中国科学: 信息科学 2023 年 第 53 卷 第 6 期: 1096–1110
SCIENTIA SINICA Informationis
论文

基于水声信道的隐蔽密钥协商方案

徐明[1,2*], 冯赫鑫[1], 关佶红[2,3]

1. 上海海事大学信息工程学院, 上海 201306
2. 同济大学电子与信息工程学院, 上海 201804
3. 嵌入式系统与服务计算教育部重点实验室 (同济大学), 上海 201804
* 通信作者. E-mail: mingxu@shmtu.edu.cn

收稿日期: 2022–07–19; 修回日期: 2022–10–07; 接受日期: 2022–10–30; 网络出版日期: 2023–06–07

国家自然科学基金联合重点项目 (批准号: U1936205)、国家自然科学基金面上项目 (批准号: 62172269) 和中国博士后科学基金项目 (批准号: 2014M561512) 资助

摘要 水声信道环境下, 传统的密钥协商协议更容易遭受信息泄漏等安全威胁, 而现有的隐蔽密钥协商协议由于受限于平方根定律, 隐蔽通信速率不超过 $O(1/\sqrt{n})$. 为解决上述难题, 本文提出了一种基于水声信道的隐蔽密钥协商方案. 在优先提取阶段, 发送方以一定的功率向接收方发送均匀分布的随机消息, 而接收方根据水下噪声方差信息, 通过 Gibbs 采样计算出估计消息, 并使用对数似然比检验获取初始密钥来减少消息传输时的不确定性和误比特率. 信息调和阶段, 发送方将伴随式发送给接收方, 而接收方将接收到的伴随式与优先提取阶段得到的对数似然比序列进行联合解码来获得错误比特的位置信息, 经过比特翻转后得到与发送方完全一致的最终密钥. 通过假设检验理论和信息论, 证明了方案的保密性、隐蔽性和可靠性. 仿真结果表明, 所提方案比现有方案性能有所提升.

关键词 水声信道, 隐蔽密钥协商, 优先提取, 信息调和, 对数似然比检验

1 引言

随着各个沿海国家对开发海洋资源和维护国家海洋权益的日益重视, 海洋信息的获取、传输、处理和融合在海洋科学研究、环境调查、资源开发、权益维护与安全防卫中发挥了重要的作用, 并因其应用环境的特殊性而成为信息科学研究的热点之一 [1]. 水声通信是海洋中无线信息传输的主要技术手段. 水下节点通常部署在无人值守的恶劣环境中以及水声信道 (underwater acoustic channel, UAC) 的开放性使得水下信息传输面临的安全问题更为严重 [2]. 密钥协商协议是密码学基本原语之一, 允许通信双方在不安全的信道环境下协商出公共密钥, 为合法节点的通信安全提供认证性、机密性和完整性保护 [3]. 文献 [4] 提出了利用无线信道的特征参数作为共享随机源的思想. 由于无线信道固有的随机性和互易性, 合法通信双方可以在较短的信道相干时间内互发导频信号获得相关性较高的信道特

引用格式: 徐明, 冯赫鑫, 关佶红. 基于水声信道的隐蔽密钥协商方案. 中国科学: 信息科学, 2023, 53: 1096–1110, doi: 10.1360/SSI-2022-0291
Xu M, Feng H X, Guan J H. Covert secret-key agreement scheme based on an underwater acoustic channel (in Chinese). Sci Sin Inform, 2023, 53: 1096–1110, doi: 10.1360/SSI-2022-0291

征, 通过提取特征参数产生密钥, 并且能够随着信道物理特征的改变, 快速进行更新 [5]. 进一步, 文献 [6] 将智能超表面天线配置在基站设备端用于密钥生成, 通过捷变控制智能超表面单元相移变化生成随机快变波束, 从而使密钥容量不受制于自然信道变化速度, 因此适应性更好. 然而, 由于水下通常采用声呐进行通信, 而水声信道具有传输速率低、误码率高、时延高和带宽窄等特性, 使得传统的密钥协商协议越来越容易遭受信息泄漏等安全威胁. 因此, 如何确保合法节点在密钥协商过程中以较低的概率被非法检测方侦测到信息传输尤为关键. 近年来, 一些学者在密钥协商协议中引入隐蔽通信技术, 利用加密算法将需要隐藏的密钥嵌入到公开信息中, 使得嵌入后的消息与原消息的相对熵尽可能小, 达到迷惑非法检测方的目的. 文献 [7] 提出了隐蔽通信的概念和隐蔽通信速率的平方根定律, 给出了隐蔽通信速率的上界. 文献 [8] 提出了噪声墙的概念, 当非法检测方接收信号信噪比小于噪声墙时, 无法通过假设检验判断通信方是否传输信息. 文献 [9] 利用噪声墙实现了隐蔽通信, 证明了窃听者对接收噪声的功率具有不确定性时可以突破平方根定律的约束, 使渐进隐蔽速率达到正常数, 并给出了通信方传输功率的上界, 但是该方案中的鲁棒性检测仅考虑了非法检测方检测性能的下界, 故不具有代表性. 文献 [10] 提出了一种基于状态依赖离散无记忆信道的隐蔽密钥协商方案, 推导出非法检测方可以任意选择信道状态时的隐蔽密钥容量, 并证明了当发送方到接收方和非法检测方的信道相互独立时, 隐蔽密钥容量等于信道的隐蔽容量. 然而, 该方案没有考虑到水下环境噪声存在不确定性的情况, 这将导致解码器通过广播消息和输入序列联合解码时产生误差, 增加了误比特率并降低了隐蔽密钥生成速率. 此外, 水声信道中的噪声除了存在环境噪声, 还包含特定地点噪声 (site-specific noise) [11]. 其中, 环境噪声包括热噪声、船只噪声、湍流噪声和风成噪声, 可被建模为服从高斯 (Gauss) 分布的粉色噪声. 特定地点噪声通常在一些固定区域出现, 例如, 渔业捕捞作业时产生的噪声. 与环境噪声不同, 特定地点噪声通常包含显著的非高斯分量, 可被建模为服从拉普拉斯 (Laplace) 分布的粉色噪声. 然而, 现有研究忽略了特定地点噪声对隐蔽密钥协商协议性能的影响. 此外, 在水声信道环境下, 其固有的传输损失增加了通信双方数据传输的不确定性和误比特率 (bit error rate, BER), 降低了密钥生成速率. 针对上述问题, 本文建立了一个包含特定地点噪声源的隐蔽密钥协商系统模型. 在此基础上, 提出了一种基于水声信道的隐蔽密钥协商方案. 该方案中, 发送方以一定的功率向接收方发送均匀分布的随机消息, 而接收方根据水下噪声方差信息, 通过 Gibbs 采样计算出估计消息, 然后使用对数似然比 (log-likelihood ratio, LLR) 检验获取初始密钥, 再根据 Slepian-Wolf 编码原理进行信息调和生成最终密钥, 从而降低了通信双方数据传输的不确定性和误比特率, 确保发送方在低信噪比情况下仍然可以进行隐蔽密钥协商. 本文的主要贡献如下: (1) 针对水声信道环境下固有的噪声干扰和传输损失, 建立了相应的隐蔽密钥协商系统模型, 并给出了隐蔽密钥协商方案的形式化定义. (2) 提出了一种基于水声信道的隐蔽密钥协商方案, 给出了对数似然比检验的最优检验阈值, 优化了误比特率, 最后通过仿真实验和对比数据验证了本文方案的有效性. (3) 通过贝叶斯 (Bayes) 统计得出平均隐蔽概率并由此推导出非法检测方的最优检测阈值, 给出了发送方服从隐蔽性约束时传输功率的上界以及服从可靠性约束时传输功率的下界. (4) 通过可靠性分析, 证明了本文方案可以将隐蔽通信速率从现有的 $O(1/\sqrt{n})$ 提升到 $O((\rho^{4\varepsilon-1}+1-1/\rho)/\sqrt{n})$, 并推导出本文方案的最大隐蔽密钥生成速率.

2 系统模型

2.1 隐蔽密钥协商系统模型

本文考虑一个如图 1 所示的水声信道环境下的隐蔽密钥协商系统模型. 该模型由合法发送方 Alice,

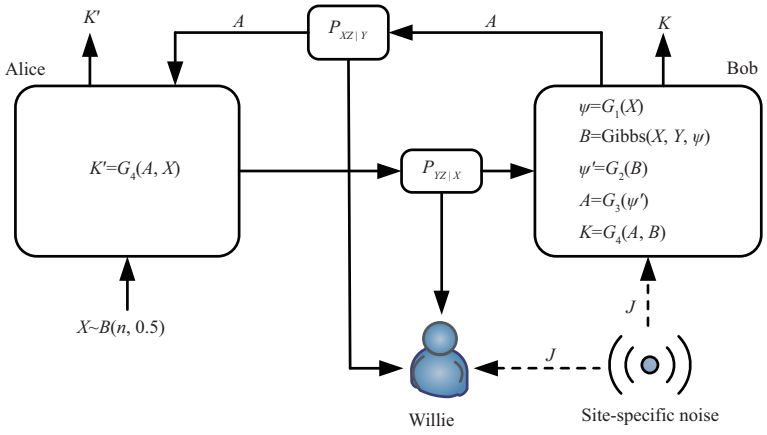

图 1 (网络版彩图) 水声信道环境下的隐蔽密钥协商系统模型

Figure 1 (Color online) Covert secret-key agreement system model for the UAC

合法接收方 Bob 和主动非法检测方 Willie 组成. Alice 通过水声信道传输包含 n 个二进制相移键控 (binary phase shift keying, BPSK) 符号的信号 X_n, 且 $X_n \sim (n, 0.5)$, 平均传输功率上界为 P_t, 则 Bob 或 Willie 接收到的信号可表示为

$$y_{i,k} = \frac{\sqrt{P_t}x_k\Omega_{ai}}{H_{ai}} + v_i + v_i', \tag{1}$$

其中, $i \in \{b, \omega\}$, b 代表 Bob, ω 代表 Willie, $k \in 1, \ldots, L$, H_{ai} 为 Alice 与 Bob 或 Willie 之间的传输损失, 满足 $E[|H_{ai}|^2] = \eta\log(d_{ai}) + \alpha(\theta)\frac{d_{ai}}{1000}$, d_{ai} 为 Alice 与 Bob 或 Willie 之间的距离, α 为吸收衰减系数, 其值由载波频率 θ 决定, 可由 Thorp 经验公式 $\alpha(\theta) = 0.036\theta^{3/2}$ 计算得出 [12], η 为传播损失系数, 其值由信道结构决定. $x_k = a$, $a \in \{-1, 1\}$ 为 Alice 发送的信号比特, Ω_{ai} 为 Alice 与 Bob 或 Willie 之间的水声信道冲激响应, 满足 $E[|\Omega_{a\omega}|^2] = \sigma_g^2$, $E[|\Omega_{ab}|^2] = \sigma_h^2$, 则 Bob 或 Willie 的平均接收功率 $P_{ai} = \frac{P_t\Omega_{ai}^2}{H_{ai}^2}$, v_i 为 Bob 或 Willie 的环境噪声变量, 服从复圆对称广义生成高斯分布 [13], 即 $v_i \sim CN(0, \sigma_i^2)$, v_i' 为特定地点噪声变量, 服从拉普拉斯分布, 即 $v_i' \sim \text{La}(0, 0.5\sqrt{P_j})$, $E(v_i') = 0$, $D(v_i') = P_j$. 特定地点噪声作为独立的噪声源会对 Bob 或 Willie 的平均接收功率产生影响, 此时在 Bob 或 Willie 处所产生的额外平均接收功率可表示为 $P_{ji} = \frac{P_j\Omega_{ji}^2}{H_{ji}^2}$, 其中, j 代表特定地点噪声源, H_{ji} 代表特定地点噪声源与 Bob 或 Willie 之间的传输损失, Ω_{ji} 代表特定地点噪声源与 Bob 或 Willie 之间的水声信道冲激响应, 满足 $E[|\Omega_{j\omega}|^2] = \sigma_{j\omega}^2$, $E[|\Omega_{jb}|^2] = \sigma_{jb}^2$. 由于水下噪声是多种噪声源共同作用的结果, 往往存在不确定性. 假设噪声功率服从对数均匀分布, 其概率密度函数可表示为 [14]

$$f_m(x) = \begin{cases} \frac{1}{2\ln(\rho)x}, & \frac{1}{\rho}\sigma_{mi}^2 \leqslant x \leqslant \rho\sigma_{mi}^2, \\ 0, & \text{others}, \end{cases} \tag{2}$$

其中 ρ 代表噪声不确定度, 单位为 dB, σ_{mi}^2 代表 i 处的基本噪声水平. 水声信道的平均误比特率可表示为 $P_{ai}(\gamma_{ai}) = \frac{1}{2}\sqrt{\frac{\gamma_{ai}}{1+\gamma_{ai}}} < 0.5$ [15], γ_{ai} 为水声信道的平均信噪比, 可表示为 $\gamma_{ai} = \frac{P_t\Omega_{ai}^2}{H_{ai}^2\sigma_i^2}$.

2.2 敌手模型

Willie 基于二元假设检验判断 Alice 是否进行了信号传输. 不同于文献 [9] 的鲁棒性检测, 本文假定 Willie 采用能量检测法, 若 Willie 能够收集到的信号样本数量 N 趋于无限, 通过中心极限定理可

以近似得到其统计检验量 $T(y_\omega)=(1/N)y_\omega^H y_\omega=(1/N)\sum_{n=1}^{N}\left|y_\omega[n]^2\right|>\gamma$, γ 代表 Willie 探测器设定的检测阈值. 令 H_0 代表 Alice 没有传输信号, H_1 代表 Alice 传输了信号, D_0 和 D_1 代表对假设检验的二维判决, 则误检率 P_{FA} 可表示为 $P_{FA}=P(D_1|H_0)=\Pr(T(y_\omega)>\gamma|H_0)$, 漏检率 P_{MD} 可表示为 $P_{MD}=P(D_0|H_1)=\Pr(T(y_\omega)<\gamma|H_1)$, 隐蔽概率可表示为 $\xi=P_{FA}+P_{MD}\geqslant 1-\varepsilon$. 隐蔽密钥协商要求 $E[\min_\gamma(P_{FA}+P_{MD})]\geqslant 1-\varepsilon$, 即 $\xi_{\min}\geqslant 1-\varepsilon$, ξ 代表隐蔽性约束. 当 $\xi=0$ 时, Willie 可以无差错地检测到密钥协商过程; 当 $\xi=1$ 时, Willie 对密钥协商过程一无所知, 等效于随机猜测. 本文假设 Willie 为主动非法检测方, 具有最优检测性能, 可以主动调整探测器的检测阈值使得探测时的隐蔽概率最小, 并且完全知晓信道的状态信息. 因此, 探测器的最优检测阈值可表示为

$$\gamma^*=\arg\min_{\gamma}\xi. \tag{3}$$

3 隐蔽密钥协商方案

本节首先给出隐蔽密钥协商方案的形式化定义以及本文方案的主要步骤, 包括优先提取和信息调和. 其中, 优先提取是指若合法通信双方的信道质量低于非法检测方, 那么存在一个随机变量使得合法通信双方经过一系列的信息交流, 能够从中提取出有用的信息串, 而且合法接收方对该信息串的不确定性要小于非法检测方对该信息串的不确定性. 信息调和是指合法通信双方交换冗余信息并利用纠错技术使得合法接收方以很高的概率确定密钥信息, 而非法检测方却不能完全确定密钥信息. 然后, 我们对算法中的检验阈值进行分析, 发现其最优值与整体误比特率的关系, 并通过计算得到最优检验阈值.

3.1 形式化定义

首先给出隐蔽密钥协商方案的形式化定义.

定义1 存在一个密钥协商方案 G, 具体表示为 5 元组 $G=(M_n,n,\tau,\varepsilon,\upsilon)$, 其中 M_n 代表消息, n 代表消息长度, τ 表示保密性约束, ε 表示隐蔽性约束, υ 表示可靠性约束, 其中, τ, ε, υ 为任意小的正数. 当密钥协商方案 G 满足以下 3 个性能指标, 即

$$\begin{aligned}&\text{保密性}\quad S(G)\triangleq\mathbb{D}(P_{AYZ}||P_{AKYZ})\leqslant\tau,\\&\text{隐蔽性}\quad C(G)=\xi=P_{FA}+P_{MD}\geqslant 1-\varepsilon,\\&\text{可靠性}\quad P(G)\triangleq P(K\neq K')\leqslant\upsilon,\end{aligned}$$

其中 $S(G)$ 代表密钥泄漏率, $\mathbb{D}(\cdot)$ 代表相对熵, P_{AYZ} 代表 Alice 消息比特对应的索引 A, Bob 收到的序列 Y 和 Willie 收到的序列 Z 的联合分布, P_{AKYZ} 代表以上三者与 Alice 生成的密钥 K 的联合分布, $C(G)$ 代表隐蔽概率, $P(G)$ 代表解码错误概率, K' 代表 Bob 生成的密钥, 该密钥协商方案 G 被称为隐蔽密钥协商方案.

基于水声信道的隐蔽密钥协商方案包含优先提取和信息调和 2 个部分. 合法双方 Alice 和 Bob 需要在 Willie 的监视下进行隐蔽密钥协商. 为了满足方案的可靠性和隐蔽性, Alice 需要以 $P_t^-\leqslant P_t\leqslant P_t^+$ 的功率传输信号, 其中, P_t^- 为 Alice 隐蔽传输功率的下界. 若 Alice 的发送功率低于此下界, 则 Bob 不能可靠地解码 Alice 传输的消息. P_t^+ 为 Alice 隐蔽传输功率的上界. 若 Alice 的发送功率超过此上界, Willie 就会以一定的概率检测到合法节点的消息传输. 在隐蔽密钥协商过程中, 只要 Alice 的发送功率满足 $P_t^-\leqslant P_t\leqslant P_t^+$, 则 Bob 能够正确解码消息并且不会向 Willie 泄漏密钥协商的任何信息.

3.2 优先提取

优先提取可以让通信双方从 q 个随机生成的均匀分布信号中提取出相同的比特串组成初始密钥. 为了提高隐蔽密钥生成速率, Bob 根据水声信道转移概率计算出接收信号序列 Y_n 中每个信号比特的 LLR 值, 然后结合水下噪声方差信息, 通过 Gibbs 采样计算出 Alice 发送的信号序列 X_n 的估计序列. Gibbs 采样通过对条件分布的迭代抽样, 从联合分布中生成样本, 并根据给定的噪声方差推导出模型参数, 因此可以得到准确的估计序列 [16]. 然后, Bob 通过检验阈值 Λ 对估计序列进行 LLR 检验来提取满足筛选条件的比特. 其中, 检验阈值会随着信道参数的改变而发生改变, 但总存在一个最优检验阈值使得隐蔽密钥协商的总体误比特率最低. 最后, Bob 将提取出的比特索引反馈给 Alice, 然后合法通信双方分别从 X_n 和 B_n 中提取出满足阈值条件的信号比特生成初始密钥. 在此过程中, Alice 不需要知道 Bob 选择的检验阈值, 因此该参数的设定不需要协商. 假设在优先提取之前, 合法通信双方共同约定的密钥长度为 D, 则优先提取的具体过程可表示如下.

(1) Alice 随机生成一个长度为 n 的均匀分布信号序列 X_n 发送给 Bob.

(2) 当 Bob 接收到信号序列 $Y_n=(y_{b,0},y_{b,1},\dots,y_{b,L-1})$ 后, 根据公开函数 $G_1:Y\to\Psi$ 计算 Y_n 中每个信号比特 $y_{b,k}\in Y$ 的 LLR 值, 即

$$\psi_k=G_1(y_{b,k})=\left|\ln\frac{P(x_k=1|\frac{\Omega_{ab}}{H_{ab}},y_{b,k})}{P(x_k=-1|\frac{\Omega_{ab}}{H_{ab}},y_{b,k})}\right|=\left|\ln\frac{\exp(-\frac{|y_{b,k}-\frac{\Omega_{ab}}{H_{ab}}|^2}{2(\sigma_b^2+P_{jb})})}{\exp(-\frac{|y_{b,k}+\frac{\Omega_{ab}}{H_{ab}}|^2}{2(\sigma_b^2+P_{jb})})}\right|=\frac{2P_{ab}}{\sigma_b^2+P_{jb}}y_{b,k}. \tag{4}$$

(3) Bob 生成一个均匀分布的随机序列 B_n^0, 再根据条件概率 $P_b^I=P(b_k=a|\bar{b}_k,Y_n,\psi_k)$ 计算出 X_n 的估计序列 $B_n^I=(b_0^I,b_1^I,\dots,b_{n-1}^I)$, 其中, I 为 Gibbs 采样的迭代次数 ($I>0$), $\bar{b}_k=(b_0^{(I)},\dots,b_{k-1}^{(I)},b_{k+1}^{(I-1)},b_{n-1}^{(I-1)})$, 条件概率 P_b^I 可由式 (5) 得出

$$P(b_k=a'|\bar{b}_k,Y_n,\psi_k)=C\cdot\exp\left\{\sum_{i=0}^{L-1}\left(-\frac{1}{D(v+v')}\left|y_{b,i}-\frac{\Omega_{ab}}{H_{ab}}b_i\right|^2\right)\right\}\times P(b_k=a'), \tag{5}$$

其中 $D(v+v')$ 为水下噪声方差, $P(b_k=a)$ 可由 ψ_k 计算得出, C 为度量常数, 满足 $P(b_k=1|\bar{b}_k,Y_n)+P(b_k=-1|\bar{b}_k,Y_n)=1$, 迭代次数 I 满足变分距离 $V_T(P_b^I,P_b^{I-1})\leqslant e'$ [17], $e'>0$, 其值由可靠性约束 v 确定. 此时 Bob 通过公开函数 $G_2:B\to\Psi'$ 得到 B_L 中每个信号比特的 LLR 值 $\psi_k'\in\Psi'$, 构成 LLR 序列 $\Psi_n'=(\psi_0',\psi_1',\dots,\psi_{n-1}')$, 其中 G_2 可表示为

$$\psi_k'=G_2(b_k)=\left|\ln\frac{P(b_k=1|\bar{b}_k,\frac{\Omega_{ab}}{H_{ab}},Y_n,\psi_k)}{P(b_k=-1|\bar{b}_k,\frac{\Omega_{ab}}{H_{ab}},Y_n,\psi_k)}\right|=\left|\ln\frac{\prod_{k=1}^{K}P(y_{b,k}=1|\frac{\Omega_{ab}}{H_{ab}},B_n)}{\prod_{k=1}^{K}P(y_{b,k}=-1|\frac{\Omega_{ab}}{H_{ab}},B_n)}\right|+|\psi_k|. \tag{6}$$

然后根据公开函数 $G_3:\Psi'\to\mathrm{A}$ 筛选出 Ψ_n' 中 LLR 值 ψ_k' 符合阈值条件 $|\psi_k'|>\Lambda$ 的索引 $k\in A$, 并将这些索引反馈给 Alice.

(4) Alice 和 Bob 根据公开函数 $G_4:A\to U$ 分别从 X_n 和 B_n 中提取出这些索引所对应的 X_n 和 B_n 中的值.

(5) 若通过步骤 (4) 提取出的信号比特总长度小于 D, 当 Bob 将索引反馈给 Alice 后, Alice 继续发送第 $q+1$ 个均匀分布的信号进行下一次迭代. 令 l_γ 为 Bob 反馈的信号长度, 则下一次迭代需要满足的条件为

$$\Delta_q=\sum_{\gamma=1}^{q}l_\gamma<D\ \text{且}\ \Delta_0=0. \tag{7}$$

若通过步骤 (4) 提取出的信号比特总长度大于 D, 则 Bob 舍去多余部分, 将 $D-\Delta_{q-1}$ 的索引发送给 Alice, 并终止提取过程.

(6) Alice 和 Bob 将每次迭代提取出的 x_k 和 b_k 进行连接获得各自的初始密钥 K' 和 K.

3.3 信息调和

水声信道中存在的噪声干扰和传输损失会导致优先提取后得到的初始密钥仍然会有小概率不一致, 因此需要进行信息调和获得完全一致的最终密钥. 根据 Slepian-Wolf 编码原理, Alice 通过反馈索引计算出 LLR 序列, 并将该序列对应的码字的陪集和奇偶校验矩阵结合得到的伴随式发送给 Bob. 由于 Bob 在优先提取过程中得到的 LLR 序列可以看作受噪声影响后的版本, 两者具有相关性, 因此 Bob 对接收到的伴随式与优先提取得到的 LLR 序列进行联合解码, 即可获得不一致比特的位置信息. 又因为密钥比特是根据每个信号比特的 LLR 值生成的, 两者具有一一对应的关系, 因此根据该信息对初始密钥的相同位置进行比特翻转, 即可获得完全一致的最终密钥. 具体过程如下.

(1) Alice 和 Bob 共享一个包含 2^D 个码字 $\{b_0,b_1,\ldots,b_{2^D-1}\}$ 的码本, 码本中任意 2 个码字间汉明 (Hamming) 距离的最小值为 $d_{\min}$. 该码本对 Willie 公开, 码本对应的陪集 $\boldsymbol{e}=[e_1,e_2,\ldots,e_D]$, 纠错码的生成矩阵为 $\boldsymbol{G}$, 奇偶校验矩阵为 $\boldsymbol{H}$.

(2) Alice 根据 LLR 序列 ψ_A 选择对应的码字 b_A, 即 $b_A=\arg\min_{b_i}||\psi_A-b_i\boldsymbol{G}||$, 其中 $i\in 1,2,\ldots,2^D-1$, b_A 的陪集 $\boldsymbol{e}_p=\psi_A-b_A\boldsymbol{G}$, $p\in 1,\ldots,D$. 然后, Alice 将 $\boldsymbol{e}_p$ 和 $\boldsymbol{H}$ 相乘得到伴随式 $\boldsymbol{s}$, 即 $\boldsymbol{s}=\boldsymbol{H}\boldsymbol{e}_p$.

(3) Bob 根据接收到的伴随式 $\boldsymbol{s}$ 求得对应的陪集元素 $\boldsymbol{e}_p$, 并与原先得到的 LLR 序列 ψ_b' 进行联合解码, 得到 $b_B=\arg\min_{b_i}||\psi_b'-(\boldsymbol{e}_p+b_i\boldsymbol{G})||$, 最后, 通过 b_B 求得 $\mu_p=\boldsymbol{e}_p+b_B\boldsymbol{G}$, 此时 μ_p 就为原先提取位更新后的 LLR 值.

(4) Bob 采用最大似然解码计算 μ_p 获取协商位的位置信息, 并根据该信息对初始密钥的相同位置进行比特翻转, 获得与 Alice 完全一致的最终密钥, 其纠错能力可表示为 $\lfloor\frac{d_{\min}-1}{2}\rfloor$.

现在对本文方案的复杂度进行分析. 首先, 对隐蔽密钥协商方案的通信轮数进行分析. 令最终密钥长度为 D, 每个均匀分布信号序列长度为 n, 则隐蔽密钥通信轮数为 $\lceil\frac{D}{e''n}\rceil$, 其中, e'' 代表隐蔽密钥生成速率. 然后, 对优先提取算法部分的计算复杂度进行分析. 其中, LLR 计算的复杂度为 $O(n)$, Gibbs 采样的复杂度为 $O(I)$, LLR 检验提取密钥的复杂度为 $O(n)$. 因此, 优先提取过程的计算复杂度为 $O(2n+I)$, 总复杂度为 $O(\lceil\frac{D}{e''n}\rceil\cdot(2n+I))$. 当 n 趋向于无穷时, 通信轮数趋近于 1, 则复杂度可近似表示为 $O(n)$.

3.4 检验阈值选择

检验阈值 Λ 的选择会影响因噪声干扰或传输损失导致的信号传输错误概率, 因此 Λ 的选择很大程度上决定了隐蔽密钥协商的整体误比特率, 故最优检验阈值可建模为

$$\Lambda^*=\mathrm{argmin}P(\varsigma), \tag{8}$$

其中 $P(\varsigma)$ 为隐蔽密钥协商的整体误比特率.

由全概率公式可得 $P(\varsigma)=P\{\varsigma\cap S\}+P\{\varsigma\cap S^C\}=(1-P\{S^C\})P\{\varsigma|S\}+P\{S^C\}P\{\varsigma|S^C\}$, 其中 $P\{S\}$ 代表密钥协商过程中达到检验阈值的概率, $P\{S^C\}$ 代表密钥协商过程中没有达到检验阈值的概率. 令 $P(\varsigma_1)=(1-P\{S^C\})P\{\varsigma|S\}$, $P\{\varsigma_2\}=P\{S^C\}P\{\varsigma|S^C\}$, 则 $P\{\varsigma\}=P(\varsigma_1)+P\{\varsigma_2\}$, $P\{S^C\}=1-P_{ab}(\gamma_{ab})\exp(-\frac{1-P_{ab}(\gamma_{ab})}{1-2P_{ab}(\gamma_{ab})}\Lambda)-(1-P_{ab}(\gamma_{ab}))\exp(-\frac{1-P_{ab}(\gamma_{ab})}{1-2P_{ab}(\gamma_{ab})}\Lambda)$, $P\{\varsigma|S^C\}$ 代表隐蔽密钥协商过程中

没有达到检验阈值时的误比特率, 可表示为 $P\{\varsigma|S^C\}=P_{ab}(\gamma_{ab})$, $P\{\varsigma|S\}$ 代表隐蔽密钥协商过程中达到检验阈值时的误比特率, 根据全概率公式可展开为 $P(\varsigma|S)=P_B(\gamma_B)\exp(-\frac{1-P_{ab}(\gamma_{ab})}{1-2P_{ab}(\gamma_{ab})})\Lambda$. 将概率整合可以得到未达到检验阈值时的误比特率 $P(\varsigma_1)=P_{ab}(\gamma_{ab})^2\exp(\frac{2P_{ab}(\gamma_{ab})-2}{1-2P_{ab}(\gamma_{ab})}\Lambda)+(1-P_{ab}(\gamma_{ab}))P_{ab}(\gamma_{ab})\exp(-\frac{1}{1-2P_{ab}(\gamma_{ab})}\Lambda)$. 同理可得, 达到检验阈值时的误比特率 $P\{\varsigma_2\}=P_{ab}(\gamma_{ab})-P_{ab}(\gamma_{ab})^2\exp(\frac{P_{ab}(\gamma_{ab})-1}{1-2P_{ab}(\gamma_{ab})}\Lambda)-P_{ab}(\gamma_{ab})(1-P_{ab}(\gamma_{ab}))\exp(-\frac{P_{ab}(\gamma_{ab})}{1-2P_{ab}(\gamma_{ab})}\Lambda)$.

为了推导出最优检验阈值, 需要求出函数 $P(\varsigma)$ 的极值点, 即 $\partial P(\varsigma)/\partial\Lambda$, 此时可以得到最优检验阈值为

$$\Lambda^*=\frac{1-2P_{ab}(\gamma_{ab})}{1-P_{ab}(\gamma_{ab})}\ln\left(\frac{1}{P_{ab}(\gamma_{ab})}\right). \tag{9}$$

4 性能分析

本节首先对所提的隐蔽密钥协商方案进行性能分析, 包括保密性、隐蔽性和可靠性, 然后推导出隐蔽通信速率, 最后得出 Willie 的最优检测概率以及本文方案的隐蔽密钥生成速率.

4.1 保密性

根据互信息和相对熵的定义, 密钥泄漏率可表示为

$$\begin{aligned}S(G)&\overset{(a)}{\leqslant}D(P_{KYZ}||P_{KY}\times P_Z)\overset{(b)}{\leqslant}V_T(P_{YKZ};P_{YK}\times P_Z)+H(2V_T(P_{YKZ};P_{YK}\times P_Z))\\&\overset{(c)}{\leqslant}V_T(P_{YKZ};P_{YK}\times P_Z)\left(1+\log_2\frac{e}{2}V_T(P_{YKZ};P_{YK}\times P_Z)\right)\overset{(d)}{\leqslant}2^{-\epsilon'\omega_n\sqrt{n}}\left(1+\log_2\frac{e}{2}+\epsilon'\omega_n\sqrt{n}\right),\end{aligned} \tag{10}$$

其中不等式 (a) 根据相对熵定义得出, 不等式 (b) 由文献 [18, 命题 17.1] 得到, 不等式 (c) 是因为 $H_b(x)\leqslant x\log\frac{e}{x}$, 不等式 (d) 是因为 ε' 为任意小的正数, $\omega_n\in\omega(\frac{\log n}{\sqrt{n}})\cap o(1)$. 当 $n\to\infty$ 时, 密钥泄漏率趋近于 0, 因此本文所提的隐蔽密钥协商方案符合保密性约束.

4.2 隐蔽性

Willie 基于二元假设检验判断 Alice 是否进行了信号传输. 根据 Willie 的误检率 P_{FA} 和漏检率 P_{MD} 可以得到隐蔽概率 $\xi=P_{FA}+P_{MD}$. 隐蔽密钥协商要求 $E[\min_\gamma(P_{FA}+P_{MD})]\geqslant 1-\varepsilon$, 即 $\xi_{\min}\geqslant 1-\varepsilon$. 当 $\xi=0$ 时, Willie 可以无差错地检测到密钥协商过程; 当 $\xi=1$ 时, Willie 对密钥协商过程一无所知, 等效于随机猜测. 因此, Alice 通过控制发射功率使得 $\xi\to 1$ 就可以防范敌手模型. 令 P_0 为 Alice 未发送消息时, 即 H_0 为真时 Willie 检测到的概率分布, P_1 为 Alice 发送消息时, 即 H_1 为真时 Willie 检测到的概率分布. Willie 基于二元假设检验得到的概率分布可表示为 $H_0:P_0=P_{j\omega}+\sigma_\omega^2$, $H_1:P_1=P_{a\omega}+P_{j\omega}+\sigma_\omega^2$. 根据相对熵定义可以得到 $D(P_0||P_1)=\frac{1}{2}(\ln\frac{P_{a\omega}+P_{j\omega}+\sigma_\omega^2}{P_{j\omega}+\sigma_\omega^2}-\frac{P_{j\omega}+\sigma_\omega^2}{P_{a\omega}+P_{j\omega}+\sigma_\omega^2})$, 隐蔽概率可表示为 $C(G)=P_{FA}+P_{MD}=1-V_T(P_0,P_1)$. 根据 Pinsker 不等式, 即 $V_T(P_0,P_1)\leqslant\sqrt{\frac{1}{2}D(P_0||P_1)}$, 可以得到 Willie 检测出错的概率为

$$C(G)=1-V_T(P_0,P_1)\leqslant 1-\sqrt{\frac{1}{2}D(P_0||P_1)}=1-\sqrt{\frac{1}{4}\left(\ln\frac{P_{a\omega}+P_{j\omega}+\sigma_\omega^2}{P_{j\omega}+\sigma_\omega^2}-\frac{P_{j\omega}+\sigma_\omega^2}{P_{a\omega}+P_{j\omega}+\sigma_\omega^2}\right)}. \tag{11}$$

因为 $D(P_0||P_1)$ 的前三阶导数对 P_a 与 P_j 是连续的, 所以可以根据泰勒 (Taylor) 公式可对其进行展开, 其二阶导数为 $\frac{P_{a\omega}^2}{2}\frac{\partial D(P_0||P_1)}{\partial P_a^2}|_{P_{a\omega}=0}$. 根据文献 [19], 二次相对熵 $\frac{\partial D(P_0||P_1)}{\partial P_{a\omega}^2}|_{P_{a\omega}=0}=\frac{1}{2(P_{j\omega}+\sigma_\omega^2)^2}$,

其值只与水下噪声功率有关, 因此二阶导数为 $\frac{P_{a\omega}^2}{2}\frac{\partial D(P_0||P_1)}{\partial P_a^2}|_{P_{a\omega}=0}=\frac{P_{a\omega}^2}{4(P_{j\omega}+\sigma_\omega^2)^2}$. 其三阶导数为泰勒余项, 可表示为 $\frac{P_{a\omega}^3}{3}\frac{\partial D(P_0||P_1)}{\partial P_{a\omega}^3}|_{P_{a\omega}=0}=\frac{P_{a\omega}^3(\xi'-2(P_{j\omega}+\sigma_\omega^2))}{6(\xi'+P_{j\omega}+\sigma_\omega^2)^2}$, 其中 $0<\xi'<P_{a\omega}$. 利用二阶导数对其进行定界, 可以得到变分距离的上界为 $V_T(P_0^n,P_1^n)\leqslant\frac{P_{a\omega}}{2(P_{j\omega}+\sigma_\omega^2)}\sqrt{\frac{n}{2}}\leqslant\varepsilon$. 令 $P_{a\omega}\leqslant\frac{cf(n)}{\sqrt{n}}$ 为 Alice 的发射功率约束, 其中 $f(n)$ 为某一函数, c 取 $2\sqrt{2}\theta$, θ 为任意小的正数, 此时上界可表示为 $V_T(P_0^n,P_1^n)\leqslant\frac{P_{a\omega}}{2(P_{j\omega}+\sigma_\omega^2)}\sqrt{\frac{n}{2}}\leqslant\frac{\theta\cdot f(n)}{P_{j\omega}+\sigma_\omega^2}$. 若 Alice 知道窃听方噪声功率的下界, 可以设置 $f(n)=P_{j\omega}+\hat{\sigma}_\omega^2$ 来满足隐蔽条件; 若 Alice 不知道窃听者处的噪声功率, 此时设置 $f(n)=O(1)$ 即可.

4.3 可靠性

若 Alice 从随机码本中任意选择一个码字 $c(W_k)$ 发送给 Bob, Bob 使用最大似然解码器解码, 则解码器出错事件 $\varepsilon_i(c(W_k))$ 可定义为 Bob 解码得到的码字 $c(W_k)$ 与码本中另一个码字 $c(W_i), i\neq k$ 相等. 因此解码错误概率可以表示为 $P(G)\leqslant E_{c(W_k)}[\sum_{i=0,i\neq k}^{2^{nR}}P(\varepsilon_i(c(W_k)))]=\sum_{i=0,i\neq k}^{2^{nR}}E_{c(W_k)}[P(\varepsilon_i(c(W_k)))]$, 其中, $E_X(\cdot)$ 为随机变量 X 的期望. 令 $d=c(W_k)-c(W_i)$, 则 $\|d\|_2$ 为两个码字之间的距离, 其中 $\|\cdot\|_2$ 为 L_2 范式, $d_j\sim N(0,2P_{ab})$, $j=1,2,\ldots,n$, $\|d\|_2^2=2P_{ab}U$, 其中 $U\sim\chi_n^2$, χ_n^2 为服从自由度 n 的卡方分布. 根据文献 [20] 可得 $E_{c(W_k)}[P(\varepsilon_i(c(W_k)))]=E_U[Q(\sqrt{\frac{P_{ab}U}{2(P_{jb}+\sigma_b^2)}})]$, 其中 $Q(x)=\frac{1}{\sqrt{2\pi}}\int_x^\infty \mathrm{e}^{-t^2/2}\mathrm{d}t$, $Q(x)\leqslant\frac{1}{2}\mathrm{e}^{-x^2/2}$, 则 $E_{c(W_k)}[P(\varepsilon_i(c(W_k)))]\leqslant 2^{-n/2}(\frac{1}{2}+\frac{P_{ab}}{2(P_{jb}+\sigma_b^2)})^{-n/2}$, 因此可得

$$P(G)\leqslant 2^{nR-\frac{n}{2}\mathrm{lb}(1+P_{ab}/2(P_{jb}+\sigma_b^2))}, \tag{12}$$

其中 R 为隐蔽通信速率, 取值范围为 $0\leqslant R\leqslant 1$. 令 $R=\frac{1}{4}\mathrm{lb}(1+\frac{cf(n)}{2\sqrt{n}(P_{jb}+\sigma_b^2)})$, 则当 n 增加时, 解码错误概率以指数级速率降低为 0.

本文方案的可靠性与传输能力 (即通信速率) 有关. 根据文献 [9] 可知, 窃听者对接收噪声的功率具有不确定性时可以突破平方根定律的限制, 使渐进隐蔽通信速率达到正常数, 所以本文方案考虑存在特定地点噪声以及噪声不确定性的情况, 并结合水声信道状态计算出最优检验阈值, 减轻了水下噪声对合法方的影响, 提高了通信速率. 由于本文方案考虑了噪声对合法方的影响, 所以解码错误概率就与 Alice 和 Bob 之间的干扰信噪比有关, 表示为 $\gamma_0=\frac{P_{ab}}{P_{jb}+\sigma_b^2}$, 其中 P_{ab}, P_{jb} 为常数, 因此一定存在一个足够大的干扰信噪比, 使得隐蔽通信速率 R 为常速率且服从可靠性约束. 此时, Alice 的传输功率 P_{ab} 不再受到消息长度 n 的约束而只受到隐蔽性约束, 即 $P_{ab}\leqslant cf(\rho)$. 其中, $f(\rho)=\frac{\rho^{4\varepsilon-1}+2\sigma_j^2\lambda_2-1/\rho}{2}\frac{\sigma_h^2\sigma_n^2H_{a\omega}^2}{(\sigma_g^2)^2H_{ab}^2}$, ρ 为噪声不确定度, 将 $f(\rho)$ 代入 R 可得隐蔽通信速率为 $O((\rho^{4\varepsilon-1}+1-\frac{1}{\rho})/\sqrt{n})$. 因为 $\rho>1$ 且 $\varepsilon>0$, 所以 $\rho^{4\varepsilon-1}+1-\frac{1}{\rho}>1$, 即隐蔽通信速率优于 $O(1/\sqrt{n})$.

最后, 推导 Alice 发射功率的下界. 由于水下噪声存在不确定性, 使得通信速率出现一定程度的波动, 对于系统设置好的隐蔽通信速率 R 存在不达标的情况, 导致接收到的消息不能被正确解码, 其概率为

$$P(\varepsilon')=P\left(\sigma_b^2>\frac{P_{ab}}{2^R-1}-P_{jb}\right)=\int_{\frac{P_{ab}}{2^R-1}-P_{jb}}^{\infty}f_b(x)\mathrm{d}x=\frac{1}{2\ln(\rho)}\ln\left(\frac{\rho\sigma_n^2(2^R-1)}{P_{ab}-P_{jb}(2^R-1)}\right). \tag{13}$$

因为 $P(\varepsilon')$ 需要服从可靠性约束, 即 $P(\varepsilon')=\frac{1}{2\ln(\rho)}\ln(\frac{\rho\sigma_n^2(2^R-1)}{P_{ab}-P_{jb}(2^R-1)})\leqslant\upsilon$, 因此可得 $P_{ab}\geqslant\frac{\sigma_n^2(2^R-1)}{\rho\upsilon}+P_{jb}(2^R-1)$. 此时可以得到 Alice 发射功率的下界

$$P_t^-\geqslant\left(\frac{\sigma_n^2(2^R-1)}{\rho\upsilon}+P_{jb}(2^R-1)\right)\frac{1}{H_{ab}^2\Omega_{ab}^2}. \tag{14}$$

4.4 最优检测阈值

假设 Willie 知晓 Alice 到 Willie 的信道转移概率以及 P_0 和 P_1, 此时 Willie 可以设置最优检测阈值将非法检测的错误率降至最低. 为了得到其最优检测阈值, 必须量化系统的隐蔽概率. 为此, 本文通过贝叶斯统计来衡量系统的平均隐蔽概率. 其中, Willie 通过贝叶斯统计来量化隐蔽概率以求得其最优检测阈值, 即平均隐蔽概率最小时的检测阈值, 而 Alice 通过贝叶斯统计得到 Willie 采用最优检测阈值时的平均隐蔽概率, 并通过这个概率计算出满足本文方案隐蔽性的发射功率. 采用噪声功率先验分布平均值作为度量, 平均隐蔽概率可表示为

$$\xi\left(\frac{\Omega_{j\omega}}{H_{j\omega}}\right)=1-\int_0^{\infty} f_X\left(x|\frac{\Omega_{j\omega}}{H_{j\omega}}\right)\cdot\int_{\max(\gamma-\sigma\frac{\sigma_j^2P_{j\omega}}{H_{j\omega}^2}-\frac{\sigma_g^2P_{a\omega}}{H_{a\omega}^2},\frac{1}{\rho}\sigma_\omega^2)}^{\min(\gamma-\frac{\sigma_j^2P_{j\omega}}{H_{j\omega}^2},\sigma_\omega^2\rho)} f_\omega(y)\mathrm{d}y\mathrm{d}x.$$

当探测器检测阈值 $\gamma<\sigma_\omega^2/\rho+\sigma\frac{^2P_{j\omega}}{H_{j\omega}^2}$ 时, 平均隐蔽概率为 1 ; 当 $\gamma>\rho\sigma_\omega^2+\frac{\sigma_j^2P_{j\omega}}{H_{j\omega}^2}$ 时, $\xi(\frac{\Omega_{j\omega}}{H_{j\omega}})$ 为单调递增函数, 为了使平均隐蔽概率最小, 一定会落入区间 $[\sigma_\omega^2/\rho+\frac{\sigma_j^2P_{j\omega}}{H_{j\omega}^2},\rho\sigma_\omega^2+\frac{\sigma_j^2P_{j\omega}}{H_{j\omega}^2}]$, 此时

$$\begin{aligned}\xi\left(\frac{\Omega_{j\omega}}{H_{j\omega}}\right)=&1-\frac{\ln(\rho(\gamma/\sigma_n^2-\frac{\sigma_j^2P_{j\omega}}{H_{j\omega}^2}))}{2\ln(\rho)}\\&+\frac{1}{2\ln(\rho)}\int_0^{(\frac{\gamma}{\sigma_n^2}-\frac{\sigma_g^2\lambda_1}{H_{a\omega}^2}-\frac{1}{\rho})\frac{1}{\lambda_2}}\left(f_X\left(x|\frac{\Omega_{j\omega}}{H_{j\omega}}\right)\ln\left(\rho\left(\frac{\gamma}{\sigma_n^2}-\frac{\sigma_g^2\lambda_1}{H_{a\omega}^2}-x\lambda_2\right)\right)\right)\mathrm{d}x,\end{aligned}\tag{15}$$

其中 $\lambda_1=P_{a\omega}/\sigma_n^2$, $\lambda_2=P_{j\omega}/\sigma_n^2$. 根据式 (15) 可以得到

$$\xi\left(\frac{\Omega_{j\omega}}{H_{j\omega}}\right)=\begin{cases}1-\frac{\ln(\rho(\gamma/\sigma_n^2-\frac{\sigma_j^2\lambda_2}{H_{j\omega}^2}))}{2\ln(\rho)}, & \frac{\sigma_j^2}{H_{j\omega}^2}\geqslant(\frac{\gamma}{\sigma_n^2}-\frac{\sigma_g^2\lambda_1}{H_{a\omega}^2}-\frac{1}{\rho})\frac{1}{\lambda_2},\\ 1+\frac{1}{2\ln(\rho)}\ln\left(1-\frac{\frac{\sigma_g^2P_{a\omega}}{H_{a\omega}^2}}{\gamma-\frac{\sigma_j^2P_{j\omega}}{H_{j\omega}^2}}\right), & \frac{\sigma_j^2}{H_{j\omega}^2}<(\frac{\gamma}{\sigma_n^2}-\frac{\sigma_g^2\lambda_1}{H_{a\omega}^2}-\frac{1}{\rho})\frac{1}{\lambda_2}.\end{cases}\tag{16}$$

当 $\gamma\geqslant\frac{\sigma_g^2P_{a\omega}}{H_{a\omega}^2}+\frac{\sigma_j^2P_{j\omega}}{H_{j\omega}^2}+\sigma_n^2/\rho$ 时, $\xi(\frac{\Omega_{j\omega}}{H_{j\omega}})$ 单调递增; 当 $\gamma<\frac{\sigma_g^2P_{a\omega}}{H_{a\omega}^2}+\frac{\sigma_j^2P_{j\omega}}{H_{j\omega}^2}+\sigma_n^2/\rho$ 时, $\xi(\frac{\Omega_{j\omega}}{H_{j\omega}})$ 单调递减. 又因为 $\gamma\in[\sigma_\omega^2/\rho+\frac{\sigma_j^2P_{j\omega}}{H_{j\omega}^2},\sigma_\omega^2\rho+\frac{\sigma_j^2P_{j\omega}}{H_{j\omega}^2}]$, 所以可以推导出 Willie 的最优检测阈值为

$$\gamma^*=\min\left\{\frac{\sigma_g^2P_{a\omega}}{H_{a\omega}^2}+\frac{\sigma_j^2P_{j\omega}}{H_{j\omega}^2}+\sigma_n^2/\rho,\sigma_n^2\rho+\frac{\sigma_j^2P_{j\omega}}{H_{j\omega}^2}\right\}.\tag{17}$$

将式 (17) 代入式 (16) 可得

$$\xi_{\min}=\begin{cases}1-\frac{\ln(1+\frac{\sigma_g^2\rho\lambda_1}{H_{a\omega}^2}-\frac{\sigma_j^2\rho\lambda_2}{H_{j\omega}^2})}{2\ln(\rho)}, & \frac{\sigma_g^2}{H_{a\omega}^2}<(\rho-\frac{1}{\rho})\frac{1}{\lambda_1},\\ 0, & \frac{\sigma_g^2}{H_{a\omega}^2}\geqslant(\rho-\frac{1}{\rho})\frac{1}{\lambda_1}.\end{cases}\tag{18}$$

对式 (18) 进行积分, 可以得到最小平均隐蔽概率

$$\xi_{\min}=\int_0^{(\rho-\frac{1}{\rho})\frac{1}{\lambda_1}}\left(1-\frac{\ln(1+\rho x\lambda_1-\frac{\sigma_j^2\rho\lambda_2}{H_{j\omega}^2})}{2\ln(\rho)}\right)\frac{H_{a\omega}^2\mathrm{e}^{-\frac{H_{a\omega}^2x}{\sigma_g^2}}}{\sigma_g^2}\mathrm{d}x$$

$$= 1 - \frac{\mathrm{e}^{\frac{1}{\frac{\rho\sigma_g^2\lambda_1}{H_{a\omega}^2} - \frac{\sigma_j^2\rho\lambda_2}{H_{j\omega}^2}}}}{2\ln(\rho)} \left[\mathrm{Ei}\left(-\frac{\rho}{\frac{\sigma_g^2\lambda_1}{H_{a\omega}^2} - \frac{\sigma_j^2\lambda_2}{H_{j\omega}^2}} \right) - \mathrm{Ei}\left(-\frac{1}{\rho(\frac{\sigma_g^2\lambda_1}{H_{a\omega}^2} - \frac{\sigma_j^2\lambda_2}{H_{j\omega}^2})} \right) \right], \tag{19}$$

其中 $\mathrm{Ei}(x) = \int_{-\infty}^{x} t^{-1}\mathrm{e}^t \mathrm{d}t$ 为指数分布函数. 当 x 远大于 1 时, $\mathrm{Ei}(-x) = -0.5\mathrm{e}^{-x}\ln(1+0.5x)$. 因此在低信噪比时, 即 $\sigma_g^2\lambda_1$ 远小于 1 时, 式 (19) 可近似表达为

$$\xi_{\min} \approx 1 - \frac{1}{4\ln(\rho)} \ln\left(1 + \frac{2\sigma_g^2\rho\lambda_1}{H_{a\omega}^2} - \frac{2\sigma_j^2\rho\lambda_2}{H_{j\omega}^2} \right). \tag{20}$$

4.5 隐蔽密钥生成速率

本小节将推导出发送方服从隐蔽性约束时所能达到的最大隐蔽密钥生成速率以及发送方传输功率的上界. 其中, 隐蔽密钥生成速率指传输每个符号时生成的隐蔽密钥比特数. 当主动非法检测方 Willie 噪声功率服从对数均匀分布, 且合法发送方 Alice 服从隐蔽性约束时, Alice 传输功率存在上界 P_t^+. 由式 (4) 和 (6) 可以得到隐蔽密钥生成速率

$$R' = \Pr\left(P_t^+ > \frac{\Lambda H_{ab}^2 (P_{jb} + \sigma_b^2)}{2\Omega_{ab}^2} \right). \tag{21}$$

因为式 (20) 需要满足隐蔽性约束 $\xi_{\min} \geqslant 1-\varepsilon$, 所以 $\frac{1}{4\ln(\rho)}\ln(1 + \frac{2\sigma_g^2\rho\lambda_1}{H_{a\omega}^2} - \frac{2\sigma_j^2\rho\lambda_2}{H_{j\omega}^2}) \geqslant 1-\varepsilon$, 因此可以得到 Alice 发射功率的上界

$$P_t^+ \leqslant \frac{\rho^{4\varepsilon-1} + 2\frac{\sigma_j^2\lambda_2}{H_{j\omega}^2} - \frac{1}{\rho}}{2} \frac{\sigma_n^2 H_{a\omega}^6}{\sigma_g^4}. \tag{22}$$

将式 (22) 代入式 (21) 推导出隐蔽密钥生成速率

$$R' = \Pr\left(\sigma_h^2 > \frac{\Lambda(P_{jb} + \sigma_b^2)\sigma_g^4 H_{ab}^2}{(\rho^{4\varepsilon-1} + \frac{2\sigma_j^2\lambda_2}{H_{j\omega}^2} - 1/\rho)\sigma_n^2 H_{a\omega}^6} \right) = \exp\left(-\frac{\Lambda(P_{jb} + \sigma_b^2)\sigma_g^4 H_{ab}^2}{(\rho^{4\varepsilon-1} + \frac{2\sigma_j^2\lambda_2}{H_{j\omega}^2} - 1/\rho)\sigma_n^2\sigma_h^2 H_{a\omega}^6} \right). \tag{23}$$

4.6 能量消耗

合法通信双方的消息传输会产生能量消耗. 假设合法通信双方第 i 轮通信时在距离 d_{ab} 上传输一个长度为 n 的消息, 所消耗的能量可表示为 $E_{ab}^i = (P_t + P_r) \times T_{ab}$, 其中, P_t 代表 Alice 的发射功率, P_r 代表 Bob 的接收功率, T_{ab} 代表传输时间, 可表示为 $T_{ab} = \frac{n}{R}$. 因此, 总体能量消耗可表示为 $E_{ab} = \sum_i E_{ab}^i \approx \lceil \frac{D}{e''n} \rceil \times (P_t + P_r) \times T_{ab}$. 根据公式可以看出, 能量消耗与通信轮数、功率以及传输时间有关. 本文方案由于受限于可靠性和隐蔽性约束, Alice 的发射功率存在下限和上限. 为了保证通信速率, 本文方案选择上限作为发射功率.

5 仿真结果

5.1 实验参数设置

本小节将通过仿真实验对本文所提的隐蔽密钥协商方案进行性能评估. 实验采用的工具为 Matlab R2020a, 并通过水声工具箱 Bellhop 编辑水体环境. 其中, 水声信道环境文件 *.env 中的数据采用

表 1　实验参数的默认值

Table 1　Default values of experimental parameters

Parameter	Value	Unit
Transceiver horizontal distance d_{ab}	5	km
The distance between the illegal detection party and the transmitter $d_{a\omega}$	3	km
The impulse response of the UAC	45	dB
Noise power	-20	dB
Absorption attenuation coefficient α	4	m
Transmission loss coefficient η	10	–
Noise uncertainty ρ	2	dB
Receiving power	0.8	W
Secrecy constraint τ	10^{-6}	–
Covertness constraint ε	10^{-6}	–
Reliability constraint υ	10^{-6}	–

了 2017 年 7 月 26~28 日在距离新斯科舍海岸 10 km 处, 哈利法克斯海滩和圣玛格丽特大坝入口海域的海试实测数据 [21]. 其中, 海域水平范围为 10 km, 深度为 80 m, 声波频率为 2 kHz, 平均声速为 1481 m/s, 平均浪高 0.6 m, 风向为西南风, 平均风速 6 m/s, 海洋状态在世界气象组织标准所定的状态 2 与状态 3 之间变化, 发送方停泊在海深 33 m 处, 接收方为带有 5 阵元垂直线列阵的全向水听器的多通道记录仪, 深度约为 38 m, 沉积物层的深度为 80 m, 沉积物层的声速在 1730~1850 m/s 之间, 沉积物的衰减系数为 0.1~0.8 dB/m/kHz. 此外, 为了满足系统应用需求, 可靠性约束的取值为 10^{-6}, 保密性约束和隐蔽性约束的取值为相同数量级, 其他实验参数的默认值如表 1 所示, 所选海域的传输损失变化情况如图 2 所示.

5.2　实验结果与分析

本文方案在优先提取阶段采用 Gibbs 采样进行 10 次迭代后满足收敛条件. 图 3 描述了本文方案在不同检验阈值下的误比特率. 从图 3 中可以看出, 一定存在最优检验阈值使得整体误比特率最低, 因为整体误比特率 $P\{\varsigma\}$ 由未达到检验阈值时的误比特率 $P(\varsigma_1)$ 和达到检验阈值时的误比特率 $P\{\varsigma_2\}$ 组成, $P(\varsigma_1)$ 与检验阈值成反比, $P\{\varsigma_2\}$ 与检验阈值成正比, 所以它们之和一定存在一个极值点使得 $P\{\varsigma\}$ 最低. 并且, 当信噪比 γ_{ab} 为 -5 dB 时, 最优检验阈值为 4.14; 当信噪比 γ_{ab} 为 -6 dB 时, 最优检验阈值为 3.91, 因此最优检验阈值与信噪比成正比.

进一步, 我们将本文方案与文献 [5,10] 的方案进行对比分析. 其中, 文献 [10] 是一种通用的隐蔽密钥协商方案, 文献 [5] 是一种基于水声信道的密钥协商方案, 但是该方案没有考虑密钥协商过程中消息传输的隐蔽性, 因此我们将与文献 [5] 比较除隐蔽性的其他性能指标.

图 4 描述了不同信噪比下的整体误比特率. 从图中可以看出, 在相同信噪比情况下, 文献 [5] 的整体误比特率要低于文献 [10] 的整体误比特率, 这是因为不同于文献 [10] 通过均匀分布的初始序列进行密钥生成, 文献 [5] 基于累积分布函数对水声信道进行量化, 使合法双方获得高相关度的初始序列, 所以误比特率更低; 本文方案的整体误比特率要低于文献 [5] 的整体误比特率, 这是因为本文方案针对水声信道的信道状态采用了 LLR 算法消除了特定地点噪声对传输的影响, 并使用 Gibbs 采样和最优检验阈值来减少噪声不确定性和水声信道传输损失带来的影响.

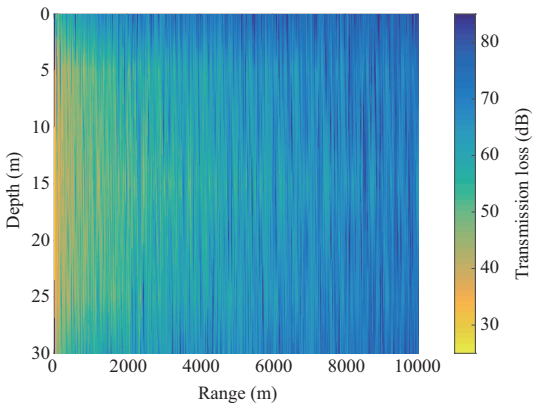

图 2 (网络版彩图) 所选海域的传输损失变化情况

Figure 2 (Color online) The variation of transmission losses in the selected sea area

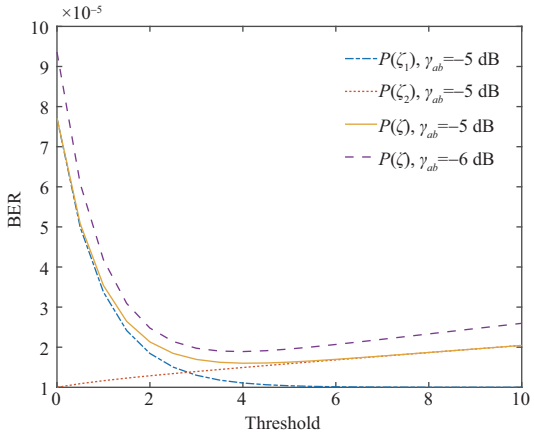

图 3 (网络版彩图) 不同检验阈值下的误比特率

Figure 3 (Color online) The BER under different thresholds

图 5 描述了平均隐蔽概率随噪声不确定度 ρ 的变化情况. 当信噪比 γ_{ab} 相同时, 本文方案的平均隐蔽概率要高于文献 [10], 并且文献 [10] 在噪声不确定度较低时, 平均隐蔽概率出现为零的情况, 这是因为文献 [10] 假设非法检测方不会采取任何手段增加自己的非法检测成功率, 限制了非法检测方的检测能力, 因此在非法检测方选择最优检测阈值时, 文献 [10] 的平均隐蔽概率就会有所降低且会出现为零的情况. 本文方案通过贝叶斯统计求出了非法检测方的最优检测阈值, 结合隐蔽性约束, 得到了合法方传输功率的上界. 只要合法方的传输功率不超过上界, 即使 Willie 对 Alice 和 Bob 的信道状态信息拥有完全的知识, 平均隐蔽概率仍然可以在噪声不确定度较低的情况下接近 1. 此外, 信噪比的改变对本文方案的隐蔽概率影响较小, 而文献 [10] 随着信噪比的降低, 不仅平均隐蔽概率为 0 的概率变大, 而且平均隐蔽概率也急剧降低. 与文献 [10] 相比, 本文方案的平均隐蔽概率提高了 34.67%.

图 6 描述了不同收发机水平距离下的隐蔽密钥生成速率. 其中, 码字长度为 1024 比特. 从图中可以看出, 收发机水平距离相同情况下本文的隐蔽密钥生成速率要高于文献 [10] 的隐蔽密钥生成速率, 这是因为文献 [10] 没有考虑水下噪声的不确定性, 导致解码器通过广播消息和输入序列联合解码时产生了误差, 从而降低了隐蔽密钥生成速率. 本文方案根据水声信道转移概率和水下噪声方差信息, 通过 Gibbs 采样降低了密钥生成的通信轮数, 从而提高了隐蔽密钥生成速率. 与文献 [10] 相比, 本文方案的隐蔽密钥生成速率平均提高了 25.70%.

图 7 描述了生成不同长度密钥时的消息长度. 从图中可以看出, 本文方案生成相同长度密钥时所需的消息长度平均要比文献 [10] 低 11.32%, 这是因为文献 [10] 每一轮通信的复杂度近似为 $O(n)$, 而本文方案的隐蔽通信速率可以突破平方根定律的限制, 每一轮通信过程中可以用来生成密钥的消息长度比文献 [10] 更长, 所以通信轮数比文献 [10] 更少, 为文献 [10] 的 $1/(\rho^{4\varepsilon-1}+1-1/\rho)$.

图 8 描述了生成不同长度密钥时的信息泄漏率. 从图中可以看出, 随着密钥长度的增加, 信息泄漏率呈现指数下降趋势. 此外, 在生成密钥长度相同的情况下, 文献 [5] 的信息泄漏率最高, 本文方案和文献 [10] 的信息泄漏率相同, 这是因为文献 [5] 没有考虑隐蔽性, 所以其信息泄漏率与敌手正确窃听消息的概率有关, 而本文方案和文献 [10] 考虑了消息传输过程的隐蔽性, 因此信息泄漏率更低. 与文献 [5] 相比, 本文方案的信息泄漏率平均降低了 58.35%.

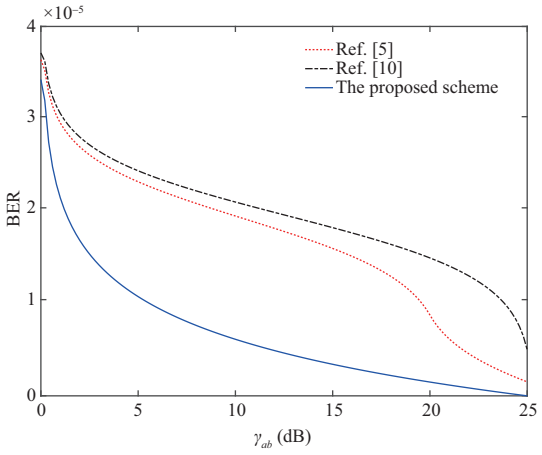

图 4 (网络版彩图) 不同信噪比下的整体误比特率

Figure 4 (Color online) The BER under different signal-to-noise ratios

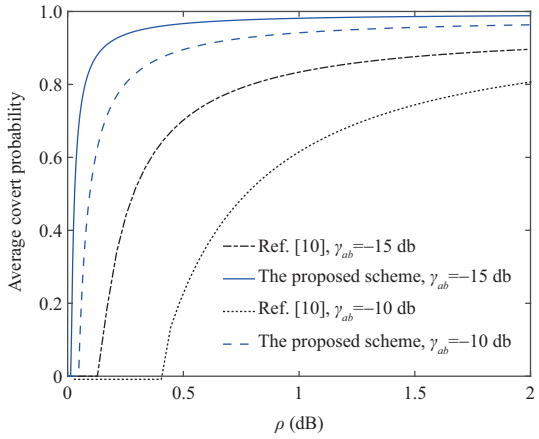

图 5 (网络版彩图) 平均隐蔽概率与噪声不确定度的变化情况

Figure 5 (Color online) The variation of average covert probability and noise uncertainty

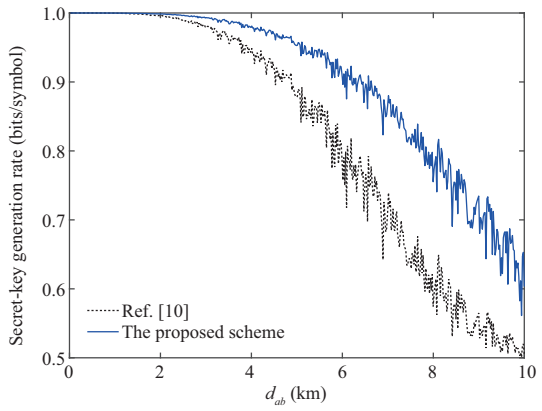

图 6 (网络版彩图) 不同收发机水平距离下的隐蔽密钥生成速率

Figure 6 (Color online) The covert secret-key generation rate under different transmission distances

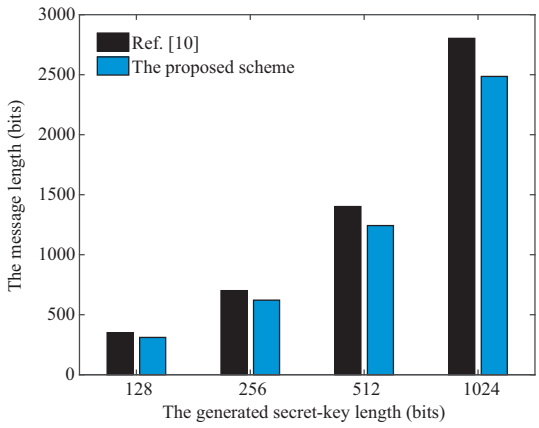

图 7 (网络版彩图) 生成不同长度密钥时的消息长度

Figure 7 (Color online) The message length under different generated secret-key lengths

图 9 描述了不同收发机水平距离下的总体能量消耗. 从图中可以看出, 本文方案的能量曲线波动最小, 这是因为本文方案考虑了特定地点噪声对协议性能的影响. 此外, 本文方案的总体能量消耗比文献 [5] 平均减少了 44.36%, 比文献 [10] 平均减少了 12.19%, 这是因为本文方案需要控制发射功率来确保隐蔽性, 因此总体能量消耗比文献 [5] 更少. 另一方面, 与文献 [10] 相比, 本文方案的隐蔽通信速率突破了平方根定律的限制, 因此消息传输时间更少, 总体能量消耗也就更少.

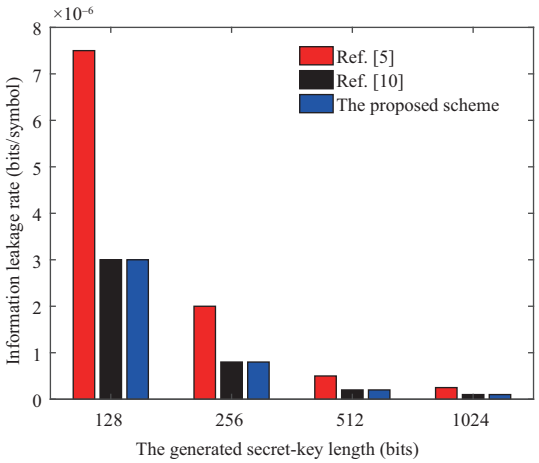

图 8 (网络版彩图) 生成不同长度密钥时的信息泄漏率

Figure 8 (Color online) The information leakage rate under different generated secret-key lengths

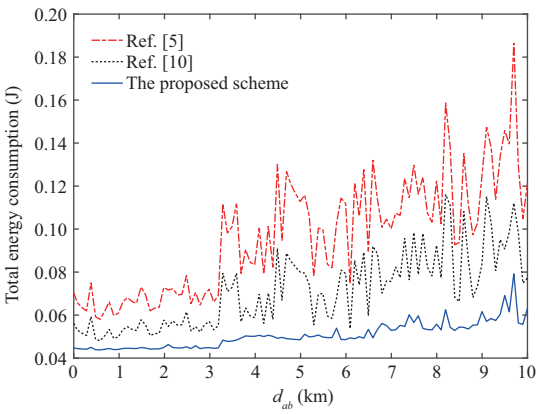

图 9 (网络版彩图) 不同收发机水平距离下的总体能量消耗

Figure 9 (Color online) The total energy consumption under different transmission distances

6 结论

本文针对传统密钥协商协议在水声信道环境下存在的信息泄漏问题, 提出了一种基于水声信道的隐蔽密钥协商方案. 通过分析整体误比特率, 求出最优检验阈值, 并利用假设检验, 推导出主动非法检测方的最优检测阈值, 以及发送方的平均隐蔽概率和隐蔽密钥生成速率, 最后推导出发送方传输功率的上界和下界, 证明了发送方在低信噪比情况下仍然可以进行隐蔽密钥协商. 仿真实验结果表明, 本文方案的主要性能指标优于现有方案. 所研究内容对水声信道环境下的隐蔽密钥协商和隐蔽通信具有一定的参考价值. 后续的研究工作将考虑多用户情况下的隐蔽密钥协商问题.

参考文献

1 Song Y. Underwater acoustic sensor networks with cost efficiency for Internet of underwater Things. IEEE Trans Ind Electron, 2021, 68: 1707–1716

2 Wang S, He Z, Niu K, et al. New results on joint channel and impulsive noise estimation and tracking in underwater acoustic OFDM systems. IEEE Trans Wireless Commun, 2020, 19: 2601–2612

3 Yang Y T, Zhang Y Z, Li Z C, et al. RAKA: new authenticated key agreement protocol based on Ring-LWE. J Comput Res Dev, 2017, 54: 2187–2192 [杨亚涛, 张亚泽, 李子臣, 等. RAKA: 一种新的基于 Ring-LWE 的认证密钥协商协议. 计算机研究与发展, 2017, 54: 2187–2192]

4 Maurer U M. Secret key agreement by public discussion from common information. IEEE Trans Inform Theor, 1993, 39: 733–742

5 Huang Y, Zhou S, Shi Z, et al. Channel frequency response-based secret key generation in underwater acoustic systems. IEEE Trans Wireless Commun, 2016, 15: 5875–5888

6 Yang J, Ji X S, Huang K Z, et al. Secret key generation scheme based on RIS antenna for static environments. Sci Sin Inform, 2022, 52: 253–269 [杨杰, 季新生, 黄开枝, 等. 静态场景下基于 RIS 天线的物理层密钥生成方案. 中国科学: 信息科学, 2022, 52: 253–269]

7 Bash B A, Goeckel D, Towsley D. Limits of reliable communication with low probability of detection on AWGN channels. IEEE J Sel Areas Commun, 2013, 31: 1921–1930

8 Tandra R, Sahai A. SNR walls for signal detection. IEEE J Sel Top Signal Process, 2008, 2: 4–17

9 Lee S, Baxley R J, Weitnauer M A, et al. Achieving undetectable communication. IEEE J Sel Top Signal Process, 2015, 9: 1195–1205
10 Tahmasbi M, Bloch M R. Covert secret key generation with an active warden. IEEE Trans Inform Forensic Secur, 2020, 15: 1026–1039
11 Stojanovic M, Preisig J. Underwater acoustic communication channels: propagation models and statistical characterization. IEEE Commun Mag, 2009, 47: 84–89
12 Diamant R, Lampe L, Gamroth E. Bounds for low probability of detection for underwater acoustic communication. IEEE J Ocean Eng, 2017, 42: 143–155
13 Gurugopinath S, Anand G V. Narrowband detection of underwater acoustic signal under noise uncertainties. In: Proceedings of Oceans 2015, Genova, 2015. 1–5
14 He B, Yan S, Zhou X, et al. On covert communication with noise uncertainty. IEEE Commun Lett, 2017, 21: 941–944
15 Proakis J G. Digital Communications. 4th ed. New York: McGraw Hill, 2001
16 Mv A R, Ghosh P K. PSFM—a probabilistic source filter model for noise robust glottal closure instant detection. IEEE ACM Trans Audio Speech Lang Process, 2018, 26: 1645–1657
17 Chen R, Liu J S, Wang X D. Convergence analyses and comparisons of Markov chain Monte Carlo algorithms in digital communications. IEEE Trans Signal Process, 2002, 50: 255–270
18 Csiszar I, Korner J. Information Theory: Coding Theorems for Discrete Memoryless Systems. Cambridge: Cambridge University Press, 2011
19 Kullback S. Information Theory and Statistics. New York: Dover Publications, 1997
20 Madhow U. Fundamentals of Digital Communication. Cambridge: Cambridge University Press, 2008
21 Miron-Morin M, Barclay D R, Bousquet J F. The oceanographic sensitivity of the acoustic channel in shallow water. IEEE J Ocean Eng, 2020, 46: 675–686

Covert secret-key agreement scheme based on an underwater acoustic channel

Ming XU[1,2*], Hexin FENG[1] & Jihong GUAN[2,3]

1. *College of Information Engineering, Shanghai Maritime University, Shanghai* 201306*, China*;
2. *College of Electronics and Information Engineering, Tongji University, Shanghai* 201804*, China*;
3. *Key Laboratory of Embedded System and Service Computing* (*Tongji University*)*, Ministry of Education, Shanghai* 201804*, China*
* Corresponding author. E-mail: mingxu@shmtu.edu.cn

Abstract In an underwater acoustic channel (UAC) environment, traditional secret-key agreement protocols are more vulnerable to security threats, such as information leakage. Moreover, the covert communication rate of existing covert secret-key agreement protocols does not exceed $O(1/\sqrt{n})$ due to the square root law. To solve the above problems, this paper proposes a covert secret-key agreement scheme based on a UAC. In the advantage distillation stage, the transmitter sends uniformly distributed random messages to the receiver within a certain range of power. The receiver calculates the estimated messages using Gibbs sampling according to the variance of the underwater noise. The receiver also uses the log-likelihood ratio (LLR) test to extract the initial key so as to reduce the uncertainty and the bit error rate of the data transmission between two legitimate parties. In the information reconciliation stage, the receiver jointly decodes the received syndrome and the LLR sequence obtained during the advantage extraction stage to obtain the location information of the error bits and finally obtains a key that is identical to the one in the transmitter after bit-flipping. The secrecy, covertness, and reliability of the proposed scheme are proved by the theory of hypothesis testing and information theory. The simulation results show that the proposed scheme improves performance compared with the existing scheme.

Keywords underwater acoustic channel, covert secret-key agreement, advantage distillation, information reconciliation, log-likelihood ratio (LLR) test