mathcal{A}$ can not derive the session key $SK_{ij} = h(RID_{TA} \,||T_1 \,||T_2' \,||A_i \,||Z_j)$ and $V_j = h(SK_{ij} \,||T_1 \,||T_2')$. Thus, TUAS-RESG is also resilient against the smart meter impersonation attack.

Ephemeral secret leakage (ESL) attack: The shared secret session key between U_i and SM_j during the authentication and key agreement phase is calculated as $SK_{ij} = h(RID_{TA} \,||T_1 \,||T_2 \,||A_i \,||Z_j)$. The session key security (SK-security) depends on the following two cases:

Case 1. Suppose the ephemeral (short term) secrets ru_i and rs_j are revealed to an adversary $\mathcal{A}$. However, without having the long-term secrets RID_i, RID_{TA}, PW_i, σ_i, RID_{SM_j} and s_i, it is difficult for $\mathcal{A}$ to calculate SK_{ij}.

Case 2. Assume that the long-term secrets RID_i, RID_{TA}, PW_i, σ_i, RID_{SM_j} and s_i are revealed to $\mathcal{A}$. Then, without having the ephemeral secrets ru_i and rs_j, it is difficult for $\mathcal{A}$ to calculate SK_{ij}.

It is then clear that $\mathcal{A}$ can calculate SK_{ij} only if the ephemeral secrets and long-term secrets are known to him/her. Even if SK_{ij} is revealed to $\mathcal{A}$ in a particular session, all other session keys in previous and future sessions are different due to usage of both long-term secrets and fresh ephemeral random nonces. Thus, the leakage of a session key will have no effect on the security of other previous and future sessions for secure communications [20]. Hence, TUAS-RESG provides both perfect forward and backward secrecy, and also it provides the SK-security.

Anonymity and untraceability: Due to usage of the random nonces and current timestamps, the messages $Msg_1 = \langle X_i, R_i^*, A_i, T_1 \rangle$, $Msg_2 = \langle Y_j, V_j, T_2 \rangle$ and $Msg_3 = \langle ACK_i, T_3 \rangle$ exchanged during the login, and authentication and key agreement phases are distinct for each session. Therefore, an adversary $\mathcal{A}$ can not trace the user as well as smart meter. Moreover, these messages do not involve the pseudo-identities RID_i, RID_{TA} and RID_{SM_j}, and they are embedded in the collision-resistant one-way hash function $h(\cdot)$ (see Definition 1). Therefore, TUAS-RESG provides both anonymity and untraceability properties.

Password change attack: Suppose an adversary $\mathcal{A}$ has lost/stolen mobile device MD_i of a registered user U_i. $\mathcal{A}$ can then extract the important information $\{RID_i, R_i, BI_i, CI_i, RID'_{TA}, s_i^*, \tau_i, Gen(\cdot), Rep(\cdot), h(\cdot), t\}$ stored in MD_i's memory by applying the power analysis attacks [31], [32]. To change the password PW_i to another password PW_i', $\mathcal{A}$ requires to input correct ID_i, PW_i and BIO_i of U_i. Without these valid user credentials, local password and biometric verification will fail at the mobile device MD_i. Thus, $\mathcal{A}$ can not provide any other fake password PW_i' and fake biometrics in order to change the password PW_i to PW_i'. As a result, TUAS-RESG is secure against the password change attack.

VI. Comparative Study

In this section, we compare computation and communication costs, and functionality features of TUAS-RESG with other related schemes, such as the schemes of Wu-Zhou [25], Xia-Wang [26], Tsai-Lo [19], Odelu *et al.* [20] and Jo *et al.* (Protocol II) [21].

We use the following notations for the computational cost analysis. T_b, T_{ecm}, T_{eca}, T_m, T_e, T_s, T_{cert}, T_{cert_ver}, T_{fe}, T_h, T_{ecdsa_sig} and T_{ecdsa_sigver} denote time taken for a bilinear pairing operation, an ECC point multiplication operation, an ECC point addition operation, a multiplication operation, a modular exponentiation operation, a symmetric encryption/decryption operation, a certificate generation

operation, a certificate verification operation, fuzzy extractor $Gen(\cdot)/Rep(\cdot)$ operation, a one-way hash operation, an ECDSA (elliptic curve digital signature algorithm) signature generation and an ECDSA signature verification, respectively. Since the execution time of XOR operation is negligible, we do not consider this in computation time calculation as given in [19].

The execution times of different cryptographic operations on different platforms are given in Table II as provided in [40]. We assume $T_s \approx T_h$ and omit T_m in calculating the execution timings as it requires very low execution time than T_e, i.e., $T_m << T_e$. Further, $T_{eca} << T_e$, and we also assume $T_{eca} \approx T_h$.

TABLE II
EXECUTION TIME OF DIFFERENT CRYPTOGRAPHIC OPERATIONS [40]

Entity	T_b	T_{ecm}	T_e	T_h
Pentium IV	$3.16ms$	$1.17ms$	$< 1ms$	$0.01ms$
HiPerSmart Card	$0.38s$	$0.13s$	$< 0.1s$	$0.001s$

The computational costs for the authentication and key agreement phase of TUAS-RESG and other related schemes are compared in Table III. It is assumed that the computation of smart meter side and user/service provider/data collection unit side are performed on the HiPerSmart card and Pentium IV plaforms, respectively. In TUAS-RESG, the computation costs required for each SM_j and MD_i are $5T_h + 4T_{ecm} + 2T_{eca} \approx 0.527$s and $T_{fe}+8T_h+2T_{ecm} \approx 3.59$ms, respectively. From Table III, it is clear that TUAS-RESG requires less overall computation cost as compared to other schemes [19], [20], [25], [26].

The bit lengths of various parameters to estimate the required communication bits in various schemes are assumed as follows. Random number/nonce is 128 bits; identities and message digests are each 160 bits; elements in bilinear map groups G_1 and G_2 are 320 and 512 bits, respectively; and timestamp is 32 bits. Moreover, ECC signature is 320 bits and message warrant is 160 bits. In TUAS-RESG, the communication costs for the messages Msg_1, Msg_2 and Msg_3 are 832, 512 and 192 bits, respectively. Thus, the total communication cost in TUAS-RESG is 1536 bits. On the other hand, the schemes of Wu-Zhou [25], Xia-Wang [26], Tsai-Lo [19], Odelu *et al.* [20] and Jo *et al.* [21] require 3648, 1376, 1408, 1920 and 2464 bits, respectively. The communication costs of different schemes given in Table IV show that the proposed is efficient as compared to the schemes of Wu-Zhou [25], Odelu *et al.* [20] and Jo *et al.* [21], whereas it is also comprable with the schemes of Xia-Wang [26] and Tsai-Lo [19].

The functionality features comparison provided in Table V indicate that TUAS-RESG and Odelu *et al.*'s scheme [20] perform better than other schemes. Wu and Zhou's scheme [25] does not provide man-in-middle attack protection and also other required features as mentioned in Table V. Xia-Wang's scheme [26] fails to provide the security functionalities including strong credentials' privacy and SK-security. Except TUAS-RESG and Odelu *et al.*'s scheme [20], all other existing schemes fail to provide the required security functionalities including the strong credentials' privacy and SK-security under the widely-accepted CK-adversary model. Furthermore, only TUAS-RESG provides additional functionality features, such as password and biometric update phase, dynamic smart meter addition phase. In addition, TUAS-RESG also protects password change attack. Considering security and functionality features, and efficiency in terms of communication and computation costs, TUAS-RESG performs better than all the other schemes shown in Table V.

TABLE III
COMPUTATION COSTS COMPARISON

Scheme	CT_1	CT_2
[25]	$3T_{ecm}+T_m+T_h+T_{cert}$ ≈ 0.523s	$4Tecm + 4T_h + T_s + T_{cert\_ver}$ ≈ 5.91ms
[26]	$T_s + 4T_h$ ≈ 0.005s	$4T_h$ ≈ 0.04ms
[19]	$4T_{ecm} + T_e + 5T_h$ ≈ 0.625s	$3T_{ecm}+2T_b+T_e+5T_h$ ≈ 10.88ms
[20]	$3T_{ecm} + T_e + 6T_h$ ≈ 0.496s	$2T_{ecm}+2T_b+T_e+6T_h$ ≈ 9.72ms
[21] (Protocol II)	$T_{ecm} + 3T_h + 2T_e + 2T_{ecdsa\_sig}$ ≈ 0.397s	$2T_h+3T_{ecdsa\_sig}+2T_e +3T_{ecdsa\_sigver}+2T_b$ ≈ 16.99ms
TUAS-RESG	$5T_h+4T_{ecm}+2T_{eca}$ ≈ 0.527s	$T_{fe} + 8T_h + 2T_{ecm}$ ≈ 3.59ms

Note: CT_1 and CT_2 denote computation costs at smart meter side and user/service provider/data collection unit side in login and authentication phases, respectively.

TABLE IV
COMMUNICATION COSTS COMPARISON

Scheme	Communication cost	Number of messages
Wu-Zhou [25]	3648	4
Xia-Wang [26]	1376	5
Tsai-Lo [19]	1408	3
Odelu *et al.* [20]	1920	3
Jo *et al.* (Protocol II) [21]	2464	3
TUAS-RESG	1536	3

VII. PRACTICAL PERSPECTIVE: NS2 SIMULATION STUDY

The practical demonstration of TUAS-RESG and other related schemes, such as the schemes of Tsai and Lo [19], Odelu *et al.* [20], Jo *et al.* (Protocol II) [21], Wu and Zhou [25], and Xia and Wang [26], has been performed through the widely-accepted NS2 2.35 simulator [41].

A. Simulation Parameters and Environment

TUAS-RESG and other related schemes [19], [20], [21], [25], [26] are simulated on Ubuntu 14.04 LTS platform using the NS2 2.35 simulator [41]. The simulation parameters are given in Table VI. The network is simulated for 1800 seconds (i.e. 30 minutes). The following three network scenarios are considered in the simulation:

- Scenario 1. It consists of 10 $U_i/MD_i/SM_i/IDS_i$s and 10 $SM_j/SP_j/DCU_j/IDC_j$s.
- Scenario 2. It consists of 20 $U_i/MD_i/SM_i/IDS_i$s and 10 $SM_j/SP_j/DCU_j/IDC_j$s.

TABLE V
FUNCTIONALITIES COMPARISON OF VARIOUS RELATED SCHEMES

Feature	[25]	[26]	[19]	[20]	[21]	Our
$F1$	✓	×	✓	✓	✓	✓
$F2$	×	×	✓	✓	✓	✓
$F3$	✓	✓	✓	✓	✓	✓
$F4$	✓	✓	×	✓	✓	✓
$F5$	×	✓	✓	✓	✓	✓
$F6$	×	×	✓	✓	✓	✓
$F7$	×	×	×	✓	✓	✓
$F8$	×	×	×	✓	×	✓
$F9$	×	×	×	×	×	✓
$F10$	×	×	×	×	×	✓
$F11$	×	×	×	×	×	✓
$F12$	×	×	×	×	×	✓
$F13$	×	×	✓	✓	×	✓
$F14$	×	×	✓	✓	×	✓
$F15$	×	×	×	×	×	✓

Note: $F1$: protection against impersonation attacks; $F2$: providing perfect forward secrecy; $F3$: protection against replay attack; $F4$: protection against privileged-insider attack; $F5$: protection against man-in-the-middle attack; $F6$: whether a smart meter and user/service provider mutually authenticate each other without the help of the trusted anchor/authority; $F7$: providing strong smart meter credentials' privacy; $F8$: providing SK-security; $F9$: password update phase; $F10$: biometric update phase; $F11$: dynamic smart meter addition phase; $F12$: offline password guessing attack protection; $F13$: anonymity; $F14$: untraceability; $F15$: password change attack protection
✓: the scheme is secure or supports that feature; ×: the scheme is insecure or it does not support that feature.

TABLE VI
SIMULATION PARAMETERS USED IN ALL SCHEMES

Parameter	Description
Platform	Ubuntu 14.04 LTS
Tool used	NS2 2.35
Network coverage area	$5 \times 5\ km^2$
Number of smart meters SM_j	10 (for scenarios 1, 2, 3)
Number of mobile users U_i	10 (for Scenario 1) 20 (for Scenario 2) 30 (for Scenario 3)
Mobility of users U_i	$2m$, $10m$, $15m$ per second (for scenarios 1, 2, 3)
Simulation time	1800 seconds

- Scenario 3. It consists of 30 $U_i/MD_i/SM_i/IDS_i$s and 10 $SM_j/SP_j/DCU_j/IDC_j$s.

Here, SM_i, IDS_i, DCU_j and IDC_j represent i^{th} smart meter, i^{th} smart sensor, j^{th} data collection unit and j^{th} data collector in other related schemes [19], [20], [21], [25], [26].

In each scenario, we have different types of exchanged messages for various schemes and their communication costs (in bits) are provided in Table VII. The speeds of different vehicles in TUAS-RESG are considered as 2 meters per second (mps), 10 mps and 15 mps. In other schemes, the entities are considered as static.

B. Discussion on Simulation Results

We have computed various network performance parameters, such as throughput (in bps), end-to-end delay (in seconds) and packet delivery ratio during the simulation.

1) Impact on Throughput: Throughput is calculated as the number of bits transmitted per unit time. The throughputs (in bps) of TUAS-RESG under three scenarios are shown in Figure 3(a). The throughput can be computed as $\frac{n_r \times n_{pkt}}{T_d}$, where T_d is the total time (in seconds), n_{pkt} the size of a packet, and n_r the total number of received packets. Note that the simulation time is $1800s$, which is the total time. Scenarios 1, 2 and 3 have the throughput values as 110.35 bps, 215.34 bps and 326.83 bps, respectively. The throughput values increase with the number of increasing users/vehicles as more vehicles interact with the smart meter, and thus, the number of exchanged messages is high from scenarios 1 to 2, and also from scenarios 2 to 3. We have also compared the throughput of TUAS-RESG with the schemes of Tsai and Lo [19], Odelu *et al.* [20], Jo *et al.* [21], Wu and Zhou [25], and Xia and Wang [26]. Throughput of TUAS-RESG is less than the schemes of Jo *et al.* [21], Wu and Zhou [25], Odelu *et al.* [20] as TUAS-RESG has less communication cost and it uses small size of messages for authentication. Though the throughput of TUAS-RESG is more than the scheme of Xia and Wang [26] but it can be accepted as it provides more functionality features.

2) Impact on End-to-End Delay: The end-to-end delay (EED) is derived as the average time taken by data packets to arrive at a destination from a source. Figure 3(b) shows EEDs of TUAS-RESG under scenarios 1, 2 and 3. EED can be expressed as $\sum_{i=1}^{n_{pkt}}(T_{rec_i} - T_{send_i})/n_{pkt}$, where T_{rec_i} and T_{send_i} are the receiving and sending time of a packet i, respectively, and n_{pkt} is the total number of packets. EEDs are $0.03167s$, $0.05055s$ and $0.08379s$ for scenarios 1, 2 and 3, respectively. Note that the value of EED increases with the increasing number of users/vehicles. Increment in the number of users causes more exchanged messages and it further incurs congestion, and thus, EED increases from scenarios 2 and 3. We have also compared EED of TUAS-RESG with the schemes of Tsai and Lo [19], Odelu *et al.* [20], Jo *et al.* [21], Wu and Zhou [25], and Xia and Wang [26]. The EED of TUAS-RESG is less than the schemes of Tsai and Lo [19], Odelu *et al.* [20] and Wu and Zhou [25] as it is efficient and uses small size of messages for authentication. Though the EED of TUAS-RESG is more than the schemes of Xia and Wang [26] and Jo *et al.* [21] but it can be accepted as it provides more functionality features.

3) Impact on Packet Delivery Ratio: Packet delivery ratio (PDR) is the ratio of total transmitted packets to the total received packets. The PDRs of TUAS-RESG under scenarios 1, 2 and 3 are shown in Figure 3(c). The PDRs of TUAS-RESG are 0.99, 0.97 and 0.96 for scenarios 1, 2 and 3, respectively. PDR decreases with increasing number of users/vehicles from scenarios 1 to 2 and also from scenarios 2 to 3. This is because in case of more users, more messages are exchanged, and hence, it causes congestion in the network. Since TUAS-RESG is lightweight and it uses small packet sizes, so PDR decrement is also less. In addition, we have compared PDR of TUAS-RESG with the schemes of Tsai and Lo [19], Odelu *et al.* [20], Jo *et al.* [21], Wu and Zhou [25], and Xia and Wang [26]. The PDR of TUAS-RESG is comparable with the existing schemes.

VIII. CONCLUSION

In this paper, a new remote user authentication scheme is presented for a renewable energy based smart grid envi-

TABLE VII
EXCHANGED MESSAGES BETWEEN ENTITIES IN SIMULATION

Exchanged messages between entities	[19]	[20]	[21] (Protocol II)	[25]	[26]	TUAS-RESG
$U_i/SM_i/IDS_i \rightarrow SP_j/DCU_j/IDC_j$	608 bits	1088 bits	512 bits	1312 bits	288 bits	832 bits
$SP_j/DCU_j/IDC_j \rightarrow U_i/SM_i/IDS_i$	480 bits	672 bits	1344 bits	928 bits	288 bits	512 bits
$U_i/SM_i/IDS_i \rightarrow SP_j/DCU_j/IDC_j$	320 bits	160 bits	608 bits	–	160 bits	192 bits

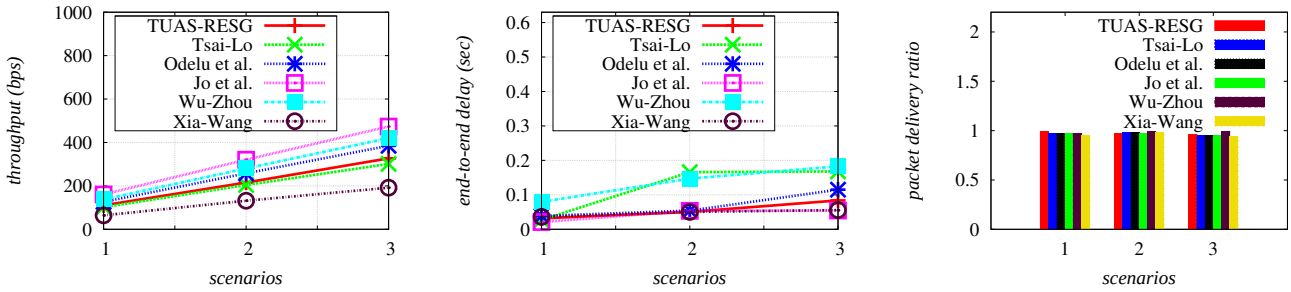

Fig. 3. (a) Throughput (b) End-to-end delay (c) Packet delivery ratio

ronment. TUAS-RESG is lightweight as compared to other existing schemes as it uses elliptic curve operations instead of costly modular exponentiation and bilinear pairing operations. The security of TUAS-RESG is thoroughly analyzed, and it shows that TUAS-RESG has the ability to defend various known attacks. In addition, TUAS-RESG supports additional functionality features, such as password and biometric update phase, and smart meter addition phase. Moreover, TUAS-RESG provides better trade-off among security, functionality features, and communication and computation costs as compared to other schemes. Finally, the simulation results using the NS2 simulator demonstrate the practicality of TUAS-RESG.

ACKNOWLEDGMENTS

This work has been partially supported by National Funding from the FCT - Fundação para a Ciência e a Tecnologia through the UID/EEA/50008/2013 Project, by the Government of the Russian Federation, Grant 074-U01, by Finep, with resources from Funttel, Grant No. 01.14.0231.00, under the Centro de Referência em Radicomunicações - CRR project of the Instituto Nacional de Telecomunicações (Inatel), Brazil, and by Ciência sem Fronteiras of CNPq, Brazil, through the process number 207706/2014-0.

REFERENCES

[1] K. Mahmood, S. A. Chaudhry, H. Naqvi, T. Shon, and H. F. Ahmad, "A lightweight message authentication scheme for smart grid communications in power sector," *Computers & Electrical Engineering*, vol. 52, pp. 114 – 124, 2016.

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

[3] R. Yu, W. Zhong, S. Xie, C. Yuen, S. Gjessing, and Y. Zhang, "Balancing Power Demand Through EV Mobility in Vehicle-to-Grid Mobile Energy Networks," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 1, pp. 79–90, 2016.

[4] G. A. Shah, V. C. Gungor, and O. B. Akan, "A Cross-Layer QoS-Aware Communication Framework in Cognitive Radio Sensor Networks for Smart Grid Applications," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 3, pp. 1477–1485, 2013.

[5] A. A. Khan, M. H. Rehmani, and M. Reisslein, "Cognitive Radio for Smart Grids: Survey of Architectures, Spectrum Sensing Mechanisms, and Networking Protocols," *IEEE Communications Surveys Tutorials*, vol. 18, no. 1, pp. 860–898, 2016.

[6] M. H. Rehmani, M. E. Kantarci, A. Rachedi, M. Radenkovic, and M. Reisslein, "IEEE Access Special Section Editorial Smart Grids: a Hub of Interdisciplinary Research," *IEEE Access*, vol. 3, pp. 3114–3118, 2015.

[7] M. Erol-Kantarci and H. T. Mouftah, "Energy-Efficient Information and Communication Infrastructures in the Smart Grid: A Survey on Interactions and Open Issues," *IEEE Communications Surveys Tutorials*, vol. 17, no. 1, pp. 179–197, 2015.

[8] F. Akhtar and M. H. Rehmani, "Energy replenishment using renewable and traditional energy resources for sustainable wireless sensor networks: A review," *Renewable and Sustainable Energy Reviews*, vol. 45, pp. 769–784, 2015.

[9] N. Nezamoddini, S. Mousavian, and M. Erol-Kantarci, "A risk optimization model for enhanced power grid resilience against physical attacks," *Electric Power Systems Research*, vol. 143, pp. 329–338, 2017.

[10] T. Gazdar, A. Rachedi, A. Benslimane, and A. Belghith, "A distributed advanced analytical trust model for VANETs," in *IEEE Global Communications Conference (GLOBECOM'12)*, Anaheim, California, USA, 2012, pp. 201–206.

[11] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "A Job Market Signaling Scheme for Incentive and Trust Management in Vehicular Ad Hoc Networks," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 8, pp. 3657–3674, 2015.

[12] T. Gazdar, A. Benslimane, A. Belghith, and A. Rachedi, "A secure cluster-based architecture for certificates management in vehicular networks," *Security and Communication Networks*, vol. 7, no. 3, pp. 665–683, 2014.

[13] A. Rachedi and A. Benslimane, "Security and Pseudo-Anonymity with a Cluster-Based Approach for MANET," in *IEEE Global Telecommunications Conference (GLOBECOM'08)*, New Orleans, LO, USA, 2008, pp. 1–6.

[14] A. Alnasser and N. E. Rikli, "Design of a Trust Security Model for Smart Meters in an Urban Power Grid Network," in *Proceedings of the 10th ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet'14)*, Montreal, QC, Canada, 2014, pp. 105–108.

[15] H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung, "Efficient authentication and key management mechanisms for smart grid communications," *IEEE Systems Journal*, vol. 8, no. 2, pp. 629–640, 2014.

[16] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An efficient merkle-tree-

based authentication scheme for smart grid," *IEEE Systems Journal*, vol. 8, no. 2, pp. 655–663, 2014.
[17] T. W. Chim, S. M. Yiu, V. O. K. Li, L. C. K. Hui, and J. Zhong, "PRGA: Privacy-Preserving Recording amp; Gateway-Assisted Authentication of Power Usage Information for Smart Grid," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 85–97, 2015.
[18] A. C. F. Chan and J. Zhou, "Cyber-Physical Device Authentication for the Smart Grid Electric Vehicle Ecosystem," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 7, pp. 1509–1517, 2014.
[19] J.-L. Tsai and N.-W. Lo, "Secure Anonymous Key Distribution Scheme for Smart Grid," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 906–914, 2016.
[20] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably Secure Authenticated Key Agreement Scheme for Smart Grid," *IEEE Transactions on Smart Grid*, 2016, DOI: 10.1109/TSG.2016.2602282.
[21] H. J. Jo, I. S. Kim, and D. H. Lee, "Efficient and Privacy-Preserving Metering Protocols for Smart Grid Systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1732–1742, 2016.
[22] I. Doh, J. Lim, and K. Chae, "Secure Authentication for Structured Smart Grid System," in *International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS'15)*, Fukuoka, Japan, 2015, pp. 200–204.
[23] N. Saxena, B. J. Choi, and R. Lu, "Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 907–921, 2016.
[24] D. He, H. Wang, M. K. Khan, and L. Wang, "Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography," *IET Communications*, vol. 10, no. 14, pp. 1795–1802, 2016.
[25] D. Wu and C. Zhou, "Fault-tolerant and scalable key management for smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 375–381, 2011.
[26] J. Xia and Y. Wang, "Secure key distribution for the smart grid," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1437–1443, 2012.
[27] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," *IEEE Communications Surveys Tutorials*, vol. 16, no. 4, pp. 1933–1954, 2014.
[28] J. Dai, M. Dong, R. Ye, A. Ma, and W. Yang, "A review on electric vehicles and renewable energy synergies in smart grid," in *China International Conference on Electricity Distribution (CICED'16)*, Shenzhen, China, 2016, pp. 1–4.
[29] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.
[30] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1086–1090, 2009.
[31] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.
[32] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proceedings of Advances in Cryptology - CRYPTO'99, LNCS*, vol. 1666, 1999, pp. 388–397.
[33] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *International Conference on the Theory and Applications of Cryptographic Techniques– Advances in Cryptology (EUROCRYPT'01)*. Innsbruck (Tyrol), Austria: Springer, 2001, pp. 453–474.
[34] R. Canetti and H. Krawczyk, "Universally Composable Notions of Key Exchange and Secure Channels," in *International Conference on the Theory and Applications of Cryptographic Techniques– Advances in Cryptology (EUROCRYPT'02)*, Amsterdam, The Netherlands, 2002, pp. 337–351.
[35] "Secure Hash Standard," FIPS PUB 180-1, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, April 1995. Available at http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf. Accessed on April 2017.
[36] A. K. Das, "A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks," *Peer-to-Peer Networking and Applications*, vol. 9, no. 1, pp. 223–244, 2016.
[37] V. Odelu, A. K. Das, and A. Goswami, "SEAP: Secure and efficient authentication protocol for NFC applications using pseudonyms," *IEEE Transactions on Consumer Electronics*, vol. 62, no. 1, pp. 30–38, 2016.
[38] V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 9, pp. 1953–1966, 2015.
[39] P. Sarkar, "A Simple and Generic Construction of Authenticated Encryption with Associated Data," *ACM Transactions on Information and System Security*, vol. 13, no. 4, pp. 1–16, 2010, article No. 33.
[40] Y. M. Tseng, S. S. Huang, T. T. Tsai, and J. H. Ke, "List-free id-based mutual authentication and key agreement protocol for multiserver architectures," *IEEE Transactions on Emerging Topics in Computing*, vol. 4, no. 1, pp. 102–112, 2016.
[41] "The Network Simulator-ns-2," http://www.isi.edu/nsnam/ns/. Accessed on April 2016.

Mohammad Wazid (S'17) received the M.Tech. degree in computer network engineering from Graphic Era University, Dehradun, India and the Ph.D. degree in computer science and engineering from the International Institute of Information Technology (IIIT), Hyderabad, India. His current research interests include cryptography and network security. He has published more than 40 papers in international journals and conferences in the above areas.

Ashok Kumar Das (M'17) received the Ph.D. degree in computer science and engineering, the M.Tech. degree in computer science and data processing, and the M.Sc. degree in mathematics from IIT Kharagpur, India. He is currently an Assistant Professor with IIIT Hyderabad, India. His current research interests include security in vehicular ad hoc networks, smart grid, Internet of Things (IoT), Cyber-Physical Systems and cloud computing, and remote user authentication. He has authored over 140 papers in international journals and conferences in the above areas. He was a recipient of the Institute Silver Medal from IIT Kharagpur.

Neeraj Kumar (M'16) received the Ph.D. degree in computer science and engineering from Shri Mata Vaishno Devi University, Katra (J&K), India, in 2009. He was a Post-Doctoral Research Fellow at Coventry University, Coventry, U.K. He is currently an Associate Professor with the Department of Computer Science and Engineering, Thapar University, Patiala, India. He has authored more than 160 technical research papers published in leading journals and conferences from the IEEE, Elsevier, Springer, John Wiley, etc. He has guided many research scholars leading to Ph.D. and M.E./M.Tech.

Joel J. P. C. Rodrigues [S'01–M'06–SM'06] is professor at the National Institute of Telecommunications (Inatel), Brazil and senior researcher at the Instituto de Telecomunicações, Portugal. He has been professor at UBI, Portugal and visiting professor at UNIFOR. He received the Academic Title of Aggregated Professor in informatics engineering from UBI, the Habilitation in computer science and engineering from the University of Haute Alsace, France, a PhD degree in informatics engineering and an MSc degree from the UBI, and a five-year BSc degree (licentiate) in informatics engineering from the University of Coimbra, Portugal. He is the leader of NetGNA Research Group. He has authored or coauthored over 500 papers in refereed international journals and conferences, 3 books, and 2 patents. He is member of the Internet Society, an IARIA fellow, and a senior member ACM and IEEE.