Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

An improved Merkle hash tree based secure scheme for bionic underwater acoustic communication

Masoud KAVEH, Abolfazl FALAHATI[†‡]

Department of Electrical Engineering, Iran University of Science and Technology, Tehran 13114-16846, Iran

[†]E-mail: afalahati@iust.ac.ir

Received Jan. 24, 2020; Revision accepted June 23, 2020; Crosschecked Mar. 16, 2021

Abstract: Recently, bionic signals have been used to achieve covert underwater acoustic communication (UWAC) with high signal-to-noise ratios (SNRs) over transmission systems. A high SNR allows the attackers to proceed with their mischievous goals and makes transmission systems vulnerable against malicious attacks. In this paper we propose an improved Merkle hash tree based secure scheme that can resist current underwater attacks, i.e., replay attack, fabricated message attack, message-altering attack, and analyst attack. Security analysis is performed to prove that the proposed scheme can resist these types of attacks. Performance evaluations show that the proposed scheme can meet UWAC limitations due to its efficiency regarding energy consumption, communication overhead, and computation cost.

Key words: Dolphin whistle; Improved Merkle hash tree; Secure underwater acoustic communication (UWAC)
https://doi.org/10.1631/FITEE.2000043 **CLC number:** TP309; TN929.3

1 Introduction

Underwater acoustic communication (UWAC) systems require more effort than ground-based wireless systems. Because of the high energy absorption of water, acoustic signals are used instead of radio waves, which provides many handicaps, such as exceptional multipath propagation interference (Falahati et al., 1991; Zielinski et al., 1995), low communication bandwidth, long propagation delays, high bit error rates, and very noisy environments (van Walree and Otnes, 2013; Mosavi et al., 2018). Due to these unique characteristics, UWAC is very vulnerable to malicious attacks.

Many schemes have been proposed for covert UWAC within the last few years, such as direct sequence spread spectrum (DSSS) (Yang and Yang, 2008; Mosavi et al., 2016). The most challenging problem of such schemes is the high signal-to-noise ratio (SNR) requirement to successfully communicate messages, but the high SNR exposes the communication system to possible attacks. The employment of a pseudo-random feature and the high probability of eavesdropping by trained sonar operators are other drawbacks of such schemes. Therefore, there are many incentives to use underwater bionic signals to achieve a secure UWAC link. In other words, instead of simply reducing the SNR of a transmission system to a certain minimum, some proposed schemes use a modulation waveform that naturally exists in the underwater environment (Liu et al., 2013b), such as sea lion (Jia et al., 2015) and dolphin sounds (Han X et al., 2014). This technique is an entirely different method to achieve covert UWAC.

The employment of dolphin sounds is currently popular (Liu et al., 2013a, 2016). The unique characteristics of dolphin sound components (clicks and whistles) make them ideal for secure UWAC. Thus, in addition to good covert performance at high SNRs, these components have the following beneficial features:

[‡] Corresponding author
ORCID: Abolfazl FALAHATI, https://orcid.org/0000-0003-1682-6563

1. Energy concentration at a 1 to 9 kHz frequency band (low-frequency characteristics), which is very appropriate for long-distance underwater transmission (Han GJ et al., 2015; Huang et al., 2016; Luo et al., 2016; Mobasseri and Lynch, 2016).

2. A significant reduction in the bit error rate due to the proper cross-correlation characteristics of these whistles (Li et al., 2015).

In this paper we propose a "secure" and "efficient" scheme according to the limitations of the designed UWAC system to resist possible attacks, i.e., replay attack, fabricated message attack, message-altering attack, and analyst attack.

An improved Merkle hash tree (MHT) is proposed for this issue. MHT (Merkle, 1980) is a hash-based authentication scheme that is commonly used in many applications (Mosavi and Kaveh, 2018). Furthermore, the Advanced Encryption Standard (AES) (Ferguson et al., 2001) is used to ensure the confidentiality of messages. "Efficient" indicates that the proposed secure scheme added to the system must be lightweight according to the limitations of the UWAC components. In addition, the energy consumption of the sub-surface systems must be considered because of their energy limitations, the narrowband UWAC communication channel, and the computation costs of the UWAC components. The proposed scheme is compared with the standard MHT (SMHT) based authentication (Mosavi and Kaveh, 2018) and Rivest-Shamir-Adleman (RSA) based authentication schemes (Rivest et al., 1978) in terms of energy efficiency, communication overhead, and computation cost. The contributions of this paper can be summarized as follows:

1. To achieve good covert performance of UWAC at high SNR levels, dolphin whistles are employed as an information career. Furthermore, deploying a bionic signal can remove the need of error correction codes and lead to reduced costs that can be added by an encryption system.

2. To achieve fully secure bionic-based UWAC, an improved MHT is proposed to resist these previously mentioned attacks. The lightweight design of the improved MHT permits the computation of every node in the tree with the least use of hash functions and can be used to easily obtain the root node value (X_1, 2^n). This allows the proposed method to perform as an efficient secure system according to UWAC channel limitations regarding energy efficiency, communication overhead, and computation cost.

2 Analysis of dolphin sounds

The sound signals of dolphins are divided into three types: clicks, whistles, and burst pulses. Clicks and whistles are used for localization and communication, respectively. The third type of sound signal is used for sending emergency and analog messages (Li et al., 2015). Click signals have durations that last from ten to a few hundred milliseconds. The duration of whistles lasts from hundreds of milliseconds to a few seconds.

Such communication signals resemble that of a narrowband frequency modulation (FM) waveform. In the proposed method, whistles are used for information transmission. Fig. 1 shows the recorded experimental period of dolphin whistles. Fig. 2 indicates that the energy of dolphin whistles is concentrated at

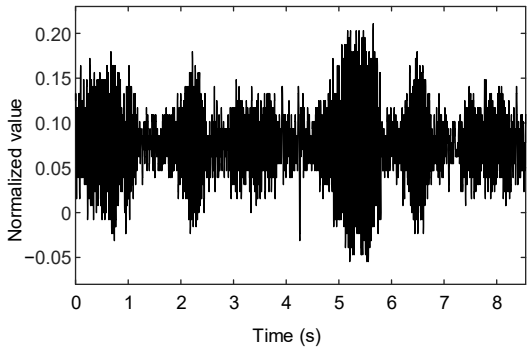

Fig. 1 Time duration waveform of a dolphin whistle

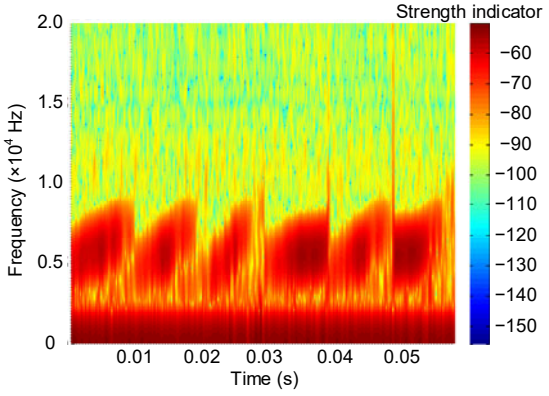

Fig. 2 Energy spectrogram from a time-frequency analysis of a dolphin whistle (References to color refer to the online version of this figure)

1–9 kHz (the short time Fourier transform of the recorded whistle).

Fig. 3 shows the timing delay of dolphin whistles for coding duration time T_{di}, which refers to each whistle signal that corresponds to a whistle time delay difference, and T_i is the duration of each whistle signal. According to the example in Fig. 1, the dolphin whistle sample includes six symbols with different information. These information symbols can be denoted as $W_1(t)$, $W_2(t)$, $W_3(t)$, $W_4(t)$, $W_5(t)$, and $W_6(t)$. Table 1 shows the normalized auto-correlation and cross-correlation coefficients of the six mentioned symbols.

First, at the transmitter end, serial information is converted into a parallel form. Based on the values of the parallel form of information, the whistle symbol selector determines which signal should be sent. The received signal is redeployed into N match-filters to perform the correlation calculations. Due to the good correlation characteristics of the whistles, the transmitted whistle will be easily determined, because the other (N−1) branches irrelevant with the transmitted whistle have too small correlation values. As a result, a good correlation performance of the whistle signals is a key point of the proposed scheme, guaranteeing the avoidance of generating error bits at the receiver end and consequently removing the overhead of the error correction codes from the system.

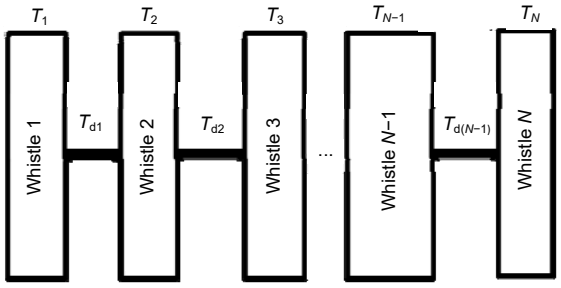

Fig. 3 The time delay coding scheme of dolphin whistles

Table 1 Correlation coefficients of the dolphin whistle

Signal	Correlation coefficient					
	$W_1(t)$	$W_2(t)$	$W_3(t)$	$W_4(t)$	$W_5(t)$	$W_6(t)$
$W_1(t)$	1.00	−0.16	0.08	−0.03	−0.18	0.00
$W_2(t)$	−0.16	1.00	−0.06	−0.20	0.14	0.04
$W_3(t)$	0.08	−0.06	1.00	0.02	−0.08	0.09
$W_4(t)$	−0.03	−0.20	0.02	1.00	0.16	0.00
$W_5(t)$	−0.18	0.14	−0.08	0.16	1.00	−0.08
$W_6(t)$	0.00	0.04	0.09	0.00	−0.08	1.00

In this study, a collection of whistle signals are chosen that have small cross-correlation coefficients based on the statistical properties of dolphin whistles listed in Table 1. $W_1(t)$, $W_3(t)$, $W_4(t)$, and $W_6(t)$ are used as communication signals. According to the transmitted information sequence, the signal selector chooses one from $W_1(t)$, $W_3(t)$, $W_4(t)$, and $W_6(t)$ and transmits the respective whistle. Therefore, the information carried by each signal is two bits. For example, assume that $W_1(t)$, $W_3(t)$, $W_4(t)$, and $W_6(t)$ are mapped to 00, 01, 10, and 11, respectively. To send the word "hi" with "01 10 10 00 01 10 10 01" binary codes, $W_3(t)$, $W_4(t)$, $W_4(t)$, $W_1(t)$, $W_3(t)$, $W_4(t)$, $W_4(t)$, and $W_3(t)$ should be sent, sequentially.

3 System and threat model

Consider a UWAC system with a populated friendly sub-surface, such as autonomous underwater vehicles (AUVs) and submarines, a surface command center (SCC), and an eavesdropper (Eve). An AUV can obtain data from the underwater environment or collect information from the sensor nodes (Ahmed et al., 2017). Every sub-surface has power-saving capabilities and is equipped with computation resources, sensing, and UWAC facilities. The computation efficiency and power consumption must be considered for the sub-surfaces because their computation and power resources are limited. SCC collects the reported data from sub-surfaces. Due to the arrival of too many reports, computation efficiency is a challenging problem for SCC as well. All reports indicate that the sub-surface information sent to SCC is featured with a certain format and SCC knows the format.

The UWAC system may be attacked by Eve who knows all of the UWAC information and can capture the communicated reports between the sub-surface and SCC. It is assumed that Eve can launch the following attacks (Jiang, 2019):

1. Replay attack. Eve can capture the previous message and then replays it to SCC. In other words, SCC receives the out-of-time message from Eve. Therefore, it is necessary to use an authentication scheme to identify the correct time of all received reports.

2. Fabricated message attack. In this case, SCC receives a bogus message from Eve that might affect SCC's decisions. Therefore, it is necessary to use an authentication scheme to identify illegal message sources and detect fabricated reports.

3. Message-altering attack. The reported messages from a sub-surface can be captured and tampered by Eve in the UWAC channel. If this happens, integrity will be compromised and SCC cannot access the correct information. Therefore, the techniques for ensuring the integrity of the messages must be considered.

4. Analyst attack. In this case, Eve eavesdrops the communicated messages from a sub-surface and tries to discover further details. Therefore, the confidentiality of the system is menaced, and as a result, the techniques must be used to make the system secure against a massage analysis attack.

4 Secure scheme proposed for UWAC

In this section, a secure scheme for UWAC is analyzed based on an improved MHT technique. MHTs are cryptographic hash based data structures that form as a tree. In this tree, each leaf node is considered a child and each non-leaf node is calculated from the hash of its children. The Merkle tree has a ramified factor of two; i.e., each non-leaf node has two children. The authentication path information (API) is the key point of MHT-based authentication that verifies each leaf node.

Fig. 4 shows an MHT with a height of three and eight leaves. The value of each internal node is derived from its children's nodes. For example, if we have h_i=Hash(D_i), the value of $h_{5,6}$ is equal to Hash($h_5||h_6$). In the given notations, Hash represents the cryptographic hash function, and the root node can be calculated as the same, i.e., $h_{1,8}$=Hash ($h_{1,4}||h_{5,8}$). An important point that should be considered is that every leaf node is verified with the root node and its corresponding API. For instance, if SCC stores $h_{1,8}$, the fifth sent data (D_5) from a sub-surface is authenticated by the corresponding API= {h_6, $h_{7,8}$, $h_{1,4}$}. In other words, SCC computes $h_{5,6}$=Hash($h_5||h_6$), $h_{5,8}$=Hash($h_{5,6}||h_{7,8}$), and $h_{1,8}$= Hash($h_{5,8}||h_{1,4}$) and compares the computed root value with the existing one. If the two root values are the same, then SCC accepts D_5.

An improved MHT is proposed in the rest of this section. If the proposed tree has height n, then it will have 2^n leaf nodes. The required ciphered messages, which must be produced by a tree, determine the value of n. For instance, if SCC wants to receive reports from each sub-surface every 12 min, there are 120 ciphered messages that are communicated between them in one day. Therefore, an MHT with n=7 indicates that 128 leaves are made.

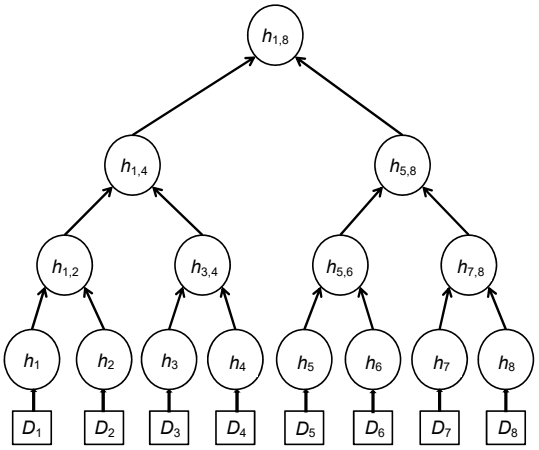

Fig. 4 A Merkle hash tree with a height of three and eight leaf nodes

Due to the cryptographic hash based scheme of the proposed method, it is necessary to show that a collision cannot occur; i.e., if h_i=Hash(D_i), there is no fabricated D_i^* that satisfies h_i=Hash$\left(D_i^*\right)$. Actually, we want to prove that the probability of Hash(D_i)= Hash$\left(D_i^*\right)$ is negligible. Suppose that h is a hash function that generates z-bit (z=2^q, $q\in\{1, 2, \ldots\}$) cryptographic hash values. Therefore, for a random message D, there are 2^z possible values for $h(D)$. In this study, we calculate how many fabricated messages may be delivered to SCC when a collision occurs. Let $P(u)$ denote the probability of more than one collision occurring when u fabricated messages have been sent to SCC, and E_u denotes the event that the i^{th} fabricated message collides with $h(D_i)$. Therefore, the following relationships are obtained (Diffie and Hellman, 1976):

$$\Pr[E_i]=(i-1)/2^z, \tag{1}$$

$$\begin{aligned} P(u) &= \Pr[E_1 \vee E_2 \vee ... \vee E_u] \\ &\le \Pr[E_1] \vee \Pr[E_2] \vee ... \vee \Pr[E_u] \\ &\le 0/2^z + 1/2^z + ... + (u-1)/2^z \\ &= u(u-1)/2^{z+1}. \end{aligned} \tag{2}$$

According to inequality (2), the upper bound for $P(u)$ grows with $O(2^{z-1}u^2)$. When $P(u)$ tends to 0.5, $u^2=2^z$, and thus $u=2^{z/2}$. Therefore, for the occurrence of a collision with a 50% chance, $2^{z/2}$ fabricated messages are needed to launch into SCC. For example, for z=128, Eve must launch 2^{64} fabricated messages for a collision to occur with a 50% chance in SCC. However, D_i varies every few minutes, and because of its time-limited period, the probability of a collision to occur is negligible. Hence, both the security and efficiency of UWAC are maintained. To prove this statement, security analyses of the proposed secure UWAC system are performed in Section 5.

Due to limited energy and computation resources in UWAC vehicles, we propose an improved MHT to increase the energy and computation efficiency.

Since every sub-surface simply collects underwater reports and performs XOR operation, its computation complexity may be very low. However, according to Fig. 4, SCC must compute three hashes to obtain the corresponding root value. Generally, for a tree with height n, SCC should cost n hashes to compute the root value of each message, and a larger n has a large computation cost. Therefore, we propose an improved MHT as shown in Fig. 5. According to Fig. 5, h_i=Hash(C_i) is first obtained. However, unlike Fig. 4 for computing the upper nodes, children perform XOR instead of hashing. This continues until the root value is achieved. For example, we had API$_5$={h_6, $h_{7,8}$, $h_{1,4}$} in Fig. 4, and the corresponding root value was computed as $h_{5,6}$=Hash(h_5||h_6), $h_{5,8}$=Hash($h_{5,6}$||$h_{7,8}$), and $h_{1,8}$=Hash($h_{1,4}$||$h_{5,8}$). Here, API$_5$ is {h_6, $X_{7,8}$, $X_{1,4}$}, and the corresponding root value, $X_{1,8}$, is computed as $X_{5,6}=h_5 \oplus h_6$, $X_{5,8}=h_{5,6} \oplus h_{7,8}$, and $X_{1,8}=h_{1,4} \oplus h_{5,8}$, where $\oplus$ represents the XOR operation. Thus, instead of using three hashes in this example, we can use only one. As a result, in an improved MHT with height n, the number of hashes used can be reduced to one for each root value computation.

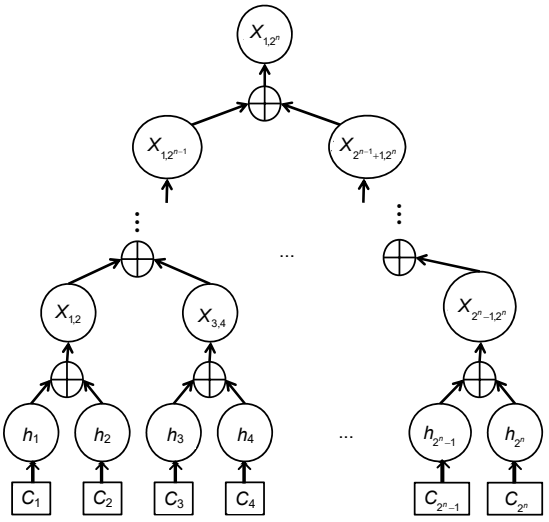

Fig. 5 An improved Merkle hash tree with height *n* and 2*n* leaf nodes

It is supposed that every sub-surface in the UWAC system S_j (j=1, 2, …, number of sub-surfaces) securely communicates with SCC through a secure key establishment protocol like the Diffie–Hellman key agreement scheme (Diffie and Hellman, 1976). Therefore, a session key, K_j, is shared between SCC and S_j. Also, AES is shared by SCC and S_j, and is a symmetric encryption (Enc) and decryption (Dec) algorithm.

According to Fig. 5, every sub-surface S_j constructs an improved MHT with 2^n leaves. S_j generates $C_i = \mathrm{Enc}_{K_j}(m_i \,||\, \mathrm{TS}_i)$, where m_i is the underwater report, TS$_i$ is the predefined time stamp, and i=1, 2, …, 2^n. Then, S_j can compute the 2^n leaf nodes by cryptographic one-way hash functions as h_i=Hash(C_i). By achieving real-time data collection and sending, the use of a time stamp is necessary for every message. Generally, every report sent by S_j can be dated by minute, day, month, and year. How long the time period is to send two consecutive reports and what kind of TS is used for each report should be noted to determine the value of n and the number of leaf nodes for the corresponding MHT. For example, if SCC receives reports from S_j every 12 min, there are 120 C_i, which are communicated between them in a day. Therefore, an MHT with a height of n=7 and 128 leaves can be made for S_j every day.

After computing leaf nodes h_i, the value of internal nodes is computed from their children nodes, e.g., for $X_{1,2}=h_1 \oplus h_2$ and $X_{2^{n-1},2^n} = X_{2^{n-1}} \oplus X_{2^n}$.

Therefore, S_j computes the values of the tree from its leaf nodes to the root node, recursively. The value of the root node can be computed as follows:

$$X_{1,2^n} = X_{1,2^{n-1}} \oplus X_{2^{n-1}+1,2^n}. \tag{3}$$

Within this context, S_j can create a set of data in the form of [C_i, API$_i$], where C and API represent the cipher text of TS||m and the authentication path information, respectively. In addition, S_j generates a cipher text C_{root_j} of the root node value $X_{1,2^n}$, i.e., $C_{\text{root}_j} = \text{Enc}_{K_j}(X_{1,2^n})$, where K_j is the session key and Enc is the AES encryption algorithm. SCC receives C_{root} and decrypts it, i.e., $X_{1,2^n} = \text{Dec}_{K_j}(C_{\text{root}_j})$ is used to obtain the root value. Then, SCC saves the corresponding root value for each sub-surface S_j. Now, S_j can send the set of [C_i, API$_i$] to SCC using dolphin whistles.

By authentically receiving the reports, SCC can perform the following steps:

1. SCC can detect the replay attack as shown in Fig. 6. For example, suppose that S_1 sends C_i to SCC, where Hash(C_i)=d. First, SCC checks the ID and confirms that it is S_1. Then, the corresponding set of previously received hash values is returned. If d is a member of the corresponding set of previously received hash values, then the replay attack will be detected. Assume that the set of previously received hashes is $\{c, d, e, f\}$. Then Hash(C_i) is compared with

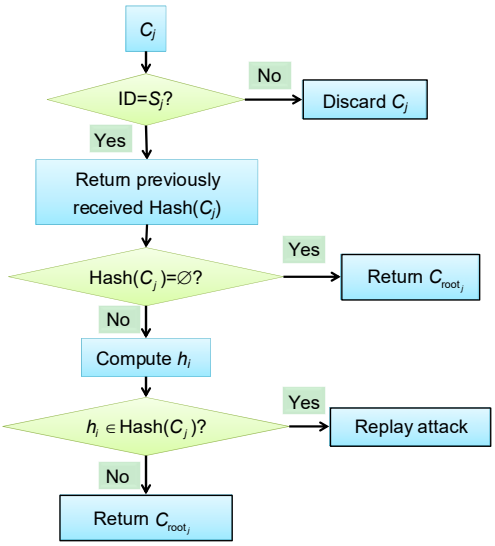

Fig. 6 Replay attack detection

all four parameters. Since d is a member of the mentioned set, C_i is considered a replayed message and SCC discards it.

2. SCC has to determine if the received report is from the sub-surfaces or from Eve. It is then necessary to authenticate the source of the messages. As previously stated, SCC receives C_{root_j} and [C_i, API$_i$]. With these hash values, SCC can perform message source authentication. For example, S_1 sends [C_1, API$_1$] to SCC, and since the SCC has saved the corresponding root node value $X_{1,2^n}$ before, SCC can now compute h_1=Hash(C_1). Furthermore, with $\text{API}_1=\{h_2, X_{3,4}, X_{5,8}, \cdots, X_{2^{n-1}+1,2^n}\}$, SCC can compute the corresponding root node value as

$$\begin{cases} X_{1,2} = h_1 \oplus h_2, \\ X_{1,4} = h_{1,2} \oplus h_{3,4}, \\ X_{1,8} = h_{1,4} \oplus h_{5,8}, \\ \quad \vdots \\ X_{1,2^{n-1}} = h_{1,2^{n-2}} \oplus h_{2^{n-2}+1,2^{n-1}}, \\ X_{1,2^n} = h_{1,2^{n-1}} \oplus h_{2^{n-1}+1,2^n}. \end{cases} \tag{4}$$

Next, SCC compares the computed $X_{1,2^n}$ with the stored one. If the two root node values are equal, then message source authentication is ensured and SCC accepts the report. In this case, SCC appends h_1 into a set of previously received hashes.

In addition to authentication, the proposed scheme ensures the confidentiality and integrity of the reports as well. Assume that Eve records the sent report and will recover the plaintext. Since the AES algorithm is secure (Ferguson et al., 2001), Eve cannot discover the plaintext without having the session key. Therefore, this scheme is confidential as long as the key is not leaked. However, SCC receives the cipher text C_i and obtains the plaintext by running the AES decryption algorithm, i.e., $m_i \,||\, \text{TS}_i = \text{Dec}_{K_j}(C_i)$. Because of the time delay propagation of the underwater acoustic environment, SCC checks the freshness of the received report according to the following inequality:

$$|\,\text{TS}_i - \text{TS}_{\text{local}}\,| \le \theta, \tag{5}$$

where TS_{local} is the current local time in SCC, and θ is a predefined threshold. If inequality (5) does not hold, SCC discards the report; otherwise, SCC compares the obtained plaintext m_i with the certain format of reports that are known by SCC. If the underwater report is featured in a special format, then SCC accepts it. Otherwise, the report is not interrogated and SCC discards it.

5 Security analysis

In this section, we indicate how the proposed scheme can resist the UWAC mentioned attacks including the replay attack, fabricated message attack, message-altering attack, and analyst attack.

5.1 Replay attack resistance

According to Fig. 6, SCC can detect a replay attack after receiving [C_i, API_i]. In more detail, it first computes Hash(C_i) and then compares it with a set of hash values of previously received reports. If any value in the mentioned set is not equal to Hash(C_i), it can be concluded that C_i is not replayed. However, if one of the hash values of the previously received reports is equal to Hash(C_i), the replay attack is detected and SCC discards the message. Therefore, the proposed scheme can resist the replay attack.

5.2 Fabricated message attack resistance

As previously mentioned and according to Eq. (4), SCC can authenticate the source of the received message after receiving [C_i, API_i], and after computing the corresponding root node value using Hash(C_i) and API_i, it compares the computed root node value $X_{1,2^n}$ with the stored one, i.e., C_{root_j}. If two mentioned values are equal, then SCC accepts the report. Otherwise, the fabricated message attack will be detected and SCC discards it. Note that Eve does not have any access to the stored database in sub-surfaces, and subsequently, she never knows their secret information. In addition, it is proved that MHT is secure (Merkle, 1980). Therefore, the proposed scheme fulfills requirements of message source authentication. Furthermore, inequality (2) proves that the probability of a collision occurring is negligible, and thus Eve cannot send a fabricated message C_i' to SCC where Hash(C_i)=Hash(C_i'). As a result, the proposed scheme resists the fabricated message attack.

5.3 Message-altering attack resistance

After the message and its source authentication are received, SCC decrypts C_i and obtains the plaintext by running the AES algorithm, i.e., $m_i \| TS_i = Dec_{K_j}(C_i)$. As previously mentioned, all reports that sub-surfaces send to SCC are in a certain format, and SCC knows the format. Therefore, SCC compares m_i with the stored format in its database and checks if m_i is featured in the format or not. If m_i is featured in the format, SCC accepts the report. Otherwise, a message-altering attack is detected and SCC discards the message. Therefore, the proposed method can resist a message-altering attack.

5.4 Analyst attack resistance

In this proposed secure scheme, S_j encrypts the plaintext using an AES encryption algorithm, i.e., $C_i = Enc_{K_j}(m_i \| TS_i)$, and sends C_i to SCC. If an analyst (Eve) captures C_i, it can never obtain the plaintext $m_i \| TS_i$ without knowing the session key K_j, because it is assumed that the AES encryption algorithm is secure. Therefore, the proposed scheme can resist an analyst attack.

6 Performance and efficiency analysis

In this section, we show how much the proposed scheme is efficient. Hence, the proposed scheme is compared with SMHT- and RSA-based authentication algorithms in terms of energy efficiency, communication overhead, and computation cost.

6.1 Energy efficiency

As previously mentioned, the limitation of energy resources is one of the most challenging problems in UWAC. Thus, the methods proposed for securing UWAC must not require much energy consumption overhead (i.e., should be as low as possible) to the sub-surface devices. Because there is no energy restriction for SCC, in this subsection we study how much energy consumption the security procedures add to the sub-surfaces. Due to the high computation complexity of the RSA algorithm, like choosing a pair

of large prime numbers, the RSA signature, and other factors, there are greater energy consumption costs compared with the SMHT method and the proposed scheme. Since the XOR operation has a very limited complexity in comparison with the generated hash values, the number of hash functions used determines the amount of added energy consumption in each sub-surface for the implementation of authenticating procedures. In the SMHT method, every sub-surface should generate hash values according to the following equation:

$$N_{\text{hash}} = 2^n + 2^{n-1} + ... + 2^1 + 1 = 2^{n+1} - 1, \quad (6)$$

where N_{hash} is the number of hash values generated in each tree, and n is the height of the tree. Furthermore, in the proposed scheme, we simply use 2^n hash values to make the tree, and this is almost half the number of hash values generated in SMHT, i.e., $2^n/(2^{n+1}-1)\approx 0.5$. Therefore, the proposed secure scheme is more energy-efficient than the SMHT- and RSA-based schemes.

6.2 Communication overhead

It is important to consider communication overhead. There is a direct relation between the communication overhead that the security of the system adds and the number of whistles, which S_j has to send to SCC for each report. In this subsection, the communication overhead that the proposed authentication scheme adds to the system is compared with that of the RSA algorithm.

As previously mentioned, SCC needs to receive API_i to authenticate the source of the message. Every API consists of n z-bit messages where n is the height of the tree and z demonstrates a z-bit cryptographic hash function. Hence, the generic communication overhead is $n \times z$ bits in this case. For example, if $n=7$ and the output of the hashes used is $z=128$ bits, the communication overhead is $7\times128=896$ bits. However, the RSA authentication scheme, where S_j sends an RSA signature to SCC, has a 1024-bit choice, which is the popular choice. In the UWAC system and when an SCC receives reports from many sub-surfaces, the differences of communication overhead between the proposed scheme and the RSA authentication scheme are more obvious. Therefore, the proposed authentication scheme is more efficient than the RSA authentication scheme in terms of communication overhead.

6.3 Computation cost

In this subsection, the computation costs of the proposed authentication scheme, SMHT-based scheme, and RSA-based scheme are compared with those of SCC and sub-surfaces. According to Eq. (6), every sub-surface generates $(2^{n+1}-1)$ hash values to create a tree, while 2^n hashes are required to generate the improved MHT. The 2^{n-1} XOR operators are also used to create the improved MHT; however, we assume that the XOR operation has a very limited computation complexity in comparison with the generated hash values.

Table 2 shows the observed execution time of a cryptographic hash, an RSA signature, and an RSA signature verification, which are implemented on an Intel Pentium IV 3.0-GHz machine (Dai, 2019). Assuming $n=7$, the required time for generating a tree in the SMHT scheme is 0.02346 ms, while it is 0.011 776 ms for the proposed scheme. However, the computation cost of sending a message is close to zero for SMHT and the proposed scheme. In contrast with the RSA-based scheme it is negligible because an RSA signature is executed in 2.25 ms. As a result, the proposed scheme is more efficient than the SMHT- and RSA-based schemes in terms of computation complexity of sub-surfaces.

Table 2 Execution time of cryptographic operations

Cryptographic operation	Execution time
One cryptographic hash	0.092 μs
One RSA signature	2.250 ms
One RSA signature verification	0.100 ms

In SCC, the most computation cost is spent in computing the root node value of each report in the SMHT authentication scheme. In this way, SCC can obtain the root node value $X_{1,2^n}$ using the corresponding C_i and API_i. Thus, SCC should launch n hash functions to authenticate the source of the message. However, in the proposed authentication scheme, SCC needs to compute only one hash value and $n-1$ XORs. Regardless of the computation complexity of the XOR operator, the proposed scheme can reduce the computation cost to $(n-1)/n\times100\%$, and

for a larger n this is a significant amount. Fig. 7 shows the changes in the computation cost curves while increasing the number of sub-surfaces in SCC. According to Fig. 7, the proposed authentication scheme has the most efficient response in terms of computation cost in SCC.

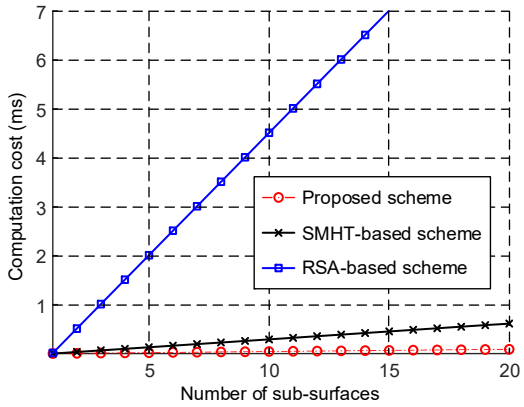

Fig. 7 Computation cost of SCC

7 Conclusions

Due to the suitable properties for long-distance underwater transmission and low bit error rate because of the good correlation characteristics of the dolphin whistle, this process has been used as an information carrier in this paper. Furthermore, an improved Merkle hash tree has been proposed to establish secure and efficient underwater acoustic communication. The security analysis indicates that the proposed scheme resists underwater attacks, i.e., replay attack, fabricated message attack, message-altering attack, and analyst attack. In addition, the performance and efficiency evaluations show that the proposed method is efficient in terms of energy consumption, communication overhead, and computation cost.

Contributors

Masoud KAVEH and Abolfazl FALAHATI designed the research. Masoud KAVEH did the simulations and processed the data. Masoud KAVEH and Abolfazl FALAHATI verified the protocol, drafted the manuscript, and revised and finalized the paper.

Compliance with ethics guidelines

Masoud KAVEH and Abolfazl FALAHATI declare that they have no conflict of interest.

References

Ahmed M, Salleh M, Channa MI, 2017. Routing protocols based on node mobility for underwater wireless sensor network (UWSN): a survey. *J Netw Comput Appl*, 78:242-252. https://doi.org/10.1016/j.jnca.2016.10.022

Dai W, 2019. Crypto++ 5.6.2 Benchmark13. http://www.cryptopp.com/

Diffie W, Hellman M, 1976. New directions in cryptography. *IEEE Trans Inform Theory*, 22(6):644-654. https://doi.org/10.1109/TIT.1976.1055638

Falahati A, Woodward B, Bateman SC, 1991. Underwater acoustic channel models for 4800 b/s QPSK signals. *IEEE J Ocean Eng*, 16(1):12-20. https://doi.org/10.1109/48.64881

Ferguson N, Schroeppel R, Whiting D, 2001. A simple algebraic representation of Rijndael. Proc 8th Annual Int Workshop on Selected Areas in Cryptography, p.103-111. https://doi.org/10.1007/3-540-45537-X_8

Han GJ, Jiang JF, Sun N, et al., 2015. Secure communication for underwater acoustic sensor networks. *IEEE Commun Mag*, 53(8):54-60. https://doi.org/10.1109/MCOM.2015.7180508

Han X, Yin JW, Du PY, et al., 2014. Experimental demonstration of underwater acoustic communication using bionic signals. *J Appl Acoust*, 78:7-10. https://doi.org/10.1016/j.apacoust.2013.10.009

Huang Y, Zhou SL, Shi ZJ, et al., 2016. Channel frequency response-based secret key generation in underwater acoustic systems. *IEEE Trans Wirel Commun*, 15(9): 5875-5888. https://doi.org/10.1109/TWC.2016.2572106

Jia YC, Liu GJ, Zhang LH, 2015. Bionic camouflage underwater acoustic communication based on sea lion sounds. Int Conf on Control, Automation and Information Sciences, p.1-5. https://doi.org/10.1109/ICCAIS.2015.7338688

Jiang SM, 2019. On securing underwater acoustic networks: a survey. *IEEE Commun Surv Tutor*, 21(1):729-752. https://doi.org/10.1109/COMST.2018.2864127

Li H, He YH, Cheng XZ, et al., 2015. Security and privacy in localization for underwater sensor networks. *IEEE Commun Mag*, 53(11):56-62. https://doi.org/10.1109/MCOM.2015.7321972

Liu SZ, Qiao G, Yu Y, et al., 2013a. Biologically inspired covert underwater acoustic communication using high frequency dolphin clicks. IEEE Conf on Oceans, p.1-5. https://doi.org/10.23919/OCEANS.2013.6741138

Liu SZ, Qiao G, Ismail A, 2013b. Covert underwater acoustic communication using dolphin sounds. *J Acoust Soc Am*, 133(4):EL300-EL306. https://doi.org/10.1121/1.4795219

Liu SZ, Ma TL, Gang Q, et al., 2016. Bionic communication by dolphin whistle with continuous-phase based on MSK modulation. Proc IEEE Int Conf on Signal Processing, Communications and Computing, p.1-5. https://doi.org/10.1109/ICSPCC.2016.7753725

Luo Y, Pu L, Peng Z, et al., 2016. RSS-based secret key generation in underwater acoustic networks: advantages,

challenges, and performance improvements. *IEEE Commun Mag*, 54(2):32-38. https://doi.org/10.1109/MCOM.2016.7402258

Merkle RC, 1980. Protocols for public key cryptosystems. IEEE Symp on Security and Privacy, p.122-134. https://doi.org/10.1109/SP.1980.10006

Mobasseri BG, Lynch RS, 2016. Information embedding in sonar by modifications of time-frequency properties. *IEEE J Ocean Eng*, 41(1):139-154. https://doi.org/10.1109/JOE.2015.2390734

Mosavi MR, Kaveh M, 2018. Covert and secure underwater acoustic communication using Merkle hash tree and dolphin whistle. *J Electron Cyber Def*, 6(2):135-146.

Mosavi MR, Kaveh M, Khishe M, et al., 2016. Design and implementation a sonar data set classifier by using MLP NN trained by improved biogeography-based optimization. Proc 2nd National Conf on Marine Technology, p.1-6.

Mosavi MR, Kaveh M, Khishe M, et al., 2018. Design and implementation a sonar data set classifier using multi-layer perceptron neural network trained by elephant herding optimization. *Iran J Mar Technol*, 5(1):1-12.

Rivest RL, Shamir A, Adleman L, 1978. A method for obtaining digital signatures and public-key cryptosystems. *Commun ACM*, 21(2):120-126. https://doi.org/10.1145/359340.359342

van Walree PA, Otnes R, 2013. Ultrawideband underwater acoustic communication channels. *IEEE J Ocean Eng*, 38(4):678-688. https://doi.org/10.1109/JOE.2013.2253391

Yang TC, Yang WB, 2008. Performance analysis of direct-sequence spread-spectrum underwater acoustic communications with low signal-to-noise-ratio input signals. *J Acoust Soc Am*, 123(2):842-855. https://doi.org/10.1121/1.2828053

Zielinski A, Yoon YH, Wu LX, 1995. Performance analysis of digital acoustic communication in a shallow water channel. *IEEE J Ocean Eng*, 20(4):293-299. https://doi.org/10.1109/48.468243