IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 16, 2020, accepted February 29, 2020, date of publication March 10, 2020, date of current version March 18, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2979906

A Secure Remote Mutual Authentication Scheme Based on Chaotic Map for Underwater Acoustic Networks

SHUAILIANG ZHANG, XIUJUAN DU, AND XIN LIU
Computer Department, Qinghai Normal University, Xining 810008, China
Academy of Plateau Science and Sustainability, Xining 810008, China

Corresponding author: Xiujuan Du (dxj@qhnu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61962052 and Grant 61902273, in part by the Innovation Team Foundation of Qinghai Office of Science and Technology under Grant 2020-ZJ-903, in part by the Key Laboratory of IoT of Qinghai under Grant 2020-ZJ-Y16, in part by the Hebei IoT Monitoring Center under Grant 3142016020, and in part by the Research Fund for the Chunhui Program of Ministry of Education of China.

ABSTRACT Underwater acoustic networks (UANs) have emerged as a new wireless sensor network structure widely used in many applications. Sensor nodes are usually placed in a hostile and unattended underwater environment to gather information with limited resource. Since the underwater information is sensitive and special, only authenticated users have rights to get the information. The existing secure resource-constrained authentication schemes are not inapplicable for underwater acoustic networks, so a lightweight authentication scheme is the primarily task in underwater acoustic networks. In this paper, we present a chaotic maps remote user authentication and key agreement scheme for underwater acoustic networks based on the DLP and DHP, in which only authenticated users have rights to obtain the information. The proposed scheme applies the lightweight cryptographic primitives, such as one-way hash function and chaotic maps to accomplish mutual authentication and key agreement for underwater acoustic networks. The security of the proposed scheme is certified by applying the BAN logic and Random Oracle Model. Security analysis shows that our proposed scheme is safe and can meet ten security requirements and seven security goals. Performance analysis shows that our proposed scheme is more efficient compared with other resource-constrained schemes.

INDEX TERMS Authentication, chaotic maps, DHP, DLP, lightweight.

I. INTRODUCTION

With the increasing frequency of human activities in the ocean, more and more information need to be transmitted from the underwater environment, and the underwater acoustic networks (UANs) communication technology has been widely applied in scientific expedition, marine engineering construction, investigation and development of submarine mineral resources, and military fields. These applications have also put forward higher requirements for the reliability and safety of underwater acoustic network communications.

The sensor nodes are often placed in a hostile and unattended underwater environment to gather information, so it is necessary to guarantee the secure communication among the sensor node, the user and the gateway node. Besides, the underwater acoustic channel is a public circumstance, which makes underwater acoustic communication more vulnerable to various attacks [1]. Recent studies on UANs mainly focus on network construction or protocol management [2], while only a few studies have been done on network safety [1]–[5]. Consequently, we chiefly study the safety matters for UANs in this scheme. Authentication is the first line of defense to achieve secure communication. Since the information gathered by underwater sensor nodes is sensitive and protected, only authenticated users have rights to get the information.

Despite UANs possess certain analogous characteristics with other constrained resource wireless sensor networks, for instance, nodes are placed in an unattended environment and nodes are battery-powered [4], [17], UANs are fully distinct from other wireless senor networks in a great many of respects: absorption and attenuation, multi-channel

The associate editor coordinating the review of this manuscript and approving it for publication was Javed Iqbal.

propagation, Doppler frequency shift, time-varying, environmental noise. In addition, the construction cost of underwater sensor nodes is higher than other conventional sensor nodes [2]. Therefore, due to these differences, the existing secure authentication schemes with constrained resources are not inapplicable for underwater acoustic networks. Underwater acoustic networks communication requires a new authentication scheme.

An excellent authentication and key agreement scheme enables two or more parties to transmit data safely over a public channel, and communication parties can encrypt and decrypt the information through the negotiated session key [21]. The sensor node has constrained resource and weak calculation and storage abilities, so a lightweight authentication and key agreement scheme is necessary in such a network. Based on the analysis of some previous literatures, we come to a conclusion that lightweight authentication methods are roughly divided into three types. The first type is merely based on the one-way hash function [6]–[11]. The second type applies the Elliptic Curve to accomplish the authentication [22]–[27]. The last type, which is also adopted in this scheme, is the chaotic maps [12]–[21].

Next, we give a brief explanation of the three types of lightweight authentication schemes. Das [6] proposed the robust password-based remote user authentication scheme using smart card for the Integrated EPR Information System, and Li *et al.* [7] also introduced secure remote user authentication and key agreement scheme for the Integrated EPR Information System at the same year. They both applied the lightweight hash function to fulfill mutual authentication in their schemes. Nevertheless, Jung *et al.* [8] showed that Das [6] and Li *et al.* [7] suffered from off-line password guessing attack, user impersonate attack, could not protect user anonymity, and did not provide password change section. Koya and Deepthi [9] presented a hybrid anonymous authentication scheme using the physiological signal to overcome sensor node impersonation attack and Chang and Le [10] came up with an efficient and flexible authentication scheme, which provides perfect forward and backward secrecy. Kumar *et al.* [11] carried out mutual authentication among the user, the gateway and the sensor node for secure detection in coal mines.

Lin [12] presented an improved authentication scheme by applying the property of Chebyshev chaotic maps to achieve user anonymity and good efficiency. Zhu [13] pointed out that static ID is unable to protect user anonymity in client–server environment and dynamic ID in the authentication scheme based on Chebyshev chaotic maps can resist active attacks as well as has better computational efficiency. However, Truong *et al.* [14] showed the scheme is vulnerable to malicious user attack and common session key attack. Truong *et al.* [14] also showed the scheme [13] is not able to achieve perfect forward security. The anonymity protection is very vital in three-party communication wireless sensor network [15], medical information networks [16], [17], and roaming authentication networks [18]. Xie *et al.* [19] first carried out three-party password authenticated scheme without utilizing timestamp based on chaotic maps instead of modular exponentiation and scalar multiplication on an elliptic curve. Their protocol is robust enough to withstand various attacks. Lee *et al.* [20] proposed a new three-party authentication scheme on the foundation of chaotic maps without using password, which had the ability to boycott the password guessing attack and protect user from forgery attack. In the opinion of Lee *et al.* [20], there are three problems in the scheme [19], which are anonymity of users, on-line password guessing attack and password table maintenance problem. Unfortunately, Jabbari and Mohasefi [21] proved that scheme [20] fails to guarantee user anonymity.

Elliptic curves are also used in many environments to implement authentication, such as multi-server environment [22], agriculture monitoring environment [23], IOT environments [24], [25], medical information system environment [26], cloud computing environment [27]. Compared with other lightweight authentication schemes, Chebyshev chaotic maps have higher level of efficiency and security [1], [6], [18], [20], [28].

The chief contributions of this scheme are as follows:

1) Our proposed scheme accomplishes mutual authentication among the user, the gateway and the sensor node by conducting two full rounds of four messages flows. The first message is from the user to the gateway node, the second is from the gateway node to the sensor node, the third is from the sensor node to the gateway node and the last message is from the gateway node to the user.
2) In our proposed scheme, we devise a smart card pre-authentication mechanism to inspect the legitimacy of the user at the login terminal, we use random number mechanism to protect the user anonymity and we employ the timestamp mechanism to guarantee the freshness of the messages.
3) The security of the proposed scheme is certified by applying the BAN logic and Random Oracle Model. Security analysis shows that our proposed scheme is safe and can meet ten security requirements and seven security goals. Performance analysis shows that our proposed scheme is more efficient and robust compared with other resource-constrained schemes.
4) As far as we know, we are the first to apply Chebyshev chaotic maps to underwater environments and design a remote user authentication mechanism suitable for underwater acoustic networks communication.

The rest of this paper is presented as follows. In Section II, we discuss some basic mathematical preliminaries needed for describing and analyzing our scheme. In Section III, we present the underwater model and requirements. In Section IV, we introduce our proposed scheme in detail. In Section V and Section VI, we demonstrate the safety and feasibility of our proposed scheme through formal and informal analysis. In Section VII, we make a comparison

among our proposed scheme with other schemes. Finally, we make a conclusion in Section VIII.

II. PRELIMINARIES

In this section, we will chiefly present some definitions about the Chebyshev chaotic maps and one-way hash function. Some notations and abbreviations used in this paper are briefly presented in table 1.

TABLE 1. Notations and abbreviations.

Symbol	Description
UANs	Underwater acoustic networks
RC	Registration center
$GWID_k$	Identity of gateway
$SNID_j$	Identity of sensor node
ID_i	Identity of user
PW_i	Password of user
r_i , r_p , rsc , rsn	Random numbers
T_i	Current timestamp
ΔT	Maximum time interval
SC	Smart card

A. CHEBYSHEV CHAOTIC MAPS

Definition 1: Chebyshev polynomial is presented as:

$$T_n(x) = \cos(n \cdot \arccos(x)), \quad x \in [-1, 1]$$

We calculate the first six terms:

$$\begin{aligned} T_0(x) &= 1 \\ T_1(x) &= x \\ T_2(x) &= 2x^2 - 1 \\ T_3(x) &= 4x^3 - 3x \\ T_4(x) &= 8x^4 - 8x^2 + 1 \\ T_5(x) &= 16x^5 - 20x^3 + 5x \end{aligned}$$

From first six recurrent terms, Chebyshev polynomial is expressed as:

$$T_n(x) = 2xT_n(x) - T_{n-2}(x), (n \geq 2)$$

The semi group property and chaos property are two primary properties possessed in Chebyshev polynomial.

Definition 2 (Semi Group Property):

$$\begin{aligned} T_g(T_h(x)) &= \cos(g \cdot \arccos(\cos(h \cdot \arccos(x)))) \\ T_h(T_g(x)) &= \cos(h \cdot \arccos(\cos(g \cdot \arccos(x)))) \\ T_g(T_h(x)) &= T_h(T_g(x)) \end{aligned}$$

Definition 3 (Chao Property): The Chebyshev polynomials map $T_n(x) : [-1, 1] \rightarrow [-1, 1]$ of degree $n > 1$ is a chaotic map with invariant density as: $\partial(x) = 1/\pi\sqrt{1 - x^2}$ for the Lyapunov exponent $\lambda = \ln n$.

B. ENHANCED CHEBYSHEV CHAOTIC MAPS

Definition 1 (Enhanced Chebyshev Polynomial is Expressed as):

$$T_n(x) = 2xT_n(x) - T_{n-2}(x) \bmod q$$

where q is a large prime and $x \in (-\infty, +\infty)$ [19]. The enhanced Chebyshev chaotic maps still has semi group property and chaos property.

Definition 2 (DLP): Given α and β, it is unable to compute an integer λ to compute $T_\lambda(\alpha) \bmod q = \beta$.

Definition 3 (DHP): Given α, $T_\lambda(\alpha)$ and $T_\beta(\alpha)$, it is unable to compute $T_{\lambda\beta}(\alpha)$.

C. HASH FUNCTION

Hash function plays a very important role in the field of modern cryptography and information security. Messages of arbitrary length are compacted into a fixed-length bit string by a specific hash function. Let the function $H : \{0, 1\}^\alpha \rightarrow \{0, 1\}^n$ is a hash function with an output length of n, and then the function H satisfies hashing, resistance to weak (strong) collision, one-way and validity, details see references [29], [30].

III. UNDERWATER MODEL AND REQUIREMENTS

In this section, we first present network model, communication model and threat model. Next, we propose the security requirements and goals.

A. NETWORK MODEL

There are four parties in our proposed scheme that the RC(Registration Center), the gateway node(GWN), the user and the sensor nodes(SNs). The registration center is only for off-line registration of the sensor nodes and the gateway nodes, and does not participate in the communication process. In fact, only three parties that the sensor nodes, the gateway nodes and the users send messages to each other.

The gateway node is a trustful party with larger memory and higher security, which is used to validate the user and the sensor node by swapping messages between the user and the sensor nodes, perform mutual authentication and negotiate session key.

The sensor node is a specific sensor device with restricted resource, which is often placed in a hostile and unattended underwater environment to gather data.

The user first needs to register at the gateway node and then becomes a valid user through mutual authentication and finally gets the information gathered by the sensor nodes.

B. COMMUNICATION MODEL

We consider an underwater acoustic communication model with four messages interchange in our proposed scheme as shown in figure 1. By conducting two full rounds of four messages flows [33], the user, the gateway node and the sensor node are able to successfully validate each other. The

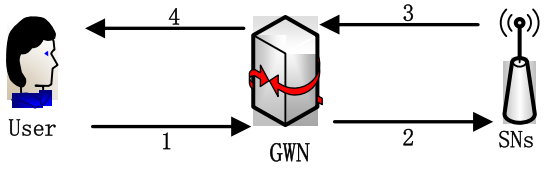

FIGURE 1. Communication model.

TABLE 2. Security requirements and goals.

Security requirements	Security goals
SR1: Man-in-the-middle attack	SG1: Perfect forward security
SR2: Node capture attack	SG2: Integrity of information
SR3: Gateway by pass attack	SG3: Sound reparability and scalability
SR4: Denial of service attack	SG4: Timely error detection
SR5: Traceability attack	SG5: Mutual authentication
SR6: Smart card loss attack	SG6: Sensor node anonymity
SR7: Replay attack	SG7: User anonymity
SR8: Session key attack	
SR9: Insider attack	
SR10: User impersonation attack	

user dispatches the login request message $\{LH_6, LH_{10}, T_1\}$ to the GWN. The GWN dispatches the message $\{LH_{15}, T_2\}$ to the sensor node. The sensor node dispatches the message $\{LH_{17}, LH_{19}, LH_{20}, T_3\}$ to the GWN. The GWN dispatches the message $\{LH_{21}, LH_{22}, LH_{17}, T_4\}$ to the user.

C. THREAT MODEL

We consider the threat model for designing our scheme similar to that in [32].

D. SECURITY REQUIREMENTS AND GOALS

In 2012, Madhusudhan and Mittal [31] advanced a new standard of nine security requirements and ten goals for a secure remote user authentication mechanism. In 2016, Wang and Wang [32] indicated that though the standard advanced in literature [31] is superior to the others, it still has redundancies and ignores some intrinsic collisions among the standard. The author then proposed twelve independent evaluation criteria. In 2018, Wang *et al.* [33] made some simple modifications on these twelve criteria. We refer to the above standards and according to the characteristics of underwater acoustic communication, the evaluation standards in our proposed scheme should meet the following security requirements and goals.

IV. OUR PROPORSED SCHEME

There are eight sections in our scheme: initialization section, gateway node registration section, sensor node registration section, user registration section, login section, authentication and key management section, sensor node section, password change section.

A. INITIALIZATION SECTION

Step1: The RC(Registration Center) freely chooses a high entropy integer x.

Step2: The RC randomly choose c as its private key, and computes $Q_{RC} = T_c(x) \bmod q$ as its public key, where q is a large prime number.

Step3: The RC chooses a hash function $h()$ and keeps c secretly. Then, RC publishes parameter $\{q, x, Q_{RC}, h()\}$.

B. GATEWAY NODE REGISTRATION

Step1: The RC chooses $GWID_k$ as an identity for the gateway node, and computes $Gw_k = h(GWID_k||c)$.

Step2: The RC sends $(GWID_k, Gw_k)$ to the gateway node.

C. SENSOR NODE REGISTRATION

Step1: The RC chooses $SNID_j$ as an identity for the sensor node, and according to topological relationship, computes

$$S_j = h(SNID_j||GWID_k||c).$$

Step2: The RC sends $(SNID_j, S_j)$ to the sensor node.

The registration of the sensor node and the gateway node is executed in a safe off-line environment prior to their deployment in the target topology area. After completing the above tasks, the RC sends the information $(SNID_j, S_j)$ to the gateway node according to topological relationship. The gateway node stores $\{GWID_k, Gw_k, SNID_j, S_j\}$ in the memory safely.

D. USER REGISTRATION

Step1: The user freely chooses his identity ID_i, one random number r_i, his password PW_i, and the other random number r_p.

Step2: The user computes $RID_i = h(ID_i||r_i)$, $RPW_i = h(PW_i||r_p)$ and sends the request (RID_i, RPW_i) to the gateway node via a safe channel.

Step3: After getting the request message, the gateway node generates a random number g and computes $LH_0 = T_g(x) \bmod q$, $LH_1 = h(RID_i||GWID_k) \oplus h(RPW_i||g)$, $LH_2 = h(Gw_k) \oplus h(RID_i||RPW_i)$. The gateway node stores $\{h(), LH_1, LH_2\}$ in a smart card(SC) and issues SC to the user safely.

Step4: After getting the SC, the user computes $LH_3 = r_i \oplus h(ID_i||PW_i)$, $LH_4 = r_p \oplus h(ID_i||PW_i)$, $LH_5 = h(RID_i||r_i) \oplus h(RPW_i||r_p)$. The user issues $\{LH_3, LH_4, LH_5\}$ into smart card. Finally, SC includes $\{h(), LH_1, LH_2, LH_3, LH_4, LH_5\}$.

E. LOGIN SECTION

Step1: After inserting SC into the card reader of a specific terminal device, the user inputs his identity ID_i and password PW_i.

Step2: The SC computes: $r_i^* = LH_3 \oplus h(ID_i||PW_i)$, $r_p^* = LH_4 \oplus h(ID_i||PW_i)$, $RID_i^* = h(ID_i||r_i^*)$, $RPW_i^* = h(PW_i||r_p^*)$, $LH_5^* = h(RID_i^*||r_i^*) \oplus h(RPW_i^*||r_p^*)$.

Step3: The SC inspects that the equation $LH_5^* = LH_5$ is true or not. If the equation is true, the identity and password are validated successfully. If not, terminate this section instantaneously.

Step4: The SC produces a random digit rsc and computes $LH_6 = T_{rsc}(x) \bmod q$, $K_{U-G} = T_{rsc}T_g(x) \bmod q$, $LH_7 = LH_1 \oplus h(T_1)$, $LH_8 = LH_2 \oplus h(RID_i||RPW_i)$, $LH_9 = h(T_1||LH_1||LH_2)$, $LH_{10} = E_{K_{U-G}}(LH_7||LH_8||LH_9)$, where T_1 is the current timestamp.

Step5: The SC dispatches the login request message $\{LH_6, LH_{10}, T_1\}$ to the gateway node.

F. AUTHENTICATION AND KEY MANAGEMENT SECTION

Step1: After getting the login request message $\{LH_6, LH_{10}, T_1\}$, the gateway node first computes whether $T_2 - T_1 \leq \Delta T$ holds, where T_2 is the time when the gateway node gets the request message, and ΔT is the allowable maximum

TABLE 3. Login section.

User	GWN
Insert SC into the card reader and input ID_i and PW_i SC computes: $LH_6 = T_{rsc}(x) \bmod q$ $r_i^* = LH_3 \oplus h(ID_i \| PW_i)$ $r_p^* = LH_4 \oplus h(ID_i \| PW_i)$ $RID_i^* = h(ID_i \| r_i^*)$ $RPW_i^* = h(PW_i \| r_p^*)$ $LH_5^* = h(RID_i^* \| r_i^*) \oplus h(RPW_i^* \| r_p^*)$ Inspects the equation: $LH_5^* = LH_5$? SC produces a random digit *rsc* SC computes: $K_{U-G} = T_{rsc}T_g(x) \bmod q$ $LH_7 = LH_1 \oplus h(T_1)$ $LH_8 = LH_2 \oplus h(RID_i \| RPW_i)$ $LH_9 = h(T_1 \| LH_1 \| LH_2)$ $LH_{10} = E_{K_{U-G}}(LH_7 \| LH_8 \| LH_9)$ Sends $\{LH_6, LH_{10}, T_1\}$ to the GWN	

transmission time interval. If hold, proceed to the step2, if not, terminate this section instantaneously.

Step2: The gateway node computes $K_{U-G} = LH_6 \cdot LH_0 = T_{rsc}T_g(x) \bmod q$, $LH_{11} = D_{K_{U-G}}(LH_{10})$, decrypts LH_{10} with K_{U-G}, and then obtains $\{LH_7, LH_8, LH_9\}$.

Step3: The gateway node computes $LH_1^* = LH_7 \oplus h(T_1)$, $LH_2^* = LH_8 \oplus h(RID_i||RPW_i)$, $LH_9^* = h(T_1||LH_1^*||LH_2^*)$.

Step4: The gateway node inspects that the equation $LH_9^* = LH_9$ is true or not. If the equation holds, the user is validated successfully. If not, terminate this section instantaneously.

Step5: The gateway node computes $K_{G-S} = T_{S_j}T_g(x) \bmod q$, $LH_{12} = h(S_j) \oplus h(RID_i||RPW_i)$, $LH_{13} = h(SNID_j) \oplus h(Gw_k)$, $LH_{14} = LH_2 \oplus h(T_2)$, $LH_{15} = E_{K_{G-S}}(LH_{12}||LH_{13}||LH_{14})$, and dispatches the message $\{LH_{15}, T_2\}$ to the sensor node.

Step6: Upon getting the message $\{LH_{15}, T_2\}$ at time T_3, the sensor node checks the freshness of time T_2 by the means of $T_3 - T_2 \leq \Delta T$. If hold, proceed to the step7, if not, terminate this section instantaneously.

Step7: The sensor node computes $K_{G-S} = T_{S_j}T_g(x) \bmod q$, $LH_{16} = D_{K_{G-S}}(LH_{15})$, decrypts LH_{15} with K_{G-S}, and then obtains $\{LH_{12}, LH_{13}, LH_{14}, LH_6\}$.

Step8: The sensor node computes $h(RID_i||RPW_i)^* = h(S_j) \oplus LH_{12}$, $h(Gw_k)^* = h(SNID_j) \oplus LH_{13}$, $LH_{14}^* = h(Gw_k)^* \oplus h(RID_i||RPW_i)^* \oplus h(T_2)$.

Step9: The sensor node inspects that the equation $LH_{14}^* = LH_{14}$ is true or not. If the equation holds, the gateway node is validated successfully. If not, terminate this section instantaneously.

Step10: The sensor node produces a random digit *rsn* and computes: $LH_{17} = T_{rsn}(x) \bmod q$, $LH_{18} = T_{rsn}T_{rsc}(h(SNID_j||S_j)||h(Gw_k)||h(RID_i||RPW_i)) \bmod q$, $LH_{19} = h(LH_{18}||h(SNID_j||S_j)||h(T_2))$, $LH_{20} = h(SNID_j||S_j) \oplus h(T_3)$.

TABLE 4. The message from the gateway to the sensor node.

GWN	SN
Inspect: $T_2 - T_1 \leq \Delta T$ Computes: $K_{U-G} = T_{rsc}T_g(x) \bmod q$ Decrypts: LH_{10} Obtains: $\{LH_7, LH_8, LH_9\}$ Computes: $LH_1^* = LH_7 \oplus h(T_1)$ $LH_2^* = LH_8 \oplus h(RID_i \| RPW_i)$ $LH_9^* = h(T_1 \| LH_1^* \| LH_2^*)$. Inspects: $LH_9^* = LH_9$? Computes: $K_{G-S} = T_{S_j}T_g(x) \bmod q$ $LH_{12} = h(S_j) \oplus h(RID_i \| RPW_i)$ $LH_{13} = h(SNID_j) \oplus h(Gw_k)$ $LH_{14} = LH_2 \oplus h(T_2)$ $LH_{15} = E_{K_{G-S}}(LH_{12} \| LH_{13} \| LH_{14} \| LH_6)$ Sends $\{LH_{15}, T_2\}$ to the SN	

TABLE 5. The message from the sensor node to the gateway.

SN	GWN
Inspects: $T_3 - T_2 \leq \Delta T$ Computes: $K_{G-S} = T_{S_j}T_g(x) \bmod q$ Decrypts: LH_{15} Obtains: $\{LH_{12}, LH_{13}, LH_{14}, LH_6\}$. Computes: $h(RID_i \| RPW_i)^* = h(S_j) \oplus LH_{12}$ $h(Gw_k)^* = h(SNID_j) \oplus LH_{13}$ $LH_{14}^* = h(Gw_k)^* \oplus h(RID_i \| RPW_i)^* \oplus h(T_2)$. Inspects: $LH_{14}^* = LH_{14}$? Produces a random digit *rsn* Computes: $LH_{17} = T_{rsn}(x) \bmod q$ $LH_{18} = T_{rsn}T_{rsc}(h(SNID_j \| S_j) \| h(Gw_k) \| h(RID_i \| RPW_i)) \bmod q$ $LH_{19} = h(LH_{18} \| h(SNID_j \| S_j) \| h(T_2))$ $LH_{20} = h(SNID_j \| S_j) \oplus h(T_3)$ Sends $\{LH_{17}, LH_{19}, LH_{20}, T_3\}$ to the GWN	

The sensor node dispatches the message $\{LH_{17}, LH_{19}, LH_{20}, T_3\}$ to the gateway node.

Step11: Upon getting the message $\{LH_{17}, LH_{19}, LH_{20}, T_3\}$ at time T_4, the gateway node checks the freshness of time T_3 by the means of $T_4 - T_3 \leq \Delta T$. If hold, proceed to the step12, if not, terminate this section instantaneously.

TABLE 6. The message from the gateway to the user.

GWN	User
Inspects: $T_4 - T_3 \le \Delta T$ Computes: $h(SNID_j \| S_j)^* = LH_{20} \oplus h(T_3)$, $LH_{18}^* = T_{rsn}T_{rsc}(h(SNID_j \| S_j)^* \| h(Gw_k) \| h(RID_i \| RPW_i)) \bmod q$ $LH_{19}^* = h(LH_{18}^* \| h(SNID_j \| S_j)^* \| h(T_2))$ Inspects: LH_{19}^*=LH_{19} ? Computes: $LH_{21} = h(SNID_j \| S_j) \oplus h(T_4)$ $LH_{22} = h(h(SNID_j \| S_j) \| h(T_1) \| LH_{18} \| h(Gw_k))$ Sends $\{LH_{21}, LH_{22}, LH_{17}, T_4\}$ to the user	

Step12: The gateway node computes $h(SNID_j||S_j)^* = LH_{20} \oplus h(T_3)$, $LH_{18}^* = T_{rsn}T_{rsc}(h(SNID_j||S_j)^*||h(Gw_k)||h(RID_i||RPW_i)) \bmod q$, $LH_{19}^* = h(LH_{18}^*||h(SNID_j||S_j)^*||h(T_2))$.

Step13: The gateway node inspects that the equation $LH_{19}^* = LH_{19}$ is true or not. If the equation is true, the sensor node is validated successfully. If not, terminate this section instantaneously.

Step14: The gateway node computes LH_{21}=$h(SNID_j||S_j)\oplus h(T_4)$, $LH_{22} = h(h(SNID_j||S_j)||h(T_1)||LH_{18}||h(Gw_k))$. The gateway node dispatches the message $\{LH_{21}, LH_{22}, LH_{17}, T_4\}$ to the user.

Step15: Upon getting the message $\{LH_{21}, LH_{22}, LH_{17}, T_4\}$ at time T_5, the SC checks the freshness of time T_4 by the means of $T_5 - T_4 \le \Delta T$. If hold, proceed to the step16, if not, terminate this section instantaneously.

Step16: The SC computes: $h(SNID_j||S_j)^* = LH_{21} \oplus h(T_4)$, $h(Gw_k)^* = LH_2 \oplus h(RID_i||RPW_i)$, $LH_{18}^* = T_{rsn}T_{rsc}(h(SNID_j||S_j)^*||h(Gw_k)^*||h(RID_i||RPW_i)) \bmod q$, $LH_{22}^* = h(h(SNID_j||S_j)^*||h(T_1)||LH_{18}^*||h(Gw_k)^*)$.

Step17: The user inspects that the equation $LH_{22}^* = LH_{22}$ is true or not. If the equation is true, the user validates both the gateway node and the sensor node successfully. If not, terminate this section instantaneously. Thus, we have established mutual authentication among the user, the gateway and the sensor node in our scheme and negotiated a session key $SK = LH_{18}$.

G. SENSOR NODE ADDITION SECTION

After forming the underwater wireless sensor network, a new node is likely to be putted in the target topology area because the sensor nodes are small devices with confining energy and memory [4], [12]. For the sake of adding new nodes to the target topology area, the RC executes the 4.3 section in a safe off-line environment prior to their deployment in the target topology area. Therefore, the RC can successfully put the new sensor nodes into the target topology area after carrying out the sensor node registration section.

TABLE 7. The calculation of session key.

User	
Inspects: $T_5 - T_4 \le \Delta T$? Computes: $h(SNID_j \| S_j)^* = LH_{21} \oplus h(T_4)$ $h(Gw_k)^* = LH_2 \oplus h(RID_i \| RPW_i)$ $LH_{18}^* = T_{rsn}T_{rsc}(h(SNID_j \| S_j)^* \| h(Gw_k)^* \| h(RID_i \| RPW_i)) \bmod q$ $LH_{22}^* = h(h(SNID_j \| S_j)^* \| h(T_1) \| LH_{18}^* \| h(Gw_k)^*)$ Inspects: $LH_{22}^* = LH_{22}$? Negotiates session key: $SK = LH_{18}$	

H. PASSWORD MODIFICATION SECTION

When the user is prepared to change his primitive password PW_i to a new password PW_i^{new}, the user executes the following steps.

Step1: After inserting SC into the card reader of a specific end, the user inputs his identity ID_i and password PW_i.

Step2: The SC computes: $r_i^* = LH_3 \oplus h(ID_i||PW_i)$, $r_p^* = LH_4 \oplus h(ID_i||PW_i)$, $RID_i^* = h(ID_i||r_i^*)$, $RPW_i^* = h(PW_i||r_p^*)$, $LH_5^* = h(RID_i^*||r_i^*) \oplus h(RPW_i^*||r_i^*)$.

Step3: The SC inspects that the equation $LH_5^* = LH_5$ is true or not. If the equation is true, the identity and password are validated successfully. If not, terminate this section instantaneously.

Step4: The user inputs a new password PW_i^{new} and random digit r_p^{mew}. Next, The SC computes $RPW_i^{new} = h(PW_i^{new}||r_p^{new})$, $LH_1^{new} = LH_1 \oplus h(RPW_i||g) \oplus h(RPW_i^{new}||g)$, $LH_2^{new} = LH_2 \oplus h(RID_i||RPW_i) \oplus h(RID_i||RPW_i^{new})$, $LH_3^{new} = LH_3 \oplus h(ID_i||PW_i) \oplus h(ID_i||PW_i^{new})$, $LH_4^{new} = r_p^{new} \oplus h(ID_i||PW_i^{new})$, $LH_5^{new} = LH_5 \oplus h(RPW_i||r_p) \oplus h(RPW_i^{new}||r_p^{new})$.

Step5: The SC will replace the corresponding parameters.

V. SECURITY ANALYSIS

In this section, we will apply the BAN logic and Random Oracle Model as the formal analysis and informal analysis to verify that our proposed scheme is robust and secure against various attacks.

A. SECURITY PROOF BASED ON BAN-LOGIC

BAN-login is used for checking out the validity and practicality of the proposed scheme in tripartite mutual authentication and key agreement among the user, the gateway node and the sensor node.

Some symbols needed in the BAN-logic are represented as follows, where $\mathbb{N}$ and $\mathbb{R}$ denote statements, ρ denotes a principal, and K_{x-y} is a notation for cryptographic encryption key.

1. $\rho| \equiv \mathbb{N}$: Principal ρ believes $\mathbb{N}$ is genuine.
2. $\rho \lhd \mathbb{N}$: Principal ρ receives a message containing $\mathbb{N}$, that is, principal β sends a message containing $\mathbb{N}$ to ρ.

3. $\rho| \sim \mathbb{N}$: Principal ρ has sent a message containing $\mathbb{N}$.
4. $\rho| \Rightarrow \mathbb{N}$: Principal ρ has jurisdiction over $\mathbb{N}$.
5. #($\mathbb{N}$): $\mathbb{N}$ is fresh, that is, $\mathbb{N}$ has not been sent as part of a message before the current round, where $\mathbb{N}$ is generally a temporary value.
6. $\rho \overset{K}{\longleftrightarrow} \beta$: K is the shared key between principal ρ and principal β, and no one knows K except principal ρ and principal β and their trust principals.
7. $\{\mathbb{N}\}_K$: Encrypt $\mathbb{N}$ with key K.
8. $< \mathbb{N} >_{\mathbb{R}}$: The combination of $\mathbb{N}$ and $\mathbb{R}$.

Then, we introduce some significant BAN logic postulates rules as below:

Rule(1). Message-meaning rule: $\frac{\rho| \equiv \rho \overset{K}{\longleftrightarrow} \beta, \rho \lhd \{\mathbb{N}\}_K}{\rho| \equiv \rho \sim \mathbb{N}}$.

Rule(2). Nonce-verification rule: $\frac{\rho| \equiv \#\mathbb{N}, \rho| \equiv \beta \sim \mathbb{N}}{\rho| \equiv \beta| \equiv \mathbb{N}}$

Rule(3). Jurisdiction rule: $\frac{\rho| \equiv \beta| \equiv \mathbb{N}, \rho| \equiv \beta \Rightarrow \mathbb{N}}{\rho| \equiv \mathbb{N}}$

Rule(4). Freshness rule: $\frac{\rho| \equiv \# \mathbb{N}}{\rho| \equiv \#(\mathbb{N}, \mathbb{R})}$

Rule(5). Belief rule: $\frac{\rho| \equiv \beta| \equiv (\mathbb{N}, \mathbb{R})}{\rho| \equiv \beta| \equiv \mathbb{N}}$

On the basis of BAN logic, we ought to achieve eight authentication goals to verify that our scheme is safe.

Goa1: $GW_k| \equiv (U_i \overset{K_{U-G}}{\longleftrightarrow} GW_k)$
Goa2: $GW_k| \equiv U_i| \equiv (U_i \overset{K_{U-G}}{\longleftrightarrow} GW_k)$
Goa3: $SN_j| \equiv (GW_k \overset{K_{G-S}}{\longleftrightarrow} SN_j)$
Goa4: $SN_j| \equiv GW_k| \equiv (GW_k \overset{K_{G-S}}{\longleftrightarrow} SN_j)$
Goa5: $GW_k| \equiv (SN_j \overset{K_{G-S}}{\longleftrightarrow} GW_k)$
Goa6: $GW_k| \equiv SN_j| \equiv (SN_j \overset{K_{G-S}}{\longleftrightarrow} GW_k)$
Goa7: $U_i| \equiv (GW_k \overset{K_{U-G}}{\longleftrightarrow} U_i)$
Goa8: $U_i| \equiv GW_k| \equiv (GW_k \overset{K_{U-G}}{\longleftrightarrow} U_i)$

Next, we make some evident and essential presumptions to explicate our proposed scheme.

P1: $U_i| \equiv \#(T_1)$
P2: $U_i| \equiv (U_i \overset{K_{U-G}}{\longleftrightarrow} GW_k)$
P3: $U_i| \equiv \#(T_4)$
P4: $U_i| \equiv GW_k \Rightarrow (GW_k \overset{K_{U-G}}{\longleftrightarrow} U_i)$
P5: $GW_k| \equiv \#(g)$
P6: $GW_k| \equiv \#(S_j)$
P7: $GW_k| \equiv \#(T_2)$
P8: $GW_k| \equiv (U_i \overset{T_{rsc}(x) \bmod q}{\longleftrightarrow} GW_k)$
P9: $GW_k| \equiv U_i \Rightarrow (GW_k \overset{K_{U-G}}{\longleftrightarrow} U_i)$
P10: $GW_k| \equiv SN_j \Rightarrow (SN_j \overset{K_{G-S}}{\longleftrightarrow} GW_k)$
P11: $GW_k| \equiv \#(SNID_j)$
P12: $GW_k| \equiv (SN_j \overset{T_{S_j}(x) \bmod q}{\longleftrightarrow} Gw_k)$
P13: $SN_j| \equiv \#(SNID_j)$
P14: $SN_j| \equiv \#(S_j)$
P15: $SN_j| \equiv \#(g)$
P16: $SN_j| \equiv GW_k \Rightarrow (GW_k \overset{K_{G-S}}{\longleftrightarrow} SN_j)$
P17: $SN_j| \equiv (GW_k \overset{LH_0}{\longleftrightarrow} SN_j)$

Here, we show the four idealized modality of the transmitted messages sequences among the user U_i, the gateway node GW_k and the sensor node SN_j. M1 is from the user to the gateway node. M2 is from the gateway node to the sensor node. M3 is from the sensor node to the gateway node. M4 is from the gateway node to the user.

M1: $U_i \rightarrow GW_k : (LH_6, LH_{10}, T_1) < \{((RID_i, GWID_k), (RPW_i, g), T_1), (((RID_i, RPW_i), Gw_k), \quad (RID_i, RPW_i)), (T_1, LH_1, LH_2)\}_{LH6}, LH6, T_1 >$

In the light of M1, we are able to gain
S1: $GW_k \lhd < LH_6, LH_{10}, T_1 >$
In the light of S1, P8 and R(1), we are able to gain
S2: $GW_k| \equiv U_i \sim < LH_7, LH_8, LH_9 >$
In the light of P5, R(4), we are able to gain
S3: $GW_k| \equiv \#(RID_i, GWID_k, RPW_i, g, T_1, Gw_k)$
In the light of S3, S2 and R(2), we are able to gain
S4: $GW_k| \equiv U_i| \equiv (RID_i, GWID_k, RPW_i, g, T_1, Gw_k)$
In the light of S4 and $K_{U-G} = T_{rsc}T_g(x) \bmod p$, we are able to gain
S5: $GW_k| \equiv U_i| \equiv (U_i \overset{K_{U-G}}{\longleftrightarrow} GW_k)$ **Goal 2**
In the light of S5, P9 and R(3), we are able to gain
S6: $GW_k| \equiv (U_i \overset{K_{U-G}}{\longleftrightarrow} GW_k)$ **Goal 1**

M2: $GW_k \rightarrow SN_j : (LH_{15}, T_2) < \{((RID_i, RPW_i), S_j), (SNID_j, Gw_k), (((RID_i, RPW_i), Gw_k), T_2)\} >$

In the light of M2, we are able to gain
S7: $SN_j \lhd < LH_{15}, T_2 >$
In the light of S7, P17 and R(1), we are able to gain
S8: $SN_j| \equiv GW_k \sim < LH_{12}, LH_{13}, LH_{14}, LH_6 >$
In the light of P13, P14, P15 and R(4) we are able to gain
S9: $SN_j| \equiv \#(RID_i, RPW_i, S_j, SNID_j, Gw_k, g, T_2)$
In the light of S9, S3 and R(2), we are able to gain
S10: $SN_j| \equiv GW_k| \equiv (RID_i, RPW_i, S_j, SNID_j, Gw_k, g, T_2)$
In the light of S10 and $K_{G-S} = T_gT_{S_j}(x) \bmod p$, we are able to gain
S11: $SN_j| \equiv GW_k| \equiv (GW_k \overset{K_{G-S}}{\longleftrightarrow} SN_j)$ **Goal 4**
In the light of S11, P16 and R(3), we are able to gain
S12: $SN_j| \equiv (GW_k \overset{K_{G-S}}{\longleftrightarrow} SN_j)$ **Goal 3**

M3: $SN_j \rightarrow GW_k : (LH_{17}, LH_{19}, LH_{20}, T_3) < \{SK, (SK, (SNID_j, S_j), T_2), ((SNID_j, S_j), T_3)\}, T_{rsn}(x) \bmod q, T_3 >$

In the light of M3, we are able to gain
S13: $GW_k \lhd < LH_{17}, LH_{19}, LH_{20}, T_3 >$
In the light of S13, P12 and R(1), we are able to gain
S14: $GW_k| \equiv SN_j \sim < LH_{17}, LH_{19}, LH_{20} >$
In the light of P5, P6, P7 and R(4), we are able to gain
S15: $GW_k| \equiv \#(SK, SNID_j, S_j, T_2, T_3, g)$
In the light of S14, S15 and R(2), we are able to gain
S16: $GW_k| \equiv SN_j| \equiv (SK, SNID_j, S_j, T_2, T_3, g)$
In the light of S16 and $K_{G-S} = T_gT_{S_j}(x) \bmod p$, we are able to gain
S17: $GW_k| \equiv SN_j| \equiv (SN_j \overset{K_{G-S}}{\longleftrightarrow} GW_k)$ **Goal 6**
In the light of S17, P10 and R(3), we are able to gain
S18: $GW_k| \equiv (SN_j \overset{K_{G-S}}{\longleftrightarrow} GW_k)$ **Goal 5**

M4: $GW_k \rightarrow U_i : (LH_{17}, LH_{21}, LH_{22}, T_4) < (T_{rsn}(x) \bmod q), ((SNID_j, S_j), T_4), ((SNID_j, S_j), T_1, SK, Gw_k), T_4 >$

In the light of M4, we are able to gain
S19: $U_i \lhd < LH_{17}, LH_{21}, LH_{22}, T_4, GW_k \overset{K_{U-G}}{\longleftrightarrow} U_i >$
In the light of S19, P2 and R(1), we are able to gain

S20: $U_i| \equiv GW_k \sim< LH_{17}, LH_{21}, LH_{22}, T_4, GW_k \overset{K_{U-G}}{\longleftrightarrow} U_i >$

In the light of P1, P3 and R(4), we are able to gain

S21: $U_i| \equiv \#(T_{rsn}(x) \bmod q, SNID_j, S_j, T_1, T_4, SK, GW_k \overset{K_{U-G}}{\longleftrightarrow} U_i)$

In the light of S22, S21and R(2), we are able to gain

S22: $U_i| \equiv GW_k| \equiv (T_{rsn}(x) \bmod q, SNID_j, S_j, T_1, T_4, SK, GW_k \overset{K_{U-G}}{\longleftrightarrow} U_i)$

In the light of S22, we are able to gain

S23: $U_i| \equiv GW_k| \equiv (GW_k \overset{K_{U-G}}{\longleftrightarrow} U_i)$ **Goal 8**

In the light of S23, P4 and R(3), we are able to gain

S24: $U_i| \equiv (GW_k \overset{K_{U-G}}{\longleftrightarrow} U_i)$ **Goal 7**

B. SECURITY PROOF BASED ON RANDOM ORACLE MODEL

In this part, we perform the formal security analysis of our scheme applying the random oracle model to verify that our proposed scheme is robust and safe. We employ the similar method as shown in [11], [34]–[38]. We present two random oracles:

Reveal: This random oracle will unconditionally output fixed-length bit string μ from the designated hash function $\mu = h(\gamma)$.

Extract: This random oracle will unconditionally output λ from the designated chaotic map $T_\lambda(x) \bmod q = \beta$.

Theorem 1: Under the assumption that the one-way hash function, DLP and DHP closely behave like a random oracle, then our proposed scheme is provably secure against an aggressor obtaining the session key among the user, the gateway and the sensor node.

Proof: Using the upper random oracles to construct an aggressor Γ who is able to derive the identity of a rightful user, the secret key session key among the user, the gateway and the sensor node. The aggressor Γ apply the random oracles to operate the experimental algorithm $EXP^{HASH,DLP,DHP}_{RMACCMUA}$ for our proposed remote mutual authentication scheme based on chaotic maps for underwater acoustic networks, which is presented in Algorithm1. Let us define the success probability for $EXP^{HASH,DLP,DHP}_{RMACCMUA}$ as $succ = |\Pr|EXP^{HASH,DLP,DHP}_{RMACCMUA} = 1| - 1|$ where, $\Pr[E]$ denotes the probability of an event E. We define $Adv(et, q_R, q_E) = \max_A\{succ\}$ as the advantage function for this experiment, where the maximum is defined overall Γ with execution time et, and the number of queries q_R and q_E made to the Reveal and Extract. Our scheme is verified robust and secure against an aggressor Γ for session key if $Adv(et, q_R, q_E) \leq \varepsilon$, for any sufficiently small $\varepsilon > 0$. In this experiment, if the aggressor Γ is able to invert the one-way hash function $h()$ and crack DLP and DHP, then he can successfully obtain communication session key and win the game. Nevertheless, it is noticeable that the execution of inverting the hash function and cracking DLP and DHP is impracticable in polynomial time. In other words, $Adv^{HASH}_\Gamma(t1) \leq \varepsilon$ and $Adv^{DLP,DHP}_\Gamma(t2) \leq \varepsilon$ for any sufficiently small $\varepsilon > 0$ according to the section 2.3, Definition 2 and Definition 3. Therefore, we have $Adv(et, q_R, q_E) \leq \varepsilon$. This verifies that our proposed scheme is provably robust and secure against an adversary for deriving session key.

Algorithm 1 $EXP^{HASH,DLP,DHP}_{RMACCMUA}$

1: Eavesdrop the message $\{LH_6, LH_{10}, T_1\}$, $\{LH_{15}, T_2\}$, $\{LH_{17}, LH_{19}, LH_{20}, T_3\}$, $\{LH_{21}, LH_{22}, LH_{17}, T_4\}$ during the login and authentication section.
2: Call Extract on LH_6 and get $rsc^* \leftarrow$ Reveal(LH_6)
3: Call Extract on LH_0 and get $g^* \leftarrow$ Reveal(LH_0)
4: call Reveal on input LH_8 to get RID_i, RPW_i as $(RID^*_i||RPW^*_i) \leftarrow$ Reveal(LH_8)
5: if $(Gw^*_k = Gw_k)$ then
6: computes: $LH^*_2 = h(Gw^*_k) \oplus h(RID^*_i||RPW^*_i)$
7: if $(GWID^*_k = GWID_k)$ then
8: computers: $LH^*_1 = h(RPW^*_i||g^*) \oplus h(GWID^*_k||RID^*_i)$
9: if $T^*_1 = T_1$ then
10: computes $LH^*_9 = h(T^*_1||LH^*_1||LH^*_2)$
11: Call Reveal on LH_{12} and get $S^*_j \leftarrow$ Reveal(LH_{12})
12: Call Reveal on LH_{13} and get $SNID^*_j \leftarrow$ Reveal(LH_{13})
13: if $(T^*_2 = T_2)$ then
14: computes: $LH^*_{14} = LH^*_2 \oplus h(T^*_2)$
15: Call Extract on LH^*_{17} and get $rsn^* \leftarrow$ Reveal(LH^*_{17})
16: compute: $LH^*_{18} = T_{rsn}T_{rsc}(h(SNID_j||S_j)^*||h(Gw_k)||h(RID_i||RPW_i)) \bmod q$
17: if $(LH^*_{19} = LH_{19})$ then
18: get the shared session key among user, gateway and sensor node.
19: else return 0
20: end if
21: else return 0
22: end if
23: else return 0
24: end if
25: else return 0
26: end if
27: else return 0
28: end if

VI. INFORMAL ANALYSIS AND DISCUSSION

In this section, through the informal security analysis and discussion we show that our proposed scheme is robust and is able to withstand various attacks.

A. USER ANONYMITY

Our proposed scheme provides the anonymity for the user identity in the exchange of transmitted information. The user computes $RID_i = h(ID_i||r_i)$ in the registration section and $LH_9 = h(T_1||LH_1||LH_2)$ in the login section. The aggressor cannot get the r_i because of the one-way hash function and cannot obtain the g because of the discrete logarithm. So, our proposed scheme fulfill the characteristics of user anonymity.

B. SENSOR NODE ANONYMITY

Sensor node anonymity is that the sensor node's authentic identity is concealed. In our proposed scheme, the sensor node's real identity $SNID_j$ does not save any information, and any aggressor is unable to get the sensor node's real identity straight from the communication information. Because the sensor node registration is executed in a secure off-line environment prior to their deployment in the target topology area, without knowing the private key of the RC and the identity of target gateway node, it is impractical for the aggressor to get the authentic identity saved in $S_j = h(SNID_j||GWID_k||c)$. So, our proposed scheme fulfill the characteristics of sensor node anonymity.

C. MUTUAL AUTHENTICATION

Mutual authentication denotes that the user, the gateway node and the sensor node in UANs are able to authenticate each other. In the user registration section, after getting the registration request message (RID_i, RPW_i), the gateway node generates a random digit g and computes $\{LH_0, LH_1, LH_2\}$. In the user login section, the SC inspects that the equation $LH_5^* = LH_5$ is true or not. If the equation is true, the identity and password are validated successfully. Then, the SC produces a random digit rsc and computes $LH_6, K_{U-G}, LH_7, LH_8, LH_9, LH_{10}$. The SC dispatches the login request message $\{LH_6, LH_{10}, T_1\}$ to the gateway node.

In the authentication and key management section, the gateway node computes K_{U-G}, decrypts LH_{10} with K_{U-G}, and then obtains $\{LH_7, LH_8, LH_9\}$. The gateway node inspects that the equation $LH_9^* = LH_9$ is true or not. If the equations holds, the user is validated successfully. After that, the gateway node computes $K_{G-S}, LH_{12}, LH_{13}, LH_{14}$ and dispatches message $\{LH_{15}, T_2\}$ to the sensor node. The sensor node computes K_{G-S}, decrypts LH_{15} with K_{G-S}, and then obtains $\{LH_{12}, LH_{13}, LH_{14}, LH_6\}$. The sensor node inspects that the equation $LH_{14}^* = LH_{14}$ is true or not. If the equations holds, the gateway node is validated successfully. Then, the sensor node produces a random digit rsn and computes $LH_{18}, LH_{19}, LH_{20}$. The sensor node dispatches the message $\{LH_{17}, LH_{19}, LH_{20}, T_3\}$ to the gateway node. After getting the message, the gateway node inspects that the equation $LH_{19}^* = LH_{19}$ is true or not. If the equations holds, the sensor node is validated successfully. The gateway node computes LH_{21}, LH_{22}, and dispatches message $\{LH_{21}, LH_{22}, LH_{17}, T_4\}$ to the user. After getting the message $\{LH_{21}, LH_{22}, LH_{17}, T_4\}$, the user inspects that the equation $LH_{22}^* = LH_{22}$ is true or not. If the equation is true, the user validates both the gateway node and the sensor node successfully.

D. INSIDER/USER IMPERSONATION ATTACK

In our proposed scheme, an aggressor is unable to imitate the user. Supposing an inner aggressor intends to imitate the user, he needs to get $LH_9 = h(T_1||LH_1||LH_2)$, $LH_{10} = E_{K_{U-G}}(LH_7||LH_8||LH_9)$, in other words, an inner aggressor requires to get the secret value $\{rsc, g, RID_i, RPW_i\}$. Only the legal user is aware of the values $\{rsc, r_i, r_p\}$, and the gateway node will compute and inspect LH_9. It is impractical for the inner aggressor to get the precise values $\{rsc, r_i, r_p\}$ in polynomial time. Therefore, the aggressor is unable to imitate the user because he is unable to get the precise secret values from the transmitted information between the user and the gateway node. Similarly, the aggressor is unable to imitate other communications.

E. SESSION KEY ATTACK

After finishing the mutual authentication, our scheme negotiates a robust session key $SK = LH_{18} = T_{rsn}T_{rsc}(h(SNID_j||S_j)||h(Gw_k)||h(RID_i||RPW_i)) \bmod q$ to transmit information safely. As we can see, the session key is shielded by hash function, DLP and DHP. If an aggressor plans to get the session key, he is obliged to get the covert parameters $\{SNID_j, S_j, Gw_k, RID_i, RPW_i, q, rsc, rsn\}$. In order to get the aforementioned parameters, an aggressor must try various ways to get $\{SNID_j, c, GWID_k, ID_i, r_i, PW_i, r_q, q, rsc, rsn\}$, it is impractical to the get aforementioned parameters in polynomial time. Hence, the session key in our proposed scheme is safe enough.

F. REPLAY ATTACK

In our proposed scheme, we apply the timestamp method to guarantee the freshness of transmitted messages. If an aggressor transmits the captured history information to the communication partner, the session will be terminated instantaneously, because the threshold time is greater than ΔT. If an aggressor fabricates the transmitted information $\{LH_{17}, LH_{19}, LH_{20}, T_3\}$ in the public channel with the current timestamps T_a, he first gets $\{rsn, rsc, SNID_j, S_j, Gw_k, RID_i, RPW_i, T_2\}$. Nevertheless, it is impractical to get the aforementioned parameters in polynomial time. Even though the aggressor fabricates the transmitted information $\{LH_{17}, LH_{19}, LH_{20}, T_3\}$, the gateway node will inspect that the equation $LH_{19}^* = LH_{19}$ is true or not. Similarly, the aggressor is unable to replay or fabricate other information flows. Hence, Our proposed scheme is able to boycott replay attacks.

G. SMART CARD LOSS ATTACK

In our proposed scheme, we use smart card to achieve mutual authentication. So, we ought to consider the situation that the smart card is lost. The SC include $\{h(), LH_1, LH_2, LH_3, LH_4, LH_5\}$, where, $LH_1 = h(RID_i||RPW_i) \oplus h(RPW_i||g)$, $LH_2 = h(Gw_k) \oplus h(RID_i||RPW_i)$, $LH_3 = r_i \oplus h(ID_i||PW_i)$, $LH_4 = r_p \oplus h(ID_i||PW_i)$, $LH_5 = h(RID_i||r_i) \oplus h(RPW_i||r_i)$, r_i, r_p and g are the random digits produced by the user and the gateway node separately. If the parameters are divulged, the aggressor has no opportunity to get any valuable information about LH_2, because he cannot crack the RC to get the private key c and also has no chance to get identity and password from LH_1, because he cannot invert the hash function in a valid polynomial time. In summary,

even though the smart card is lost, our proposed scheme is still robust and can boycott the smart card loss attack.

H. TRACEABILITY ATTACK

Traceability is that an aggressor can follow the sensor node and the user in diverse sessions section. The sensor node produces random digit rsn and computes $T_{rsn}(x) \bmod q$. The user produces random digit rsc and computes $T_{rsc}(x) \bmod q$. Finally, the session key between the user and the sensor node is $LH_{18} = T_{rsn}T_{rsc}(h(SNID_j||S_j)||h(Gw_k)||h(RID_i||RPW_i)) \bmod q$. The diverse users have diverse RID_i, RPW_i and the different sensor nodes have diverse $SNID_j, S_j$, which makes the session key is different in different communications. It is impractical for the aggressor to trace the user and the sensor node. Therefore, our proposed scheme can boycott the tracking attacks against the user and the sensor node.

I. DENIAL OF SERVICE ATTACK

In our proposed scheme, we devise a smart card pre-authentication mechanism during the login section to inspect the legitimacy of user at the login terminal. After inserting SC into the card reader of a specific terminal device, the user inputs his identity ID_i and password PW_i. The SC computes $r_i^* = LH_3 \oplus h(ID_i||PW_i), r_p^* = LH_4 \oplus h(ID_i||PW_i), RID_i^* = h(ID_i||r_i^*), RPW_i^* = h(PW_i||r_p^*), LH_5^* = h(RID_i^*||r_i^*) \oplus h(RPW_i^*||r_i^*)$ and compares the value LH_5^* with the locally stored value LH_5. Only all the information is correct, the equation $LH_5^* = LH_5$ hold. The SC can directly inspect the validity of the user without transmitting any information. Denial of service attack cannot be implemented by continuously inputting false identity and password. Therefore, through the smart card pre-authentication mechanism, our protocol is able to boycott denial of service attack.

J. GATEWAY BY PASS ATTACK

Supposing an aggressor succeed in catching the message $\{LH_{15}, T_2\}$ transmitted from the gateway node to the sensor node in public channel, where $LH_{15} = E_{K_{G-S}}(LH_{12}||LH_{13}||LH_{14}||LH_6)$. Subsequently, the aggressor fabricates the other message $\{LH_{15}, T_2\}$ and dispatches to the destination node. If the sensor node treats the message $\{LH_{15}^*, T_2\}$ as legitimate information, the aggressor successfully masquerade himself as a legal gateway. Nevertheless, if the aggressor wants to compute $\{LH_{15}^*, T_2\}$, he has to compute $K_{G-S} = T_{S_j}T_g(x) \bmod q, LH_{12} = h(S_j) \oplus h(RID_i||RPW_i), LH_{13} = h(SNID_j) \oplus h(Gw_k), LH_{14} = LH_2 \oplus h(T_2)$. However, the calculation of LH_{12}, LH_{13} and LH_{14} must depends on parameters $\{RID_i, RPW_i, S_j\}, \{SNID_j, Gw_k\}, \{RID_i, RPW_i, Gw_k\}$ respectively. It is apparent that the aggressor is unable to acquire the aforementioned parameters because of the property of the irreversible hash function, DLP and DHP. Similarly, the aggressor is unable to fabricate other gateway nodes information flows. Therefore, our proposed scheme can boycott the gateway by pass attack.

K. NODE CAPTURE ATTACK

Supposing an aggressor succeed in catching a sensor node stochastically in the destination field. As the sensor nodes are not loaded with tamper-resistant hardware, the aggressor is able to acquire all the secret information stored in the sensor node containing the random digit rsn, S_j and session key. In our proposed scheme, every sensor node has its own identity $SNID_j$ and related S_j. The session key is produced by using the random digits rsn and rsc. Every session key is diverse between the user and the sensor node. The sensor node is dispatched with $(SNID_j, S_j)$ prior to their deployment in the target topology area and the aggressor is able to acquire the secret information $(SNID_j, S_j)$ of the captured sensor node merely. Nevertheless, Other sensor nodes that are not caught are still able to safely exchange information with the lawful users. Consequently, the caught sensor node will not divulge any useful information about the other non-caught sensor nodes. Hence, our proposed scheme can boycott the node capture attack.

L. MAN-IN-THE-MIDDL ATTACK

Man-in-the-middle attack means that an aggressor masquerades himself as a legal participant in the process of authentication. In our proposed scheme, M3 is information from the sensor node to the gateway node. If the aggressor is intends to disguises himself as a legitimate sensor node, he needs to construct the message $\{LH_{17}, LH_{19}, LH_{20}, T_3\}$, where $LH_{20} = h(SNID_j||S_j) \oplus h(T_3), LH_{19} = h(LH_{18}||h(SNID_j||S_j)||h(T_2))$, in other words, the aggressor needs to gain initial values $\{SNID_j, GWID_k, c, ID_i, r_i, PW_i, r_p, rsc, rsn\}$. Among them, r_i and r_p are random digits that cannot be completed by random guessing at the same time. It is impractical for the aggressor to compute the parameters $\{c, rsc, rsn\}$ in polynomial time according to DLP and DHP. Besides, the aggressor is unable to compute the $SK = LH_{18} = T_{rsn}T_{rsc}(h(SNID_j||S_j)||h(Gw_k)||h(RID_i||RPW_i)) \bmod q$, because the rsc and rsn are provisionally produced random digits in every session. Therefore, the aggressor cannot masquerade himself as a legal participant and our proposed scheme is able to boycott the man-in-the-middle attack.

M. PERFECT FORWARD SECURITY

In our proposed scheme, the session key between the user and the sensor node is computed: $RID_i = h(ID_i||r_i), RPW_i = h(PW_i||r_p), Gw_k = h(GWID_k||c), LH_6 = T_{rsc}(x) \bmod q, LH_{17} = T_{rsn}(x) \bmod q, SK = LH_{18} = T_{rsn}T_{rsc}(h(SNID_j||S_j)||h(Gw_k)||h(RID_i||RPW_i)) \bmod q$.

Even though the private key of gateway node g is divulged, an aggressor is unable to get rsc and rsn to calculate the session key between the user and the sensor node. The session key depends on the DLP and DHP. An aggressor is unable to get rsn from $LH_{17} = T_{rsn}(x) \bmod q$ and rsc from $LH_6 = T_{rsc}(x) \bmod q$ in polynomial time. Hence, our proposed scheme is able to offer perfect forward security.

N. INTEGRITY OF INFORMATION

In our proposed scheme, we apply encryption and verification to guarantee the integrity of the transmitted information. In our tripartite mutual authentication scheme, the dispatched information from the user to the gateway node is encrypted with K_{U-G} and verified by LH_9. The dispatched information from the gateway node to the sensor node is encrypted with K_{G-S} and verified by LH_{14}. The dispatched information from the sensor node to the gateway node is verified by LH_{19}. The dispatched information from the gateway node to the user is verified by LH_{22}. If any bit information is lost or wrong during transmission, the equation fails and the receiver will reject the request and terminate the session instantaneously. Therefore, our proposed scheme is able to guarantee the integrity of the transmitted information.

O. SOUND REPARABILITY AND SCALABILITY

In our scheme, the user is able to change his primitive password PW_i to a new password PW_i^{new} freely and safely and the completion of password modification does not require any aid from the gateway node. Furthermore, the aggressor has no ability to revise the password even thought he gains the smart card and the password, which is because the inexact password and random digit will be inspected the equation LH_5^*.

After forming the underwater wireless sensor network, a new node is likely to be putted in the target topology area because the sensor nodes are small devices with confining energy. For the sake of adding new nodes to the target topology area, the RC executes the sensor node registration section in a safe off-line environment prior to their deployment in the target topology area. Therefore, the RC can successfully put the new sensor nodes into the target topology area after carrying out the 4.3 section. In conclusion, our proposed scheme realizes the sound reparability and scalability.

P. TIMELY ERROR DETECTION

In our proposed scheme, no matter what is wrong, the scheme will detect it timely. In the login section, we devise a smart card pre-authentication mechanism to inspect the legitimacy of the user at the login terminal. In the authentication and key agreement section, the first message is from the user to the gateway node, the second is from the gateway node to the sensor node, the third is from sensor node to the gateway node and the last message is from the gateway node to the user. When the gateway node gets the message from the user, if in step1 $T_2 - T_1 > \Delta T$ and in step4 $LH_9^* \neq LH_9$, the scheme will timely detect error and terminates communication instantaneously. When the sensor node obtains the message from the gateway node, if in step6 $T_3 - T_2 > \Delta T$ and in step9 $LH_{14}^* \neq LH_{14}$, the scheme will timely detect that there is something wrong and terminate the communication at once. When the gateway node receives the message from the sensor node, if in step11 $T_4 - T_3 > \Delta T$ and in step13 $LH_{19}^* \neq LH_{19}$, the scheme will timely detect that the message is not right and terminates the communication right away. When the user acquires the message from the gateway node, if in step15 $T_5 - T_4 > \Delta T$ and in step18 $LH_{22}^* \neq LH_{22}$, the scheme will timely detect that the message is incomplete and terminate the communication immediately. In summary, our proposed scheme has the ability to detect errors timely.

VII. COMPARISON

This section contrasts our proposed scheme with other correlative schemes [15], [39], [20], [19], [40] in the aspects of security, computation and storage in the login and authentication sections, which are analyzed in 7.1 security comparison, 7.2 computation comparison and 7.3 storage comparison in detail. The reason why we choose these schemes for comparison is that these schemes are all three-party communication based on chaotic map.

A. SECURITY COMPARISION

In this portion, we will contrast the security of our proposed scheme with other schemes [15], [39], [20], [19], [40] in table 8.

TABLE 8. The security comparison.

	[15]	[39]	[20]	[19]	[40]	Ours
S1	F	T	T	T	F	T
S2	F	F	F	F	F	T
S3	T	T	F	F	F	T
S4	F	T	F	F	F	T
S5	F	T	T	F	F	T
S6	T	T	F	F	T	T
S7	T	F	F	T	T	T
S8	T	T	T	T	T	T
S9	F	T	T	F	T	T
S10	F	T	T	T	T	T
S11	T	F	F	T	T	T
S12	F	F	F	F	F	T
S13	F	F	F	F	F	T
S14	T	F	F	F	F	T
S15	T	T	T	T	T	T
S16	F	T	F	F	F	T
S17	T	T	T	F	T	T

S1: Man-in-the-middle attack. S2: Node capture attack. S3: Gateway by pass attack. S4: Denial of service attack.S5: Traceability attack. S6: Smart card loss attack. S7: Replay attack. S8: Session key attack. S9: Insider attack. S10: user impersonation attack. S11: Perfect forward security. S12: Integrity of information.S13: Sound reparability and scalability. S14: Timely error detection. S15: Mutual authentication. S16: Sensor node anonymity. S17: User anonymity. T:can. F: cannot or not mention.

As shown in the table 8, our proposed scheme is able to boycott multiple attacks and meet more security goals contrasted with other previous schemes [15], [39], [20], [19], [40]. Our scheme and the other schemes both have ability to meet S8 and S15,while the other schemes all have no ability to meet S2, S12 and S13. Schemes [15], [40] cannot resist man-in-middle attack, and also schemes [20], [19], [40] will suffer from the gateway by pass attack. Our proposed scheme and scheme [2] can avoid denial of service attack, while schemes [15], [19], [40] will sustain traceability attack. Schemes [39], [20] fail to withstand replay attack and perfect forward security, while schemes [20], [19] are subjected to smart card loss attack. Schemes [15], [19] fail to resist insider

TABLE 9. Computation comparison.

scheme	User	SN(User)	GW(server)	Total	Time
[15]	4h+2c+2s	3h+2c	6h+2s	13h+4c+4s	3.109ms
[39]	7h+2s	6h+1s	7h+1s	20h+4s	1.5ms
[20]	4h+4c+2s	(4h+3c+2s)	(4h+4c+4s)	12h+11c+8s	7.136ms
[19]	5h+3c+2s	(5h+3c+2s)	(4h+2c+4s)	14h+8c+8s	5.822ms
[40]	10h+3c	8h+2c	11h+1c	29h+6c	3.717ms
Ours	11h+2c+1s	5h+2c+1s	11h+3c+2s	27h+7c+4s	4.951ms

TABLE 10. Storage comparison.

Storage comparison								
	User storage		SN(User) storage		GW(Server) storage		SC storage	Total storage
scheme	Dispatching	Getting	Dispatching	Getting	Dispatching	Getting		
[15]	448bit	320bit	320bit	448bit	448bit	448bit	640	2432bit
[39]	384bit	256bit	256bit	384bit	384bit	384bit	896	2048bit
[20]	384bit	256bit	(768bit)	(640bit)	(256bit)	(512bit)	0	2816bit
[19]	448bit	256bit	(896bit)	(704it)	(256bit)	(640bit)	0	3200bit
[40]	512bit	640bit	768bit	704bit	1344bit	1280bit	640	5248bit
Ours	288bit	416bit	416bit	160bit	576bit	704bit	640	2560bit

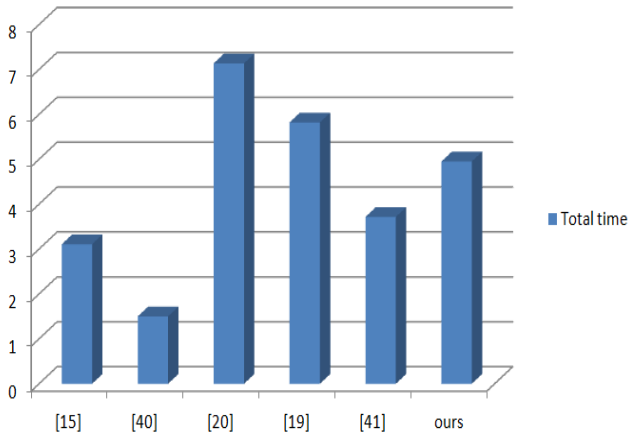

FIGURE 2. Computation comparison.

attack and only scheme [15] cannot withstand user impersonation attack. Only scheme [15] and our scheme realize timely error detection function. Only scheme [39] and our scheme achieve sensor node anonymity, while only scheme [19] do not implement user anonymity.

B. COMPUTATION COMPARISION

In this portion, we will contrast the computation of our proposed scheme with other schemes [15], [39], [20], [19], [40] in table 9 and figure 2. Since the time for computing XOR operation and string concatenation is ignored as compared with the other operations[16], [26], [40], we only consider the time to calculate one-way hash function, Chebyshev polynomial and symmetric key encryption/ decryption. For comparing the computation cost with other schemes, all operations were implemented at IDEA jdk 1.8.0_60 using an Intel(R)Core(TM)i5-42102M CPU @ 2.60GHz with 8G memory in win7 64-bit. The computational times of hash function, Symmetric encryption/decryption and Chebyshev polynomial are approximately 0.033ms, 0.21ms and 0.46ms respectively.

Since the scheme [39] only employ the hash function and symmetric key encryption/ decryption operations, scheme [39] takes the least time. Although the scheme [40] merely apply the hash function and chaotic maps, the computing time is still longer than scheme [15]. Schemes [15], [20], [19] and our proposed scheme all require hash function, chaotic maps and symmetric key encryption/ decryption three operations to achieve mutual authentication. Compared with the schemes [15], our scheme needs more time to complete mutual authentication. However, the number of exchange messages in our scheme is four, scheme [15] requires three messages exchange to accomplish mutual authentication. Compared with the schemes [19], [20], the computational scheme is more efficient and applies UANs.

C. STORAGE COMPARISION

In this portion, we will contrast the storage of our proposed scheme with other schemes [15], [39], [20], [19], [40] in the login and authentication section in table 10 and figure 3.

We suppose that user identity and password are 64 bits, the timestamp is 32 bits, the other values are all 128 bits. In our scheme, the smart card contains the elements $\{h(), LH_1, LH_2, LH_3, LH_4, LH_5\}$, so the smart card storage cost is 640$(128 + 128 + 128 + 128 + 128)$ bits, which is the same as schemes [15], [40], but lower than schemes [39]. The schemes [19], [20] do not make use of smart card.

User dispatches the message $\{LH_6, LH_{10}, T_1\}$ to the gateway node and the storage cost is 288$(128 + 128 + 32)$ bits.

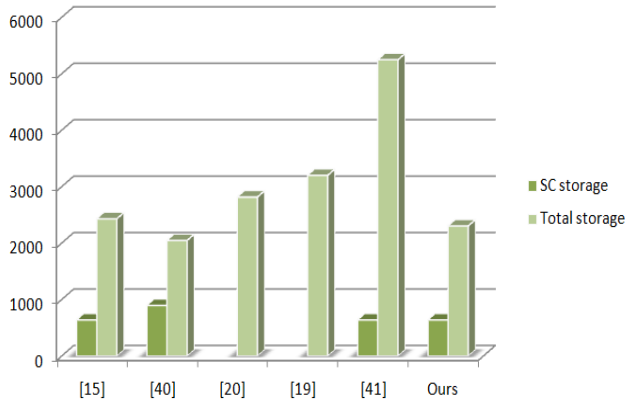

FIGURE 3. Storage comparison.

User gets the message $\{LH_{21}, LH_{22}, LH_{17}, T_4\}$ from the gateway node and the storage cost is $416(128 + 128 + 128 + 32)$ bits.

Gateway node dispatches the message $\{LH_{15}, T_2\}$ to the sensor node and the cost is $160(128+32)$ bits. Gateway node dispatches the message $\{LH_{21}, LH_{22}, LH_{17}, T_4\}$ to the user and the cost is $416(128 + 128 + 123 + 32)$ bits. Gateway node gets the message $\{LH_6, LH_{10}, T_1\}$ from user and the cost is $288(128 + 128 + 32)$ bits. Gateway node gets the message $\{LH_{17}, LH_{19}, LH_{20}, T_3\}$ from sensor node and the cost is $416(128 + 128 + 128 + 32)$ bits.

Sensor node dispatches the message $\{LH_{17}, LH_{19}, LH_{20}, T_3\}$ to the gateway node and the cost is $416(128+128+128+32)$ bits. Sensor node gets the message $\{LH_{15}, T_2\}$ from the gateway node and the cost is $160(128 + 32)$ bits.

Consequently, the total storage cost in our scheme is 2560 bits. We also calculate the total storage of other schemes in [15], [39], [20], [19], [40] separately. The energy is mainly consumed for dispatching/getting the message [41]. The total storage cost in our scheme is 2560bits, which is higher than schemes [15], [39], but lower than schemes [20], [19], [40]. Scheme [39] shows that scheme [15] is vulnerable to sensor node impersonation attack and man-in-the-middle attack. The number of transmitted messages in scheme [39] is three, however, our scheme demands four messages to finish mutual authentication, so our total storage is slightly higher than scheme [39].

VIII. CONCLUSION

In this article, we present a chaotic maps remote user authentication and key agreement scheme for underwater acoustic networks. Our scheme turns out to be robust and secure based on the DLP and DHP. By applying the BAN logic and random oracle model, we have certified that our scheme is able to accomplish mutual authentication and negotiate session key among the user, the gateway and the sensor node. We have showed that our proposed scheme is safe and can meet ten security requirements and seven security goals. Besides, our scheme is more efficient compared with the other previous schemes.

REFERENCES

[1] C. Peng, X. Du, K. Li, and M. Li, "An ultra-lightweight encryption scheme in underwater acoustic networks," *J. Sensors*, vol. 2016, pp. 1–10, Mar. 2016.
[2] G. Han, J. Jiang, N. Sun, and L. Shu, "Secure communication for underwater acoustic sensor networks," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 54–60, Aug. 2015.
[3] E. Souza, H. C. Wong, I. Cunha, A. A. F. Loureiro, L. F. M. Vieira, and L. B. Oliveira, "End-to-end authentication in under-water sensor networks," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2013, pp. 000299–000304.
[4] X. Du, C. Peng, and K. Li, "A secure routing scheme for underwater acoustic networks," *Int. J. Distrib. Sensor Netw.*, vol. 13, no. 6, pp. 1–13, Jun. 2017.
[5] R. Diamant, P. Casari, and S. Tomasin, "Cooperative authentication in underwater acoustic sensor networks," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 954–968, Feb. 2019.
[6] A. K. Das, "A secure and robust password-based remote user authentication scheme using smart cards for the integrated EPR information system," *J. Med. Syst.*, vol. 39, no. 3, p. 25, Mar. 2015.
[7] C.-T. Li, C.-Y. Weng, C.-C. Lee, and C.-C. Wang, "A hash based remote user authentication and authenticated key agreement scheme for the integrated EPR information system," *J. Med. Syst.*, vol. 39, no. 11, p. 144, Nov. 2015.
[8] J. Jung, D. Kang, D. Lee, and D. Won, "An improved and secure anonymous biometric-based user authentication with key agreement scheme for the integrated EPR information system," *PLoS ONE*, vol. 12, no. 1, 2017, Art. no. e0169414.
[9] A. M. Koya and P. P. Deepthi, "Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network," *Comput. Netw.*, vol. 140, pp. 138–151, Jul. 2018.
[10] C.-C. Chang and H.-D. Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 357–366, Jan. 2016.
[11] D. Kumar, S. Chand, and B. Kumar, "Cryptanalysis and improvement of an authentication protocol for wireless sensor networks applications like safety monitoring in coal mines," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 2, pp. 641–660, Feb. 2019.
[12] H.-Y. Lin, "Improved chaotic maps-based password-authenticated key agreement using smart cards," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 20, no. 2, pp. 482–488, Feb. 2015.
[13] H. Zhu, "Cryptanalysis and improvement of a mobile dynamic ID authenticated key agreement scheme based on chaotic maps," *Wireless Pers. Commun.*, vol. 85, no. 4, pp. 2141–2156, Dec. 2015.
[14] T.-T. Truong, M.-T. Tran, and A.-D. Duong, "Improved Chebyshev polynomials-based authentication scheme in client-server environment," *Secur. Commun. Netw.*, vol. 2019, pp. 1–11, Jan. 2019.
[15] S. Kumari, X. Li, F. Wu, A. K. Das, H. Arshad, and M. K. Khan, "A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps," *Future Gener. Comput. Syst.*, vol. 63, pp. 56–75, Oct. 2016.
[16] L. Zhang, H. Luo, L. Zhao, and Y. Zhang, "Privacy protection for point-of-care using chaotic maps-based authentication and key agreement," *J. Med. Syst.*, vol. 42, no. 12, p. 250, Dec. 2018.
[17] G. Gao, X. Peng, Y. Tian, and Z. Qin, "A chaotic maps-based authentication scheme for wireless body area networks," *Int. J. Distrib. Sensor Netw.*, vol. 12, no. 7, Jul. 2016, Art. no. 2174720.
[18] Q. Xie, B. Hu, X. Tan, and D. S. Wong, "Chaotic maps-based strong anonymous authentication scheme for roaming services in global mobility networks," *Wireless Pers. Commun.*, vol. 96, no. 4, pp. 5881–5896, Oct. 2017.
[19] Q. Xie, J. Zhao, and X. Yu, "Chaotic maps-based three-party password-authenticated key agreement scheme," *Nonlinear Dyn.*, vol. 74, no. 4, pp. 1021–1027, Dec. 2013.
[20] C.-C. Lee, C.-T. Li, S.-T. Chiu, and Y.-M. Lai, "A new three-party-authenticated key agreement scheme based on chaotic maps without password table," *Nonlinear Dyn.*, vol. 79, no. 4, pp. 2485–2495, Mar. 2015.
[21] A. Jabbari and J. B. Mohasefi, "Improvement in new three-party-authenticated key agreement scheme based on chaotic maps without password table," *Nonlinear Dyn.*, vol. 95, no. 4, pp. 3177–3191, Mar. 2019.
[22] M. Qi and J. Chen, "Anonymous biometrics-based authentication with key agreement scheme for multi-server environment using ECC," *Multimedia Tools Appl.*, vol. 78, no. 19, pp. 27553–27568, Oct. 2019.

[23] R. Ali, A. K. Pal, S. Kumari, M. Karuppiah, and M. Conti, "A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring," *Future Gener. Comput. Syst.*, vol. 84, pp. 200–215, Jul. 2018.
[24] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K.-R. Choo, "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.
[25] A. Ghani, K. Mansoor, S. Mehmood, S. A. Chaudhry, A. U. Rahman, M. N. Saqib, "Security and key management in IoT-based wireless sensor networks: An authentication protocol using symmetric key," *Int. J. Commun. Syst.*, vol. 32, no. 16, p. e4139, 2019.
[26] S. Qiu, G. Xu, H. Ahmad, and L. Wang, "A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems," *IEEE Access*, vol. 6, pp. 7452–7463, 2017.
[27] S. Namasudra and P. Roy, "A new secure authentication scheme for cloud computing environment," *Concurrency Comput., Pract. Exper.*, vol. 29, no. 20, p. e3864, 2017.
[28] H. Lai, M. A. Orgun, J. Xiao, J. Pieprzyk, L. Xue, and Y. Yang, "Provably secure three-party key agreement protocol using Chebyshev chaotic maps in the standard model," *Nonlinear Dyn.*, vol. 77, no. 4, pp. 1427–1439, Sep. 2014.
[29] M. Gohar, F. Bashir, J.-G. Choi, S.-J. Koh, and W. Ahmad, "A hash-based distributed mapping control scheme in mobile locator-identifier separation protocol networks," *Int. J. Netw. Manage.*, vol. 27, no. 2, p. e1961, Mar. 2017.
[30] S. Jangirala, S. Mukhopadhyay, and A. K. Das, "A multi-server environment with secure and efficient remote user authentication scheme based on dynamic ID using smart cards," *Wireless Pers. Commun.*, vol. 95, no. 3, pp. 2735–2767, Aug. 2017.
[31] R. Madhusudhan and R. C. Mittal, "Dynamic ID-based remote user password authentication schemes using smart cards: A review," *J. Netw. Comput. Appl.*, vol. 35, no. 4, pp. 1235–1248, Jul. 2012.
[32] D. Wang and P. Wang, "Two birds with one stone: Two-factor authentication with security beyond conventional bound," *IEEE Trans. Depend. Sec. Comput.*, vol. 15, no. 4, pp. 708–722, Jul./Aug. 2015.
[33] D. Wang, W. Li, and P. Wang, "Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 4081–4092, Sep. 2018.
[34] D. Mishra, A. K. Das, and S. Mukhopadhyay, "A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards," *Expert Syst. Appl.*, vol. 41, no. 18, pp. 8129–8143, 2014.
[35] Y. Lu, L. Li, H. Peng, and Y. Yang, "A secure and efficient mutual authentication scheme for session initiation protocol," *Peer-to-Peer Netw. Appl.*, vol. 9, no. 2, pp. 449–459, Mar. 2016.
[36] S. A. Chaudhry, I. Khan, A. Irshad, M. U. Ashraf, M. K. Khan, and H. F. Ahmad, "A provably secure anonymous authentication scheme for session initiation protocol," *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 5016–5027, 2016.
[37] J. Jung, J. Moon, D. Lee, and D. Won, "Efficient and security enhanced anonymous authentication with key agreement scheme in wireless sensor networks," *Sensors*, vol. 17, no. 3, p. 644, 2017.
[38] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and V. Gupta, "Design of a secure anonymity-preserving authentication scheme for session initiation protocol using elliptic curve cryptography," *J. Ambient Intell. Humanized Comput.*, vol. 9, no. 3, pp. 643–653, Jun. 2018.
[39] J. Li, W. Zhang, S. Kumari, K.-K.-R. Choo, and D. Hogrefe, "Security analysis and improvement of a mutual authentication and key agreement solution for wireless sensor networks using chaotic maps," *Trans. Emerg. Telecommun. Technol.*, vol. 29, no. 6, p. e3295, Jun. 2018.
[40] A. Irshad, S. A. Chaudhry, Q. Xie, X. Li, M. S. Farash, S. Kumari, and F. Wu, "An enhanced and provably secure chaotic map-based authenticated key agreement in multi-server architecture," *Arabian J. Sci. Eng.*, vol. 43, no. 2, pp. 811–828, Feb. 2018.
[41] R. Amin and G. P. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," *Ad Hoc Netw.*, vol. 36, no. 1, pp. 58–80, 2016.

SHUAILIANG ZHANG received the bachelor's degree in computer science and technology from the Henan Institute of Science and Technology, Xinxiang, China, in 2015. He is currently pursuing the Ph.D. degree in computer science and technology with Qinghai Normal University, Xining. His research interests include network and information security, wireless sensor networks, and underwater sensor networks.

XIUJUAN DU received the M.S. degree in radio physics from Lanzhou University, Lanzhou, China, and the Ph.D. degree in computer application technology from Tianjin University, Tianjin, China. She is currently a Professor with the Provincial Key Laboratory of the Internet of Things, Qinghai Normal University, Xining, China. Her research interests include network and information security, mobile ad hoc networks, and underwater sensor networks, including network modeling, network protocol design, performance evaluation, optimization algorithms, and distributed computing and their applications. She has received the New Century Excellent Talent from Education Ministry, China, in 2011.

XIN LIU received the bachelor's degree in computer science and technology from Shanxi University, Taiyuan, China, in 2004. She is currently pursuing the Ph.D. degree in computer science and technology with Qinghai Normal University, Xining, China. Her research interests include wireless sensor networks and underwater sensor networks, including network modeling and network protocol design.