

# SDBR: A Secure Depth-Based Anonymous Routing Protocol in Underwater Acoustic Networks

Chunyan Peng, Xiujuan Du\*

*School of Computer Science and Technology, Qinghai Normal University, Xining 810008, Qinghai, China*

---

## Abstract

Underwater Acoustic Networks (UANs) adopt acoustic communication. The opening and sharing features of underwater acoustic channel make communication in UANs vulnerable to eavesdropping and interfering, and UANs appeal for higher security. This paper presents a secure and depth-based anonymous routing (SDBR) protocol tailored for UANs. Based on bilinear pairings and hash function, by involving limited computation and communication resources, SDBR protocol achieves the backward and forward secrecy for underwater depth-based routing protocol. Theoretical analysis shows that SDBR protocol can provide identity confidentiality, location privacy and routing anonymity as well as decrease computation and communication costs.

*Keywords:* anonymous communication; depth-based routing; lightweight; security; underwater acoustic network

(Submitted on April 5, 2017; Revised on June 21, 2017; Accepted on August 20, 2017)

© 2017 Totem Publisher, Inc. All rights reserved.

---

## 1. Introduction

Underwater Acoustic Networks (UANs) are a novel type of underwater network systems, which emphasize on effective safeguarding of the national marine rights and interests [11,15,23]. UANs have been applied to many fields such as monitoring underwater environment, exploring underwater resource, collecting oceanic data, and preventing disaster etc.

Even though UANs have a slice of shared properties with terrestrial sensor networks, such as a large number of nodes and limited power energy, UANs are significantly different from terrestrial sensor networks in a multitude of aspects: narrow bandwidth, long propagation delay, node passive mobility, and high error probability. RF signal in terrestrial wireless sensor networks at a node's maximum transmission power is not able to spread more than 1 m in underwater environment [13,19], laser and radio waves cannot satisfy long distance communication in water either. UANs adopt acoustic communication, which can meet with long distance transmission [1,2, 5,10,20]. RF signal propagates at a speed of  $3 \times 10^8$  m/s, but acoustic signal propagates at speed of 1500 m/s in water, which is much lower than the speed of RF. All of these factors such as path loss, noise, multi-path, Doppler spread gives rise to higher bit-error in acoustic channels [24,25,28]. UANs also suffer from rigid resource constraints, such as limited battery life and computational power. Acoustic communication is characterized by limited bandwidth, long propagation delay and low data rate, and the open acoustic channel makes UANs more vulnerable to jamming attacks or DoS attacks. Therefore, these characteristics of UANs make the existing work in terrestrial sensor networks unsuitable for UANs and bring about many security challenges. UANs also require security mechanisms and algorithms to maintain the confidentiality and integrity of important messages. The messages include nodes' information, routing items, and data. The nodes' information can be concealed in the process of routing, and the data can be encrypted in the transmitting process by anonymous communication, which is a common method in the field of information security.

Coordination and sharing of information among sensor nodes require secure communication. Since the acoustic channel is open, an attacker can easily eavesdrop on the messages transmitted over the network, and adversaries can also create routing

---

\* Corresponding author.

E-mail address: [dxj@qhnu.edu.cn](mailto:dxj@qhnu.edu.cn).

loops or black holes to disrupt the routing. Anonymous communication is widely studied in terrestrial networks, and various defense mechanisms have been developed as safeguards.

To design a secure routing protocol for UANs is challenging due to the severe limitations such as high propagation delay, low bandwidth, and high energy consumption for communication. Given the constrained capabilities of UANs and the characteristics of the aqueous environments, secure communication techniques should be required. However, limited work has been performed on developing secure communication mechanisms and anonymous routing to protect underwater networks so far. In UANs, the integrity and confidentiality of routing messages should be considered so that sensed information can be processed and managed safely. Moreover, when designing a new secure routing protocol, the algorithm should be lightweight in terms of computation cost and bandwidth cost.

In this paper, the authors focus on a standard geographic routing protocol for UANs, known as Depth Based Routing (DBR) protocol [30]. DBR does not require full-dimensional location information of sensor nodes and only needs local depth information. A key advantage of DBR is that it can handle network dynamics efficiently without the assistance of a localization service. DBR is energy efficient and very suitable for UANs. However, DBR greedily forwards data packets towards the water surface based on the depth information of each node, which increases security threats and makes malicious attacker easily exploit the system loophole from a security standpoint. This paper discusses the security issues of UANs and proposes a novel and secure protocol called as secure depth-based routing (SDBR) on the basis of DBR protocol.

The paper provides the following contributions. First of all, the paper presents a practical and efficient solution to implement anonymous communication in UANs, which can provide identity confidentiality, location privacy and routing anonymity, and protect end-to-end confidentiality and integrity between a source node and a sink node. Secondly, our anonymous algorithm is based on bilinear pairings and depth-based routing protocol, and the anonymous algorithm introduces limited communication overhead and less energy consumption. Theory analysis shows that it is indeed valid. To the best of our knowledge, this is the first secure anonymous protocol based on nodes' depth which has been implemented in UANs. Simulation results show that our anonymous routing algorithm is suitable for underwater acoustic networking environment.

The remainder of this paper is organized as follows. In Section 2, related work along with motivation is presented. In Sections 3, the secure depth-based routing protocol model is discussed. Section 4 presents our proposed anonymous algorithm. Section 5 analyzes the security of SDBR and compares its performance with other lightweight protocols. Section 6 concludes the paper.

## 2. Related Work

UANs are highly constrained in terms of bandwidth and propagation delay. Battery life is sensor nodes' main limitation because the nodes require considerable energy to transmit packets. The mobile nature of sensor nodes in the aqueous environment also makes the acoustic transmission mechanisms less reliable and more energy demanding. The security of UANs has been an increasing serious problem, but limited work has been conducted on studying security mechanisms in UANs. Research on UANs security continues to be in its nascent stages owing to various restrictions. However, the necessity of security technology for UANs is raised rapidly. Anonymity is an old issue that was discussed for Ad Hoc networks and terrestrial sensor networks to guarantee the security of nodes [17,22,30], and it has become a new concern for UANs recently. A few related works in anonymity routing and security-related technologies of UANs are presented in the following paragraphs.

Cong and Yang et al. analyzed the threats and attacks on UANs security [4]. Underwater sensor nodes can be easily intercepted by an adversary and packets are at risk of tampering. Owing to the characteristics of UANs and underwater channels, UANs are vulnerable to malicious attacks. Dong and Liu et al. stated security issues in UANs and proposed a layered security system in [6]. The layered security system has a host of limits on resisting blended attacks. Furthermore, the authors suggested that the security mechanism should be indispensable and layered to overcome the limitations of UANs. However, they did not address how to carry it out and never provided an efficient security scheme.

The application environments of UANs were studied, and the goals and challenges of UANs security were investigated. Wei and Yang *et al.* suggested the node's security should remain essential [27]. The transmitted data and the privacy of nodes such as identity, location, depth etc. need to be protected in the process of communication. Many scholars put forward anonymous routing protocols in terrestrial wireless sensor networks [17,22,30], which are mostly based on public key

cryptography system, and consume a lot of energy and time due to their computational complexity. However, these existing anonymous mechanisms are clearly not suitable for UANs due to the limitations of subsurface environment.

In 2004, Zhu and Wan *et al.* proposed a mobile Ad Hoc Network anonymous routing communication scheme called as ASR [30]. This scheme provides identical anonymity between the source node and the destination node. ASR has the stronger capability to resist variety attacks, but the scheme requirements pre-shared session key for communicating nodes and cannot satisfy the backward and forward security. Seys and Preneel *et al.* put forward an anonymous communication scheme named ARM [22] in 2006, which needs pre-shared session keys and a pre-shared pseudonym list. The scheme requires more storage space. Lu and Cao *et al.* put forward a routing protocol known as SAR in 2007, which can provide the anonymity from the source node to the destination node [17]. SAR was the key exchange protocol that can be authenticated. However, when a node broadcasts a packet, its identity will be recorded down by the predecessor and successor node, so the adversaries have opportunities to attack these nodes according to the tracking information.

UANs cannot directly use the anonymous routing protocol designed for WSNs. Therefore, the authors provide a security protocol that can be suitable for UANs in [27]. In addition, considering security in UANs will no doubt increase the overhead of communication. The authors suggested that a transmitter and a receiver should use the symmetric key for data encryption and decryption, which were also recommended in the article. In the process of anonymous correspondence, symmetric cryptography should be used in UANs in order to reduce the computational overheads.

Gianluca and Angelica provided a secure FLOOD routing protocol for UANs [9]. Upon receiving a route discovery message, a node forwards it unless the node has already done it. In order to protect the integrity and confidentiality of the discovery message, the authors extended the FLOOD protocol into a new protocol called as SeFLOOD. SeFLOOD can protect control messages by establishing link-layer pair-wise keys and encrypting control messages by the logical key tree architecture. The authors supposed that group keys were 128-bit long and used ECC-180 digital signature to authenticate them. But FLOOD protocol is the simplest routing protocol in which a node broadcasts a message to other nodes, all nodes in its corresponding range will listen and receive the message, and judge whether it needs to forward the message or not. So SeFLOOD protocol consumes more energy of underwater nodes.

Yan and Shi *et al.* presented a standard geographic routing protocol named Depth-based Routing protocol (DBR) for UANs [29]. Without any routing control message, packets are routed based on depth information of nodes in DBR. Since DBR is not related to security issues, Zuba and Fagan *et al.* analyzed the security vulnerabilities of DBR and investigate the effects of location spoofing on a standard DBR protocol [31]. Consequently it is extremely necessary to reinforce DBR protocol by increasing some secure schemes.

In this paper, a practical and efficient anonymous routing protocol based on DBR protocol for UANs is provided, called as SDBR. Compared with other people's work, we not only put forward the security architecture, but also realized the specific algorithm. The proposed security framework of UANs can provide identity confidentiality, location privacy and routing anonymity, and protect end-to-end confidentiality and integrity between a source node and a sink node. The provided anonymous algorithm mainly combines DBR protocol and the theory of bilinear pairings. The anonymous algorithm introduces limited communication, computational overhead and less energy consumption. In addition, the new provided security algorithm is indeed valid by analysis of performance and real data. To the best of our knowledge, SDBR is the first secure anonymous routing protocol based on node's depth information. Theoretical analysis and simulation results show that SDBR protocol is more suitable for UANs than SeFLOOD in terms of energy costs.

### 3. Overview DBR Protocol

#### 3.1. The Analysis of DBR

DBR is a standard geographic routing protocol based on the depth information of each sensor that can be measured by the depth sensor. In order to further control the number of nodes taking part in packet forwarding, the author involved depth threshold  $d_{th}$ . When a node receives a packet, it forwards the packet if its depth is smaller than the depth of previous node minus  $d_{th}$ . Otherwise, it discards the packet. The author proposed a holding time in order to reduce the number of redundant forwarding packets in DBR. DBR can work well in the multiple-sink underwater sensor architecture [21]. Its communication architecture is given by Figure 1.

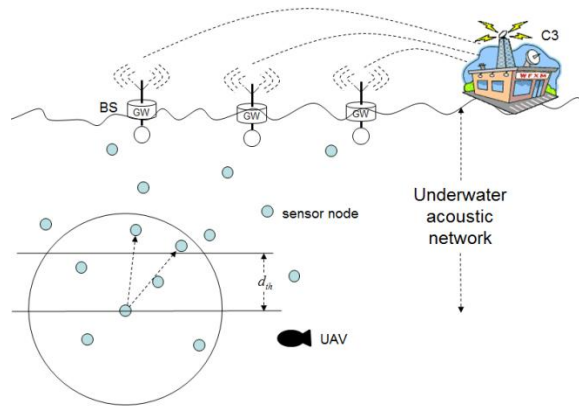


Figure 1. The network architecture for DBR

The reasons that our secure protocol is based on DBR protocol are as follows. (1) It does not require full dimensional location information. (2) It can handle dynamic networks with favorable energy efficiency. (3) It takes advantage of multiple-sink network architecture without introducing extra cost. Many researchers provided a multitude of improved schemes respectively on the fundamental algorithm of DBR. EEDBR is an energy efficient routing protocol in which the depth of sensor nodes is used during forwarding data packets [26]. In order to improve the network lifetime, the residual energy of the sensor nodes is also taken into account in EEDBR. Threshold-Optimized DBR (AMCTD) explored the optimal weight function to achieve longer network lifetime [12]. CoDBR was proposed in succession in [18]. To enhance network performance, CoDBR used a cooperation-based scheme. The depth information of each node was used in these aforementioned routing protocols, but the security problem was not considered in these routing protocols, as well as in DBR. Malicious attackers can easily invade the system. After the analysis of the protocol, we can draw a conclusion that the routing protocols based on the depth are not secure routing protocols from the following points.

- The attackers can try to falsify the depth information in order to obtain the superiority of forwarding the packets.
- Malicious users can tamper with the holding time to disrupt the routing.

In order to resist all kinds of attacks such as anonymity communication attacks, temporal attacks, etc., a solution that can fortify the security of DBR should be proposed. Our protocol is an optimized protocol, which mainly focuses on anonymous routing and reinforces the security of DBR. The ID, depth and routing information of nodes cannot be obtained easily by adversaries by using anonymous routing.

### 3.2. The Framework of Secure DBR

In this paper, a framework of anonymous communication routing is presented. The framework provides the following security elements: sender anonymity, receiver anonymity, link anonymity, data privacy, and energy preservation.

There are two phases to confirm a routing in the secure DBR. One phase is routing discovery, the other is routing recovery. In the routing discovery phase, the source node needs to decide the next forwarding nodes according to the depth threshold value of  $d_{th}$  and the depth of the next node, and then transmit the data packet to the next hop. Then the next nodes continue to forward until to the sink node. The sink node broadcasts the recovery packets to the source node in the routing recovery phase. In our SDBR, more than one route items can be established in one node, and a session key between the node pair should be negotiated in advance. The routing discovery and recovery phase in UANs based on DBR are illustrated in Figure 2.

The energy and computation resources of a node is very limited and sensor nodes are mobile with water current, so routing time is not too long and the encryption algorithm is not too complex. Asymmetric encryption algorithm is with high computational complexity, energy consumption, and operation time. Therefore, the complexity of the algorithm should be reduced as far as possible and the theory of bilinear pairing is used in SDBR.

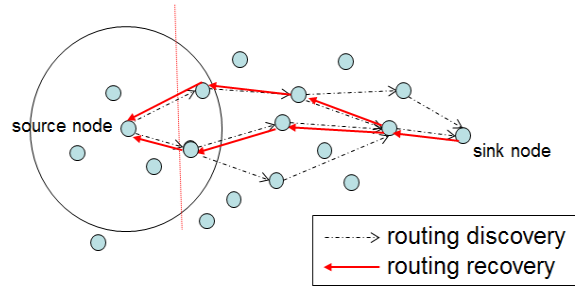


Figure 2. The routing discovery and recovery phase.

## 4. The Process of Anonymous Communication

### 4.1. Anonymity

Anonymity mainly includes three parts: identity confidentiality, location privacy and routing anonymity. Identity confidentiality requires the following: (1) The forwarding nodes in the routing process are unaware of real identities of the source node and the destination node; (2) Source and destination nodes are unconscious of identities of the intermediate nodes. Location privacy requires the following: (1) All of intermediate nodes are not aware of real location information of source and destination nodes; (2) All of intermediate nodes do not know and cannot judge the distance and the hop counts to communication node. Routing anonymity requires the following: (1) All forwarding nodes cannot track the source node and the destination node; (2) If the nodes which are not in the routing path are unable to obtain any session information; (3) It is very formidable for an attacker to deduce the routing path from the source node to the destination node.

The anonymous routing protocol should have the ability of resisting common active and passive attacks. This protocol can make the discovery and maintenance of routing more secure and efficient. In general, there are three participants in routing protocols, source node, destination node, and intermediate nodes. A routing protocol can be also divided into three phases. The first part is the discovery phase. The source node sends the route discovery messages to the destination node via a series of intermediate nodes. After receiving the routing discovery message, the destination node (i.e. the sink node) initiates to the routing recovery phase and returns the recovery message along the opposite path. Finally, after the routing is set up, the source node and destination node can communicate with each other to transmit data, which is the third stage. In the next section, the authors firstly interpret the fundamental knowledge used in provided anonymous communication protocol.

### 4.2. Bilinear Pairing

Bilinear pairing is a very important concept in cryptography system based on identities of sensor nodes. Bilinear mapping can be constructed by the Weil Pairing or Tate Pairing in the elliptic curve [26,3,8]. Assume  $G_1$  and  $G_2$  are two groups with order of prime  $q$ .  $G_1$  is an additive group,  $G_2$  is a multiple group. Let  $p$  denote a generator of  $G_1$ . The discrete logarithm problem in Group  $G_1$  and  $G_2$  is a NP difficult problem [14,16]. A map  $e$  from group  $G_1$  to group  $G_2$ :  $G_1 \times G_1 \rightarrow G_2$  is called a bilinear map if it satisfies the following properties:

- (1) Bilinearity.  $\forall P, Q, R \in G_1$ ,  $e(P, Q+R) = e(P, Q)e(P, R)$ ,  $e(P+Q, R) = e(P, R)e(Q, R)$ ,  $e(aP, bQ) = e(P, Q)^{ab}$  for all integers  $a, b$
- (2) Non-degradation.  $\exists P, Q \in G_1$ ,  $e(P, Q) \neq 1$
- (3) Calculation.  $\forall P, Q \in G_1$ ,  $e(P, Q)$  can be calculated in effective polynomial time.

Since the calculation complexity of hyperbola is very high, it is necessary to select suitable algorithm to reduce the time for setting up a route so that it can improve the efficiency of setting up routing to a certain extent, which can be calculated within polynomial time.

### 4.3. SDBR

#### 4.3.1 Symbol Description of SDBR

Several notations to simplify the illustration of new scheme will be introduced. Table 1 summarizes these notations and their corresponding meanings.

Table 1. Notations

Symbol	Definition
$\oplus$	the exclusive-OR operation
$\parallel$	Conjunction operation
$P$	A big prime
$G_1$	An additional group of order $P$
$G_2$	A multiple group of order $P$
$S_{pri}$	System private key
$S_{pub}$	System public key
$S_i$	The private key of node i
$P_i$	The public key of node i
$R_{seq}$	Identifier of a specific routing
$N_i$	$N_0$ is source node; $N_n$ is sink node; $N_i (0 < i < n)$ is forwarding node
$ID_i$	Identity of node i
$K_{ij}$	The share key between node i and node j
$E_{K_{ij}}(m)$	To encrypt message $m$ with the key $K_{ij}$
$D_{K_{ij}}(m)$	To decrypt message $m$ with the key $K_{ij}$
$H(\bullet)$	Hash Function
$SK_{ij}$	Static session key of node i and node j

#### 4.3.2 System Initialization

Assume that each node has the same transmission range and each node has already obtained the unique ID value in advance. In addition, all of sink nodes have the same stationary ID value.

At first, autonomous underwater vehicles (UAVs) or BS are commonly acted as PKG(Private Key Generator) in UANs. Galindo and Roman et al. have already proposed that non-interactive key agreement, which is pairings based and the best solution for key distribution in large UWSN [7]. In this paper, this key agreement scheme is used in SDBR. PKG generates the system parameters:  $p, G_1, G_2, e : G_1 \times G_1 \rightarrow G_2$  and a hash function:  $H(\bullet) : \{0,1\} \rightarrow G_1$ .

PKG generates a pair of system public key and system private key  $(S_{pub}, S_{pri})$ ,  $S_{pub} = S_{pri}P$ . Each node selects its node  $ID_i$ , and computes its public key  $P_i = H(ID_i)$ , the private key is  $s_i = S_{pri}P_i$ .

#### 4.3.3 Secure Protocol

The proposed secure aforementioned protocols are divided into three phases: the routing discovery, the routing recovery, and the data transmission. The section will discuss the detailed process of each phase in the following paragraphs.

##### (1) Routing request

The source node  $N_0$  has neither any available routing nor a shared session key before sending confidential information to the sink node  $N_n$ . Therefore, it needs to establish more than one route items in a lot of communication nodes and negotiate a session key in advance. The source node  $N_0$  generates a request routing package and broadcasts it to some nodes with the depth difference of the source node and the next hop node is greater than  $d_{th}$ .

a. The source node  $N_0$  selects a random number  $Rand$ , and then computes the value of  $K_{ij} = H(e(S_i, P_j))$ , and  $X = H(ID_i) \oplus H(e(S_{pub}, P_j))$ .

b. The source node  $N_0$  generates the routing request package by computing  $M_0 = [R_{req\_seq} \parallel RandP_i \parallel Hop \parallel X \parallel E_{K_{ij}}(H(ID_j))]$ . Here,  $R_{req\_seq}$  is a unique identification of the request routing package.  $RandP_i$  is used to detect if this node has already processed the packet in request phase.  $Hop$  denotes the maximum hop counts in packets transferring process.  $X$  presents the encrypted  $ID_i$  of source node  $N_0$ ,  $E_{K_{ij}}(H(ID_j))$  denotes to encrypt the  $ID_j$  of the next node  $N_j$  with the public key  $K_{ij}$ .

c. When an intermediate node receives the routing request packet, the node will check if the value  $hop \rightarrow 0$  is established. If  $hop \rightarrow 0$  is true, then continue; else it will stop verifying. In the next moment the intermediate node will check whether the routing item  $R_{req\_seq}$  exists in the route items. If  $R_{req\_seq}$  exists, the package has already received, so the node will discard it right now; otherwise, the node will store the result  $RandP_i$  in its buffers. Then compute  $H(e(p, S_j))$  and verify it by the Eq.(1):

$$H(e(p, S_j)) = H(e(p, S_{pri}P_j)) = H(e(p, P_j))^{S_{pri}} = H(e(S_{pri}P, P_j)) = H(e(S_{pub}, P_j)) \quad (1)$$

$ID_i$  of the source node can be computed by the following Eq.(2):

$$H(ID_i) = X \oplus H(e(S_{pri}P, P_j)) = X \oplus H(e(S_{pub}, P_j)) \quad (2)$$

So, if  $K_{ji} = K_{ij}$  is established, which can be verified by the Eq.(3):

$$\begin{aligned} K_{ji} &= H(e(H(ID_i), S_j)) = H(e(H(ID_i), S_{pri}P_j)) = H(e(H(ID_i), P_j))^{S_{pri}} = H(e(S_{pri}H(ID_i), P_j)) \\ &= H(e(S_{pri}P_i, P_j)) = H(e(S_i, P_j)) = K_{ij} \end{aligned} \quad (3)$$

Then  $ID_j$  can be decrypted by  $E_{K_{ij}}(H(ID_j))$ . If  $ID_j$  is equal to  $ID_n$ , the current node is sink node; otherwise,  $ID_j$  changes the value of  $Hop$  by using the expression  $Hop \rightarrow$  in the message  $M_0$ , and continues to transfer  $M_0$  to other intermediate nodes, then the node  $ID_j$  adds this routing item  $R_{req\_seq}$ .

## (2) Routing recovery

The routing recovery process is initiated by the destination node. The purpose is to confirm more than one route from the destination node to the source node in the opposite direction. Here, more than one route had better be confirmed since the connectivity for UANs is unstable. When the sink node  $N_n$  receives the request packet, it will learn that there is a source node  $N_0$  desires to communicate securely with itself. The sink node  $N_n$  begins to construct the routing recovery packet, and then broadcasts in its allowed range by using DBR protocol.

The destination node  $N_n$  chooses a random number  $R_{rec\_seq}$  as an unique ID for the routing recovery packet and computes the session key  $SK_{ji}$  for the current communication by Eq.(4):

$$SK_{ji} = H(e(RandP_i, S_j)) \quad (4)$$

Then the destination node  $N_n$  begins to construct the routing recovery packet. The routing recovery packet  $M_1$  can be computed by Eq.(5) and then the destination node  $N_n$  broadcasts it by using DBR protocol.

$$M_1 = [R_{rec\_seq} \parallel RandP_n \parallel pP_n] \quad (5)$$

Here,  $R_{rec\_seq}$  is the unique ID of the recovery routing item,  $RandP_n$  denotes that the sink node  $N_n$  is sending a routing recovery packet,  $pP_j$  denotes that the sink node  $N_n$  sends the recovery package.

c. When the node receives the routing recovery packet, it will check whether there is the route identification  $R_{rec\_seq}$  in the routing table of the current node at first. If there is a recovery packet, then the packet has been received at this node, it should be discarded; otherwise, the node will check if there is a  $RandP_i$  in the nodes buffer. If there is, it must be either the source node or the intermediate node of the routing. If it is a source node, the session key can be calculated by Eq.(6) and the session key is the same as that the destination node shared.

$$\begin{aligned}
SK_{ij} &= H(e(RandS_i, P_j)) = H(e(RandS_{pri} P_i, P_j)) = H(e(RandP_i, P_j))^{S_{pri}} = H(e(RandP_i, S_{pri} P_j)) \\
&= H(e(RandP_i, S_j)) = SK_{ji}
\end{aligned} \tag{6}$$

If it is not a source node, it must be a forwarding node. When it receives the routing recovery packet, it can continue to broadcast it to other neighbor nodes based on the depth threshold  $d_{th}$ . It will establish a routing and negotiate a shared session key from the source node to the destination node. If  $SK_{ij} = SK_{ji}$  is established and  $SK_{ji}$  is equal to  $SK_{ji}$  in Eq.(4), then the security communication can be carried out between the two nodes.

### (3)Data transmission

The process of data transmission begins when a secure communication channel has been set up successfully between the source node  $N_0$  and the destination node  $N_n$  after the route request phase and the route recovery phase.

a. If the source node  $N_0$  sends a message  $M$  to the destination node  $N_n$  and they can communicate with each other, it will look up in the local routing table and find the next hop according to  $R_{rec\_seq}$ . After the public key  $P_i$  and the session key  $SK_{ij}$  of the next hop are ascertained, the source node  $N_0$  can generate the encrypted data packets and broadcast it in its allowed range by using DBR protocol by Eq.(7).

$$C = [R_{data\_seq} || E_{SK_{ij}}(M) || RandP_i] \tag{7}$$

Here,  $R_{data\_seq}$  is a unique identification of data package,  $E_{SK_{ij}}(M)$  denotes the encrypted results with the session key between the source node and the destination node.

b. When the node receives this packet, at first it will check if the  $RandP_i$  of the node is in routing table, if there is, it must be either the destination node or the intermediate node of the current routing. Then we can decrypt  $M$  by  $M' = D_{SK_{ij}}(E_{SK_{ij}}(M))$  and calculate  $RandP_i$  because  $C$  and  $R_{data\_seq}$  are known. If  $RandP_i$  is equal to  $RandP_i$  in its buffer, it is a destination node, and the session key  $SK_{ij}$  can be used to decrypt  $C$  and the data  $M$  can be obtained. If it is an intermediate node, the routing data packets will continue broadcasting to the next node in the communication.

## 5. Performance Analyses

A complete anonymity and security analysis are in this section, and then we explain why the solution remains lightweight compared to the other protocols.

### 5.1. Anonymity Analyses

This routing protocol guarantees that the source node and the destination node can communicate with each other through a series of intermediate nodes, and the intermediate nodes in the network cannot be aware of any information about the source node and the destination node. If an attacker does not know who is the destination node and the private key of the destination node in the routing discovery phase then he cannot decrypt the information by Eq.(8):

$$\begin{aligned}
M_0 &= [R_{req\_seq} || RandP_i || Hop || X || E_{K_{ij}}(H(ID_j))] \\
X &= H(ID_i) \oplus H(e(S_{pub}, P_j))
\end{aligned} \tag{8}$$

Similarly, the attacker cannot obtain the identity information of sensor nodes that participate in the routing recovery phase due to the lack of the node's private key and the shared session key. Each node in the routing table only knows its corresponding predecessor and successor, and this node does not know which is the real source node or the sink node and hop counts from the source node to the destination node. Therefore, the protocol is satisfied with the demand of anonymity. Consequently, the adversary cannot deduce which is the source node or the destination node by tracking a packet. Only the destination node knows which is the source node by computing  $K_{ji}$ , and other nodes cannot know the information.



### 5.2. Forward and Backward security

Forward security is that if a communication session key  $SK_{ij}$  will be leaked from one node  $N_i$  to another node  $N_j$ , the previous session key is still safe. Backward security is that when the previous communication session key  $SK_{ij}$  is leaked from the node  $N_i$  to the node  $N_j$ , the current session key is still safe. After the discovery process and the recovery process in our protocol, more than one route will be established between the source node  $N_0$  and the sink node  $N_n$ , and the session key is also established for communication. From Eq. (6), it can be shown that the session key depends on the random number  $rand$ , the public key  $P_i$  and the private key  $S_i$  of sensor nodes. Because the decomposition problem is recognized as a mathematical problem, even if an attacker can obtain  $randP_0$  and  $randP_n$  simultaneously, the session key cannot be calculated. Thus, this routing protocol can guarantee the forward security. The computation of  $SK_{ij} = SK_{ji}$  is based on  $rand$  and the private key and the public key of two communication nodes, which are extremely different at each node, so the Backward security is guaranteed.

### 5.3. Complexity Analysis and Energy Cost

SDBR can guarantee integrity and confidentiality for the DBR protocol. In terms of complexity and energy cost, firstly there are few qualified nodes who anticipate the discovery phase and the recovery phase. However, the sender sends packets to all of the nodes in its corresponding range in SeFLOOD protocol. Secondly, SDBR can save more time, which spends on making an appointment and broadcasting control packets such as HELLO packets, REPORT packets, ACK packets in SeFLOOD. Thirdly, SeFLOOD protocol uses the Dijkstra algorithm to discover the neighbor routing, which has the complexity  $O(n^2)$ , but SDBR uses greedy algorithm for the best effort to forward packets based on the depth information of the nodes, which has the complexity less than  $O(n)$ . In this simulation, the depth threshold  $d_{th}$  of DBR is set to 20 meters. The bit rate is 10kbps; the maximal transmission range is 100 meters (in all directions); and the power consumption in sending, receiving, and idling mode are 2w, 0.1w, and 10mw, respectively. Total energy costs include the total energy consumed in packet delivery and the encryption algorithm. From the above three aspects of the analysis, the total sum energy costs of SeFLOOD and SDBR are compared protocol by the Figure 3.

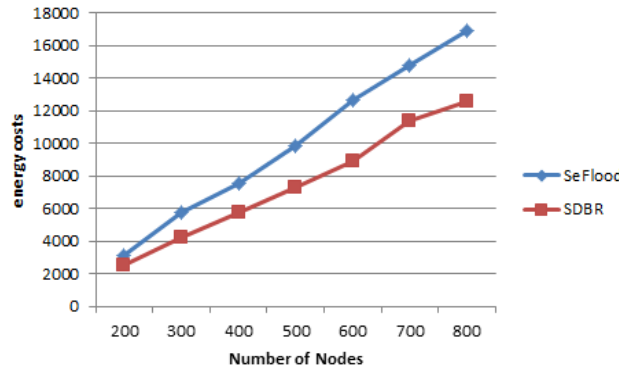


Figure 3. Energy costs

Furthermore, a large amount of public key will make the algorithm consume higher energy and higher computing time. The algorithm of the protocol should be more energy-efficient and time-efficient due to the unique features of UANs. Therefore, the design of protocol should minimize costs of the public key operations. SDBR has been compared with other anonymous routing protocols such as ASR [30], ARM [22], SAR [17] aforementioned in introduction.  $T_h$  is the using time of Hash operation, and  $T_{asym}$  is defined as the time of private key encryption.  $T_{sym}$  delegates the time of the public key encryption. Accordingly  $T_e$  is referred to as the operation time for bilinear parings and  $T_{exp}$  is referred to as the operation time for exponential. The computation complexities of all different protocols are listed by Table 2. ASR, ARM, and SAR are all lightweight anonymous routing protocols used in traditional wireless sensor networks. From Table 2, it is shown that SDBR has certain superiority in calculation.

Table 2. Computation complexity (bit)

Phase	SDBR	ASR	ARM	SAR
Request	$160 \times 4$	$192 \times 2 + 1024 + 128 \times 2$	$2 \times (128 + 160) + 192 + 1024$	1024
Recovery	$160 \times 3$	$1024 + 192$	$192 \times 2$	$1024 \times 2$
Total	1120	2880	2176	3072

SDBR only requires the identities of each sensor node in the process of computing a pairwise authenticated compared with other protocols. On the computational side, SDBR has to perform one hash operation. SDBR is the most energy efficient due to the lowest computation complexity compared with other three algorithms. It is displayed that SDBR spend sum costs from Figure 4.

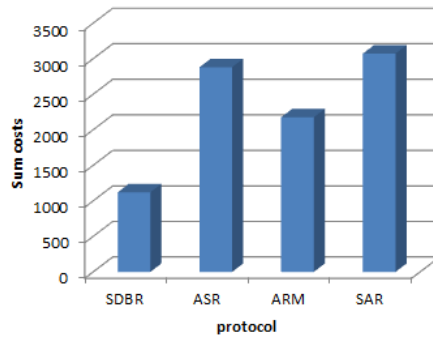


Figure 4. Sum costs

#### 5.4. Bandwidth Consumption

Lower bandwidth consumption can degrade the whole network energy consumption and make data transmission speed faster, and it is favorable to prolong the network lifetime. If we suppose the key length is 1024 bits in a cryptosystem scheme, the cryptosystem scheme based on elliptic curve ECC-160 is more lightweight than the famous RSA and Elgamal encryption algorithm. In addition, SDBR is based on the cryptosystem scheme ECC-160, and the security level of ECC-160 can be considered as that of RSA-1024 nowadays. The message is generated by  $M_0 = [R_{req\_seq} \parallel RandP_i \parallel hop \parallel X \parallel E_{K_{ij}}(H(ID_j))]$  in the routing requesting phase. The sum is up to  $160 \times 4$  bits storage consumption. Furthermore, the message is generated by  $M_1 = [R_{rec\_seq} \parallel RandP_i \parallel pP_j]$  in the routing recovery phase, which sums up to  $160 \times 3$  bits in storage consumption. Table 3 has listed different bandwidth consumptions of all kinds of phases.

Table 3. Bandwidth comparison

Algorithm	Request	Recovery	Total
SDBR	$(n+2) \cdot T_{sym} + 2T_h$	$2 \cdot T_e$	$(n+2) \cdot T_{sym} + 2 \cdot T_h + 2 \cdot T_e$
ASR	$(n+2) \cdot T_{asym} + 2 \cdot T_{exp} + 2T_h$	$(n+1) \cdot T_{asym} + (3n+5) \cdot T_{exp}$	$(2n+3) \cdot T_{asym} + (3n+7) \cdot T_{exp} + 2T_h$
ARM	$(2n+2) \cdot T_{asym} + (n+4) \cdot T_{sym} + T_{exp}$	$(n+1) \cdot T_{asym} + (n+6) \cdot T_{sym}$	$(3n+3) \cdot T_{asym} + (2n+10) \cdot T_{sym} + T_{exp}$
SAR	$(n+2) \cdot T_{asym} + 2 \cdot T_{exp} + 2T_h$	$(2n+3) \cdot T_{asym} + 3 \cdot T_{exp} + 2T_h$	$(3n+5) \cdot T_{asym} + 5 \cdot T_{exp} + 4T_h$

## 6. Conclusions

In this work, the authors have focused on the fact that UANs consume an amount of energy in sending and receiving data. This paper improves DBR protocol and proposes a security anonymous routing protocol named SDBR based on bilinear pairings for UANs. SDBR can provide identity confidentiality, location privacy and routing anonymity, and it can meet requirements of routing security. This article adopts the symmetric key mechanism rather than the public key, which greatly decreases the computational complexity of the system and the bandwidth consumption. Security analysis indicates SDBR is more suitable for UANs compared with other lightweight anonymous routing protocols. Future work will focus on the network simulation platform and evaluate SDBR in real UANs.

## Acknowledgements

This work is supported by Key lab of IoT of Qinghai (No.2017-ZJ-Y21), Hebei Engineering Technology Research Center for IoT Data acquisition & Processing, the National Social Science Foundation of China (No.15XMZ057), Qinghai Office of Science and Technology (No.2015-ZJ-904), Qinghai Social Science Foundation (No.2015-ZJ-718), the Ministry of education Chunhui projects (No. Z2015052).

## References

1. I F Akyildiz, D. Pompili and T. Melodia, "State of the art in protocol research for underwater acoustic sensor networks," *Proc of the 1st ACM international workshop on underwater networks*, pp. 7-16, New York, 2006
2. A. Caiti and A. Munafo', "Adaptive Cooperative Algorithms for AUV Networks," *IEEE International Conference on Communications Workshops (ICC 2010)*, pp. 1-5, Capetown, May 2010
3. T. Chen and H. Yu, "Bilinear Parings in Property-based attestation," *International Conference on Networks Security*, pp. 256-260, 2010
4. Y. P. Cong, G. Yang, Z. Q. Wei, and W. Zhou, "Security in underwater Sensor network," *International Conference on Communication and Mobile Computing*, 2010
5. J. H. Cui, J. Kong, M. Gerla, and S. Zhou, "The challenges of building mobile underwater wireless networks for aquatic applications," *Network, IEEE*, vol. 20, no. 3, pp. 12-18, May-June, 2006
6. Y. Dong and P. Liu, "Security consideration of Underwater Acoustic Networks," *International Congress on Acoustics, ICA*, 2010
7. A. Enge, "Bilinear pairings on elliptic curves," *HAL - INRIA*, vol.61,no.1, 2013(DOI 10.4171/LEM/61-1/2-9)
8. D. Galindo, R. Roman and J. Lopez, "A Killer Application for Pairings: Authenticated Key Establishment in Underwater Wireless Sensor Networks," *Cryptology and Network Security*, pp. 120-132, Springer Berlin Heidelberg ,2008
9. Dini Gianluca and Duca Lo Angelica, "A Secure Communication Suite for Underwater Acoustic Sensor Networks," *Sensors*, vol.12, no.11, pp. 15133-15158, 2012
10. Z. Guo, H. Luo, F. Hong, M. Yang, and M. Ni Lionel, "Current Progress and Research Issues in Underwater Sensor Networks," *Journal of Computer Research and Development*, vol. 47, no.3, pp. 377-389, 2010
11. Z. Hu, C. Wang, Y. Zhu, and D. Kong, "Signal Detection for the Underwater Acoustic Voice Communication," *Proc of the International Symposium on Test and Measurement 2003*, pp. 1-5, Washington, IEEE, 2003
12. M. R. Jafri, S. Ahmed, N. Javaid, Z. Ahmad, and R.J. Qureshi, "AMCTD: Adaptive Mobility of Courier Nodes in Threshold-Optimized DBR Protocol for Underwater Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, vol. 2014, pp. 259-273, 2014
13. D. B. Kilfoyle and A. B. Baggeroer, "The State of the Art in Underwater Acoustic Telemetry," *IEEE Journal of oceanic engineering*, Vol.25, No.1, pp. 4-27, 2000
14. F. Li and P. Liu, "An Efficient Certificateless Signature Scheme from Bilinear Parings," *International Conference on Network Computing & Information Security*, pp. 35-37, 2011
15. Q. Liang and X. Cheng, "Underwater acoustic sensor networks: Target size detection and performance analysis," *Ad Hoc Networks*, vol.7,no.4, pp. 830-808,2009
16. H. P. Liu, C. H. Lan, Y. J. Ding, and Q. J. Yue, "An ID-Based Proxy Signature Using Bilinear Pairing," *Journal of Lanzhou Jiaotong University*, 2008
17. R. Lu, Z. Cao, L. Wang, and C. Sun, "A secure anonymous routing protocol with authenticated key exchange for ad hoc networks," *Computer Standards & Interfaces*, vol. 29, no.5, pp. 521-527, 2007
18. H. Nasir, N. Javaid, H. Ashraf, and S. Manzoor, "CoDBR: Cooperative Depth Based Routing for Underwater Wireless Sensor Networks," *Broadband and Wireless Computing, Communication and Applications (BWCCA), 2014 Ninth International Conference on IEEE*, pp. 52-57,2014
19. J. Preisig, "Acoustic Propagation Considerations for Underwater Acoustic Communications Network Development," *Acm International Workshop on Underwater Networks*, vol. 11, no.4, pp. 1-5, 2006
20. J. Rice and D. Green, "Underwater acoustic communications and networks for the US Navy's Sea web Program," *Proc of the second International Conference on Sensor Technologies and Applications*, pp. 715-722, Washington, 2008
21. W. K. G. Seah and H. X. Tan, "Multipath Virtual Sink Architecture for Underwater Sensor Networks," *Research Collection School Of Information Systems*, 2001
22. S. Seys and B. Preneel, "ARM: anonymous routing protocol for mobile ad hoc networks," *Advanced Information Networking and Applications, AINA 2006, 20th International Conference on IEEE*, pp. 133-137, 2006
23. E. M. Sozer, M. Stojanovic, and J. G.Proakis, "Underwater acoustic networks," *IEEE Journal of Oceanic Engineering*, vol.25, no.1, pp. 72-83, 2000
24. M. Stojanovic. "Underwater Acoustic Communication: Design Considerations on the Physical Layer," *Wireless on Demand Network Systems and Services*, 2008
25. Y. Su, Y. Zhu, H. Mo, J. H. Cui, and Z. Jin, "UPC-MAC: A Power Control MAC Protocol for Underwater Sensor Networks," *International Conference on Wireless Algorithms, Systems, and Applications*, Vol.7992, pp.377-390,2013
26. A. Wahid ,S. Lee , H. J. Jeong , and D. Kim, "EEDBR: Energy-Efficient Depth-Based Routing Protocol for Underwater Wireless Sensor Networks," *Advanced Computer Science and Information Technology*, pp. 223-234, Springer Berlin Heidelberg, 2011
27. Z. Wei, G. Yang, Y. Cong, and J. Dong, "Analysis of security and threat of underwater wireless sensor network topology," *Proceedings of the ICCEE 2010*, Chengdu, pp. 506-510, 2010
28. P. Xie, Z. Zhou, Z. Peng, J. H. Cui, and Z. Shi, "SDRT: A reliable data transport protocol for underwater sensor networks," *Ad Hoc Networks*, vol.8, no.7, pp. 708-722, 2010
29. H. Yan, Z. J. Shi, and J. H. Cui, "DBR: Depth-Based Routing for Underwater Sensor Networks," *Lecture Notes in Computer Science*, 4982, pp. 72-86, 2008
30. B. Zhu, Z. Wan, M. S. Kankanhalli, F. Bao, and R. H. Deng, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," *IEEE International Conference on Local Computer Networks*, Vol.37, pp.102-108, 2004
31. M. Zuba, M. Fagan, J. H. Cui, and Z. Shi, "A vulnerability study of geographic routing in Underwater Acoustic Networks," *2013 IEEE Conference on Communications and Network Security (CNS)*, pp. 109-117, 2013