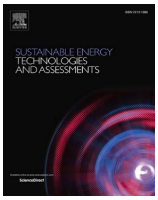
Contents lists available at ScienceDirect

Sustainable Energy Technologies and Assessments

journal homepage: www.elsevier.com/locate/seta



A secure demand response management authentication scheme for smart grid

Azeem Irshad[a], Shehzad Ashraf Chaudhry[b], Mamoun Alazab[c], Ambrina Kanwal[d], M Sultan Zia[e], Yousaf Bin Zikria[f,*]

[a] Department of Computer Science and Software Engineering, International Islamic University, Islamabad
[b] Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, Turkey
[c] College of Engineering, IT and Environment, Charles Darwin University, 0810 NT, Australia
[d] Department of Computer Science, Bahria University, Islamabad, Pakistan
[e] Department of Computer Science and IT, University of Lahore, Gujrat Campus 50700, Pakistan
[f] Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, South Korea

ARTICLE INFO

Keywords:
Smart grid
Authentication
Attacks
Anonymity
Demand response management
BAN

ABSTRACT

The electricity demands are floated through smart grid (SG) devices to a remote power management system and utility center (UC) for utilizing energy-based services, while the UCs manage the distribution of power. Nevertheless, in smart grid systems, the communication messages are susceptible to various threats, since the information related to power consumption is communicated over an unsafe public channel. Therefore, a secure authenticated key agreement scheme is crucial for dispensing energy-based services to legal subscribers. In this regard, Yu et al. designed a secure authentication scheme for smart grid-based demand response management. Nevertheless, we discover that Yu et al.'s protocol is prone to replay attack, denial-of-service attack, and many technical defects in the protocol. Thus, we propose an anonymous and lightweight authenticated key agreement protocol for smart grid-based demand response management countering the limitations in Yu *et al.*'s scheme. Our scheme may withstand known security attacks, and also supports privacy as well as mutual authentication. We evaluate the security properties of contributed protocol employing informal security analysis and proved the security of session key between the utility center and smart grid using Burrows Abadi Needham (BAN) logic analysis and ProVerif automated simulation. The achieved results sufficiently advocate the practical implementation of the scheme.

Introduction

The recent growth in information and communication technologies has led to the ease of access for the provision of services in smart grid systems. The SG systems mostly encompass smart home, smart building, smart appliances, smart meters, and renewable energy-based vehicle-to-grid systems [1–5]. More specifically, the SG using smart devices or the internet of things (IoT)-based systems has received an enhanced focus of the researchers, industry, and academia. The smart grid devices such as smart meters or IoT sensing devices are fundamental components used for collecting significant information related to power consumption, and transferring towards utility centers such as power generation centers and distributors. Per the statistics of 1988, provided by the U.S department of energy (DoE), the demand for electricity has significantly risen by an estimate of 30% as compared to a 15% rise in the transmission capacity of power [6]. That is why; the demand-response (DR) management is becoming a critical concern for ensuring the smooth power supply and consumption.

In a smart grid environment, the SG devices are mostly installed in homes, buildings, and industries, etc, collecting real-time data, and transmitting power demands towards energy producers [5]. Nonetheless, the energy producers may not handle such request demands due to difficulty in handling a volume of big data as collected by SG devices [7–8]. To handle these issues including the maintenance of stable and efficient power supply, the utility centers (UCs) make the analysis of data as collected by smart grid devices, and effectively manage DR,

[*] Corresponding author.
E-mail addresses: irshadazeem2@gmail.com (A. Irshad), sashraf@gelisim.edu.tr, ashraf.shehzad.ch@gmail.com (S.A. Chaudhry), alazab.m@ieee.org (M. Alazab), sultan.zia@cs.uol.edu.pk (M. Sultan Zia), yousafbinzikria@ynu.ac.kr (Y.B. Zikria).

https://doi.org/10.1016/j.seta.2021.101571
Received 18 October 2020; Received in revised form 29 June 2021; Accepted 17 August 2021
Available online 16 September 2021

power leakage, power load balancing, dynamic pricing strategy, as well as real-time fault detection [9]. Nevertheless, due to the insecure public channel, the data exchanged between SG devices and UC could be maliciously handled by adversaries in the form of tampering, injection, deletion, or forgery of data [10]. As a result, the malicious activities might create gaps between demand and supply of energy or related energy imbalance problems. Hence, there is a growing need for strengthening authenticated key agreement mechanisms related to the smooth flow of smart grid operations for DR management and data analytics. We illustrate a few security requirements for an effective smart grid system as given below:

- An efficient and secure authentication protocol should ensure user's privacy as well as security for communication between devices and UC.
- An efficient and secure protocol should provide resistance to impersonation, replay, offline identity or password guessing, and forgery attacks.
- A secure key agreement protocol must undertake the constraints of smart grid devices in terms of limited memory, communication bandwidth, and power consumption.

The smart grid, to a large extent, depends on the use of smart metering infrastructure (SMI) for collecting the feedback of power consumption. The collected data from SG devices may help in estimating the real-time load requirements, real-time price settings, and DR management. However, this collection of data for power consumption might result in serious privacy concerns, if the standard security solutions are not adopted. If this critical data for power consumption of any smart grid device is accidentally exposed, it may reveal the private data of clients indicating the client's routine activity or the information of power consumption. Moreover, the computational and communication-based resources in smart grid infrastructure are very limited. Hence, we need an efficient and secure authenticated key agreement procedure to preserve the client's privacy and keep the computation cost low in the resource-constrained smart grid environment.

Recently, Yu et al. [10] presented a privacy preserving authenticated key agreement scheme for DR management in smart grids environment. Yu et al. claimed that their protocol provides resistance to various known threats, however, after careful observation we discover that this protocol cannot resist various attacks, including replay attack, an offline identity-guessing attack upon stolen smart card, denial of service attack. Besides, the scheme has many technical defects in its protocol. Therefore, we propose an improved and enhanced privacy preserving lightweight authenticated key agreement protocol for DR management in smart grid systems, with proven performance efficiencies and formal analysis on security.

Attack model

We follow a widely adopted Dolev-Yao (DY) attack model [11–16] for evaluating the security strength of the proposed scheme. In accordance with DY model, the attacker may eavesdrop, modify, delete, or inject new messages into the original messages over a public channel. In the following, we take a few more assumptions of the attacker's model in addition to the competencies as defined above.

- The malicious attacker might steal the smart grid device of a user and recover all contents stored in that device by employing power analysis [17,18]. It is also assumed that the malicious attacker may capture as many smart grid devices as possible.
- The attacker could attempt different attacks such as impersonation, replay, modification, as well as a man-in-the-middle attack.
- The trusted authority (TA) and utility center are supposed to be reliable authorities that might not be physically attacked by any malevolent attacker.

Contribution

The salient points of contribution in this work are given below:

- We exhibit that Yu et al.'s protocol cannot defend several threats including replay and offline identity-guessing threats upon stolen smart cards, and denial of service (DoS) attack.
- We propose an improved, privacy-preserving lightweight authenticated key agreement scheme for a smart grid system employing pseudo-identity and removing other technical defects in the scheme. The contributed scheme might withstand impersonation attack, replay attack, DoS attack, as well as support mutual authentication.
- We employed a widely adopted logical analysis, termed as Burrows-Abadi-Needham (BAN) logic analysis for proving the mutual authentication support for the proposed scheme. We also discussed the security analysis informally for proving the resistance of our scheme against different attacks.
- We utilized Proverif automated tool for validating the security properties in terms of susceptibility against man-in-the-middle and replay threats. Furthermore, we depict the comparison for performance evaluation of contributed scheme against other protocols.

Scheme's organization

This scheme is structured as follows: Section 2 illustrates the related literature work. Section 3 presents the system's model of the contributed scheme. Section 4 revisits the working of Yu et al. protocol. Section 5 describes the cryptanalysis of Yu et al. Section 6 demonstrates the informal and formal analysis, including automated tool analysis. Section 7 presents the performance evaluation of the proposed model. The last section presents the concluded summary of findings.

Related work

We can witness several privacy-preserving and authenticated key agreement protocols for smart grid systems in a few years [19–22]. Rottondi et al., in 2014, demonstrated a secure and privacy-preserving protocol in Vehicle-to-grid communication [20]. Later, Ali et al. [19] introduced two Elliptic Curve Cryptography (ECC) and ID-based authentication protocols. Even though their scheme is immune to forgery and de-synchronization threats and also minimized computational cost on the side of a smart meter, this was susceptible to Man-in-the-Middle (MIDM) and false data injection threats. Then, Wan et al. [21] demonstrated an effective and privacy-preserving authentication scheme for a smart grid environment. Lately, the smart grid systems received more focus from research academia and industry than ever before [23–31]. Meanwhile, Tsai and Lo [26] designed the identity-based key authentication and distribution scheme for the smart grid. Then, in 2016, Odelu et al. [25] depicted that Tsai and Lo may not resist temporary session specific information leakage threat, and also fails to maintain the anonymity of smart meter. Also, Odelu et al. presented an improved authentication protocol for smart grid systems. Afterward, Doh et al. [28] introduced a secure authenticated key agreement protocol between smart meters SM and utility center UC for managing the bidirectional communication related to power consumption. Thereafter, Saxena et al. [29] designed another authentication protocol for the smart grid which was protected from attacks but does not provide untraceability and privacy. Meanwhile, He et al. [30] came up with another anonymous, ECC-oriented lightweight authentication and key distribution protocol for the smart grid environment, countering the flaws for Tsai and Lo's protocol [20]. In 2017, Wazid et al. [31] demonstrated an efficient three-factor authentication protocol for smart grid-based renewable energy systems. Similarly, Kumar et al. in 2019 [9], put forward an ECC-oriented authenticated key agreement scheme for smart grid-based DR management. Nevertheless, [9] scheme does not provide resistance to smart grid device stolen threat, impersonation,

Table 1
Tabular depiction of recent Smart Grid authentication schemes.

Scheme	Features	Drawbacks	Year
Tsai and Lo et al. [26]	Identity-based key authentication and distribution scheme	Lacks mutual authentication , suffers impersonation threat, Session specific temporary information threat	2016
Saxena et al. [29]	authentication protocol for the smart grid	Lacks untraceability and privacy features	2016
He et al. [30]	anonymous, ECC-oriented lightweight authentication and key distribution protocol for the smart grid	Lacks mutual authentication among the legal participants	2016
Wazid et al. [31]	three-factor authentication protocol for smart grid	Forgery attacks	2017
Kumar et al. [9]	an ECC-oriented authenticated key agreement scheme for smart grid	Stolen device attack, impersonation attack, session key exposure threat	2019
Yu et al. [10]	Privacy preserving scheme for DR management	Replay attack, DoS attack	2020

and session key exposure threat, and also it does not fulfill mutual authentication features according to Yu et al. [10], subsequently as shown in Table 1.

Then, Yu et al. [10] presented a privacy preserving authenticated key agreement scheme for DR management in smart grids environment. Yu et al. claimed that their protocol provides resistance to various known threats, nevertheless, after careful observation, we discover that this protocol cannot resist various attacks, including replay attack, denial of service attack, and lacks mutual authentication. Besides, the scheme has many technical defects in its protocol

System model

In this section, the DR management for the smart grid (SG) is illustrated along with the involved participating entities. The SG-network model consists of two main entities, i.e., SG device and UC as depicted in Fig. 1. There are multiple SG devices in the system, collecting power-consumption data, and providing electricity management services. A utility centermonitors the collected data related to power consumption, real-time load forecasting, and pricing, demand response, etc. After collecting it, the UC compiles the total electricity load consumption for taking measures for balancing the available power load in its limited capacity. Nevertheless, the smart grid devices are installed in the remote homes or industrial SG fields, it is recording as well as transmission might involve critical privacy concerns. A smart grid device submits the electricity consumption reports through communication ways towards utility centers. Hence, it is convenient for the consumers for staying at home without concentrating on the consumption or readings of smart metering or SG devices. Moreover, if there are not secure protocols for such communication, then any user's data from the SG device or appliance may be revealed to the attackers [32,33]. Thus, the privacy of subscribers may be violated and the recovered data may be misused for malevolent objectives. As a result, the authentication protocols in smart grid environments should be supporting users' privacy as well as immune to known attacks.

Fig. 2 represents the authentication model of the contributed protocol in smart grid environments for providing anonymity to the user and secure interaction between the user and the utility center. The proposed protocol consists of three participants: Trust authority (TA), smart grid SG device, and utility center UC. The UC as well as SG devices register their respective identities from TA, initially. Then, the TA generates corresponding credential parameters for both UC and SG devices, respectively. After the registration procedure, the SG devices may authenticate the UC during the mutual authentication phase, so that these entities may exchange power consumption reports and other feedbacks securely.

Revisiting Yu et al.'s scheme

The Yu et al.'s scheme [10], based on securing the authenticated key agreement phase for demand-response (DR) management in the smart grid system network, comprises seven procedures, such as pre-deployment phase, SG device registration phase, UC registration phase, mutual authentication. Table 2 may be consulted for understanding the notation used to describe Yu et al.'s scheme.

Pre-deployment procedure

In the pre-deployment phase, the UCj and smart grid devices SGD$_i$ get registered with trust authority (TA) before being deployed in the smart grid environment. The TA, initially, chooses unique identities, i.e. ID_i and ID_j for SGD_i and UC_j, respectively. Then, TA saves the information of identities such as ID_i in SGD_i's memory, and ID_j in UC$_j$'s memory before their deployment in the smart grid environment.

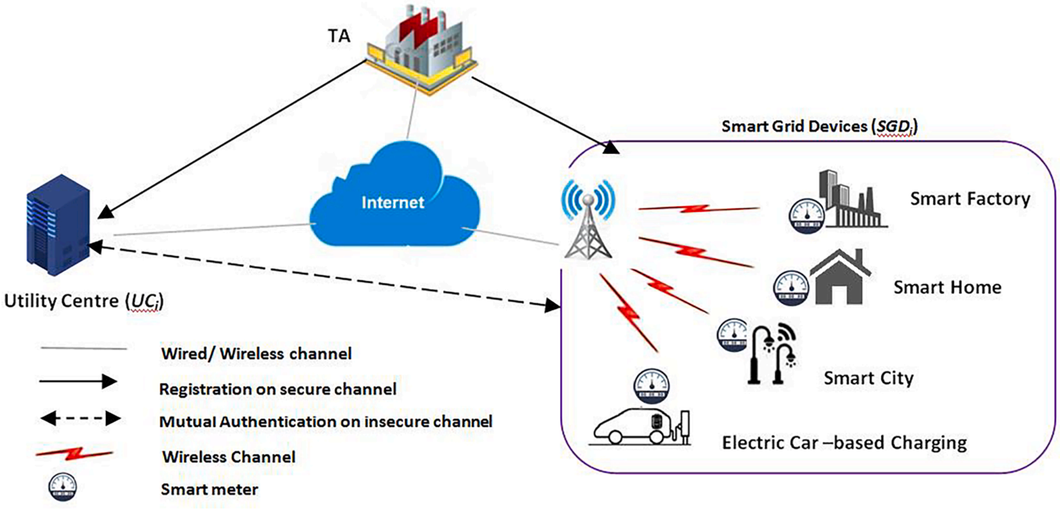
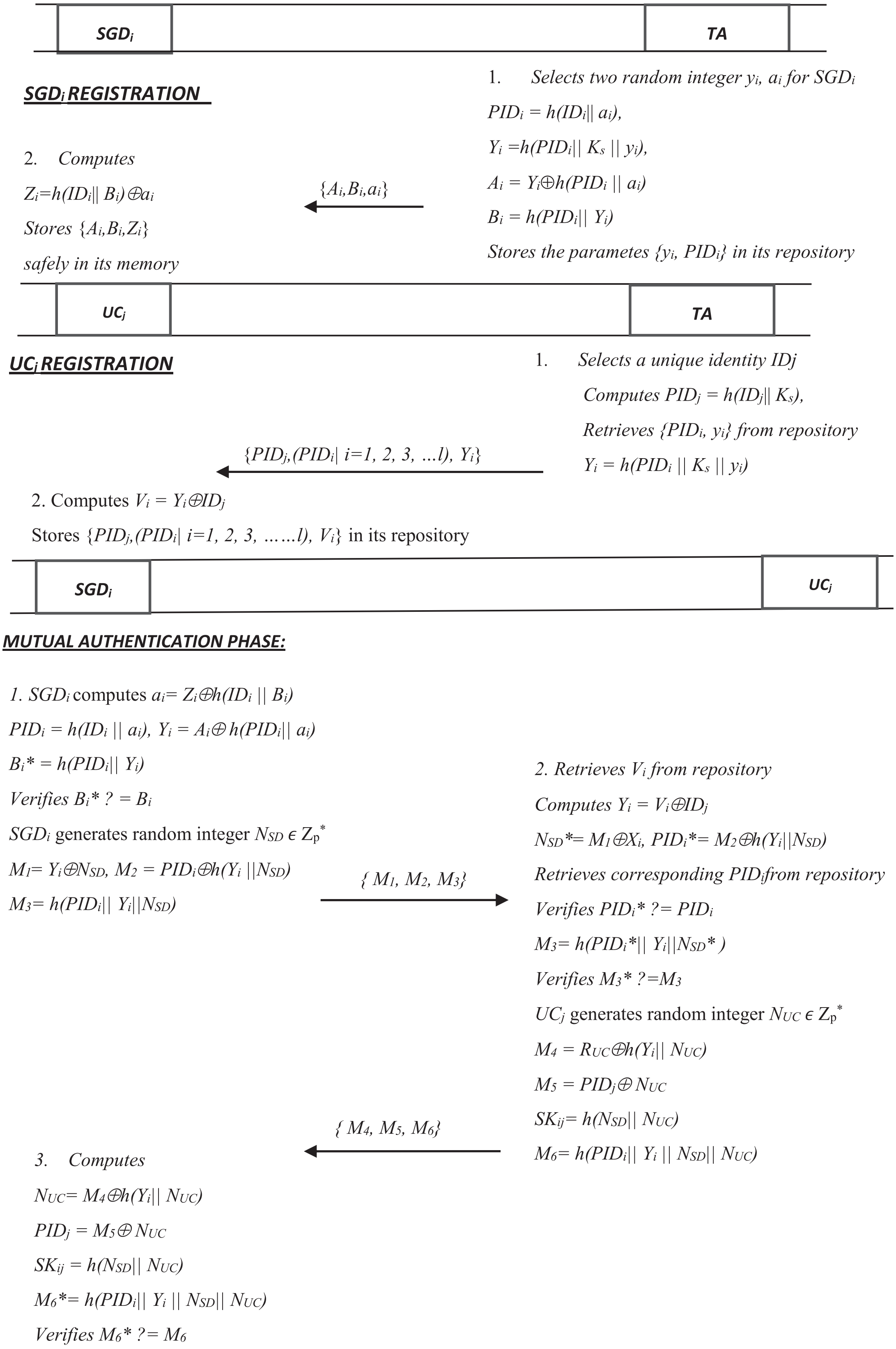

TA
Smart Grid Devices (SGD$_i$)
Internet
Smart Factory
Smart Home
Smart City
Electric Car –based Charging
Utility Centre (UC$_j$)
Wired/ Wireless channel
Registration on secure channel
Mutual Authentication on insecure channel
Wireless Channel
Smart meter

Fig. 1. Smart Grid Architecture.



SGD_i TA

SGD_i REGISTRATION

1. *Selects two random integer y_i, a_i for SGD_i*

$PID_i = h(ID_i || a_i)$,

$Y_i = h(PID_i || K_s || y_i)$,

$A_i = Y_i \oplus h(PID_i || a_i)$

$B_i = h(PID_i || Y_i)$

Stores the parametes $\{y_i, PID_i\}$ in its repository

$\{A_i, B_i, a_i\}$

2. *Computes*

$Z_i = h(ID_i || B_i) \oplus a_i$

Stores $\{A_i, B_i, Z_i\}$

safely in its memory

UC_j TA

UC_j REGISTRATION

1. *Selects a unique identity IDj*

Computes $PID_j = h(ID_j || K_s)$,

Retrieves $\{PID_i, y_i\}$ from repository

$Y_i = h(PID_i || K_s || y_i)$

$\{PID_j, (PID_i | i=1, 2, 3, \ldots l), Y_i\}$

2. Computes $V_i = Y_i \oplus ID_j$

Stores $\{PID_j, (PID_i | i=1, 2, 3, \ldots\ldots l), V_i\}$ in its repository

SGD_i UC_j

MUTUAL AUTHENTICATION PHASE:

1. SGD_i computes $a_i = Z_i \oplus h(ID_i || B_i)$

$PID_i = h(ID_i || a_i)$, $Y_i = A_i \oplus h(PID_i || a_i)$

$B_i{*} = h(PID_i || Y_i)$

Verifies $B_i{*}\ ? = B_i$

SGD_i generates random integer $N_{SD} \in Z_p^*$

$M_1 = Y_i \oplus N_{SD}$, $M_2 = PID_i \oplus h(Y_i || N_{SD})$

$M_3 = h(PID_i || Y_i || N_{SD})$

$\{M_1, M_2, M_3\}$

2. *Retrieves V_i from repository*

Computes $Y_i = V_i \oplus ID_j$

$N_{SD}{*} = M_1 \oplus X_i$, $PID_i{*} = M_2 \oplus h(Y_i || N_{SD})$

Retrieves corresponding $PID_i$from repository

Verifies $PID_i{*}\ ?= PID_i$

$M_3 = h(PID_i{*} || Y_i || N_{SD}{*})$

Verifies $M_3{*}\ ?= M_3$

UC_j generates random integer $N_{UC} \in Z_p^*$

$M_4 = R_{UC} \oplus h(Y_i || N_{UC})$

$M_5 = PID_j \oplus N_{UC}$

$SK_{ij} = h(N_{SD} || N_{UC})$

$M_6 = h(PID_i || Y_i || N_{SD} || N_{UC})$

$\{M_4, M_5, M_6\}$

3. *Computes*

$N_{UC} = M_4 \oplus h(Y_i || N_{UC})$

$PID_j = M_5 \oplus N_{UC}$

$SK_{ij} = h(N_{SD} || N_{UC})$

$M_6{*} = h(PID_i || Y_i || N_{SD} || N_{UC})$

Verifies $M_6{*}\ ?= M_6$

Fig. 2. Working of Yu et al.'s scheme [10].

Table 2
Notations description.

Notations	Description
TA:	Trusted Authority
SGD_i :	i^{th} Smart grid device
UC_j :	j^{th} Utility centre
ID_i :	SGD_i's identity
ID_j :	UC_j's identity
PID_i/PID_j	Pseudo-identities of SGD_i andUCj
K_s	Master secret key of TA
SK_{ij}:	Shared session key between SGD_i and UC_j
a_i , y_i:	Long term random variables for SGD_i
N_{SD}, N_{UC}:	Temporary nonces
$h()$:	A secure one-way hash function
$\|\|$,$\oplus$	Concatenation, XOR

Registration phase of smart grid device

The SGD_i needs to register with a trusted third party TA for receiving the services of power management. Fig. 2 depicts the registration process for SGD_i devices in Yu et al.'s protocol. The steps of this phase are illustrated below.

1. The trusted authority TA selects two random integers y_i, a_i for SGD_i. Then, TA calculates $PID_i = h(ID_i|| a_i)$, $Y_i = h(PID_i||K_s||y_i)$, $A_i = Y_i \oplus h(PID_i|| a_i)$, and $B_i = h(PID_i||Y_i)$. Then, it stores the parameters $\{y_i, PID_i\}$ in its secure repository, and submits $\{ A_i, B_i , a_i\}$ towards SGD_i.
2. After getting the message$\{ A_i, B_i , a_i\}$, the SGD_i calculates $Z_i = h(ID_i|| B_i) \oplus a_i$ and saves the parameters $\{A_i, B_i , Z_i\}$ safely in its memory.

Uc_j registration phase

The UC_j needs to get registered from TA for dispensing the services of power management. Fig. 2 depicts the UC_j registration procedure for Yu et al.'s protocol. The salient steps of the registration phase are given as under.

1. The TA, initially selects a unique identity IDj, and calculates $PID_j = h(ID_j|| K_s)$, and retrieves $\{ PID_i, y_i\}$ from its repository. Then, it further calculates $Y_i = h(PID_i||K_s||y_i)$, and submits$\{PID_j, (PID_i \mid i = 1, 2, 3, \dots l), Y_i\}$ towards UC_j.
2. The UC_j, after getting the message, further calculates $V_i = Y_i \oplus ID_j$ and saves $\{PID_j, (PID_i \mid i = 1, 2, 3, \dots l), V_i\}$ safely in its repository.

Authentication phase

In the authentication procedure of Yu et al.'s protocol, the user is provided with the anonymity feature by employing pseudo-identities as well as short term secret parameters. Before initiating the session, the SGD_i sends an authentication request towards UC_j for protected communication, and construct an agreed session key SK_{ij}. Fig. 2 demonstrates the mutual authentication procedure of Yu et al.'s protocol. The main steps of this phase are illustrated below.

1. Initially, the SGD_i by employing the stored parameters, computes $a_i = Z_i \oplus h(ID_i || B_i)$, $PID_i = h(ID_i || a_i)$, $Y_i = A_i \oplus h(PID_i|| a_i)$, and $B_i{}^* = h(PID_i || Y_i)$. Then, it verifies the equality $B_i{}^* ? = B_i$. After successful verification, the SGD_i generates random integer $N_{SD} \in \mathrm{Z_p}^*$ and computes $M_1 = Y_i \oplus N_{SD}$, $M_2 = PID_i \oplus h(Y_i || N_{SD})$ and $M_3 = h(PID_i|| Y_i|| N_{SD})$. Next, it submits the message $\{M_1, M_2, M_3\}$ to UC_j for verification.
2. The UC_j, upon receiving the message $\{ M_1, M_2, M_3\}$ retrieves V_i from repository, and computes $Y_i = V_i \oplus ID_j$, $N_{SD}{}^* = M_1 \oplus X_i$, $PID_i{}^*= M_2 \oplus h(Y_i|| N_{SD})$. Then, it further retrieves corresponding PID_i from repository, and verifies the equality for $PID_i{}^* ?= PID_i$. Next, it computes $M_3 = h(PID_i{}^*|| Y_i|| N_{SD}{}^*)$ and verifies $M_3{}^* ?=M_3$. Next, it generates random integer $N_{UC} \in \mathrm{Z_p}^*$ and computes $M_4 = N_{UC} \oplus h(Y_i|| N_{UC})$, $M_5 = PID_j \oplus N_{UC}$, $SK_{ij} = h(N_{SD}|| N_{UC})$, and $M_6 = h(PID_i || Y_i || N_{SD}|| N_{UC})$. Then, it forwards the message $\{M_4, M_5, M_6\}$ towards SGD_i.
3. Upon receiving the message, the SGD_i computes $N_{UC} = M_4 \oplus h(Y_i|| N_{UC})$, $PID_j = M_5 \oplus N_{UC}$, $SK_{ij} = h(N_{SD}|| N_{UC})$, and $M_6{}^*= h(PID_i || Y_i || N_{SD}|| N_{UC})$. Finally, it verifies $M_6{}^* ?= M_6$ and authenticates the UC_j for successful verification.

Security limitations in Yu et al.'s scheme

This section unveils few security limitations of Yu et al.'s scheme such as replay attack, lacking mutual authentication, denial-of-service attack, and technical defects in the protocol as given below:

Replay attack

The UC_j is unable to ensure the freshness of the message submitted by SGD_i. An attacker may intercept the message $\{M_1, M_2, M_3\}$,and replay anytime in the future. The UC_j after receiving the message $\{M_1, M_2, M_3\}$, retrieves V_i from repository, computes$Y_i = V_i \oplus ID_j$, $N_{SD}{}^* = M_1 \oplus X_i$, $PID_i{}^* = M_2 \oplus h(Y_i|| N_{SD})$. Onwards, it retrieves corresponding PID_i from the repository, and verifies the equality for $PID_i{}^* ?= PID_i$. Then, it computes $M_3 = h(PID_i{}^* || Y_i|| N_{SD}{}^*)$ and verifies $M_3{}^* ?=M_3$. However, despite verifying these equations twice, the UC_j does not verify the freshness of SGD_i's message and proceeds to construct the message for SGD_i without proper verifying the authenticity of the sender.

Lacking mutual authentication

As we see earlier, if an attacker intercepts the messages on the public channel, then it may initiate a replay attack towards the UC_j by forwarding the authentication request. In this way, the attacker will be able to forge the UC_j successfully, since the latter, after being failed to recognize the attacker, will be forced to construct a response message as well as reserve its resources for creating session variables as well as the constructed session key for some time period. The attacker will not be able to compute the same session key, created by UC_j. Yet, it could force the UC_j to get the attacker's focus and reserving the resources for it, which may overburden the UC_j as discussed in the next attack.

Denial-of-service attack

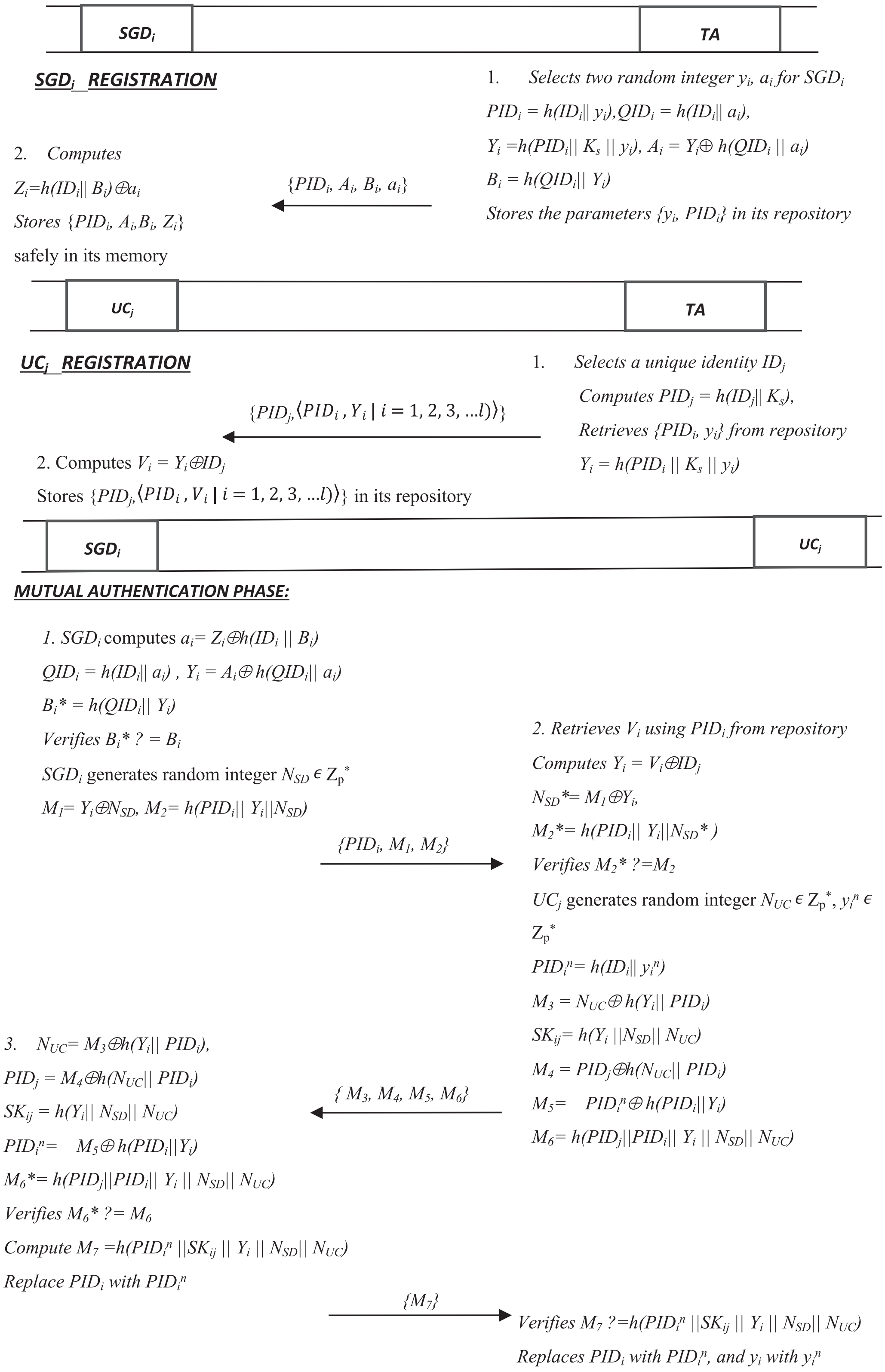
The UC_j device, after receiving the SGD_i authentication request, locates V_i corresponding to the SGD_i's device. However, the Yu et al. scheme does not identify any mechanism to locate a particular V_i from the repository. Since it takes much of the delay in finding an appropriate V_i parameter suitable to the SGD_i. Yu et al.'s scheme should have defined a type of pseudonym identity to search for a SGD_i-oriented V_i parameter from the repository. If an attacker initiates multiple fake authentication requests towards UC_j simultaneously, then the latter may not be able to handle those requests and will overburden the UC_j.

Technical defects in Yu et al.'s protocol

Yu et al.'s protocol bear some technical defects in its protocol that questions its practical implications. These defects are described below:

a) The SGD_i device is unable to extract R_{UC} from M_4, as sent by the UC_j towards SGD_i, and cannot compute a claimed session key $SK_{ij} = h(N_{SD}|| N_{UC})$. This is because, $N_{UC} = M_4 \oplus h(Y_i|| N_{UC})$ is wrongly constructed parameter, and needs revision.

b) The M_5 parameter is a useless parameter in the protocol and serves no purpose for SGD_i, since the recovered parameter $PID_j = M_5 \oplus N_{UC}$ is not utilized in any kind of confirmation. Hence the construction of protocol needs revision.


SGD_i
TA
$\underline{SGD_i}$ REGISTRATION

1. *Selects two random integer y_i, a_i for SGD_i*
$PID_i = h(ID_i \| y_i)$, $QID_i = h(ID_i \| a_i)$,
$Y_i = h(PID_i \| K_s \| y_i)$, $A_i = Y_i \oplus h(QID_i \| a_i)$
$B_i = h(QID_i \| Y_i)$
Stores the parameters $\{y_i, PID_i\}$ in its repository

$\{PID_i, A_i, B_i, a_i\}$ ←

2. *Computes*
$Z_i = h(ID_i \| B_i) \oplus a_i$
Stores $\{PID_i, A_i, B_i, Z_i\}$
safely in its memory

UC_j
TA
$\underline{UC_j}$ REGISTRATION

1. *Selects a unique identity ID_j*
Computes $PID_j = h(ID_j \| K_s)$,
Retrieves $\{PID_i, y_i\}$ from repository
$Y_i = h(PID_i \| K_s \| y_i)$

$\{PID_j, \langle PID_i, Y_i \mid i = 1, 2, 3, \ldots l \rangle\}$ ←

2. Computes $V_i = Y_i \oplus ID_j$
Stores $\{PID_j, \langle PID_i, V_i \mid i = 1, 2, 3, \ldots l \rangle\}$ in its repository

1. SGD_i computes *$a_i = Z_i \oplus h(ID_i \| B_i)$*
$QID_i = h(ID_i \| a_i)$, $Y_i = A_i \oplus h(QID_i \| a_i)$
$B_i^* = h(QID_i \| Y_i)$
Verifies $B_i^* ? = B_i$
SGD_i generates random integer $N_{SD} \in Z_p^*$
$M_1 = Y_i \oplus N_{SD}$, $M_2 = h(PID_i \| Y_i \| N_{SD})$

$\{PID_i, M_1, M_2\}$ →

2. Retrieves V_i using PID_i from repository
Computes $Y_i = V_i \oplus ID_j$
$N_{SD}^* = M_1 \oplus Y_i$,
$M_2^* = h(PID_i \| Y_i \| N_{SD}^*)$
Verifies $M_2^* ?= M_2$
UC_j generates random integer $N_{UC} \in Z_p^*$, $y_i^n \in Z_p^*$
$PID_i^n = h(ID_i \| y_i^n)$
$M_3 = N_{UC} \oplus h(Y_i \| PID_i)$
$SK_{ij} = h(Y_i \| N_{SD} \| N_{UC})$
$M_4 = PID_j \oplus h(N_{UC} \| PID_i)$
$M_5 = PID_i^n \oplus h(PID_i \| Y_i)$
$M_6 = h(PID_j \| PID_i \| Y_i \| N_{SD} \| N_{UC})$

$\{M_3, M_4, M_5, M_6\}$ ←

3. $N_{UC} = M_3 \oplus h(Y_i \| PID_i)$,
$PID_j = M_4 \oplus h(N_{UC} \| PID_i)$
$SK_{ij} = h(Y_i \| N_{SD} \| N_{UC})$
$PID_i^n = M_5 \oplus h(PID_i \| Y_i)$
$M_6^* = h(PID_j \| PID_i \| Y_i \| N_{SD} \| N_{UC})$
Verifies $M_6^* ?= M_6$
Compute $M_7 = h(PID_i^n \| SK_{ij} \| Y_i \| N_{SD} \| N_{UC})$
Replace PID_i with PID_i^n

$\{M_7\}$ →

Verifies $M_7 ?= h(PID_i^n \| SK_{ij} \| Y_i \| N_{SD} \| N_{UC})$
Replaces PID_i with PID_i^n, and y_i with y_i^n

Fig. 3. Proposed scheme.

Proposed model

The proposed model, an improvement of Yu et al.'s scheme which intends to secure the authenticated key agreement scheme for DR-management in the smart grid system network, comprises of four procedures, such as pre-deployment phase, SG device registration phase, UC registration phase, and mutual authentication phase.

Pre-deployment procedure

The pre-deployment phase of the proposed scheme is similar to Yu et al.'s phase. In this phase, the UC_j and smart grid devices SGD_i get registered with trust authority (TA) before being deployed in the smart grid environment. The TA, initially, chooses unique identities, i.e. ID_i and ID_j for SGD_i and UC_j, respectively. Then, TA saves the information of identities such as ID_i in SGD_i's memory, and ID_j in UC_j's memory before their deployment in the smart grid environment.

Registration phase of smart grid device

The SGD_i needs to register with a trusted third party TA for receiving the services of power management. Fig. 3 depicts the registration process for SGD_i devices of the proposed protocol. The involved steps of this phase are illustrated below.

1. The trusted authority TA selects two random integers y_i, a_i for SGD_i . Then, TA calculates $PID_i = h(ID_i|| y_i)$, $QID_i = h(ID_i|| a_i)$, $Y_i = h(PID_i || K_s || y_i)$, $A_i = Y_i \oplus h(QID_i || a_i)$, and $B_i = h(QID_i || Y_i)$. Then, it stores the parameters $\{y_i, PID_i\}$ in its secure repository, and submits $\{PID_i , A_i, B_i , a_i\}$ towards SGD_i.
2. After getting the message $\{A_i, B_i ,a_i\}$, the SGD_i calculates $Z_i = h(ID_i|| B_i) \oplus a_i$ and saves the parameters $\{PID_i, A_i, B_i , Z_i\}$ safely in its memory.

UC registration phase

The UC_j needs to get registered from TA for dispensing the services of power management. Fig. 3 depicts the UC_j registration procedure in our scheme. The salient steps of the registration phase are given as under.

1. The TA, initially selects a unique identity IDj, and calculates $PID_j = h(ID_j|| K_s)$, and retrieves $\{ PID_i, y_i\}$ from its repository. Then, it further calculates $Y_i = h(PID_i || K_s || y_i)$, and submits $\{PID_j, (PID_i \mid i = 1, 2, 3, ...l), Y_i\}$ towards UC_j, where l represent the number of smart grid devices.
2. The UC_j, after getting the message, further calculates $V_i = Y_i \oplus ID_j$ and saves$\{PID_j, (PID_i \mid i = 1, 2, 3, ...l), V_i\}$ safely in its repository.

Authentication phase

In the authentication procedure of the contributed model, the SGD_i or user is provided with the anonymity feature by employing pseudo-identities as well as short term secret parameters. Before initiating the session, the SGD_i submits an authentication request towards UC_j for protected communication, and construct an agreed session key SK_{ij}. Fig. 3 demonstrates the mutual authentication procedure of the contributed model. The main steps of this phase are illustrated below.

1. Initially, the SGD_i by employing the stored parameters, computes $a_i = Z_i \oplus h(ID_i || B_i)$, $QID_i = h(ID_i || a_i)$, $Y_i = A_i \oplus h(QID_i|| a_i)$, and $B_i^* = h(QID_i || Y_i)$. Then, it verifies the equality $B_i^* \ ? = B_i$. After successful verification, the SGD_i generates random integer $N_{SD} \in Z_p^*$ and computes $M_1 = Y_i \oplus N_{SD}$ and $M_2 = h(PID_i|| Y_i|| N_{SD})$. Next, it submits the message $\{PID_i, M_1, M_2\}$ to UC_j for verification.
2. The UC_j, upon receiving the message $\{PID_i, M_1, M_2\}$ retrieves V_i from repository using PID_i, and computes $Y_i = V_i \oplus ID_j$, $N_{SD}^* = M_1 \oplus X_i$. Next, it computes $M_2^*= h(PID_i^*|| Y_i|| N_{SD}^*)$ and verifies $M_2^* ?=M_2$. Next, it generates random integer $N_{UC} \in Z_p^*$ and $y_i^n \in Z_p^*$. Then, it computes $PID_i^n = h(ID_i|| y_i^n)$, $M_3 = N_{UC} \oplus h(Y_i|| PID_j)$, $SK_{ij} = h(Y_i || N_{SD}|| N_{UC})$, $M_4 = PID_j \oplus h(N_{UC}|| PID_i)$, $M_5 = PID_i^n \oplus h(PID_i ||Y_i)$, $M_6 = h(PID_j||PID_i || Y_i || N_{SD}|| N_{UC})$. Then, it forwards the message $\{M_3, M_4, M_5, M_6\}$ towards SGD_i.
3. Upon receiving the message, the SGD_i computes $N_{UC} = M_3 \oplus h(Y_i|| PID_j)$, $PID_j = M_4 \oplus h(N_{UC} || PID_i)$, $SK_{ij} = h(Y_i|| N_{SD}|| N_{UC})$, $PID_i^n = M_5 \oplus h(PID_i ||Y_i)$, $M_6^*= h(PID_j||PID_i || Y_i || N_{SD}|| N_{UC})$. Then, it verifies $M_6^* \ ?= M_6$ and authenticates the UC_j for successful verification. Next, it computes $M_7 = h(PID_i^n || SK_{ij} || Y_i || N_{SD}|| N_{UC})$ and submits the message $\{M_7\}$ towards UC_j. Finally, it replaces PID_i with PID_i^n and y_i with y_i^n in the repository.

Security analysis

This section describes the informal security analysis, formal analysis, and automated tool analysis for the proposed scheme.

Informal security analysis

This section illustrates the informal security analysis for the proposed protocol.

Resists replay attack

Unlike Yu et al., our scheme is resistant to a replay attack. An attacker may intercept the communication messages $\{PID_i , M_1\text{-}M_7\}$, and replay those messages in the future to the legal participants [34–37]. However, both participants authenticate one another on the basis of fresh random nonces N_{SD} and N_{UC} declared for each session. However, if the attacker replays the message $\{PID_i , M_1, M_2\}$ towards UC_j, the latter may annul the chances of replay attack in the third communication round message by verifying M_7. Similarly, the SGD_i may also eliminate the probability of a replay attack by verifying the equality $M_6^* \ ?= M_6$. Hence, our scheme is immune to a replay attack.

Impersonation attack

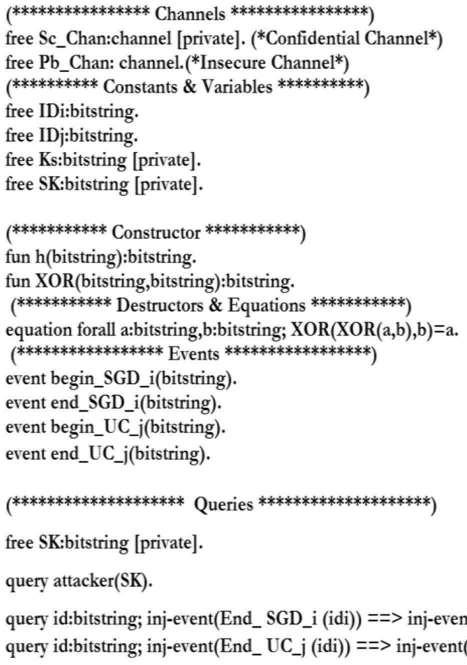
An attacker may attempt impersonation attack towards both ends, i.e. SGD_i and UC_j, however it might not be possible since an attacker needs access to PID_i and Y_i parameters for initiating this attack. Even if the attacker gets access to stolen device contents such as PID_i, yet it needs to compute SGD_i's identity, which is difficult to compute for a probabilistic polynomial time attacker [38,39]. For impersonating as a SGD_i, the attacker needs to construct valid $\{PID_i , M_1, M_2\}$, $\{ M_3, M_4, M_5, M_6\}$, and $\{M_7\}$ messages with a fresh nonce, i.e. N_{SD} and N_{UC}, which is not feasible without having access to PID_i and Y_i parameters. Hence, our scheme is protected from SGD_i and UC_j impersonation attacks.

Mutual authentication

Our scheme supports mutual authentication, since the established session key $SK_{ij} = h(Y_i|| N_{SD}|| N_{UC})$ can only be constructed by legitimate participants i.e. SGD_i and UC_j. The authentication request message $\{PID_i , M_1, M_2\}$ as submitted from SGD_i towards UC_j is verified in the second communication round after receiving $\{M_3, M_4, M_5, M_6\}$ from UC_j, where $M_1 = Y_i \oplus N_{SD}$, $M_2 = h(PID_i|| Y_i|| N_{SD})$, $M_3 = N_{UC} \oplus h(Y_i|| PID_i)$, $M_4 = PID_j \oplus h(N_{UC}|| PID_i)$, $M_5 = PID_i^n \oplus h(PID_i ||Y_i)$, $M_6 = h(PID_j|| PID_i || Y_i || N_{SD}|| N_{UC})$. Similarly, the message $\{M_3, M_4, M_5, M_6\}$ consists of the response as well as the challenge of UC_j which is verified in the third communication round message, i.e. $\{M_7\}$, where $M_7 = h(PID_i^n || SK_{ij} || Y_i || N_{SD}|| N_{UC})$. Hence, the proposed protocol affords mutual authentication to the legal participants.

Anonymity and untraceability

The proposed scheme preserves the privacy of the user or SGD_i . The attacker may not compute the identity ID_i from the stolen SGD_i's contents. The Yu et al. scheme does not provide any mechanism to restrict



```
(**************** Channels ****************)
free Sc_Chan:channel [private]. (*Confidential Channel*)
free Pb_Chan: channel.(*Insecure Channel*)
(********** Constants & Variables **********)
free IDi:bitstring.
free IDj:bitstring.
free Ks:bitstring [private].
free SK:bitstring [private].

(*********** Constructor ***********)
fun h(bitstring):bitstring.
fun XOR(bitstring,bitstring):bitstring.
 (*********** Destructors & Equations ***********)
equation forall a:bitstring,b:bitstring; XOR(XOR(a,b),b)=a.
 (***************** Events *****************)
event begin_SGD_i(bitstring).
event end_SGD_i(bitstring).
event begin_UC_j(bitstring).
event end_UC_j(bitstring).

(******************* Queries *******************)

free SK:bitstring [private].

query attacker(SK).

query id:bitstring; inj-event(End_ SGD_i (idi)) ==> inj-event(Begin_ SGD_i (idi)) .
query id:bitstring; inj-event(End_ UC_j (idi)) ==> inj-event(Begin_ UC_j (idi)) .
```

Fig. 4. Code initialization.

the traceability of the user [40,50], since the user needs to submit a parameter using which the UC_j may find V_i parameter. The proposed scheme provides a suitable mechanism for synchronization and preventing the traceability of the user by renewing PID_i parameter for each session. Hence, our scheme provides anonymity as well as untraceability to the SGD_i.

Insider attack

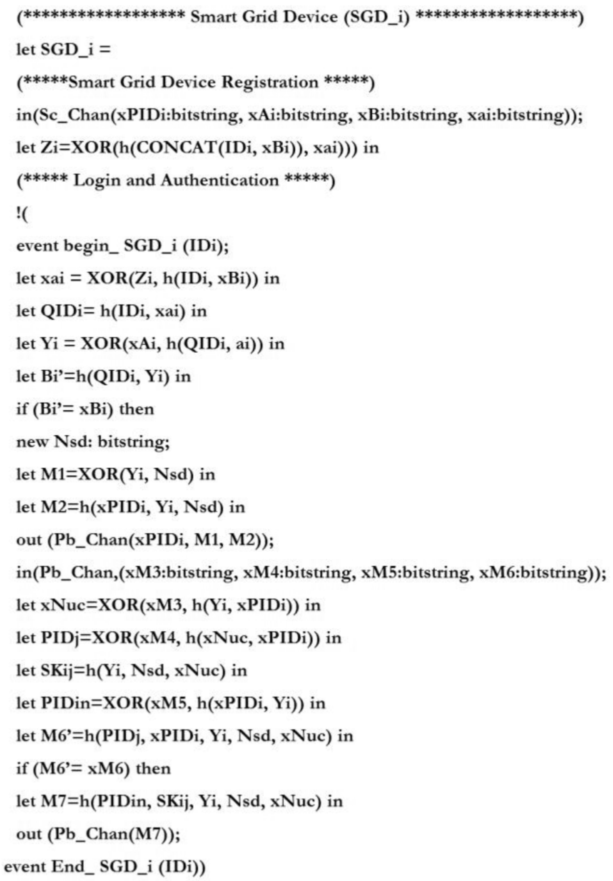
The privileged insider might happen when the managing administrator of utility center UC_j misuses the data stored in the repository for forgery or impersonating on behalf of the smart grid devices. If we assume that the malicious inside attacker $\mathscr{A}$ gets the information contents such as PID_i, V_i as stored in the repository of UC_j, the attacker might not be able to access other critical parameters such as the user's original identity ID_i and Y_i without knowing the random variable N_{SD} as well as ID_j. Hence, our scheme is protected from any kind of malicious insider attack.

Denial-of-service threat

In a contributed scheme, the UC_j may instantly locate V_i based on PID_i from its verifiers' repository [41,42,53–54]. This parameter gets refreshed in the form of PID_i^n by both the involved participants at the end of every session. The Yu et al. scheme was unable to define any mechanism on the part of UC_j for finding V_i corresponding to each individual user, which might take more delay for the server to locate from the repository, and in return, this may affect the server's availability or overburden it with too many pending requests. Hence, our scheme is safe from the denial of service attack.

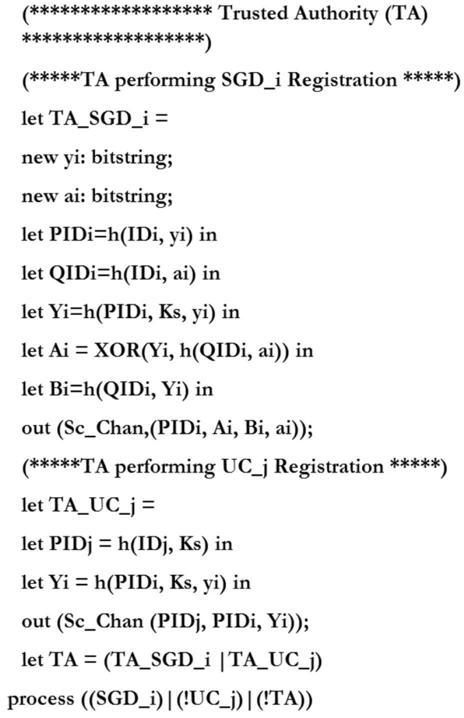
Stolen SG device attack

If an attacker gets access to stolen device SGD_i's contents such as $\{PID_i, A_i, B_i, Z_i\}$, still it will not be able to compute the identity of the user or device. This inability to determine the identity renders it unable to compute Y_i for constructing the legitimate messages. This makes the attacker incapable of login into the device successfully, and hence it may not initiate the SGD_i impersonation attack towards UC_j. Thus, our scheme is resistant to stolen SGD_i device attacks.



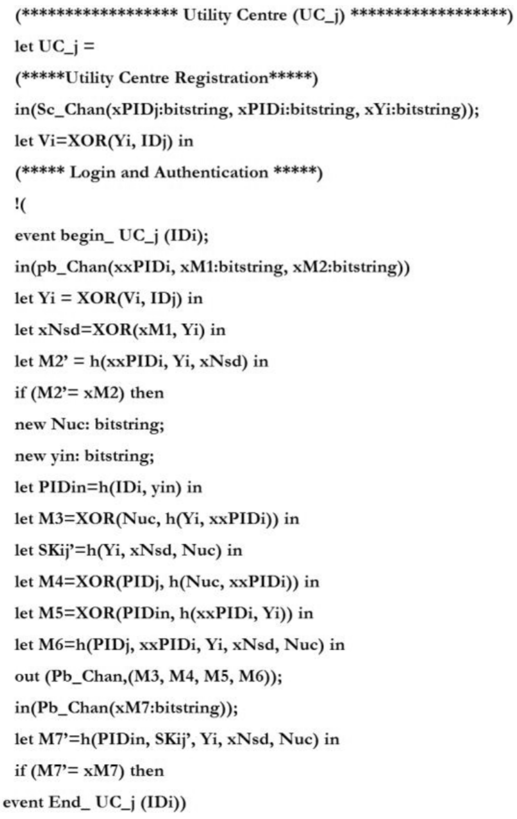
```
(****************** Smart Grid Device (SGD_i) ******************)
let SGD_i =
(*****Smart Grid Device Registration *****)
in(Sc_Chan(xPIDi:bitstring, xAi:bitstring, xBi:bitstring, xai:bitstring));
let Zi=XOR(h(CONCAT(IDi, xBi)), xai))) in
(***** Login and Authentication *****)
!(
event begin_ SGD_i (IDi);
let xai = XOR(Zi, h(IDi, xBi)) in
let QIDi= h(IDi, xai) in
let Yi = XOR(xAi, h(QIDi, ai)) in
let Bi'=h(QIDi, Yi) in
if (Bi'= xBi) then
new Nsd: bitstring;
let M1=XOR(Yi, Nsd) in
let M2=h(xPIDi, Yi, Nsd) in
out (Pb_Chan(xPIDi, M1, M2));
in(Pb_Chan,(xM3:bitstring, xM4:bitstring, xM5:bitstring, xM6:bitstring));
let xNuc=XOR(xM3, h(Yi, xPIDi)) in
let PIDj=XOR(xM4, h(xNuc, xPIDi)) in
let SKij=h(Yi, Nsd, xNuc) in
let PIDin=XOR(xM5, h(xPIDi, Yi)) in
let M6'=h(PIDj, xPIDi, Yi, Nsd, xNuc) in
if (M6'= xM6) then
let M7=h(PIDin, SKij, Yi, Nsd, xNuc) in
 out (Pb_Chan(M7));
event End_ SGD_i (IDi))
```

Fig. 5. Smart Grid Device ProVerif code.



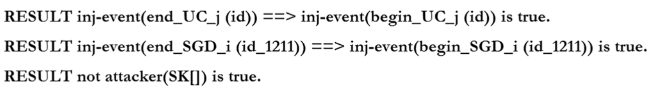
```
(****************** Trusted Authority (TA)
******************)
(*****TA performing SGD_i Registration *****)
let TA_SGD_i =
new yi: bitstring;
new ai: bitstring;
let PIDi=h(IDi, yi) in
let QIDi=h(IDi, ai) in
let Yi=h(PIDi, Ks, yi) in
let Ai = XOR(Yi, h(QIDi, ai)) in
let Bi=h(QIDi, Yi) in
out (Sc_Chan,(PIDi, Ai, Bi, ai));
(*****TA performing UC_j Registration *****)
let TA_UC_j =
let PIDj = h(IDj, Ks) in
let Yi = h(PIDi, Ks, yi) in
out (Sc_Chan (PIDj, PIDi, Yi));
let TA = (TA_SGD_i | TA_UC_j)
process ((SGD_i) | (!UC_j) | (!TA))
```

Fig. 6. Trusted Authority ProVerif code.



```
(***************** Utility Centre (UC_j) *****************)
let UC_j =
(*****Utility Centre Registration*****)
in(Sc_Chan(xPIDj:bitstring, xPIDi:bitstring, xYi:bitstring));
let Vi=XOR(Yi, IDj) in
(***** Login and Authentication *****)
!(
event begin_ UC_j (IDi);
in(pb_Chan(xxPIDi, xM1:bitstring, xM2:bitstring))
let Yi = XOR(Vi, IDj) in
let xNsd=XOR(xM1, Yi) in
let M2' = h(xxPIDi, Yi, xNsd) in
if (M2'= xM2) then
new Nuc: bitstring;
new yin: bitstring;
let PIDin=h(IDi, yin) in
let M3=XOR(Nuc, h(Yi, xxPIDi)) in
let SKij'=h(Yi, xNsd, Nuc) in
let M4=XOR(PIDj, h(Nuc, xxPIDi)) in
let M5=XOR(PIDin, h(xxPIDi, Yi)) in
let M6=h(PIDj, xxPIDi, Yi, xNsd, Nuc) in
out (Pb_Chan,(M3, M4, M5, M6));
in(Pb_Chan(xM7:bitstring));
let M7'=h(PIDin, SKij', Yi, xNsd, Nuc) in
if (M7'= xM7) then
event End_ UC_j (IDi))
```

Fig. 7. Utility Centre ProVerif code.



```
RESULT inj-event(end_UC_j (id)) ==> inj-event(begin_UC_j (id)) is true.
RESULT inj-event(end_SGD_i (id_1211)) ==> inj-event(begin_SGD_i (id_1211)) is true.
RESULT not attacker(SK[]) is true.
```

Fig. 8. Simulation results.

Threat of session key's disclosure

In the contributed protocol, the attacker will not be able to compute a valid session key. This is because the attacker may not calculate the genuine authentication request *{PID$_i$, M$_1$, M$_2$}* if it is either ignorant of the long term secret, i.e. Y_i or short-term session specific temporary secret or random nonces such as N_{SD} or N_{UC}. Both of these, long term as well short term secrets need to be compromised by the attacker for computing a valid session key $SK_{ij} = h(Y_i || N_{SD} || N_{UC})$. Hence, our scheme is immune to session key disclosure attacks.

Security analysis employing proverif tool

This section proves the authentication properties besides the secrecy of the session key by employing a formal verification tool, i.e. ProVerif [43,44]. This tool is designed on the principles

various constants, channels, equations, functions, queries, and secret keys as shown in Fig. 4. We define two channels, i.e. *Sc_chan* as secret channel and *Pb_chan* as a public channel for communicating private and public messages, respectively.

The session key secrecy and other authentication features of the contributed protocol are modeled by employing the queries and events, where SK_{ij} and SK_{ij}*'* represent the sessions computed by SGD_i and UC_j, respectively. The codes for SGD, UC and TA are shown in Fig. 5, Fig. 6 and Fig. 7, respectively.

The provided results in the first two lines of Fig. 8 show that the involved processes launched and concluded successfully. In this regard, the result in the third line of Fig. 8 illustrates that the attacker query may not reveal the session key SK as established between the procedures in the mutual authentication phase.

Security analysis using BAN logic

This sub-section presents the formal security analysis of the contributed scheme under Burrows-Abadi-Needham logic (BAN) logic [45–48,51], which ensures the security properties based on mutual authenticity among participants, key distribution between the members, and demonstrates the resistance of protocol against the disclosure of session key. We used a few symbols to elaborate on this analysis as given below.

$\boldsymbol{\Omega} \mid\equiv \boldsymbol{\delta}$: The principal **Ω** believes **δ**.

$\boldsymbol{\Omega} \lhd \boldsymbol{\delta}$: **Ω** sees **δ**.

$\boldsymbol{\Omega} \mid\sim \boldsymbol{\delta}$: **Ω** once said **δ**.

$\boldsymbol{\Omega} \mid\Rightarrow \boldsymbol{\delta}$: **Ω** has jurisdiction over **δ**.

$\#(\boldsymbol{\delta})$: The message **δ** is fresh.

$(\boldsymbol{\delta}, \boldsymbol{\delta}')$: **δ'** or **δ** are the fractions of the message **(δ, δ')**.

$\langle\boldsymbol{\delta}\rangle_{\delta'}$: The formulae **δ** is combined with formulae **δ'**.

$(\boldsymbol{\delta}, \boldsymbol{\delta}')_{K}$: **δ** or **δ'** is hashed with the key K.

$\boldsymbol{\Omega} \leftrightarrow^{K} \boldsymbol{\Omega}'$: **Ω** and **Ω'** can interact with the shared key K.

Some rules that are utilized in this analysis are given below:

R1. Message meaning rule:$\frac{\Omega|\equiv\Omega \leftrightarrow^{K}\Omega', \quad \Omega\lhd\delta_{\delta'}}{\Omega|\equiv\Omega' |\sim \delta}$

R2. Nonce verification rule:$\frac{\Omega|\equiv\#(\delta),\Omega|\equiv\Omega'|\ \delta}{\Omega|\equiv\Omega'|\equiv\delta}$

R3. Jurisdiction rule:$\frac{\Omega|\equiv\Omega'\Rightarrow\delta,\Omega|\equiv\Omega'|\equiv\delta}{\Omega|\equiv\delta}$

R4. Freshness conjuncatenation rule:$\frac{\Omega|\equiv\#(\delta)}{\Omega|\equiv\#(\delta,\delta')}$

R5. Belief rule: $\frac{\Omega|\equiv(\delta),\Omega|\equiv(\delta')}{\Omega|\equiv(\delta,\delta')}$

R6. Session keys rule:$\frac{\Omega|\equiv\#(\delta),\Omega|\equiv\Omega'|\equiv\delta}{\Omega|\equiv\Omega \leftrightarrow^{K}\Omega'}$

Our protocol must fulfill the under-mentioned goals for achieving the objectives of this proof.

Goal1 **:**$UC_j \mid\equiv UC_j \leftrightarrow^{SK} SGD_i$

Goal2 **:**$UC_j \mid\equiv \mathrm{Ui} \mid\equiv UC_j \leftrightarrow^{SK} SGD_i$

Goal3 **:**$SGD_i \mid\equiv UC_j \leftrightarrow^{SK} SGD_i$

Goal4 **:**$SGD_i \mid\equiv UC_j \mid\equiv UC_j \leftrightarrow^{SK} SGD_i$

Primarily, we transform the communication messages in the following idealized forms.

M$_1$: $SGD_i \rightarrow UC_j$: PID_i , M_1, M_2: $\{PID_i, \langle N_{SD}\rangle_{Yi}, (PID_i, N_{SD})_{Yi}\}$

M$_2$: $UC_j \rightarrow SGD_i$:M_3, M_4, M_5, M_6: $\{\langle N_{UC}\rangle_{h(Yi,\ PIDi)}, \langle PID_j\rangle_{h(NUC,\ PIDi)}, \langle PID_i^{n}\rangle_{h(PIDi,\ Yi)},$

$\mathbf{(PID_i, PID_i, N_{SD}, N_{UC})_{Yi}\}}$

M$_3$: $SGD_i \rightarrow UC_j$:M_7: $\{(PID_i^{n}, SK_{ij}, N_{SD}, N_{UC})_{Yi}\}$

Now, we establish the following assumptions for proving our goals in this study.

A1 :$SGD_i \mid\equiv \sharp N_{SD}$

A2 :$UC_j \mid\equiv \sharp N_{UC}$

A3 :$SGD_i \mid\equiv UC_j \leftrightarrow^{SK_{ij}} SGD_i$

A4 :$UC_j \mid\equiv UC_j \leftrightarrow^{SK_{ij}} SGD_i$

A5 :$SGD_i \mid\equiv UC_j \mid\Rightarrow (Y_i, PID_j)$

A6 :$UC_j \mid\equiv SGD_i \mid\Rightarrow (Y_i, PID_i)$

Thereafter, the idealized forms such as M_1, M_2 and M_3 of our scheme are evaluated in consideration with the above mentioned assumptions and rules [45–47,52].

By taking into consideration the first and third messages of the established idealized forms:

M$_1$: $SGD_i \rightarrow UC_j$: PID_i , M_1, M_2: $\{PID_i, \langle N_{SD}\rangle_{Yi}, (PID_i, N_{SD})_{Yi}\}$

M$_3$: $SGD_i \rightarrow UC_j$:M_7: $\{(PID_i^{n}, SK_{ij}, N_{SD}, N_{UC})_{Yi}\}$

Using the seeing rule, we have,

S1: $UC_j \lhd PID_i$, M_1, M_2: $\{PID_i, \langle N_{SD}\rangle_{Yi}, (PID_i, N_{SD})_{Yi}\}$

S2: $UC_j \lhd M_7$: $\{(PID_i^{n}, SK_{ij}, N_{SD}, N_{UC})_{Yi}\}$

Next, using S1, S2, A3, and *R1*, we have

Table 3
Functionality Comparison.

	Wu-Zhou [49]	Odelu et al. [25]	Tsai-Lo [26]	Kumar et al. [9]	Yu et al. [10]	Ours
Resistance from Impersonation attack	●	●	●	×	●	●
Resistance from Replay threat	●	●	●	●	×	●
Immune to Stolen smart grid device threat	●	●	●	×	●	●
Immune to Session key exposure threat	×	×	●	×	●	●
Resistance from Man-in-the-middle threat	●	●	●	●	●	●
Supports Anonymity	×	●	●	●	×	●
Supports Mutual authentication	●	●	●	×	×	●
Supports Untraceability	×	●	●	×	×	●
Immune to Denial-of-service attack	×	●	●	●	×	●
Use of lightweight crypto-primitives	×	×	×	×	●	●

●: Security property is satisfied; ×: Security property NOT satisfied

S3: $UC_j \mid\equiv SGD_i \sim \{PID_i, \langle N_{SD}\rangle_{Yi}, (PID_i, N_{SD})_{Yi}\}$
S4: $UC_j \mid\equiv SGD_i \sim \{(PID_i^n, SK_{ij}, N_{SD}, N_{UC})_{Yi}\}$
Then, using A1, S3, S4, R4, and R2, we get
S5: $UC_j \mid\equiv SGD_i \mid\equiv \{PID_i, \langle N_{SD}\rangle_{Yi}, (PID_i, N_{SD})_{Yi}\}$
S6: $UC_j \mid\equiv SGD_i \mid\equiv \{(PID_i^n, SK_{ij}, N_{SD}, N_{UC})_{Yi}\}$

While, (N_{SD}, N_{UC}) are the crucial factors for mutual authenticity and establishing the session key.

Now, using A6, S5, S6, and R3, we have
S7: $UC_j \mid\equiv \{PID_i, \langle N_{SD}\rangle_{Yi}, (PID_i, N_{SD})_{Yi}\}$
S8: $UC_j \mid\equiv \{(PID_i^n, SK_{ij}, N_{SD}, N_{UC})_{Yi}\}$
Using A3, S7, S8, and R6, we have
S9: $UC_j \mid\equiv SGD_i \mid\equiv UC_j \leftrightarrow^{SK} SGD_i$ **(Goal 2)**
Apply A6, S9, and R3, we get
S10: $UC_j \mid\equiv UC_j \leftrightarrow^{SK} SGD_i$ **(Goal 1)**
In view of the second idealized form:
M_2: $UC_j \rightarrow SGD_i$: M_3, M_4, M_5, M_6: $\{\langle N_{UC}\rangle_{h(Yi,\ PIDi)}, \langle PID_j\rangle_{h(NUC,\ PIDi)}, \langle PID_i^n\rangle_{h(PIDi,\ Yi)}, (PID_i, PID_i, N_{SD}, N_{UC})_{Yi}\}$
Using seeing rule, we have
S11: $SGD_i \triangleleft UC_j \rightarrow SGD_i$:$\{\langle N_{UC}\rangle_{h(Yi,\ PIDi)}, \langle PID_j\rangle_{h(NUC,\ PIDi)}, \langle PID_i^n\rangle_{h(PIDi,\ Yi)}, (PID_i, PID_i, N_{SD}, N_{UC})_{Yi}\}$
Using S11, A4, and R1, we get
S12: $SGD_i \mid\equiv UC_j \sim \{\langle N_{UC}\rangle_{h(Yi,\ PIDi)}, \langle PID_j\rangle_{h(NUC,\ PIDi)}, \langle PID_i^n\rangle_{h(PIDi,\ Yi)}, (PID_i, PID_i, N_{SD}, N_{UC})_{Yi}\}$
Now using A2, S12, R4, and R2 we have,
S13: $SGD_i \mid\equiv UC_j \mid\equiv \{\langle N_{UC}\rangle_{h(Yi,\ PIDi)}, \langle PID_j\rangle_{h(NUC,\ PIDi)}, \langle PID_i^n\rangle_{h(PIDi,\ Yi)}, (PID_i, PID_i, N_{SD}, N_{UC})_{Yi}\}$

Where, (N_{SD}, N_{UC}) is the critical factor used mutual authenticity and establishing the session key.

Applying A5, S13, and R3, we get
S14: $SGD_i \mid\equiv \{\langle N_{UC}\rangle_{h(Yi,\ PIDi)}, \langle PID_j\rangle_{h(NUC,\ PIDi)}, \langle PID_i^n\rangle_{h(PIDi,\ Yi)}, (PID_i, PID_i, N_{SD}, N_{UC})_{Yi}\}$
Using A4, S14, and R6, we have
S15: $SGD_i \mid\equiv UC_j \mid\equiv UC_j \leftrightarrow^{SK} SGD_i$ **(Goal 4)**
Now, considering A5, S15, and R3
S16: $SGD_i \mid\equiv UC_j \leftrightarrow^{SK} SGD_i$ **(Goal 3)**

The illustrated BAN logic analysis proves the mutual authenticity on formal lines and validates that the contributed scheme establishes a mutually agreed session key SK between SGD_i and UC_j.

Table 4
Computational cost of comparative schemes.

Schemes	Computational cost (ms)
Wu-Zhou [49]	$7T_{em} + 1T_m + 5T_h + 1\ T_{sym} + 1T_{cer\_v} \approx 528.9\ ms$
Odelu et al.[25]	$7T_{em} + 2T_e + 2\ T_b + 10T_h \approx 635.8\ ms$
Tsai -Lo [26]	$5T_{em} + 2T_e + 2\ T_b + 12T_h \approx 505.7\ ms$
Kumar et al.[9]	$12T_h + 4T_{em} \approx 268.4\ ms$
Yu et al. [10]	$16T_h \approx 11.05\ ms$
Ours	$18T_h \approx 12.43\ ms$

Table 5
Communication overhead.

Schemes	Communicational delay	Communication messages
Wu-Zhou [49]	3648 bits	4
Odelu et al. [25]	1408 bits	3
Tsai -Lo [26]	1920 bits	3
Kumar et al. [9]	1376 bits	3
Yu et al. [10]	960 bits	2
Ours	1280	3

Performance evaluation

This section evaluates the computational efficiencies and security strength of contributed models with other contemporary schemes [9,26,25,49]. In this sub-section, we calculate and evaluate the computational delay of the contributed protocol against comparative schemes [9,25–26,49]. We assume the same benchmark parameters of Yu et al.'s protocol [10] in this study to evaluate and compare the results of existing schemes with the proposed protocol. The protocols constitute several cryptographic operations bearing different time delays for each operation [55]. The time delays for various cryptographic operations are T_{cer_v}, T_{cer}, T_{ea}, T_{em}, T_{bp}, T_{sym}, T_{ex}, T_h, T_m, and denote the verification time of public key certificate, generation time of public key certificate, time for ECC point addition, time for ECC multiplication, bilinear pairing time, time for symmetric encryption or decryption, modular exponentiation time, time for one-way digest hash function, and multiplication time, respectively. The execution times of various cryptographic operations as defined above can be depicted in the estimated equivalency such as $\{T_m \approx T_e, T_{sym} \approx T_h \approx T_{ea}\}$, where $\{T_{ea} \ll T_e\}$. Our scheme depicts an enhanced performance regarding security, communication and computation in comparison with previous schemes [9–10,25–26,49] including Yu et al. According to the Yu et al., the execution delay of various cryptographic operations such as T_h, T_e, T_{em}, T_{bp} is given as $<$ 0.01 ms, $<$1ms, 1.17 ms, 3.16 ms for Pentium IV, and 0.001 s, 0.1 s, 0.13 s, and 0.38 s for HiPerSmart Card, respectively. In the mutual authentication phase, the computational cost of the contributed scheme and Yu et al. is 18 T_h and 16 T_h, respectively. As evident from Table 3, in previous schemes, [10,26,49] are unable to provide resistance against session key exposure attack. The schemes [9,10,49] fail to prevent traceability for the user or smart grid device. Similarly, [9,10] scheme does not support mutual authentication to the participants. Yu et al. scheme are found to be vulnerable to replay and denial of service attacks. The schemes [9,25–26,49] do not employ lightweight cryptographic operations, leading to the increased computational cost of protocols. Table 4 presents the computation cost comparison of our and previous schemes [9,10,25,26,49].

For communication purpose, the exchanged communication parameters such as timestamp, random integer, ECC-based point, hash digest, and identity takes 32, 160, 160, 160, and 320-bits, respectively. In the contributed scheme the authentication request message, i.e. $\{PID_i, M_1, M_2\}$, $\{M_3, M_4, M_5, M_6\}$, $\{M_7\}$ take 480 bits, 640 bits, and 160 bits, respectively. Although, the communication cost is a bit more than Yu et al., yet our protocol is far more efficient than other protocols [10,25–26,49], since the total communication overhead of our scheme is

Table 6
Storage Overhead.

Schemes	Stored message (SGD_i)	Stored message (UC_j)
Wu-Zhou [49]	–	–
Odelu et al. [25]	$K_i = 40$ *bytes*	$K_j \approx 40$ *bytes*
Tsai -Lo [26]	s_i, $R_i = 80$ *bytes*	k_j, $K_j \approx 80$ *bytes*
Kumar et al. [9]	RID_i, $TC_i = 40$ *bytes*	RID_j, $TC_j \approx 40$ *bytes*
Yu et al. [10]	PID_i, A_i, B_i, $Z_i = 80$ *bytes*	RID_i, RID_j, $Y_i = 80$ *bytes*
Ours	PID_i, A_i, B_i, $Z_i = 80$ *bytes*	RID_i, RID_j, $Y_i = 80$ *bytes*

quite lower as compared to previous schemes, except Yu et al. Table 5 depicts the communication overhead of previous schemes as well as proposed scheme. There is a tradeoff between computational or communication cost and security strength. Despite this, our scheme has a little more communication overhead; it is more secure as compared to previous protocols. The storage cost of computed cryptographic factors such as hash, identity, random integer, and public key cryptosystem-based primitives are assumed to be 4, 20, 20, and 40 bytes, respectively. Accordingly, in our scheme, the contents stored in smart cards, i. e. $\{PID_i, A_i, B_i, Z_i\}$ require $(20 + 20 + 20 + 20) = 80$ bytes, while the parameters stored in the memory of UC_j such as $\{PID_j, PID_i, Y_i\}$ require $(20 + 20 + 20) = 60$ bytes. Although, the stored parameters cost in the memory of involved entities takes a bit higher cost in the proposed scheme as compared to Yu et al. and other schemes, yet our scheme is lightweight and provably secure than previous schemes. We emphasize that in an authenticated key agreement protocol, security is at least as significant as performance efficiency, and therefore it is not advisable to drastically reduce security to enhance marginal efficiency. Hence, the increased security in the proposed scheme justifies a little more computational or storage cost in comparison with other schemes. Table 6 depicts the storage overhead comparison for the compared schemes.

Conclusion

This scheme demonstrated that Yu et al.'s protocol, a recently presented authentication protocol for a smart grid environment, stands susceptible to replay threat, denial of service threat, and technical defects in the protocol. We also prove that the Yu et al. protocol lacks mutual authentication between the smart grid device and utility center. To counter the security limitations along with other defects in Yu et al., we design a lightweight, secure, and privacy-preserving authenticated key agreement scheme for demand-response management in smart grid systems. The contributed scheme may prevent known threats such as replay threat, forgery threat, stolen device threat, and denial of service attacks. Also, the scheme supports mutual authentication, anonymity, untraceability. We employed ProVerif and BAN logic analysis to verify and validate the achieved results, which further substantiate the scheme objectives and goals reinforcing its high practical implications. In the future, we shall work on the performance efficiencies for scalability issues in relation to repository maintained on the end of utility centre.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Park YH, Park YH. Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks. Sensors 2016;16:2123.

[2] Braeken A, Kumar P, Martin A. Efficient and Privacy-Preserving Data Aggregation and Dynamic Billing in Smart Grid Metering Networks. Energies 2018;11:2085.

[3] Tonyali S, Akkaya K, Saputro N, Uluagac AS, Nojoumian M. Privacy–preserving protocols for secure and reliable data aggregation in IoT–enabled Smart Metering systems. Future Gener Comput Syst 2018;78:547–57.

[4] Irshad A, Usman M, Chaudhry SA, Naqvi H, Shafiq M. A Provably Secure and Efficient Authenticated Key Agreement Scheme for Energy Internet-Based Vehicle-to-Grid Technology Framework. IEEE Trans Ind Appl 2020;56(4):4425–35.

[5] Kumar P, Gurtov A, Sain M, Martin A, Ha PH. Lightweight authentication and key agreement for smart metering in smart energy networks. IEEE Trans Smart Grid 2019;10(4):4349–59.

[6] Department of Energy. Exploring the Imperative of Revitalizing America's Electric Infrastructure. February 2017. Available online: https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages.pdf.

[7] Gope P, Amin R, Hafizul Islam SK, Kumar N, Bhalla VK. Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. Future Generat Comput Syst 2018;83:629–37.

[8] Mahmood K, Ashraf Chaudhry S, Naqvi H, Shon T, Farooq Ahmad H. A lightweight message authentication scheme for Smart Grid communications in power sector. Comput Electr Eng 2016;52:114–24.

[9] Kumar N, Aujla GS, Das AK, Conti M. ECCAuth: Secure authentication protocol for demand response management in smart grid systems. IEEE Trans Ind Inform 2019;15:6572–82.

[10] Yu SungJin, Park KiSung, Lee JoonYoung, Park YoungHo, Park YoHan, Lee SangWoo, et al. Privacy-Preserving Lightweight Authentication Protocol for Demand Response Management in Smart Grid Environment. Appl Sci 2020;10(5):1758. https://doi.org/10.3390/app10051758.

[11] Dolev D, Yao A. On the security of public key protocols. IEEE Trans Inf Theory 1983;29(2):198–208.

[12] Desai S, Alhadad R, Chilamkurti N, Mahmood A. A survey of privacy preserving schemes in IoE enabled smart grid advanced metering infrastructure. Clust Comput 2019;22(1):43–69.

[13] Lee JY, Yu SJ, Park KS, Park YH, Park YH. Secure three-factor authentication protocol for multi-gateway IoT environments. Sensors 2019;19:2358.

[14] Chaudhry SA, Shon T, Al-Turjman F, Alsharif MH. Correcting design flaws: An improved and cloud assisted key agreement scheme in cyber physical systems. Comput Commun 2020;153:527–37.

[15] Abdalla, M., Fouque, P. A., Pointcheval, D. Password based authenticated key exchange in the three-party setting. In Proceedings of the 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, 23–26 January 2005, 65–84.

[16] Yu SJ, Park KS, Park YH. A secure lightweight three–factor authentication scheme for IoT in cloud computing environment. Sensors 2019;19:3598.

[17] Kocher, P., Jaffe, J., Jun, B. Differential power analysis. In Advances in Cryptology—CRYPTO; Lecture Notes in Computer Science; Springer: Santa Barbara, CA, USA, 1999; pp. 388–397.

[18] Messerges TS, Dabbish EA, Sloan RH. Examining smart-card security under the threat of power analysis attacks. IEEE Trans Comput 2002;51(5):541–52.

[19] Mohammadali A, Sayad Haghighi M, Tadayon MH, Mohammadi-Nodooshan A. A Novel Identity-Based Key Establishment Method for Advanced Metering Infrastructure in Smart Grid. IEEE Trans Smart Grid 2018;9(4):2834–42.

[20] Rottondi C, Fontana S, Verticale G. Enabling privacy in vehicle-to-grid interactions for battery recharging. Energies 2014;7(5):2780–98.

[21] Wan Z, Zhu W-T, Wang G. PRAC: Efficient privacy protection for vehicle-to-grid communications in the smart grid. Comput Securit 2016;62:246–56.

[22] Jiang Qi, Khan MK, Lu X, Ma J, He D. A privacy preserving three–factor authentication protocol for e-Health clouds. J Supercomput 2016;72(10):3826–49.

[23] Mahmood K, Chaudhry SA, Naqvi H, Kumari S, Li X, Sangaiahm AK. An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. Future Gener Comput Syst 2018;81:557–65.

[24] Jo HJ, Kim IS, Lee DH. Efficient and privacy-preserving metering protocols for smart grid systems. IEEE Trans Smart Grid 2016;7(3):1732–42.

[25] Odelu V, Das AK, Wazid M, Conti M. Provably secure authenticated key agreement scheme for smart grid. IEEE Trans Smart Grid 2016;9:1900–10.

[26] Tsai JL, Lo NW. Secure anonymous key distribution scheme for smart grid. IEEE Trans Smart Grid 2016;7:906–14.

[27] Mahmood K, Arshad J, Chaudhry SA, Kumari S. An Enhanced Anonymous Identity-based Key Agreement Protocol for Smart Grid Advanced Metering Infrastructure. Int J Commun Syst 2019;32(16):e4137. https://doi.org/10.1002/dac.4137.

[28] Jiang Qi, Chen Z, Ma J, Ma X, Shen J, Wu D. Optimized Fuzzy Commitment based Key Agreement Protocol for Wireless Body Area Network. IEEE Trans Emerging Top Comput 2021;9(2):839–53. https://doi.org/10.1109/TETC.624551610.1109/TETC.2019.2949137.

[29] Saxena N, Choi BJ, Lu R. Authentication and authorization scheme for various user roles and devices in smart grid. IEEE Trans Inf Forensics Secur 2016;11(5):907–21.

[30] He D, Wang H, Khan MK, Wang L. Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography. IET Commun 2016;10:1795–802.

[31] Wazid M, Das AK, Kumar N, Rodrigues JPC. Secure three-factor user authentication scheme for renewable energy based smart grid environment. IEEE Trans Ind Inform 2017;13:3144–53.

[32] Weaver, K. A Perspective on How Smart Meters Invade Individual Privacy. 2014. Available online: https://skyvisionsolutions.files.wordpress.com/2014/08/utility-smart-meters-invade-privacy-22-aug-2014.pdf (accessed on 28 March 2020).

[33] Finster S, Baumgart I. Privacy-aware smart metering: A survey. IEEE Commun Surv Tutor 2015;17(2):1088–101.

[34] Wang D, Li W, Wang P. Measuring Two-Factor Authentication Schemes for Real-Time Data Access in Industrial Wireless Sensor Networks. IEEE Trans Ind Inf 2018;14(9):4081–92.

[35] Wang D, Cheng H, Wang P, Huang X, Jian G. Zipf's Law in Passwords. IEEE Trans Inf Forensics Secur 2017;12(11):2776–91.

[36] Li X, Ma J, Wang W, Xiong Y, Zhang J. A novel smart card and dynamic ID based remote user authentication scheme for multi-server environment. Math Comput Modell 2013;58(1–2):85–95.

[37] Li X, Niu J, Khurram Khan M, Liao J. An enhanced smart card based remote user password authentication scheme. J Network Comput Appl 2013;36(5):1365–71.

[38] Li X, Xiong Y, Ma J, Wang W. An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards. J Network Comput Appl 2012;35(2):763–9.

[39] Li X, Niu J, Ma J, Wang W, Liu C. Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart card. J Network Comput Appl 2011;34(1):73–9.

[40] Hussain S, Chaudhry SA. Comments on "Biometrics-Based Privacy-Preserving User Authentication Scheme for Cloud-Based Industrial Internet of Things Deployment". IEEE Internet Things J 2019;6(6):10936–40.

[41] Jiang Qi, Ma J, Yang C, Ma X, Shen J, Chaudhry SA. Efficient end-to-end authentication protocol for wearable health monitoring systems. Comput Electr Eng 2017;63:182–95.

[42] Mansoor K, Ghani A, Chaudhry S, Shamshirband S, Ghayyur S, Mosavi A. Securing IoT Based RFID Systems: A Robust Authentication Protocol Using Symmetric Cryptography. Sensors 2019;19(21):4752. https://doi.org/10.3390/s19214752.

[43] Ghani A, Mansoor K, Mehmood S, Chaudhry SA, Rahman AU, Najmus Saqib M. Security and Key Management in IoT Based Wireless Sensor Networks: An Authentication protocol using Symmetric Key. Int J Commun Syst 2019;32(16): e4139. https://doi.org/10.1002/dac.v32.1610.1002/dac.4139.

[44] Blanchet, B. (2005). Proverif automatic cryptographic protocol verifier user manual. CNRS, Departement dInformatique, Ecole Normale Superieure, Paris.

[45] Hassan MU, Chaudhry SA, Irshad A. An Improved SIP Authenticated Key Agreement Based on Dongqing et al. Wireless Pers Commun 2020;110(4): 2087–107.

[46] Alsharif MH, Kelechi AH, Yahya K, Chaudhry SA. Machine Learning Algorithms for Smart Data Analysis in Internet of Things Environment: Taxonomies and Research Trends. Symmetry 2020;12(1):88.

[47] Alzahrani BA, Chaudhry SA, Barnawi A, Al-Barakati A, Alsharif MH. A Privacy Preserving Authentication Scheme for Roaming in IoT-Based Wireless Mobile Networks. Symmetry 2020;12(2):287. https://doi.org/10.3390/sym12020287.

[48] Burrows M, Abadi M, Needham R. A logic of authentication. ACM Trans Comput Syst 1990;8:18–36.

[49] Wu D, Zhou C. Fault-tolerant and scalable key management for smart grid. IEEE Trans Smart Grid 2011;2(2):375–81.

[50] Farivar F, Haghighi MS, Jolfaei A, Alazab M. Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT. IEEE Trans Ind Inf 2020;16(4):2716–25.

[51] Benzaid C, Lounis K, Al-Nemrat A, Badache N, Alazab M. Fast authentication in wireless sensor networks. Future Generat Comput Syst 2016;55:362–75.

[52] Alazab M, Huda S, Abawajy J, Islam R, Yearwood J, Venkatraman S, et al. A hybrid wrapper-filter approach for malware detection. J Network 2014;9(11):2878–91.

[53] Vinayakumar R, Alazab M, Srinivasan S, Pham Q-V, Padannayil SK, Simran K. A visualized botnet detection system based deep learning for the Internet of Things networks of smart cities. IEEE Trans Ind Appl 2020;56(4):4436–56.

[54] Venkatraman S, Alazab M, Vinayakumar R. A hybrid deep learning image-based analysis for effective malware detection. J Informat Secur Appl 2019;47:377–89.

[55] Kilinc HH, Yanik T. A survey of SIP authentication and key agreement schemes. IEEE Commun Surv Tutorials 2014;16(2):1005–23.