第 38 卷 第 4 期
2019 年 7 月

应用声学
Journal of Applied Acoustics

Vol. 38, No. 4
July, 2019

◇ 李启虎院士八十华诞学术论文 ◇

隐蔽通信中基于水声信道的密钥生成技术*

刘俊凯[1,2]　董阳泽[1†]　张刚强[1]

(1 水声对抗技术重点实验室　上海　201108)

(2 浙江大学　杭州　316021)

摘要　水声传感器网络实现了高度智能化、自主性强、分布式、全天候的水下信息采集、传输、处理及融合，是水下目标的监测、定位、跟踪与分类等应用的最佳选择之一。针对隐蔽传输中的加密，提出了基于水声信道响应特征产生密钥的方法，通过利用水声信道的短时相关性，通信双方实时地产生加密密钥，以保证信息的保密性能。通过将信息隐藏技术和密钥生成技术相结合，确保水声信息的隐蔽传输。仿真与试验结果表明，基于提出的密钥生成方法能够生成匹配密钥，为水声隐蔽通信提供加密支持。

关键词　水声信道，密钥，信息隐藏，信息加密

中图法分类号: TN929.3　　**文献标识码:** A　　**文章编号:** 1000-310X(2019)04-0681-07

DOI: 10.11684/j.issn.1000-310X.2019.04.027

Key generation technology based on underwater acoustic channel estimation in covert communication

LIU Junkai[1,2]　DONG Yangze[1]　ZHANG Gangqiang[1]

(1 *National Key Laboratory of Science and Technology on Underwater Acoustic Antagonizing, Shanghai* 201108, *China*)

(2 *Zhejiang University, Hangzhou* 316021, *China*)

Abstract　Take advantage of underwater acoustic sensor network (UWSN), intelligent, autonomous, distributed, all underwater information collection, transmission, processing and fusion can be performed. Thus UWSN becomes one of the best choices for underwater applications such as target monitoring, positioning, tracking and classification. Aiming at the encryption in covert communication, a method of generating key based on the response characteristics of underwater acoustic channel is proposed. By utilizing the short-term correlation of underwater acoustic channel, both the transmitter and receiver can generate encryption keys in real time to ensure the confidentiality of information. By combining information hiding technology with key generation technology, the covert transmission of underwater acoustic information can be ensured. Simulation and experimental results show that the proposed key generation method can generate matched keys as well as provide encryption support for underwater acoustic covert communication.

Key words　Underwater acoustic channel, Secret key, Information hiding, Information encryption

2019-02-14 收稿; 2019-03-08 定稿

*浙江省海洋观测 -成像试验区重点实验室资助

作者简介: 刘俊凯 (1990-), 男, 河北保定人, 硕士, 工程师, 研究方向: 水声对抗。

† 通讯作者 E-mail: dongyangze@139.com

0 引言

随着国家海洋战略的提出，各种水下测控平台大量投入到水下测控领域，为海洋开发提供支撑。在海洋开发中，如何将重要信息安全隐蔽地传输到接收端而不被截获是水声通信中需要解决的一个关键问题。佛罗里达大学的Ling等[1]研究了直接序列扩频(Direct sequence spread spectrum, DSSS)信号在隐蔽通信中的应用，但其隐蔽通信方法是通过牺牲通信速率达到的；哈尔滨工程大学在仿生隐蔽通信方面较早开展了工作，韩笑等[2]提出一种选取海豚whistles信号作为同步码和Pattern码，并以相邻whistles信号之间的时延差值携带信息的仿生水声通信技术。以上水声隐蔽通信方法中通过利用低截获概率信号或者仿生的噪声模拟通信方式来降低信号的截获概率，未从信息隐藏和加密方面进行较多考虑。

目前，基于水声信道的密钥生成算法研究相对较少，对无线领域的基于无线信道的密钥生成算法研究较多。陆军工程大学的石会等[3]比较了根据提取无线信道物理特征参数不同，生成物理密钥方案的优劣。其提取的信道特征参数包括接收信号强度、信道状态信息、信道脉冲响应与到达波角度，详细介绍了基于无线信道脉冲响应的密钥生成模型。Wilson等[4]在超宽带系统中利用丰富的多径无线信道的信道脉冲响应来产生密钥；Tope等[5]利用接收信号的包络特征生成两个用户之间相同的密钥；Lou等[6]研究了水声环境下的基于接收信号强度的密钥生成技术；Lal等[7]提出了一种基于水声信道的密钥生成协议，并验证了协议的可行性。

本文提出利用水声信道多途的幅值和时延值来生成加密密钥，通过数据加密标准(Data encryption standard, DES)算法对重要信息进行加密；然后通过采用基于离散余弦变换(Discrete cosine transformation, DCT)变换的信息隐藏技术对加密数据进行隐藏；最后，通过正交频分复用(Orthogonal frequency division multiplexing, OFDM)水声高速通信技术进行数据传输。

1 信息加密技术

1.1 信息帧结构

信息帧结构包含三部分：信息头，帧序列号，数据，如图1所示。

基于互易性原理，本文采用两个节点间独特的信道特征来产生加密密钥。信息头用来做帧同步和信道估计，帧序列号用来防止信息重发攻击，且为密钥生成中的重要部分；数据负载包含要发送的信息。密钥是由发射机和接收机两部分独立生成，融合了信道多途测量量和帧序列号。为了进一步提升密钥的随机性，将m比特伪随机序列添加到k比特的密钥后(伪随机序列是关于帧序列号的函数)。$k+m$长度的密钥保证了更高级别的信息安全性。

图1 信息帧结构

Fig. 1 Information frame structure

1.2 密钥产生过程

当节点B要向节点A发送信息时，密钥的产生过程如图2所示。

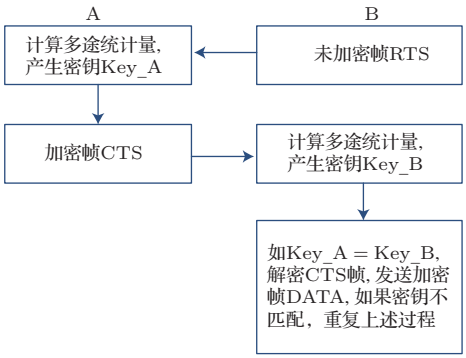


图2 密钥产生流程

Fig. 2 Key generation flow chart

节点B先发送一个未加密帧，节点A收到此帧后，通过信息头得到水声信道的脉冲响应，从而产生k长度的密钥Key_A，然后利用此密钥加密公开信息，将加密帧向节点B发送；同样，节点B接收到加密帧后产生密钥Key_B。如果Key_A、Key_B相同，帧被成功解密；否则，节点B重新向节点A发送未加密帧。如果经过N次密钥产生过程都未能正确匹配信道密钥，则采用预设的普通密钥。

1.2.1 水声信道多途量化

当估计水声信道时，先确定有效多途区分时间间隔(例如设置为1 ms)，以此时间间隔长度提取线

性调频 (Linear frequency modulation, LFM) 同步头脉冲压缩数据，取此数据段内最大值，循环此操作直至相关数据结束。接着依据峰值左右二分之一时间间隔内只存在唯一一个峰值，因而只保留最大值的原则，对上面处理后的数据进行虚假点剔除，从而得到估计的信道脉冲响应。再通过设定有效多途幅值门限来保证有效多途的抗噪声性能。最终通过预设有效多途数量来确定多途数量。

估计出水声信道脉冲函数以后，依据水声信道多途时延和幅值 (归一化处理) 来产生密钥，公式为

$$A_i' = A_i / A_{\max} / L_A, \tag{1}$$

其中，A_i' 为经过处理的第 i 条多途幅值，A_i 为未经过处理的第 i 条多途幅值，$A_{\max}$ 为信道多途幅值最大值，L_A 为幅度分级冗余量。

$$T_i' = T_i / T_{\max} / L_T, \tag{2}$$

其中，T_i' 为经过处理的第 i 条多途时延值，T_i 为未经过处理的第 i 条多途时延值，$T_{\max}$ 为信道多途时延最大值，L_T 为时延分级冗余量。

1.2.2　码字映射规则

表 1 为水声信道多途幅值大小与密钥的对应关系。

表 2 为水声信道多途时延大小与密钥的对应关系。

表 1　水声信道多途幅值大小与密钥的对应关系

Table 1　The corresponding relation between multipath amplitude of underwater acoustic channel and keys

幅值	(0,0.1]	(0.1,0.2]	(0.2,0.3]	⋯	(0.8,0.9]	(0.9,1]
密钥	1	2	3	⋯	9	1

表 2　水声信道多途时延大小与密钥的对应关系

Table 2　The corresponding relation between multipath delay of underwater acoustic channel and keys

时延	(0,0.1]	(0.1,0.2]	(0.2,0.3]	[0.3,0.4]	(0.4,0.5]	(0.5,0.6]
密钥	a	b	c	d	e	f

表 1、表 2 中密钥为十六进制表示形式。若通过水声信道生成的密钥长度不符合加密算法，则对其缺少的密钥位数进行预设密码相应位填充。

1.2.3　敏感性与稳定性优化

如果经过 M 次信息传输过程，收发两端密钥未能正确匹配，则增大幅度分级冗余量 L_A 和时延分级冗余量 L_T。通过调整以上两个控制量提高密钥生成算法的稳定性。

加密采用 DES 算法，使用 64 位密钥 (其中，包含 8 位奇偶校验，实际长度为 56 位) 对以 64 位为单位的块数据加密，产生 64 位密文数据，然后使用相同的密钥进行解密。

2　基于 DCT 的信息隐藏技术

根据人眼的视觉模型将重要信息有选择地分布到覆盖信号的变换域中，实现重要信息的隐藏。在变换域算法中，DCT 是最佳的变换，它能够很好地集中信息，并反映出人眼对视觉频率的敏感度影响。故以上方法能够较有效地降低窃听人员对嵌入信息图片的识别率。

2.1　DCT 变换原理

一个 $M \times N$ 矩阵 $\boldsymbol{A}$ 的二维 DCT 定义为

$$B_{pq} = a_p a_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_m \cos \frac{\pi(2m+1)p}{2M} \cdot \cos \frac{\pi(2n+1)q}{2N}, \tag{3}$$

其中，a_p 和 a_q 是与 M、N 有关的系数，满足如下关系：

$$a_p = \begin{cases} \dfrac{1}{\sqrt{M}}, & p = 0, \\ \sqrt{\dfrac{2}{M}}, & 1 \leqslant p \leqslant M-1, \end{cases}$$

$$a_q = \begin{cases} \dfrac{1}{\sqrt{N}}, & q = 0. \\ \sqrt{\dfrac{2}{N}}, & 1 \leqslant q \leqslant N-1. \end{cases} \tag{4}$$

为了分块 DCT 的需要，引入了 DCT 变换矩阵的概念。$M \times M$ 变换矩阵 $\boldsymbol{T}$ 为

$$\boldsymbol{T} = \begin{cases} \dfrac{1}{\sqrt{M}}, & p = 0, \\ & 0 \leqslant q \leqslant M-1, \\ \sqrt{\dfrac{2}{M}} \cos \dfrac{\pi(2q+1)p}{2M}, & 1 \leqslant p \leqslant M-1, \\ & 0 \leqslant q \leqslant M-1. \end{cases} \tag{5}$$

对于 $M \times N$ 矩阵 $\boldsymbol{A}$，$\boldsymbol{T} \times \boldsymbol{A}$ 是一个 $M \times N$ 的矩阵，该矩阵的列包含矩阵 $\boldsymbol{A}$ 列的一维 DCT。矩阵

$\boldsymbol{A}$的二维DCT可以通过$\boldsymbol{T}\times\boldsymbol{B}\times\boldsymbol{T}'$获得。因为$\boldsymbol{T}$是一个标准正交矩阵，所以它的逆变换形式和变换形式相同，因此矩阵$\boldsymbol{B}$的二维DCT由$\boldsymbol{T}'\times\boldsymbol{A}\times\boldsymbol{T}$计算得出。

2.2 信息嵌入与提取

图3为信息嵌入与提取流程。

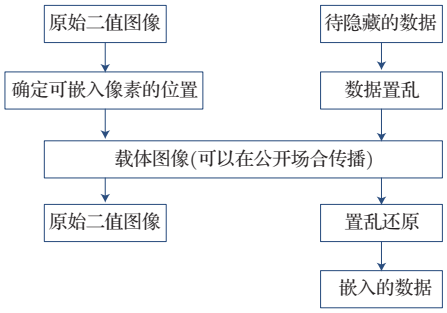


图3 信息嵌入与提取流程

Fig. 3 Flow chart of information embedding and extraction

在图3中，本文欲将重要信息隐藏在普通、公开的图片之中，从而降低窃听人员对传输信息的关注度。首先，对载体图像进行预处理。在嵌入隐藏的重要信息之前，要先对原来的图像分成8×8的像素块，对分割以后的每一个图像子块进行DCT变换，从而得到DCT系数矩阵；对DCT系数按“Z”字形式重新编排，是把一个8×8的DCT系数矩阵和一个1×16的系数矢量相对应。接下来，重要信息将以二进制流的形式嵌入到原始图像DCT系数中。最后，在重要信息嵌入到载体后，把修改以后的数组按照之前所记录排序次序放到原来所在的1×16矢量的位置上，并由这个矢量构造新的8×8的DCT系数矩阵，对新的DCT系数方块进行逆DCT变换，得到加载重要信息的载体图像。

与嵌入过程类似，首先对藏有重要信息的图像进行8×8分块，求出每块的DCT系数，然后利用密钥确定包含重要信息的方块，与此同时，利用视觉系统的照明掩蔽特性以及纹理掩蔽特性将块分类，并通过判决，提取隐藏信息。

3 仿真及结果分析

3.1 隐蔽通信系统参数

表3、表4分别为DCT变换信息隐藏参数对和DES加密算法参数列表。

表3 DCT变换信息隐藏参数

Table 3 DCT transform information hiding parameters

个数	位置
1	(4,1)与(3,2)
2	(2,2)与(1,3)

表4 DES加密算法参数

Table 4 DES encryption algorithm parameters

密钥长度	64
数据输入长度	64
数据输出长度	64
预设密钥	1234567897654321

依据传输的信息比特对表3中的信息隐藏参数对的数值进行设置。

表5为不同场景下的仿真水声信道数据，采用BELLHOP算法产生。表中数据格式：(a,b)，a代表幅值(真实幅值的100倍)；b代表时延，单位ms。

通信节点间仿真距离设定为两组，分别为500 m和498 m，水下深度均为15 m；窃听节点距某一通信节点450 m，深度为15 m。

表5 不同场景下的水声信道数据

Table 5 Underwater acoustic channel data in different scenarios

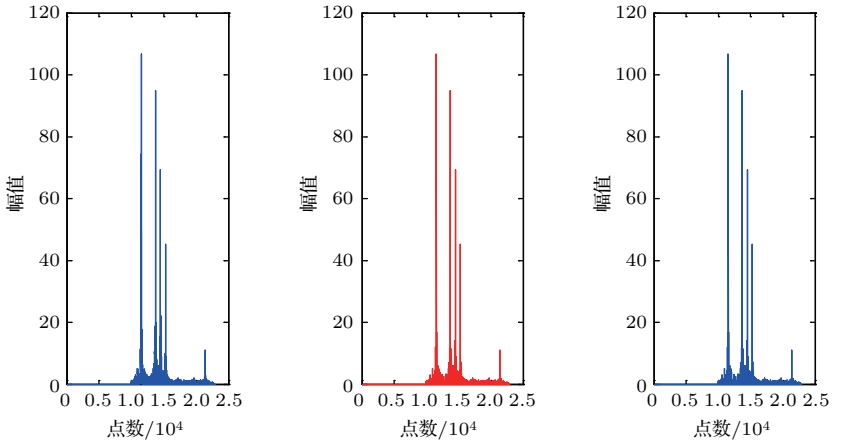
节点间距/m	多途					
	1	2	3	4	5	6
500	(1.575,341)	(−2.4,342.5)	(1.7,364.8)	(−1.38,371)	(0.95,379)	(0.25,429.5)
498	(1.6,339.6)	(−2.4,341.1)	(1.7,363.3)	(−1.38,370.2)	(0.95,378.3)	(0.25,428.5)
450	(1.8,308.5)	(−2.4,309.2)	(1.85,332)	(−1.35,339.8)	(0.88,348.2)	(0.22,4112)

3.2　仿真结果

3.2.1　信道估计结果

仿真中，水声信道数据选取两通信节点相距500 m时的数据(如表5所示)，并对生成的时域通信信号加高斯白噪声，信噪比为10 dB。

图4为采用本文提出的方法对信道进行两步估计的结果，对比图4(c)和表6中相应的信道可知，估计结果与仿真信道相吻合。



(a) LFM同步头相关结果　(b) 1 ms长度内取最大值的结果　(c) 剔除虚假点后的信道结果

图4　水声信道估计结果

Fig. 4　Estimation result of underwater acoustic channel

3.2.2　密钥生成

表6为依据水声信道估计生成密钥结果。

表6　依据水声信道生成密钥结果

Table 6　Generating keys based on underwater acoustic channel

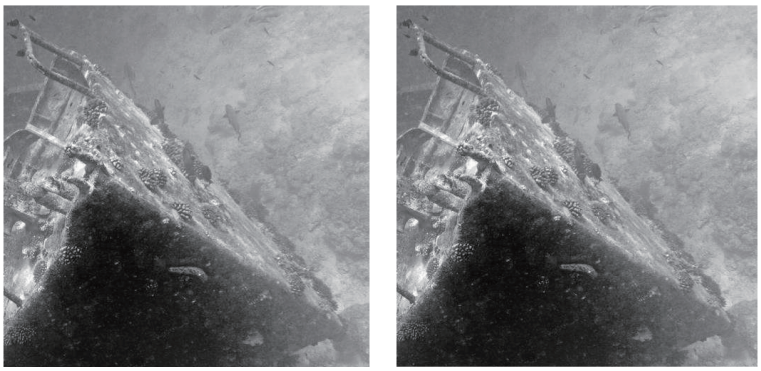
信道(节点间距离)	产生密钥
500 m	7f2a8e6e4a2d
498 m	7f2a8e6e4a2d
450 m	8f2f8e6a4c

由表6可知，当节点间距离变换不明显时，水声信道相对稳定，通信双方能够生成匹配密钥，但节点位置发生明显变换(窃听节点)，即使其知晓密钥生成算法，也无法解析出加密密钥。

3.2.3　图像加密解密

(1) 信息嵌入

采用512 × 512的水下沉船图像作为仿真载体图像(图5(a))，并将长度为704 bits的0、1序列作为重要信息隐藏在载体图像中。将原图分成8 × 8



(a) 原始图像　(b) 嵌入信息图像

图5　嵌入信息图像与原始图像对比

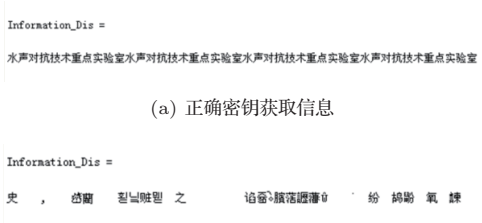
Fig. 5　Comparing embedded information image with original image

的像素块，对分割以后的每一个图像子块进行DCT变换，从而得到DCT系数矩阵。依据传输的信息比特对表4中的信息隐藏参数对进行设置。如传输的数据为01，则将(4,1)像素值设定为比(3,2)像素值小，(2,2)像素值设定为比(1,3)像素值大。再对获得的DCT系数方块进行逆DCT变换，得到加载重要信息的载体图像(图5(b))。

由图5可知，人眼看不出原图和含有重要信息的图像之间有任何区别，表明采用方法实现信息隐藏具有良好的隐蔽性。

(2) 信息提取

图6为不同密钥情况下提取信息对比例。



(a) 正确密钥获取信息

(b) 错误密钥获取信息

图6 不同密钥情况下提取信息对比例

Fig. 6 Comparisons of information extraction under different key conditions

由图6解密结果可知，即使敌方了解到有重要信息发送，且知道隐藏算法，由于其不知道密钥，即使通信方也只知道算法不知道实时的密码，其只与通信节点间的水声传输信道相关，更具安全性。

4 试验结果

项目组在厦门五缘湾水域对基于水声信道估计的密钥生成技术进行验证试验。五缘湾水深6 m，换能器置于水下3 m，相距60 m。

4.1 水声信道冲激响应稳定性验证

图7为水声信道冲激响应稳定性试验结果。

图7为节点位于水下3 m、相距60 m，带宽13 kHz ~18 kHz，时长为30 ms的LFM信号在厦门五缘湾水域的传输处理结果。当将处理结果根据时间叠堆在一起的时候，信道脉冲响应时间跨度大约为300 s，0 ms时延对应的是直达声波，从中可以得到多途扩展大约为65 ms。从整体上看可知，信道的脉冲响应稳定时长大约为5 min，能够胜任密钥产生的时间要求。

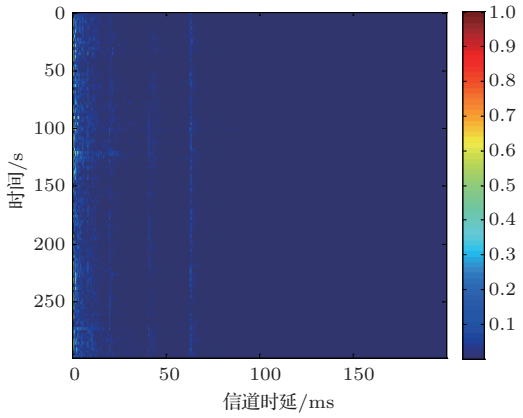


图7 水声信道冲激响应稳定性试验结果

Fig. 7 Test results of impulse response stability of underwater acoustic channel

4.2 基于水声信道冲激响应的密钥生成试验

换能器A发送一个带宽13 kHz ~ 18kHz、时长为30 ms的LFM信号；换能器B接收到换能器A发送的LFM信号后，立即返回一个相同的LFM信号。通过对往返LFM信号进行水声信道估计，并依据估计的水声信道生成加密密钥。图8为信道交互试验数据。

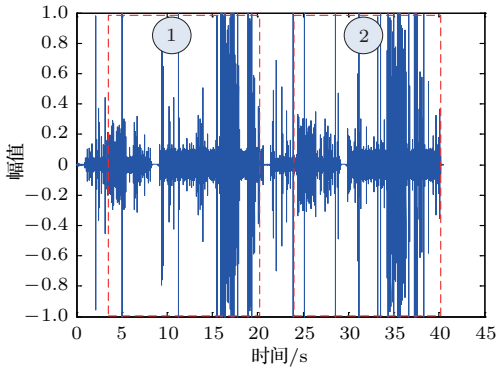
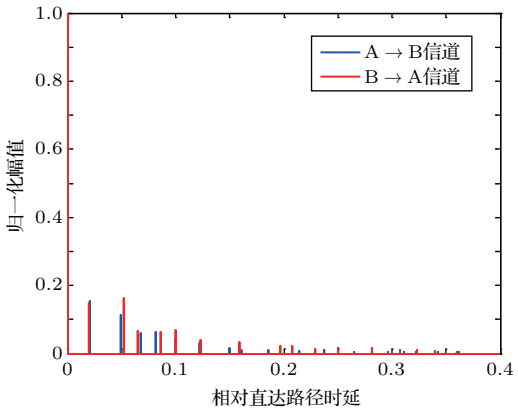


图8 信道交互试验数据

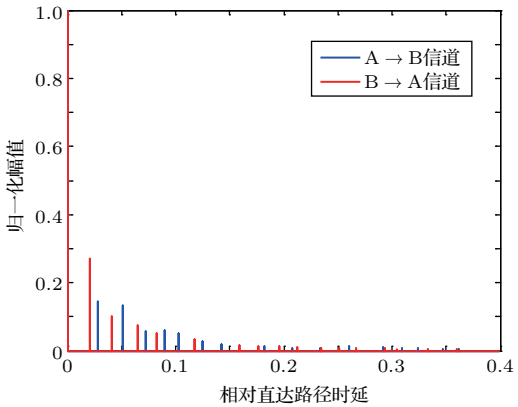
Fig. 8 Channel interaction test data

通过对两次信道交互数据(如图8所示)进行匹配相关处理，获取水声信道估计；接下来通过设定有效多途区分间隔(20 ms)、有效多途幅值门限(最大值的十分之一)和预设有效多途数量(6)来得到简化的水声估计信道，如图9所示；通过控制幅度分级冗余量(0.3)和时延分级冗余量(0.1)来生成加密密钥，结果如表7所示。

从表7可知，使用基于信道估计的密钥生成技术能够生成匹配加密密钥，为安全保密的水声通信提供一种可行的密钥生成技术。



(a) 第一次信道交互估计信道



(b) 第二 次信道交互估计信道

图 9　交互数据信道估计结果

Fig. 9　Channel estimation results based on interactive data

表 7　基于信道交互数据生成密钥

Table 7　Generating keys based on channel interactive data

信道交互次序	A→B	B→A
1	4a1c1f	4a1c1f
2	4a1d1f	4a1d1f

5　结论

针对水下信息隐蔽传输的需求，本文首先从信息加密密钥生成技术入手，利用水声信道存在明显的时变、空变、频变特性，通过匹配滤波器估计水声信道，并基于水声信道估计生成加密密钥，从而提升信息的安全性能；采用基于 DCT 的信息隐蔽方法，将传输的加密重要信息隐藏在普通载体之上，提高了信息的隐蔽性能，最终实现信息的安全隐蔽传输。仿真与试验结果验证了基于水声信道冲激响应生成加密密钥的可行性。

采用本文的实时动态密钥生成算法来进行保密通信时，由于考虑到水声信道的复杂性噪声收发两端生成密钥的不匹配状况，预设了密钥匹配不成功情况下的替代加密密钥，故当发送加密数据帧时要添加密钥标志，从而通知接收端采用的是预设密钥还是实时密钥。相对于未采用实时加密算法的通信方式额外增加一些通信数据；且水声信道的估计和密钥生成算法增加了硬件平台的计算量。但对于保密需求迫切的水下应用场合，通信数据和计算量的少许增加认为是可以接受的。

致谢　感谢重点实验室对五缘湾试验的支持以及张俊清工程师在试验过程中做出的努力。

参　考　文　献

[1] Ling J, He H, Li J, et al. Covert underwater acoustic communications[J]. Journal of the Acoustical Society of America, 2010, 128(5): 2898–2909.

[2] 韩笑, 殷敬伟, 郭龙祥, 等. 基于差分 Pattern 时延差编码和海豚 whistles 信号的仿生水声通信技术研究 [J]. 物理学报, 2013, 62(22): 224301.
Han Xiao, Yin Jingwei, Guo Longxiang, et al. Research on bionic underwater acoustic communication technology based on differential pattern time delay shift coding and dolphin whistles[J]. Acta Physica Sinica, 2013, 62(22): 224301.

[3] 石会, 龚晶, 顾里俊, 等. 一种基于信道脉冲响应 (CIR) 的物理密钥生成算法 [J]. 通信技术, 2018, 51(10): 2459–2463.
Shi hui, Gong Jing, Gu Lijun, et al. Physical key generation algorithm based on channel impulse response[J]. Communications Technology, 2018, 51(10): 2459–2463.

[4] Wilson R, Tse D, Scholtz R A. Channel identification: secret sharing using reciprocity in ultrawideband channels[J]. IEEE Transactions on Information Forensics and Security, 2007, 2(3): 364–375.

[5] Tope M A, McEachen J C. Unconditionally secure communications over fading channels[C]. Military Communications Conference, 2001, 1: 54–58.

[6] Lou Y M, Jin L, Zhong Z, et al. Secret key genneration scheme based on MIMO received signal spaces[C]. Science China: Information Science, 2016, 4: 4464–4477.

[7] Lal C, Petroccia R, Pelekanakis K. Toward the development of secure underwater acoustic networks[J]. IEEE Journal of Oceanic Engineering, 2017, 42(4): 1075–1087.