Received December 30, 2018, accepted January 8, 2019, date of publication January 21, 2019, date of current version February 8, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2893918

An Unlinkable Authentication Scheme for Distributed IoT Application

YOUSHENG ZHOU[1,2], TONG LIU[1], FEI TANG[1,2], AND MAGARA TINASHE[1]

[1]College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
[2]School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Corresponding author: Yousheng Zhou (zhouys@cqupt.edu.cn)

This work was supported in part by the Venture & Innovation Support Program for Chongqing Overseas Returnees, in part by the Chongqing Research Program of Application Foundation and Advanced Technology under Grant cstc2017jcyjAX0201, in part by the National Natural Science Foundation of China under Grant 61702067, and in part by the Science and Technology Research Project of Chongqing Municipal Education Commission under Grant KJ1600445.

ABSTRACT The Internet of Things (IoT) is an enormous ubiquitous-network, which connects the objects through various sensors. The IoT technology promotes the interconnection and fusion between the physical world and information space, and it facilitates the day-to-day life of people. However, since a lot of equipped sensors are unattended and open, the IoT must face and overcome the main problems of security and privacy. Authentication is one of the paramount security concerns in the IoT environment, in which a user could directly access data from the sensors. Therefore, we propose an authentication and key agreement scheme providing unlinkability for the IoT environment based on bilinear pairings. The formal security proof demonstrates that the proposed protocol is unforgeable under the adaptively chosen message attack, and the session key exchange is semantic secure under the eCK model. In addition, the computation and communication costs of the proposed scheme are evaluated and compared with some existing similar schemes, which exhibits that it pleasantly addresses the needs of the IoT as far as security properties and computation expenses.

INDEX TERMS Authentication, IoT, privacy-preserving, security.

I. INTRODUCTION

The Internet of Things (IoT) [1] is a huge network of things, and it can recognize, control and centrally manage all kinds of objects around us through sensors, embedded devices and so on. It opens up a new opportunity to connect people to sensor devices distributed around them. With the development of the sensor technologies, a lot of IoT applications have been designed, such as healthcare services, smart grid devices [2]–[4], smart transport systems [5], [6] and smart city etc., which enhance the living conditions greatly. In the context of IoT application domains, there exist two types of networks, i.e., distributed and centralized networks [7]. In centralized networks, the sensor nodes cannot communicate with end-user directly, while they are connected with each other by a cloud or a base station. With respect to distributed networks, the end-user can obtain information straightaway from the sensor nodes.

The sensors can gather some sensitive or classified information from its surrounding environment, then transmit data wirelessly to authorized control units in IoT applications. The gathered information is evaluated, analyzed and certain decisions are made based on the analysis to take some actions which might in turn cause grave implications. For example, a traffic monitoring system, which is responsible for the detection of traffic conditions, collecting various parameters related to road traffic flow, utilizes information collected to control the traffic. However, the traffic monitoring system is prone to some cyber attacks as lots of equipped sensors deployed in unattended environment. A malicious user may control a sensor to upload forged information to the system, which may cause traffic chaos. For ensuring network security and privacy in the IoT environment, it is vital to construct a secure protocol to achieve mutual authentication and establish a session key between users and sensor nodes [8], [9]. Besides, due to the constraint on resource of computation and communication, including the capability of CPU, the amount of memory and the computational capabilities [10]–[13], the cost of authentication and key agreement schemes should be decreased as much as possible. Therefore, an efficient authentication and key agreement schemes based on bilinear pairings is designed for the distributed Internet of things systems in this paper.

Specifically, the features of the proposed scheme are as follows:

1) Our proposed scheme achieves the unlinkability property during authentication procedure to protect users' privacy. Any two or more messages from different sessions cannot be confirmed by any third party whether these messages come from the same entity.
2) Our proposed scheme achieves anonymity. Since the real identity of user is randomized, it is kept hidden for any external unauthorized entities.
3) Our proposed scheme ensures the forward secrecy. All transmitted messages have been randomized so that any attacker cannot derive the previous session key from the current session key.
4) Our proposed scheme achieves conditional traceability to resolve possible disputes. If any dispute or misbehavior occurs during the authentication, the trusted third party can reveal the real identity of users with the exchanged authentication messages.

The remainder of this article is structured as follows: Section 2 introduces some related work about authentication schemes for IoT. Some brief preliminaries are provided in Section 3. The detailed description of the proposed protocol is presented in Section 4. Then, Section 5 offers security analysis about the proposed scheme. Section 6 gives performance evaluation. Finally, we conclude the paper.

II. RELATED WORKS

In the past decade, various authentication protocols have been put forwarded by some researchers to ensure information transmission security. Das [15] proposed a two-factor user authentication scheme by using hash function for WSNs. The idea behind this function is that gateway node will send a personalized smart card to a user during the registration process, and then the user can access information from the network using smart card and his password, and it is claimed that the protocol could resist various attacks such as impersonation, replay, and guessing attacks. However, in 2011, Yeh *et al.* [16] pointed out that Das's scheme is susceptible to insider attacks and forgery attacks. Then, an elliptic curves based user authentication scheme was designed by them to remedy these security flaws. Liu *et al.* [17] presented a simple authentication and key establishment protocol based on ECC for IoT, where OpenID technology is used to enable user to have a single account which permits the user to log in other different sites. Then, Ndibanje *et al.* [18] demonstrated Liu *et al.*'s protocol cannot resist replay and compromised device attacks, and then they proposed a symmetric encryption-based proposal based on Liu *et al.*'s scheme, in which password update procedure is added.

In 2014, Turkanovic *et al.* [19] proposed a lightweight user authentication for heterogeneous WSNs, based on the IoT notion, using symmetric cryptography, where a user can access a targeted sensor node directly through the Internet without connecting to gateway node, thereby ensuring a more direct way. However, in 2016, Farash *et al.* [20] demonstrated that Turkanovic *et al.*'s scheme exists some security weaknesses, containing sensor node impersonation attacks as well as stolen-smart card attacks and so on. Then, they proposed an improved lightweight authentication protocol for IoT environments that uses user's smart-card and password as two factors, and eliminates the afore-mentioned security shortcomings. In the same year, Amin *et al.* [21] pointed out that Farash *et al.*'s scheme is vulnerable to off-line password guessing, new-smartcard-issue, stolen-smart card as well as user impersonation attacks. Then, they presented a modified model according to Farash *et al.*'s scheme and proposed a remote-user authentication protocol for IoT, using bio-hashing function.

In 2016, Liu and Chung [22] proposed a bilinear pairing-based user authentication scheme and data transmission approach for wireless healthcare sensor networks, using passwords and smart cards. They claimed that their scheme can resist common attacks, such as offline password guessing attack, replay attack, impersonation attack. But, in 2017, Li *et al.* [23] observed that Liu *et al.*'s scheme suffers from password disclosure attacks, replay attacks, sense data disclosure attacks, stolen smart card attacks and off-line password guessing attacks, and then they proposed an enhanced user authentication and anonymity scheme for the IoT-based medical care system, which only use lightweight computations, such as XOR operation and hash function. Wang [24] observed that end-devices require weaker identities to achieve a higher privacy because once strong identities are disclosed, end-devices are completely exposed and proposed a bilinear pairings-based authentication scheme with weaker identity for IoT, which combines group signature and Shamir secret sharing scheme. Dhillon and Kalra [25] proposed a multi-factor remote user authentication in IoT environments based on XoR and hash operations.

Recently, Mishra *et al.* [26] constructed a robust authentication protocol using smart-card for IoT-based WSN, which employs password hash values and pre-shared keys to achieve authentication between the gateway node and sensor node, and they argued that it provides user anonymity and withstands various attacks. Li *et al.* [27] presented an anonymous authentication protocol for IoT environments that uses user's password, biometric information and smart-card as three factors, which is constructed by using hash function operations and XoR operations. Karati *et al.* [28] constructed a bilinear pairing-based signature scheme for industrial IoT environments without map-to-point hash function and random oracle model, which is shown to be secure and low-cost.

III. PRELIMINARIES

In this section, some of the basic concepts and properties are described briefly.

A. NETWORK MODEL

Figure 1 describes a general structure model of the Internet of Things (IoT), which is used in our proposed protocol.

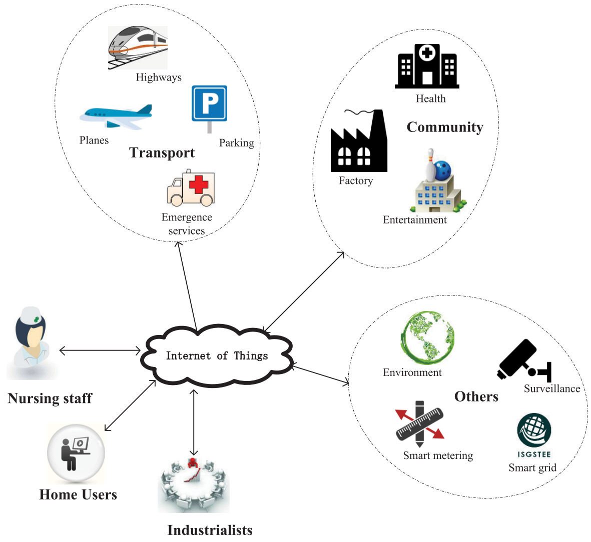


FIGURE 1. A general structure model of the Internet of things.

Figure 1 shows that all smart devices, like sensors, are connected through Internet. Various types of users, such as nursing staff, home users or industrialists, could access the data of smart devices by network and servers. A user and a smart device need to achieve mutual authentication through the Internet so that the user could access data from the smart device.

B. NOTATIONS

All symbols used in this article are listed in Table 1.

TABLE 1. Notations.

Symbol	Description
TTP	The trusted third party
U	The user
SN	The sensor node
p, q	Two large prime numbers
G_1	An additive group with the order q
G_2	A cyclic multiplicative group with the order q
h, H, H_1	One-way hash function, where $h : \{0, 1\}^* \to z_q^*, H : \{0, 1\}^* \to z_q^*, H_1 : \{0, 1\}^* \to z_q^*$
MAC	The message authentication code
e	A bilinear pairing
t_i, t_j	The current timestamp
pid_i	The alias for the ith user
Q_T	The public key of the third party
s_T	The private key of the third party
$F = (x, y)$	An elliptic curve point in a non-singular elliptic curve E_p, x and y are X-coordinate and Y-coordinate of F respectively
$\oplus$	The XOR operation
$\|\|$	The message concatenation operation

C. BILINEAR PAIRINGS

Let G_1 be a cyclic additive group generated by the prime order q and a generator P and G_2 be a cyclic multiplicative group generated by the same prime order q. There exists a bilinear map $e : G_1 \times G_1 \to G_2$ which meets the following features [29]:

- Bilinearity. For $a, b \in z_q^*$ and $A, B, C, D \in G_1$, we have:
  $e(aA, bB) = e(A, B)^{ab}$
  $e(A + B, C) = e(A, C)e(B, C)$
  $e(A, B + C) = e(A, B)e(A, C)$
- Nondegeneration. If $A \in G_1$ and $B \in G_1$, then $e(A, B) \neq 1$ and $e(A, B)$ is a generator of G_2.
- Computability. For $A, B \in G_1$, there exists an algorithm to obtain $e(A, B)$.

D. ELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM

Let G_1 be an elliptic curve group with the prime order q, whose generator is P. Then, the following intractable problems in ECC are described as follows:

- *The elliptic curve discrete logarithm* (*ECDL*) *problem*: Given points $P,\ Q \in G_1$, where $Q = aP$ for unknown $a \in z_q^*$, to find a.
- *The elliptic curve computational Diffie − Hellman* (*ECCDH*) *problem*: Given points $P,\ Q,\ R \in G_1$, where $Q = aP,\ R = bP$ for unknown $a, b \in z_q^*$, to compute abP.
- *The elliptic curve decisional Diffie−Hellman* (*ECDDH*) *problem*: Given points $P,\ Q,\ R,\ S \in G_1$, where $Q = aP,\ R = bP,\ S = cP$ for unknown $a, b, c \in z_q^*$, to decide whether $abP = cP$.

IV. THE PROPOSED SCHEME

This section presents the details of the protocol which includes the following phases: initialization phase, user registration phase, user login and request phase, and user authentication and key agreement phase. The initialization phase is used to generate system public parameters, the user registration phase is applied to produce entities' public and private key pairs, and the user authentication and key agreement phase enables user and sensor node to mutually authenticate each other.

Our scheme consists of three types of entities as shown in Figure 2: user(U), sensor node(SN) and the trusted third party(TTP). A user who uses certain application such as medical device, smart phone to access data gathered by the sensor node. *TTP* is only responsible for generating system public parameters and issues partial private key of a user, while the partial private key alone is not enough to be used to impersonate a user. Notably, *TTP* does not get involved in the authentication process.

A. INITIALIZATION PHASE

The initialization phase consists of the following steps.

1) Firstly, TTP chooses an elliptic curve additive group G_1 generated by P, whose order is the prime number q and let G_2 be a multiplicative group generated by same order, and then TTP picks three secure hash functions $h,\ H,\ H_1 : \{0, 1\}^* \to z_q^*$, a message authentication code *MAC* and a bilinear pairing e: $G_1 \times G_1 \to G_2$.

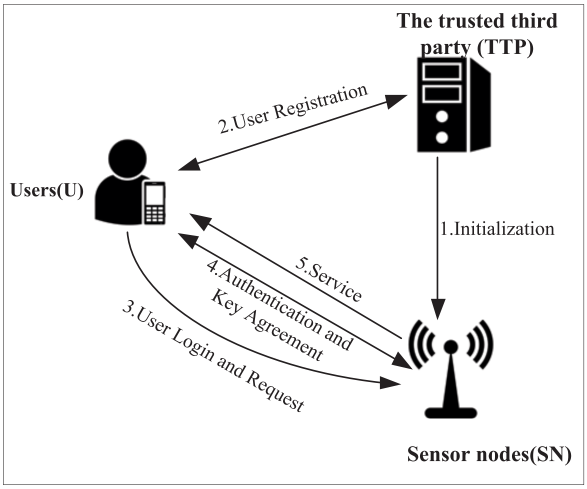


FIGURE 2. Authentication model for IoT of the proposed scheme.

2) *TTP* selects $s_T \in z_q^*$ as its private key and computes the corresponding public key $Q_T = s_T P$.
3) *TTP* sets the public $parameters = \{G_1, G_2, P, q, h, H, H_1, MAC, e, Q_T\}$ and keeps its private key secret.
4) Finally, sensor node(SN) selects $s_j \in z_q^*$ as its private key and computes his public key $Q_j = s_j P$.

B. USER REGISTRATION PHASE

1) User U selects the identity ID_i, and the password PW_i, computes $RPW_i = h(PW_i, ID_i)$ and then sends $\{ID_i, RPW_i\}$ to TTP via a secure channel.
2) After receiving $\{ID_i, RPW_i\}$, TTP picks a random number $k \in z_q^*$, computes the partial public key $Q_{i1} = kP$, partial private key $S_{i1} = s_T Q_{i1}$, user's pseudonym $pid_i = ID_i \oplus h(RPW_i, k)$ and $f_i = s_T h(pid_i) + k \bmod q$. Then, TTP returns $\{Q_{i1}, S_{i1}, f_i, pid_i\}$ to U.
3) Upon receiving $\{Q_{i1}, S_{i1}, f_i, pid_i\}$, the user U computes $h(RPW_i, k) = ID_i \oplus pid_i$ and $e_i = h(h(RPW_i, k), ID_i, PW_i)$. Then U inserts $\{f_i, pid_i, e_i\}$ into his/her smart card.
4) Lastly, U selects a random number $s_{i2} \in z_q^*$ as his/her other partial private key and computes the corresponding partial public key $Q_{i2} = s_{i2}P$. And publics his/her public keys $\{Q_{i1}, Q_{i2}\}$ and keeps its private keys $\{S_{i1}, s_{i2}\}$ secretly.

C. USER LOGIN AND REQUEST PHASE

User performs the login and request phase to access data from the sensor node, which is described as follows:

1) The user U inserts his/her smartcard and inputs ID_i, PW_i, and then the smartcart computes $h(RPW_i, k) = ID_i \oplus pid_i$, $e_i' = h(h(RPW_i, k), ID_i, PW_i)$.
2) If $e_i = e_i'$, the smart card picks a random number $r_i \in z_q^*$, computes $U_i = r_i Q_j$. Then, U sends the request message $request = \{U_i\}$ to the sensor node SN to access data via a public channel.

D. AUTHENTICATION AND KEY AGREEMENT PHASE

The following steps illustrate the authentication and key agreement process in detail.

1) Upon receiving the message *request* from U, SN chooses a random number $r_j \in z_q^*$, calculates $E_j = r_j P$, $F_j = r_j s_j^{-1} U_i = r_j s_j^{-1} r_i s_j P = r_i r_j P = (x, y)$. Then, SN generates its timestamp t_j and computes $MAC_y(t_j)$, where MAC is the message authentication code. After that, SN sends the message $\{t_j, E_j, MAC_y(t_j)\}$ to U via a public channel.
2) After receiving $\{t_j, E_j, MAC_y(t_j)\}$ from SN, U checks the validity of t_j. If it is not valid, U rejects SN; otherwise, U computes $F_i = r_i E_j = r_i r_j P = (x', y')$, $MAC_{y'}(t_j)$. Then, U checks whether the equation $MAC_{y'}(t_j) = MAC_y(t_j)$ holds. If no, U rejects SN; Otherwise, U generates its timestamp t_i and computes $rpid_i = pid_i \oplus x'$, $aid_i = h(ID_i, r_i) \oplus pid_i$, $w_i = e(S_{i1}, y'Q_j)$, $\delta = s_{i2} + f_i H(t_i, w_i, F_i) \bmod q$ and the session key $sk = H_1(F_i, h(ID_i, r_i), t_i, t_j)$. Then, U sends the message $\{\delta, t_i, rpid_i, aid_i\}$ to SN via a public channel.
3) Upon receiving the message $\{\delta, t_i, rpid_i, aid_i\}$ from U, SN firstly verifies t_i. If it is not valid, SN rejects U; otherwise, SN computes $pid_i = rpid_i \oplus x$, $h(ID_i, r_i) = aid_i \oplus pid_i$, $w_i' = e(Q_{i1}, ys_jQ_T)$ and verifies whether the equation $\delta.P = Q_{i2} + H(t_i, w_i', F_j)(h(pid_i)Q_T + Q_{i1})$ holds. If it is valid, SN calculates the session key $sk = H_1(F_j, h(ID_i, r_i), t_i, t_j)$; otherwise, SN terminates the authentication.

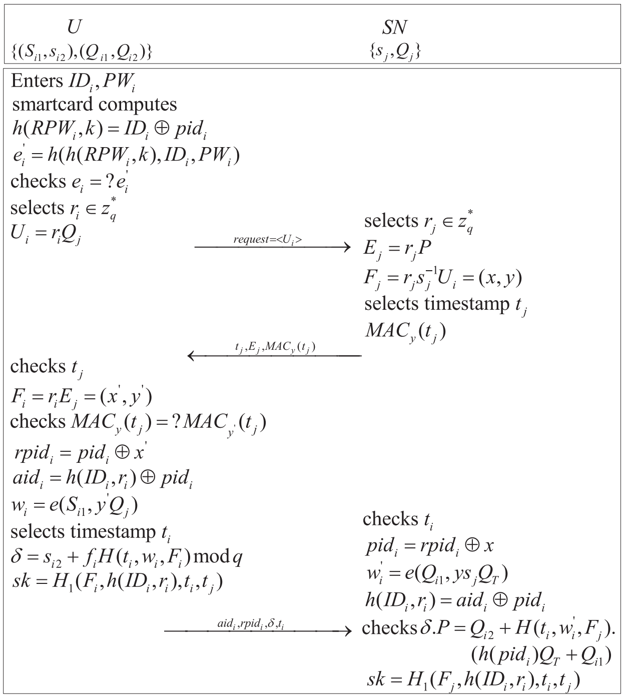

U
$\{(S_{i1}, s_{i2}), (Q_{i1}, Q_{i2})\}$
SN
$\{s_j, Q_j\}$
Enters ID_i, PW_i
smartcard computes
$h(RPW_i, k) = ID_i \oplus pid_i$
$e_i' = h(h(RPW_i, k), ID_i, PW_i)$
checks $e_i = ?e_i'$
selects $r_i \in z_q^*$
$U_i = r_i Q_j$
$request=<U_i>$
selects $r_j \in z_q^*$
$E_j = r_j P$
$F_j = r_j s_j^{-1} U_i = (x, y)$
selects timestamp t_j
$MAC_y(t_j)$
$t_j, E_j, MAC_y(t_j)$
checks t_j
$F_i = r_i E_j = (x', y')$
checks $MAC_y(t_j) = ?MAC_{y'}(t_j)$
$rpid_i = pid_i \oplus x'$
$aid_i = h(ID_i, r_i) \oplus pid_i$
$w_i = e(S_{i1}, y'Q_j)$
selects timestamp t_i
$\delta = s_{i2} + f_i H(t_i, w_i, F_i) \bmod q$
$sk = H_1(F_i, h(ID_i, r_i), t_i, t_j)$
checks t_i
$pid_i = rpid_i \oplus x$
$w_i' = e(Q_{i1}, ys_jQ_T)$
$h(ID_i, r_i) = aid_i \oplus pid_i$
$aid_i, rpid_i, \delta, t_i$
checks $\delta.P = Q_{i2} + H(t_i, w_i', F_j).$
$(h(pid_i)Q_T + Q_{i1})$
$sk = H_1(F_j, h(ID_i, r_i), t_i, t_j)$

FIGURE 3. Authentication and key establishing phase of the proposed scheme.

The summary of the authentication and key agreement phase is depicted in Figure 3.

Once SN and U successfully authenticate each other over the public channel, a secret session key sk can be agreed. otherwise, U terminates the authentication with SN.

V. SECURITY ANALYSIS

A. THE FORMAL SECURITY ANALYSIS

In this section, we show that our proposed scheme is proved unforgeable against adaptively chosen message attacks under the random oracle model [30] and the session key is semantically secure under the eCK model [38].

1) UNFORGEABILITY OF MESSAGE

In this part, our proposed scheme is to be proved unforgeable against adaptively chosen message attacks under the random oracle model. Let $U-to-SN$ denote the process that the user U communicates the sensor node SN and $SN-to-U$ denote the process that the sensor node SN communicates the user U. Obviously, the authentication of our proposed authentication is composed by $U-to-SN$ and $SN-to-U$. We prove the security by the following theorems, where the way $U-to-SN$ is proved in ***Theorem 1*** and the way $SN-to-U$ is proved in ***Theorem 2***, respectively.

Definition 1 (Unforgeability): We define a probabilistic polynomial-time adversary(PPT) $\mathcal{A}$ who wants to forge a valid message, a challenger $\mathcal{C}$ and an experiment played between $\mathcal{C}$ and $\mathcal{A}$. The proposed protocol is unforgeable against adaptively chosen message attack if no any PPT $\mathcal{A}$ wins the following experiment between $\mathcal{A}$ and $\mathcal{C}$ with a non-negligible advantage, where the adversary $\mathcal{A}$ can issue the following queries.

- *Configuration* $-$ *query*: The challenger $\mathcal{C}$ distributes $Q_T = s_T P$, generates public parameters *paramters* $= \{G_1, G_2, P, q, Q_T\}$ and returns it to $\mathcal{A}$.
- $h-$*query*: The challenger $\mathcal{C}$ can model the random oracle h by maintaining tuples (m, R_1) in a list L_h, where L_h is initially an empty set. Once the oracle h is queried by the adversary $\mathcal{A}$ with input m, $\mathcal{C}$ responds as below:
  - If L_h has already existed an item of (m, R_1), $\mathcal{C}$ returns R_1.
  - Otherwise, $\mathcal{C}$ picks a random number R_1', stores (m, R_1') into L_h and outputs R_1'.
- $H-$*query*: The challenger $\mathcal{C}$ can simulate the random oracle H by maintaining tuples (t_i, w_i, F_i, R_2) in a list L_H, where L_H is an at first void set. Once the oracle H is queried by the adversary $\mathcal{A}$ with input (t_i, w_i, F_i), $\mathcal{C}$ responds as below:
  - If L_H has already existed an item (t_i, w_i, F_i, R_2), $\mathcal{C}$ returns R_2.
  - Otherwise, $\mathcal{C}$ picks a random number R_2', stores (t_i, w_i, F_i, R_2') into L_H and outputs R_2'.
- H_1-*query*: The challenger $\mathcal{C}$ can simulate the random oracle H_1 by maintaining tuples $(F_j, R_1, t_i, t_j, R_3)$ in a list L_{H1}, where L_{H1} is initially an empty set. Once the oracle H_1 is queried by the adversary $\mathcal{A}$ with input (F_j, R_1, t_i, t_j), $\mathcal{C}$ extracts the item (m, R_1) from L_h at first and responds as below:
  - If L_{H1} has already existed an item $(F_j, R_1, t_i, t_j, R_3)$, $\mathcal{C}$ returns R_3.
  - Otherwise, $\mathcal{C}$ picks a random number R_3', stores $(F_j, R_1, t_i, t_j, R_3')$ into L_{H1} and outputs R_3'.
- $MAC-$*query*: The challenger $\mathcal{C}$ can simulate the random oracle MAC by maintaining tuples (t_j, y, M_i) in a list L_{MAC}, where L_{MAC} is initially an empty set. Once the oracle MAC is queried by the adversary $\mathcal{A}$ with input (t_j, y), $\mathcal{C}$ responds as follows:
  - If L_{MAC} has already existed an item (t_j, y, M_i), $\mathcal{C}$ returns M_i.
  - Otherwise, $\mathcal{C}$ picks a random number M_i', stores (t_j, y, M_i') into L_{MAC} and outputs M_i'.
- *Send* $-$ *query*: The adversary $\mathcal{A}$ issues this query to obtain a response corresponding to the message m. The corresponding messages will be returned.

Theorem 1: Assume that there exists a probabilistic polynomial time(PPT) adversary $\mathcal{A}$ who intends to forge a user to generate a valid message of $U-to-SN$ with a non-negligible probability ϵ. Then, there is a challenger $\mathcal{C}$, who could solve DL problem by interacting with $\mathcal{A}$ with a non-negligible probability.

Proof: Suppose $\mathcal{A}$ is able to break our proposed protocol with public data as input. It means that $\mathcal{A}$ could violate $U-to-SN$ authentication of the proposed protocol with a non-negligible advantage. Given an instance of DL problem $\{P, Q_T = xP\}$, where $x \in z_q^*$ is unknown. In order to output the answer of DL problem, $\mathcal{C}$ interacts with $\mathcal{A}$ as follows.

If $\mathcal{A}$ could pass the verification of SN successfully, he or she could generate a valid authentication message (t_i, δ, aid_i) without knowing the user's partial private key S_{i1}, where t_i is the current timestamp and $aid_i = h(ID_i, r_i) \oplus x'$, $\delta = s_{i2} + f_i H(t_i, w_i, F_i) \bmod q$. In this case, $\mathcal{A}$ obtains $H(t_i, w_i, F_i)$ through $H-query$, and Q_T through *Configuration* $-$ *query*. According to the above different oracles, $\mathcal{A}$ could play his/her fully forgery ability. According to the forking lemma [37], if $\mathcal{A}$ repeats the above queries with a different choice of R_1, then $\mathcal{A}$ is able to output another valid authentication message $\{t_i, \delta^*, aid_i\}$, where $aid_i = h(ID_i, r_i) \oplus x'$, $\delta^* = s_{i2} + f_i^* H(t_i, w_i, F_i) \bmod q$ and t_i is the current timestamp. Such that, we obtain the following two equations:

$$\begin{cases} \delta.P = Q_{i2} + R_2(R_1 Q_T + Q_{i1}) \\ \delta^*.P = Q_{i2} + R_2(R_1^* Q_T + Q_{i1}) \end{cases} \tag{1}$$

From (1), we can get

$$\begin{aligned} \delta P - \delta^* P &= (\delta - \delta^*)P \\ &= R_2(R_1 - R_1^*)Q_T \\ &= R_2(R_1 - R_1^*)s_T P \\ \Rightarrow s_T &= \frac{\delta - \delta^*}{R_2(R_1 - R_1^*)} \end{aligned}$$

Eventually, $\mathcal{C}$ obtains the output $x = \frac{\delta - \delta^*}{R_2(R_1 - R_1^*)}$ of the DL problem instance $(P, Q_T) = (P, xP)$. The advantage that $\mathcal{C}$

uses $\mathcal{A}$ to solve DL problem is $\epsilon^* \geq (1-\frac{1}{q_h})\frac{\epsilon}{q_h}$. Obviously, it contradicts with the assumption of the DL problem. Therefore, $\mathcal{A}$ cannot violate $U-to-SN$ authentication of our proposed protocol under the random oracle.

Theorem 2: Assume that there exists a probabilistic polynomial time(PPT) adversary $\mathcal{A}$ who intends to forge a sensor node to generate a valid message of $SN-to-U$ with a non-negligible advantage ϵ. In other words, the message $\{t_j, E_j, MAC_y(t_j)\}$ forged by $\mathcal{A}$, can pass the authentication. Then, there is a challenger $\mathcal{C}$ who could solve CDH problem by interacting with $\mathcal{A}$ with a non-negligible advantage $\varepsilon' \geq \varepsilon - \frac{1}{2^k} - \frac{1}{q^2}$.

Proof: Let $Event_{SN-to-U}$ denote $\mathcal{A}$ could forge an authentication message $\{t_j, E_j, MAC_y(t_j)\}$. After intercepting messages conditioned on the hypothesis that $\mathcal{A}$ does not violate $U-to-SN$ authentication of our scheme. Then, one of the following events $E_{MAC-Ture}$, $E_{U_iE_j}$, E_{q-E_j} may occur.

$E_{MAC-Ture}$: The value $MAC_y(t_j)$ is guessed correctly by the adversary $\mathcal{A}$ with the probability $\frac{1}{2^k}$, where k represents the length of the hash function MAC.

$E_{U_iE_j}$: The values U_i and E_j have been generated in a previous session, and its probability is $\frac{1}{q^2}$.

E_{q-E_j}: The oracle $MAC()$ is queried by $\mathcal{A}$ with the message $\{t_2, E_j, MAC_y(t_j)\}$.

Then, we obtain

$$\begin{aligned} Pr[Event_{SN-to-U}] &\leq (Pr[E_{MAC-Ture}] \\ &\quad + Pr[E_{U_iE_j}] + Pr[E_{q-E_j}]) \\ &= \frac{1}{2^k} + \frac{1}{q^2} + Pr[MAC_y(t_j)] \end{aligned}$$

In the defined steps of the proposed scheme, every sensor node establishes a secret value $F_j = r_j s_j^{-1} U_i = r_j r_i s_j^{-1} Q_j = (x, y)$ separately with the user. Let $E_j = aQ_j$ and $U_i = bQ_j$ with unknown $a, b \in z_q^*$. For the CDH problem instance $\left(Q_j, E_j = r_j s_j^{-1} Q_j, U_i = r_i Q_j\right)$, $\mathcal{A}$ could get the answer $r_j r_i s_j^{-1} Q_j$ with the non-negligible advantage $\varepsilon' \geq \varepsilon - \frac{1}{2^k} - \frac{1}{q^2}$. It contradicts with the hardness of CDH problem. Therefore, $\mathcal{A}$ cannot violate $U-to-SN$ authentication of our protocol.

According to ***Theorem 1*** and ***Theorem 2***, we can conclude that our proposed protocol is unforgeable against adaptively chosen message attack under the random oracle model.

2) INDISTINGUISHABILITY OF SESSION-KEY

We adopt Wazid *et al.*'s security model [38] and demonstrate that our proposed protocol provides the session-key security. The security model in our in is defined firstly as follows.

Participants. There are two participants: user(U), and sensor node(SN). Let $\prod_U^i$ denote the $i-th$ instance of U, and $\prod_{SN}^j$ represent the $j-th$ instance of SN. Any participant instance is assumed as an oracle.

Partnering. We introduce a session identification sid which is unique for each session. If instances $\prod_U^i$ and $\prod_{SN}^j$ are called partners, then the following conditions are satisfied: (1) The same session identification(sid) between $\prod_U^i$ and $\prod_{SN}^j$ is shared; (2) $\prod_U^i$ and $\prod_{SN}^j$ have accepted the session; (3) $\prod_U^i$ and $\prod_{SN}^j$ are each other's partnered peer.

Freshness. If the session key among U and SN keeps free of irrelevant the adversary $\mathcal{A}$, We call the instances U and SN are *fresh*.

Adversary. It is assumed that there exists a probabilistic polynomial-time(PPT) adversary $\mathcal{A}$ who can control all the communications by issuing a series of oracle queries during the execution of the protocol. All the adversary's queries are listed below:

- $h(x)$: Once the oracle h is queried by $\mathcal{A}$ with the message x, $\mathcal{C}$ picks a random number R_1, stores (x, R_1) into L_h and outputs R_1 to $\mathcal{A}$.
- $H_1(z)$: Once the oracle H_1 is queried by adversary $\mathcal{A}$ with the message z, $\mathcal{C}$ responds in such a way that: $\mathcal{C}$ picks a random number R_3, stores (z, R_3) into L_{H1} and outputs R_3 to $\mathcal{A}$.
- $Execute(\prod_U^i / \prod_{SN}^j)$: This query issued by the adversary $\mathcal{A}$ simulates the eavesdropping attacks on honest executions among U and SN. It outputs a transcript of the exchanged messages during the honest execution of the protocol.
- $Reaveal(\prod_U^i / \prod_{SN}^j)$: The query is designed to simulate the known session key attack. If there is a valid session for the instance $\prod_U^i / \prod_{SN}^j$, returns the shared session key to $\mathcal{A}$. Otherwise, returns null.
- $Send(\prod_U^i / \prod_{SN}^j, m)$: The adversary $\mathcal{A}$ issues this query to obtain a response message corresponding to the message m. After an execution of the defined steps, the corresponding message will be returned.
- $CorruptUser(\prod_U^i)$: The adversary $\mathcal{A}$ issues this query to corrupt the smartcard of $\prod_U^i$ and extract all stored information.
- $Test(\prod_U^i / \prod_{SN}^j)$: This query is used to model the capability of the adversary $\mathcal{A}$ to distinguish between a random number and a real session key SK by flipping an unbiased coin b. If the session key of the instance $\prod_U^i / \prod_{SN}^j$ has been defined, the session key of $\prod_U^i / \prod_{SN}^j$ will be responded to $\mathcal{A}$ if $b = 1$ or a random value will be returned if $b = 0$; otherwise, a random string will be responded.

Semantic security. The adversary $\mathcal{A}$ could issue any *Test* query to the instances after being provided with the above queries. The output of *Test* query is relevant to the bit b. Lastly, $\mathcal{A}$'s output is a result of a guessing bit b' about b. We say $\mathcal{A}$ successes if $b' = b$. Let *Succ* represent the event that $\mathcal{A}$ succeed in the game. The advantage that the adversary $\mathcal{A}$ breaks semantic security of the proposed unlinkability authentication scheme(UAS) is defined as follows:

$$Adv_{\mathcal{P}}^{UAS} = \mid 2 \cdot Pr[Succ] - 1 \mid,$$

If the advantage $Adv_{\mathcal{P}}^{UAS}$ is negligible, we say the proposed scheme is semantically secure.

Theorem 3: Let $\mathcal{A}$ denote an adversary within a polynomial time t against the proposed protocol under the random oracle model, then we have:

$$Adv_{\mathcal{P}}^{UAS} \leqslant \frac{q_h^2}{|h|} + \frac{q_{H_1}^2}{|H_1|} + \frac{2q_{send}}{|\mathcal{D}|},$$

where q_h, q_{H_1}, q_{send} represent the number of h queries, H_1 queries, and *Send* queries, respectively; $|h|$, $|H_1|$ and $|\mathcal{D}|$ denote the range space of h function and H_1 function, respectively and a uniformly distributed password dictionary.

Proof: We use $Succ_i$ to represent the event that $\mathcal{A}$ wins in the game G_i, where $i = [0, 3]$. That is to say $\mathcal{A}$ guesses bit b successfully.

Game G_0: In G_0, a real attack against our proposed scheme from $\mathcal{A}$ is simulated. Firstly, the value of b is selected randomly. According to the above definitions, we obtain:

$$Adv_{\mathcal{P}}^{UAS} = 2 \cdot Pr[Succ_0] - 1 \tag{2}$$

Game G_1: To increase the probability that $\mathcal{A}$ wins game, the query $Execute(\prod_U^i / \prod_{SN}^j)$ is used to model the eavesdropping attacks. Since its goal is to derive some information about the session key sk, $\mathcal{A}$ has to compute sk according to the definition of the proposed scheme; however, $sk = H_1(F_j, h(ID_i, r_i), t_i, t_j)$, where $F_j = r_j s_j^{-1} U_i = (x, y)$ and $h(ID_i, r_i) = aid_i \oplus rpid_i \oplus x$. Certainly, U can compute the same session key. The evaluation of sk depends on the temporary randoms r_i as well as r_j and $h(ID_i, r_i)$. Therefore, in order to obtain sk, the advantage that $\mathcal{A}$ wins game G_1 would not be increased just by eavesdropping the transmitted messages, $request = \{U_i\}$, $\{t_j, E_j, MAC_y(t_j)\}$ and $\{\delta, t_i, aid_i, rpid_i\}$, which implies that

$$Pr[Succ_1] = Pr[Succ_0] \tag{3}$$

Game G_2: This game transferred from G_1 is to simulate active attacks by adding h, H_1 and *Send* oracles in which $\mathcal{A}$ tries to forge messages. $\mathcal{A}$ intends to trick participants that the modified messages is real. By arbitrarily issuing queries to h, H_1, $\mathcal{A}$ attempts to capture collisions. Note that $request = \{U_i\}$, $\{t_j, E_j, MAC_y(t_j)\}$ and $\{\delta, t_i, aid_i, rpid_i\}$ are related to temporary random numbers as well as timestamps. Therefore, there never exist collisions even though $\mathcal{A}$ issues *Send* oracles. So, according to the birthday paradox, we get:

$$|Pr[Succ_1] - Pr[Succ_2]| \leqslant \frac{q_h^2}{2\mid h \mid} + \frac{q_{H_1}^2}{2\mid H_1 \mid} \tag{4}$$

Game G_3: G_3 models the $CorruptUser(\prod_U^i)$ query. By issuing $CorruptUser(\prod_U^i)$ oracles, $\mathcal{A}$ can get all information inserted in the smartcard, which is $\{f_i,\ pid_i,\ e_i\}$. However, because the user's identity ID_i is protected by $h(.)$ function, It is not helpful for $\mathcal{A}$ to obtain session key sk. Without the U's correct password PW_i via the password dictionary attack, it is difficult to get ID_i from pid_i. Hence, we get

$$|Pr[Succ_2] - Pr[Succ_3]| \leqslant \frac{q_{send}}{\mid \mathcal{D} \mid} \tag{5}$$

Since all the random oracles are simulated, $\mathcal{A}$ has no choice but guess the bit b by querying *Test* oracle, which leads to the following result

$$Pr[Succ_3] = \frac{1}{2} \tag{6}$$

Thus, from (3)-(6), we get

$$\begin{aligned} |Pr[Succ_0] - \frac{1}{2}| &= |Pr[Succ_0] - Pr[Succ_3]| \\ &\leqslant |Pr[Succ_0] - Pr[Succ_1]| + |Pr[Succ_1] \\ &\quad - Pr[Succ_2]| + |Pr[Succ_2] - Pr[Succ_3]| \\ &\leqslant \frac{q_h^2}{2\mid h \mid} + \frac{q_{H_1}^2}{2\mid H_1 \mid} + \frac{q_{send}}{\mid \mathcal{D} \mid}. \end{aligned}$$

From (2), we have $Pr[Succ_0] = Adv_{\mathcal{P}}^{UAS}/2 + 1/2$. Hence,

$$Adv_{\mathcal{P}}^{UAS} \leqslant \frac{q_h^2}{\mid h \mid} + \frac{q_{H_1}^2}{\mid H_1 \mid} + \frac{2q_{send}}{\mid \mathcal{D} \mid}.$$

B. THE INFORMAL SECURITY ANALYSIS

In this section, we present the informal security analysis and show that our protocol is secure to various attacks.

1) UNLINKABILITY

In our scheme, since there is the use of the current timestamps $\{t_i, t_j\}$, random values $\{r_i, r_j\}$ as well as the hash functions, all information sent by user U via public channel are random values. For two or more authentication messages that are sent by the same user, the attacker cannot determine whether these authentication messages come from the same entity, which means the user U cannot be linked to different sessions. Hence, our proposed scheme provides unlinkability and the attacker cannot trace participants by intercepting messages.

2) FORWARD SECURITY

Assume an attacker has had the current session key $sk = H_1(F_j, h(ID_i, r_i), t_i, t_j)$, he or she cannot obtain the previous session key from the current session key. Without knowing r_i and r_j chosen randomly by user and the sensor node respectively, it is difficult to compute F_j for the attacker. Therefore, our proposed protocol achieves forward security.

3) RESISTANCE AGAINST IMPERSONATION ATTACK

From ***Theorem 1.*** and ***Theorem 2.***, we can see that no attacker can forge the messages $\{t_j, E_j, MAC_y(t_j)\}$ or $\{\delta, t_i, aid_i, rpid_i\}$ to pass the verification of the user U or the sensor node SN respectively. Therefore, the proposed protocol can resist the impersonation attack.

4) RESISTANCE AGAINST REPLAY ATTACK

Because the random numbers $\{r_i, r_j\}$ and the current timestamps $\{t_i, t_j\}$ are used in the generation of the messages $\{U_i\}$, $\{t_j, E_j, MAC_y(t_j)\}$ and $\{\delta, t_i, aid_i, rpid_i\}$, messages from different sessions are distinctive, and any replayed message can be detected. Therefore, our proposed scheme can resist the replay attack.

5) RESISTANCE AGAINST STOLEN VERIFIER ATTACK

In our proposed scheme, the information $\{f_i, pid_i, e_i\}$ is stored in a user's smart card. Suppose an adversary $\mathcal{A}$ steals the smartcard and obtains the information $\{f_i, pid_i, e_i\}$. However, user's identity ID_i, password PW_i, and the secret k cannot be got or guessed correctly by the $\mathcal{A}$ because of the irreversibility of hash function $h(.)$. Besides, our proposed protocol does not store any verifier tables to check the credentials entered by the user U associated with the sensor node SN. Therefore, our proposed scheme can resist the stolen verifier attack.

6) RESISTANCE AGAINST MAN-IN-THE-MIDDLE ATTACK

Suppose that an adversary $\mathcal{A}$ intercepts the message $\{t_j, E_j, MAC_y(t_j)\}$ and he/she wants to modify it to generate another message. So, he/she selects a random number $r_j' \in z_q^*$ as well as the current timestamp t_j' and calculates $E_j' = r_j'P$. Because the adversary does not gain the sensor node's private key s_j, he/she cannot compute F_j and $MAC_y(t_j)$. Similarly, assume an adversary $\mathcal{A}$ intercepts the message $\{\delta, t_i, aid_i, rpid_i\}$ and he/she wants to modify it to generate another message. He/She selects a random $r_i' \in z_q^*$ as well as the current timestamp t_i' and calculates $F_i' = r_i'E_j$. However, he/she cannot compute pid_i, w_i, δ without the user's identity ID_i, private key (S_{i1}, s_{i2}). In conclusion, it is difficult to modify the messages $\{t_j, E_j, MAC_y(t_j)\}$ and $\{\delta, t_i, aid_i, rpid_i\}$. Therefore, our proposed scheme can resist man-in-the-middle attack.

TABLE 2. Approximate running time of various operations.

Operation	Description	Computation time(ms)
T_h	hash function operation	3×10^{-3}
$T_{pnt-mul}$	bilinear pairing operation	2.14×10^{-1}
$T_{pnt-add}$	ECC point multiplication	1.6×10^{-2}
$T_{pairing}$	ECC poitnt addition	6.07×10^{-1}

VI. PERFORMANCE COMPARISON

In this section, we present a detailed performance analysis of our scheme in the authentication and key agreement phase. Besides, our proposed protocol is compared with some existing similar schemes [31]–[36] on computation cost and communication cost during authentication and key establishing phase. Table 2 provides the approximate execution time of every operation used in calculating computational cost, and detailed description of every operation is listed as follows.

- T_h: The time cost of a hash function operation.
- $T_{pairing}$: The time cost of a bilinear pairing operation.
- $T_{pnt-mul}$: The execution time of a point multiplication interrelated with ECC.
- $T_{pnt-add}$: The execution time of a point addition interrelated with ECC.

In order to compare the computation cost of our proposed scheme with other similar schemes fairly, the experiments were performed on a macOS sierra operation system equipped with an Intel Core i5 1.6 GHz CPU. In addition, because the execution time of some operations are negligible such as XoR operation, only the operations presented in Table 2.

TABLE 3. Comparison of computation cost.

Protocol	Computation Cost
Ours	$8T_{pnt-mul} + 1T_{pnt-add} + 8T_h + 2T_{pairing}$
Li *et al.*'s **[31]**	$10T_{pnt-mul} + 4T_{pnt-add} + 5T_h + 2T_{pairing}$
Wang *et al.*'s **[32]**	$5T_{pnt-mul} + 10T_h + 2T_{pairing}$
He *et al.*'s **[33]**	$8T_{pnt-mul} + 2T_{pnt-add} + 10T_h + 2T_{pairing}$
Xiong *et al.*'s **[34]**	$7T_{pnt-mul} + 15T_h + 9T_{pairing}$
Bakhtiari *et al.*'s **[35]**	$7T_{pnt-mul} + 5T_h + 6T_{pairing}$
Liu *et al.*'s **[36]**	$6T_{pnt-mul} + 6T_h + 1T_{pairing}$

TABLE 4. Comparison of running time.

Protocol	Running time (ms)
Ours	≈ 2.886
Li *et al.*'s **[31]**	≈ 3.443
Wang *et al.*'s **[32]**	≈ 2.314
He *et al.*'s **[33]**	≈ 3.098
Xiong *et al.*'s **[34]**	≈ 6.943
Bakhtiari *et al.*'s **[35]**	≈ 5.155
Liu *et al.*'s **[36]**	≈ 1.927

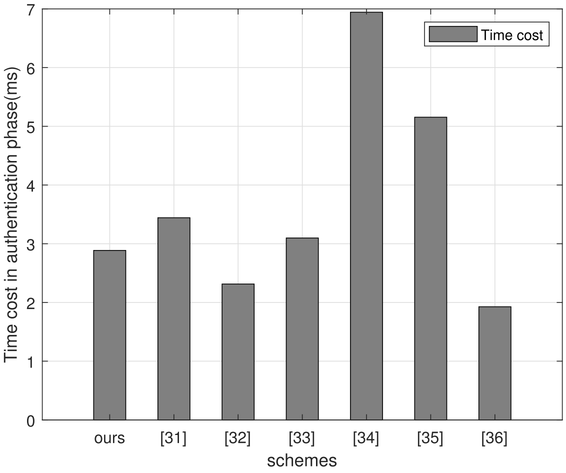


FIGURE 4. The comparison of computation cost.

From the illustrations in the Table 3, Table 4 and Figure 4, it is observed that the computation overhead of our proposed protocol is $8T_{pnt-mul} + 1T_{pnt-add} + 8T_h + 2T_{pairing}$, and the total execution time of our proposed is $(8*0.214+0.016+8*0.003+2*0.607) \approx 2886ms$. The total execution time of [31] scheme is $10T_{pnt-mul}+4T_{pnt-add}+5T_h+2T_{pairing} = (10*0.214+4*0.016+5*0.003+2*0.607) \approx 3.443ms$. The total execution time of [32] scheme is $5T_{pnt-mul}+10T_h+2T_{pairing} = (5*0.214+10*0.003+2*0.607) \approx 2.314ms$. The total execution time of [33] scheme is $8T_{pnt-mul}$ +

$2T_{pnt-add} + 10T_h + 2T_{pairing} = (8 * 0.214 + 2 * 0.016 + 10 * 0.003 + 2 * 0.607) \approx 3.098ms$. The total execution time of [34] scheme is $7T_{pnt-mul}+15T_h+9T_{pairing} = (7*0.2141+15 * 0.003 + 9 * 0.607) \approx 6.943ms$. The total execution time of [35] scheme is $7T_{pnt-mul}+5T_h+6T_{pairing} = (7*0.214+5*0.003+6*0.607) \approx 5.155ms$. The total execution time of [36] scheme is $6T_{pnt-mul}+6T_h+1T_{pairing} = (6*0.214+6*0.003+0.607) \approx 1.927ms$. And performance of our scheme has been improved compared with other schemes [31], [33]–[35]. Despite the total execution time of our proposed protocol is more than [32] and [36], ours has better security properties. Wang's scheme [32] fails to resist user's and application provider's impersonation attacks. Liu's protocol [36] is prone to privileged insider of application provider (AP) attacks, which means the adversary can impersonate client to send requested message. the reason is that network manager sends the tuple $\{I, ind_{cv}, right\}$ to the application provider but the validity of the tuple cannot be verified by AP. Therefore, the adversary can forge a valid request message according the tuple. Besides, Bakhtiari's scheme [35] is unable to resist man-in-the-middle attacks and impersonation attacks. Hence, compared with some other schemes [31], [33]–[35], the computation cost of our proposed scheme is relatively low.

To compare communication overheads of our proposed scheme with other similar schemes fairly, some assumptions are given below:

- The length of random number, timestamp or sequence number is 32 bits.
- The length of identity ID_i is 160 bits.
- The hash function used in the proposed scheme is SHA-1 [39]. Therefore, the length of hash digest is 160 bits.
- The length of an elliptic curve point $F = (x, y)$ is $(160 + 160) = 320$ bits.
- The length of a message authentication code(MAC) is 160 bits.
- Since we consider 1024-bit RSA cryptosystem, the size of encryption/decryption block is 1024 bits.

TABLE 5. The comparison of communication overheads.

Protocol	No. of messages	No. of bits
Ours	3	1344
Li *et al.*'s **[31]**	3	1984
Wang *et al.*'s **[32]**	2	1024
He *et al.*'s **[33]**	2	1856
Xiong *et al.*'s **[34]**	2	1600
Bakhtiari *et al.*'s **[35]**	5	1632
Liu *et al.*'s **[36]**	2	1472

Table 5 presents the comparison on the communication overheads of the proposed scheme and other similar schemes [31]–[36] during login and authentication phases. From the above assumptions, the communication overheads for the proposed scheme, Li's scheme [31], Wang and Zhang's scheme [32], He *et al.*'s scheme [33], Xiong and Qin's scheme [34], Bakhtiar-Chehelcheshmeh and Hosseinzadeh's scheme [35] and Liu *et al.*'s scheme [36] is 1344 bits, 1984 bits, 1024 bits, 1856 bits, 1600 bits, 1632 bits and 1472 bits, respectively.

In the proposed scheme, the size of the messages $\{U_i\}$, $\{t_j, E_j, MAC_y(t_j)\}$ and $\{\delta, t_i, aid_i, rpid_i\}$ is 320 bits, $(32 + 320 + 160) = 512$ bits, $(160 + 32 + 160 + 160) = 512$ bits, respectively. Therefore, the communication overheads of our proposed scheme is $(320 + 512 + 512) = 1344$ bits. The communication overheads of the proposed scheme is less than that in [31] and [33]–[36]. Despite the proposed scheme consumes more communication cost compared with that in [32], it provides better security and lower computation cost.

VII. CONCLUSIONS

In this paper, we present an efficient remote authentication and key-establishment protocol for IoT systems. We demonstrate that our authentication scheme provides unforgeablity of message and indistinguishability of session key under the random oracle model. In addition, the informal security analysis shows that it satisfies various desirable security properties. The performance comparison against some similar protocols shows that our scheme has relatively low computation cost and communication cost. In view of the advantages in security and performance, our proposed is more suitable for IoT applications.

REFERENCES

[1] A. Vilmos, C. Medaglia, and A. Moroni, "Vision and challenges for realising the Internet of Things," *Hot Work. Technol.*, vol. 35, no. 2, pp. 59–60, 2010.

[2] Z. Wang and H. Xie, "Privacy-preserving meter report protocol of isolated smart grid devices," *Wireless Commun. Mobile Comput.*, vol. 2017, Jun. 2017, Art. no. 2539673, doi: 10.1155/2017/2539673.

[3] Z. Wang, F. Chen, and A. Xia, "Attribute-based online/offline encryption in smart grid," in *Proc. 24th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Aug. 2015, pp. 1–5, doi: 10.1109/ICCCN.2015.7288380.

[4] H. Wang, B. Qin, Q. Wu, L. Xu, and J. Domingo-Ferrer, "TPP: Traceable privacy-preserving communication and precise reward for vehicle-to-grid networks in smart grids," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 11, pp. 2340–2351, Nov. 2015, doi: 10.1109/TIFS.2015.2455513.

[5] H. Wang and Y. Zhang, "On the security of an anonymous batch authenticated and key agreement scheme for value-added services in VANETs," *Procedia Eng.*, vol. 29, pp. 1735–1739, 2012, doi: 10.1016/j.proeng.2012.01.204.

[6] H. Wang, K. Li, K. Ota, and J. Shen, "Remote data integrity checking and sharing in cloud-based health Internet of Things," *IEICE Trans. Inf. Syst.*, vols. E99–D, no. 8, pp. 1966–1973, 2016, doi: 10.1587/transinf.2015INI0001.

[7] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2014, pp. 2728–2723, doi: 10.1109/WCNC.2014.6952860.

[8] H. Hu, Y. Liu, H. Zhang, and R. Pan, "Optimal network defense strategy selection based on incomplete information evolutionary game," *IEEE Access*, vol. 6, pp. 29806–29821, 2018, doi: 10.1109/ACCESS.2018.2841885.

[9] H. Hu, Y. Liu, H. Zhang, and Y. Zhang, "Security metric methods for network multistep attacks using AMC and big data correlation analysis," *Secur. Commun. Netw.*, vol. 2018, pp. 1–14, Jun. 2018, doi: 10.1155/2018/5787102.

[10] A. K. Das, "Improving identity-based random key establishment scheme for large-scale hierarchical wireless sensor networks," *Int. J. Netw. Secur.*, vol. 14, no. 1, pp. 1–21, 2012.

[11] C.-T. Li, "Secure smart card based password authentication scheme with user anonymity," *Inf. Technol. Control*, vol. 40, no. 2, pp. 157–162, 2011.

[12] Q. Mi, J. A. Stankovic, and R. Stoleru, "Practical and secure localization and key distribution for wireless sensor networks," *Ad Hoc Netw.*, vol. 10, no. 6, pp. 946–961, 2012, doi: 10.1016/j.adhoc.2011.12.008.

[13] W. R. Claycomb and D. Shin, "A novel node level security policy framework for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 418–428, 2011, doi: 10.1016/j.jnca.2010.03.004.

[14] D. He, Y. Gao, S. Chan, C. Chen, and J. Bu, "An enhanced two-factor user authentication scheme in wireless sensor networks," *Ad Hoc Sensor Wireless Netw.*, vol. 10, no. 4, pp. 361–371, 2010.

[15] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1086–1090, Mar. 2009, doi: 10.1109/TWC.2008.080128.

[16] H.-L. Yeh, T.-H. Chen, P.-C. Liu, T.-H. Kim, and H.-W. Wei, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 11, no. 5, pp. 4767–4779, 2011.

[17] J. Liu, Y. Xiao, and C. L. P. Chen, "Authentication and access control in the Internet of Things," in *Proc. 32nd Int. Conf. Distrib. Comput. Syst. Workshops*, Jun. 2012, vol. 34, no. 1, pp. 588–592, doi: 10.1109/ICDCSW.2012.23.

[18] B. Ndibanje, H.-J. Lee, and S.-G. Lee, "Security analysis and improvements of authentication and access control in the Internet of Things," *Sensors*, vol. 14, no. 8, pp. 14786–14805, 2014.

[19] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," *Ad Hoc Netw.*, vol. 20, pp. 96–112, 2014, doi: 10.1016/j.adhoc.2014.03.009.

[20] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Netw.*, vol. 36, pp. 152–176, Jan. 2016, doi: 10.1016/j.adhoc.2015.05.014.

[21] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, L. Leng, and N. Kumar, "Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks," *Comput. Netw.*, vol. 36, pp. 42–62, Jun. 2016, doi: 10.1016/j.comnet.2016.01.006.

[22] C.-H. Liu and Y.-F. Chung, "Secure user authentication scheme for wireless healthcare sensor networks," *Comput. Elect. Eng.*, vol. 59, pp. 250–261, Aug. 2017, doi: 10.1016/j.compeleceng.2016.01.002.

[23] C.-T. Li, T.-Y. Wu, C.-L. Chen, C.-C. Lee, and C.-M. Chen, "An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system," *Sensors*, vol. 17, no. 7, pp. 1482, 2017.

[24] Z. Wang, "A privacy-preserving and accountable authentication protocol for IoT end-devices with weaker identity," *Future Gener. Comput. Syst.*, vol. 82, pp. 342–348, May 2018.

[25] P. K. Dhillon and S. Kalra, "Secure multi-factor remote user authentication scheme for Internet of Things environments," *Int. J. Commun. Syst.*, vol. 30, no. 16, p. e3323, 2017.

[26] D. Mishra, P. Vijayakumar, V. Sureshkumar, R. Amin, S. K. H. Islam, and P. Gope, "Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks," *Multimedia Tools Appl.*, vol. 77, no. 14, pp. 18295–18325, Jul. 2018, doi: 10.1007/s11042-017-5376-4.

[27] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, "A three-factor anonymous authentication scheme for wireless sensor networks in Internet of Things environments," *J. Netw. Comput. Appl.*, vol. 103, pp. 194–204, Feb. 2018, doi: 10.1016/j.jnca.2017.07.001.

[28] A. Karati, S. K. H. Islam, and M. Karuppiah, "Provably secure and lightweight certificateless signature scheme for IIoT environments," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3701–3711, Aug. 2018.

[29] T. Van, C. A. Henk, and S. Jajodia, *Bilinear Pairings*. New York, NY, USA: Springer, 2011, p. 82.

[30] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in *Advances in Cryptology—EUROCRYPT*. Berlin, Germany: Springer, 2000, pp. 139–155.

[31] C.-T. Li, "A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card," *IET Inf. Secur.*, vol. 7, no. 1, pp. 3–10, Mar. 2013, doi: 10.1049/iet-ifs.2012.0058.

[32] C. Wang and Y. Zhang, "New authentication scheme for wireless body area networks using the bilinear pairing," *J. Med. Syst.*, vol. 39, no. 11, p. 136, Sep. 2015, doi: 10.1007/s10916-015-0331-2.

[33] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Syst. J.*, vol. 11, no. 4, pp. 2590–2601, Dec. 2017, doi: 10.1109/JSYST.2016.2544805.

[34] H. Xiong and Z. Qin, "Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 7, pp. 1442–1455, Jul. 2015, doi: 10.1109/TIFS.2015.2414399.

[35] S. Bakhtiari-Chehelcheshmeh and M. Hosseinzadeh, "A new certificateless and secure authentication scheme for ad hoc networks," *Wireless Pers. Commun.*, vol. 94, no. 4, pp. 2833–2851, Jun. 2017, doi: 10.1007/s11277-016-3721-y.

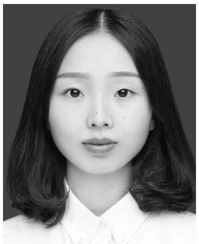
[36] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for WirelessBody area networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 332–342, Feb. 2014, doi: 10.1109/TPDS.2013.145.

[37] D. Pointcheval and J. Stern, "Security proofs for signature schemes," in *Advances in Cryptology—EUROCRYPT*. Berlin, Germany: Springer, 1996, pp. 387–398, doi: 10.1007/3-540-68339-9-33.

[38] M. Wazid *et al.*, "Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks," *IEEE Access*, vol. 5, pp. 14966–14980, 2017, doi: 10.1109/ACCESS.2017.2723265.

[39] J. H. Burrows, "Secure hash standard," Dept. Commerce, Washington, DC, USA, Apr. 1995.

YOUSHENG ZHOU received the Ph.D. degree from the Beijing University of Posts and Telecommunications, in 2011. He is currently an Associate Professor with the Chongqing University of Posts and Telecommunications. His research interests include mobile security and the IoT security.



TONG LIU is currently pursuing the master's degree with the Chongqing University of Posts and Telecommunications. Her research interests include mobile security and the IoT security.

FEI TANG received the Ph.D. degree from the Chinese Academy of Sciences, in 2015. He is currently an Associate Professor with the Chongqing University of Posts and Telecommunications. His research interests include applied cryptography and the IoT security.

MAGARA TINASHE is currently pursuing the Ph.D. degree with the Chongqing University of Posts and Telecommunications. His research interests include mobile security and the IoT security.