

抵御水下窃听：一种基于纠删码的UWSN消息转发方法

严翔渝¹, 张文哲¹, 吴洲², 刘林峰¹

(1.南京邮电大学计算机学院, 江苏 南京 210023; 2.澳门城市大学数据科学学院, 澳门 999078)

摘 要: 在水下无线传感器网络中, 节点周围可能游弋着一些窃听者(水下间谍机器人), 这些窃听者对节点通信信道进行静默监听, 难以被节点发现。为降低数据消息被窃取的风险, 在保证必需的数据消息投递率的同时减少消息转发所涉及的计算开销, 需将每个数据消息编码为 n 个消息块和 m 个校验块, 并从这 $n+m$ 个信息块中随机选择 $m+1$ 个进行轻量级加密。首先, 对信息块的转发过程进行了建模分析, 重点研究投递率、窃取率、节点存储空间限制和计算开销等关键指标, 推导出信息块持有节点对所持有信息块的转发概率和丢弃概率; 然后, 提出了基于纠删码的消息转发方法。在该方法中, 所有的信息块以分布式方式进行转发, 每个信息块持有节点根据计算获得的转发概率和丢弃概率来转发和丢弃这些信息块; 当汇聚节点接收到一个数据消息的 n 个不同的信息块时, 该数据消息就可以通过解密与解码来进行恢复。仿真结果证明, 基于纠删码的消息转发方法具有良好的性能, 在保证所需数据消息投递率的前提下, 尽可能地降低了数据消息被窃取的可能性, 并且节点在消息转发过程中承担的计算开销较小, 适用于节点存储空间受限的水下无线传感器网络。

关键词: 水下传感器网络; 水下间谍机器人; 消息转发; 纠删码

中图分类号: TP309

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2025031

Defense against underwater eavesdroppers: a message dissemination approach based on erasure code for UWSN

YAN Xiangyu¹, ZHANG Wenzhe¹, WU Zhou², LIU Linfeng¹

1. School of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

2. Faculty of Data Science, City University of Macau, Macau 999078, China

Abstract: In underwater wireless sensor network (UWSN), eavesdroppers (underwater spy-robots) could move around the nodes silently to eavesdrop on their communication channels, and they were hardly perceived by the nodes. To mitigate the risk of data message theft while ensuring the required data delivery rate and reducing computational overhead in message dissemination, each data message was encoded into n message blocks and m parity blocks. From the total $(n+m)$ information blocks, m was randomly selected for lightweight encryption. Firstly, the propagation process of the blocks was formulated, and issues such as delivery ratio, theft ratio, storage limitation,

收稿日期: 2025-02-06; 修回日期: 2025-04-08

基金项目: 国家自然科学基金(62272237)

Foundation Item: The National Natural Science Foundation of China (62272237)

引用格式: 严翔渝, 张文哲, 吴洲, 等. 抵御水下窃听: 一种基于纠删码的UWSN消息转发方法[J]. 网络与信息安全学报, 2025, 11(3): 134-149.

Citation Format: YAN X Y, ZHANG W Z, WU Z, et al. Defense against underwater eavesdroppers: a message dissemination approach based on erasure code for UWSN[J]. Chinese Journal of Network and Information Security, 2025, 11(3): 134-149.

and computational cost were specially investigated to obtain the disseminating probability and discarding probability for block holders. Then, a dissemination method based on erasure coding was proposed. In this method, information blocks were distributed in a decentralized manner. Each node holding the blocks autonomously determined whether to forward or discard them based on pre-calculated probabilities. When the sink node received n distinct information blocks of a data message, the original data could be recovered through decryption and decoding. Simulation results demonstrate that the proposed erasure coding-based dissemination method exhibits superior performance. The required data delivery rate is guaranteed, the likelihood of data theft is minimized, and the computational overhead incurred by nodes during dissemination remains low. The method is proven suitable for UWSNs with limited node storage capacity.

Keywords: underwater wireless sensor network, underwater spy-robots, message dissemination, erasure code

0 引言

作为水下监测领域的典型应用, 水下无线传感器网络 (underwater wireless sensor network, UWSN) [1-2] 凭借灵活的网络基础设施, 允许全部或部分传感器节点在水下环境中自由移动, 从而执行无人化水下监测任务。当前, UWSN 已在多个领域展现出丰富的应用场景, 如水下生物追踪[3]、资源勘探、水下污染监测和战术监视[4]。然而, 由于 UWSN 中节点具有可移动性, 节点间可用的通信链路稀少且不稳定, 因此数据消息通常无法沿着稳定的通信路径转发。这一特性与完全由锚定节点组成的水下网络的数据传输机制形成显著差异。

如图1所示, 在 UWSN 中, 可移动节点主要由水下移动载体 (如鱼类或微型航行器)、传感器和通信模块3部分构成。这些节点可对水下兴趣事件进行监测, 并将监测数据封装为数据消息, 随后通过若干间歇出现的通信链路逐跳转发至汇聚节点。

在 UWSN 的军事应用 (如战术监视) 中, 数据消息可能包含机密信息, 而水域环境可能面临水下间谍机器人等窃听者入侵[5-6]。如图1所示, 这类窃听者通常游弋在节点周围, 试图窃取节点转发的数据消息。由于窃听者从不主动与节点或其他窃听者进行通信, 其存在很难被节点感知。因此, 如何降低数据消息被窃取的风险 (即抵御水下窃听), 成为 UWSN 军事应用的关键问题。当前, 抵御水下窃听的 UWSN 消息转发技术主要面临以下挑战。

1) 窃听者难以被发现。窃听者对节点的通信信道进行静默监听, 而且不主动通信, 这种隐蔽

的监听模式使得网络节点难以实时察觉窃听行为。在此情况下, 节点转发的数据消息存在被窃取的风险。为应对该问题, 本文提出将每个数据消息编码为若干信息块, 并在消息转发前对部分信息块实施轻量级加密。

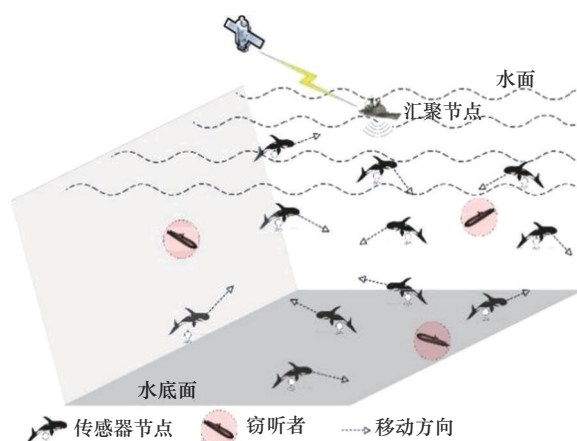


图1 被窃听者入侵的水下无线传感器网络

Figure 1 UWSN invaded by eavesdroppers

2) 数据消息投递需求。受节点移动性影响, UWSN 中节点间的相遇机会与通信链路呈现显著的间歇性特征, 导致数据消息无法通过稳定路径从源节点传输至汇聚节点。而数据消息只有成功投递至汇聚节点, 才能开展后续的分析与决策工作。因此, 数据消息投递率成为衡量 UWSN 消息转发性能的关键指标。然而, 提升投递率往往伴随着数据被窃听风险的增加。

3) 节点存储空间限制。节点的存储空间通常是有限的[7]。当 UWSN 中存在较多数据消息时, 随着消息及其信息块的不断复制与转发, 部分数据消息或信息块将因存储空间不足而

被迫丢弃。如何避免无序丢弃操作对数据消息投递造成严重影响,也是必须关注的问题之一。

4) 节点计算开销限制。受限于 UWSN 节点所搭载计算芯片的性能,节点可提供的计算资源相对有限。这就要求在消息转发过程中,编/解码与加/解密操作产生的计算开销必须控制在合理范围内,因此无法采用计算复杂度较高的编/解码与加/解密算法。

现有研究已提出多种保护数据消息转发的方法,如采用复杂加密算法对数据消息进行深度加密,或构建复杂身份认证机制用来识别窃听者,从而规避数据消息在窃听节点周边转发。然而,复杂加密与认证机制会产生巨大的计算开销,这对计算能力有限的 UWSN 节点而言是无法承受的,难以在实际场景中有效应用。

针对上述问题本文提出一种基于纠错码的 UWSN 消息转发方法。首先将每个数据消息编码成 n 个消息块和 m 个校验块,然后从这 $n + m$ 个信息块中随机选择 $m + 1$ 个信息块,在执行转发操作前对其实施轻量级加密处理。当汇聚节点接收到某个数据消息的 n 个信息块后,对这些信息块进行解密和解码,就可以复原该数据消息。该方法可以有效抵御窃听者对数据消息的窃取,主要原因如下:其一,即使窃听者获取大量信息块,但由于缺乏消息块与原始数据消息的对应标识体系,难以将窃取的信息块准确归属到具体的数据消息,从而破坏窃听者对数据的整合分析;其二,对信息块的编码与加密操作模糊了数据消息的原始语义特征,使得窃听者无法凭借直观内容判断信息块是否经过加密处理,极大增加了破解难度;其三,窃听者通常难以掌握信息块加密所采用的具体算法与密钥,缺乏解密的关键要素,进一步阻断了其窃取数据内容的途径。

本文的主要贡献如下。

1) 采用轻量级加密方法对部分信息块进行加密,并合理设置转发与丢弃概率,降低了节点的计算开销。

2) 结合分布式转发和冗余校验块设计,确保汇聚节点只有接收到足够数量的信息块才能恢复

完整数据,显著降低了数据消息的窃取率。

3) 引入了主动丢弃机制,能够动态缓解节点存储压力,有效解决存储溢出引发的无序丢弃问题。相比其他算法表现出更好的存储管理能力。

1 相关工作

1.1 DTN 和 UWSN 中的消息转发

消息转发问题已经得到了大量的研究,特别是在时延容忍网络(delay tolerant network, DTN)和 UWSN 中。文献[8]提出的洪泛转发(epidemic forwarding, EF),允许节点与所有相遇节点交换数据消息。该方法虽能实现较高的数据投递率,但存在通信开销过大的缺陷,且在节点存储空间受限场景下易引发数据消息的无序丢弃问题。文献[9]设计了一种波束宽度与方向相关的路由(beam width and direction concerned routing, BDCR)协议,通过波束宽度与三维方向特征优化转发策略,在保证较高投递率的同时提升了转发效率。文献[10]聚焦移动节点接触模式,提出一种基于规则和偶发链接的消息转发方法,通过区分节点间接触的规律性(规则接触或偶发接触)优化数据传输路径,进一步提高投递成功率。文献[11]提出了早期提前唤醒机制,通过优化节点唤醒策略加速消息转发,并降低能量消耗。文献[12]提出基于移动节点辅助的干扰避免路由协议,根据相邻区域数据包投递概率动态选择中继节点。文献[13]设计了生物启发的 UWSN 多目标进化路由协议,利用多目标遗传算法的自然进化特性实现可靠且能量感知的数据收集。文献[14]提出一种开放式低能耗水下路由方案,通过降低传输功耗来延长网络生命周期。

上述工作主要围绕数据投递率、转发时延、网络能耗等性能展开,但普遍忽略了网络中潜在的窃听威胁,尚未针对数据消息窃取问题对转发机制进行安全优化设计。

1.2 消息转发中的安全问题

目前,基于接触避免的安全路由协议研究已取得丰富的成果。这些研究通过减少数据消息在窃听者周边不安全区域的转发,从而尽可能降低数据被窃取的风险。文献[15]构建了融合投递率

与转发安全性的机会转发路径模型，并提出接触避免路由（contact avoidance routing, CAR）协议，用来将数据消息安全转发至汇聚节点，同时抵御基于接触行为的泄密攻击。需要注意的是，CAR协议的有效性依赖于一个前提假设，即窃听者可通过节点行为分析或信誉评估机制被识别^[16]。

在现有研究中，纠删码方法已被应用于数据消息转发场景。文献[17]通过评估纠删码在安全数据传输中的有效性，提出一种基于私密共享的纠删码方法，并结合长径回避、对手回避和对手邻接回避等多种策略，以提升数据消息的投递率。为实现可靠的数据传输，文献[18]设计了一种基于纠删码的多路径路由方案，旨在降低UWSN中的丢包率。该方案将每个数据包分割为若干数据块，并生成相应的冗余块。值得注意的是，该研究假设所有节点均为锚定状态，未考虑节点移动性因素，这与本文工作的研究场景存在显著差异。

此外，其他类型网络中针对安全威胁的消息转发技术研究也取得了一定成果。文献[19]提出一种适用于车联网的无证书认证和道路消息转发协议，该协议通过无证书加密技术实现认证和密钥分发，保障消息传输的安全性。文献[20]提出一种基于网络拓扑信息的车联网安全消息转发算法，可以根据消息内容动态制定合理的转发策略。文献[21]提出一种地理社会信任路由方法，根据可信度和社会性连通度区分节点，进而选择由可信节点组成的最短路径进行消息转发。文献[22]提出在转发数据消息前，将数据消息编码为若干消息片并分发给目标节点的机制。与文献[22]简单地将每个数据消息编码为 K 个消息片的机制相比，本文通过引入纠删码技术，不仅提升了数据传输的安全性，还显著优化了消息恢复效率。

2 系统模型和问题描述

2.1 UWSN 模型

假设 N 个移动节点被部署在水域 $\mathbf{D}$ 中， $\mathbf{D} \in \mathbb{R}^{+3}$ 。为便于描述，将时间划分为离散时隙，分别用 t 和 τ 表示绝对时隙和相对时隙（数据消息生成时刻对应的时隙定义为相对时隙）。每个数

据消息产生后，应在 τ^* 个时隙内从源节点转发至汇聚节点。

此外，假设有 N_e 个窃听者入侵了水域 $\mathbf{D}$ ，它们可以静默监听邻近节点的通信信道。如图2所示，窃听者通过移近信息块持有节点并监听其通信信道，可捕获该节点转发的信息块。每个节点的通信范围和存储空间分别用 r_c 和 S 表示。在每个时隙内，假设每个节点以概率 ρ 生成新的数据消息。

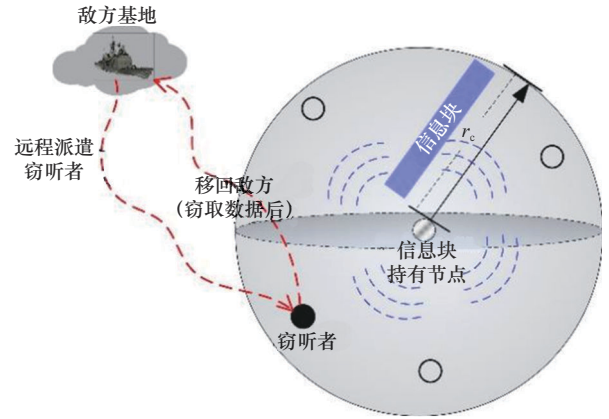


图2 窃听者窃取数据消息示意

Figure 2 Schematic of an eavesdropper intercepting data messages

设 $d(i,j)$ 表示节点 V_i 和 V_j 之间的距离。如果 $d(i,j) \leq r_c$ ，那么节点 i 与 j 之间的链接被视为潜在通信链接。受水下通信信号不规则性影响，潜在通信链接 (i,j) 的实际存在概率由以下表达式确定。

$$P_c(i,j) = \begin{cases} 0, & d(i,j) > r_c \\ c_1 \cdot \Omega(j)^{-\zeta} \cdot d(i,j)^{-\eta}, & \text{其他} \end{cases} \quad (1)$$

其中， c_1 为常数， $\Omega(j)$ 表示节点 V_j 附近的信号不规则性。该不规则性由天线方向、天线增益、电池状态、信噪比阈值和障碍物等因素共同引起^[23]。假设每个节点周围的信号不规则性服从均匀分布 $U(\Omega_{\min}, \Omega_{\max})$ ^[24]。

特别地，节点入度反映了节点接收到信息块（消息块或校验块）的可能性，即入度较大的节点能够接收到更多信息块。文献[25]的研究可证明，节点入度服从幂律分布。节点入度通过影响信息块持有节点的比例，进而对数据消息的窃取率和投递率产生作用。不失一般性，假设节点入

度分布可表示为 $\Pr(k) = \alpha \cdot k^{-\gamma}$, 其中 $\gamma = \frac{1}{\theta} + 1$ ($2 < \gamma < 3$), 且 $\alpha = \frac{1}{\sum_{k=1}^{N-1} k^{-\gamma}}$.

2.2 基于纠删码的信息块

对于每个数据消息, 源节点首先将其分解并编码为 n 个消息块 $b_1, \dots, b_n$, 然后通过里德-所罗门编码算法^[26]生成 m 个校验块 $b_{n+1}, \dots, b_{n+m}$. 为便于描述, 这里将消息块和校验块统称为信息块. 每个信息块大小 l_b 相同. 里德-所罗门编码规则如图 3 所示, 其中矩阵 $\{v_{ij}\}_{m \times n}$ 表示为范德蒙矩阵.

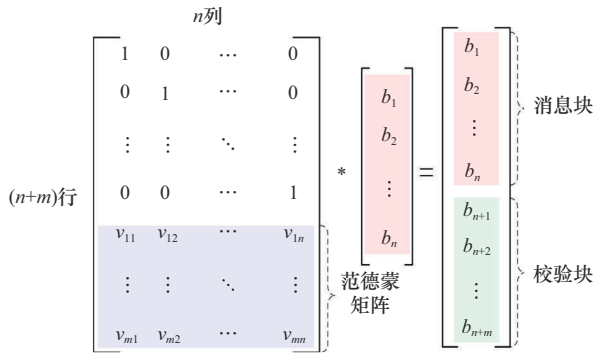


图3 里德-所罗门编码规则

Figure 3 Reed-Solomon encoding principle

从 $n + m$ 个信息块中随机选择 $m + 1$ 个信息块, 采用轻量加密方法 (如 AES 算法) 对其进行加密处理. 该数据消息的所有信息块 (共 $n + m$ 个) 在每个时隙都可能被持有节点复制并转发, 此过程持续 τ^* 个时隙, 直至汇聚节点接收到至少 n 个不同的信息块, 或者 τ^* 个时隙结束为止.

如果汇聚节点在 τ^* 个时隙结束前收到至少 n 个不同的信息块, 则可以解密其中的加密信息块, 并通过解码这 n 个信息块恢复原始数据消息. 汇聚节点成功恢复原始数据消息, 即视为该数据消息投递成功. 假设窃听者破译加密信息块的概率为 p ($p < 1$). 若窃听者捕获到某数据消息的至少 n 个信息块, 并且破译的加密块和未加密块数量达到 n , 则判定该数据消息被窃取. 图 4 和图 5 分别展示了数据消息投递成功与被窃取的过程.

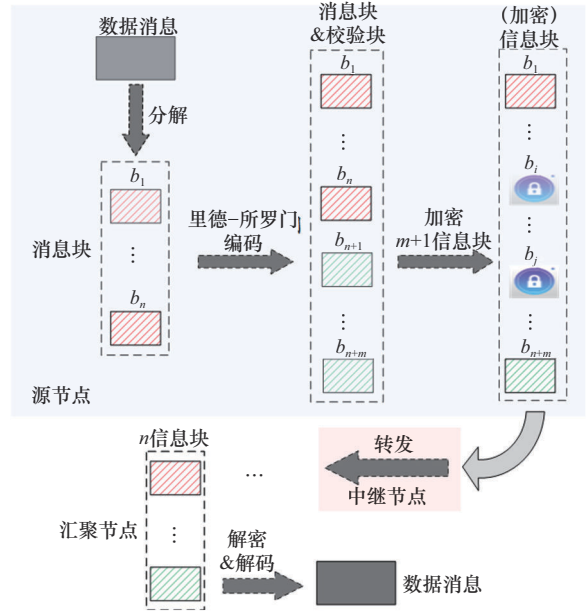


图4 数据消息投递成功过程

Figure 4 Process of successful data message delivery

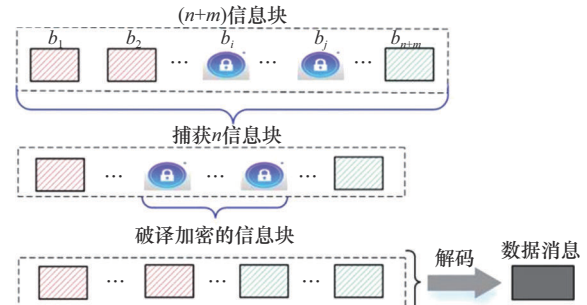


图5 数据消息被窃取过程

Figure 5 Data message interception process

2.3 目标函数

在每个时隙中, 节点感知兴趣事件并产生 $N \cdot \rho$ 个新的数据消息. 在每个数据消息生成后的 τ^* 个时隙内, 其信息块会被复制并转发, 超过 τ^* 个时隙的数据消息的所有信息块将被节点直接丢弃. 因此, 在每个时隙中, 信息块的总数可表示为 $N^2 \cdot \rho \cdot (n + m) \cdot \sum_{\tau=0}^{\tau^*-1} H(\tau)$, 其中 $H(\tau)$ 表示在第 τ 个相对时隙某个信息块的持有节点比例.

在节点存储受限的 UWSN 中, 为降低数据消息窃取率, 同时保证所需的最低数据消息投递率, 并且限制节点的计算开销, 抵御水下窃听的 UWSN 消息转发问题目标可以表示为:

$$\min \mathcal{E}(\tau^*), \text{ s.t. } \begin{cases} \mathcal{R}(\tau^*) \geq \tilde{\mathcal{R}} \\ \mathcal{S}(\tau^*) \leq \frac{S}{l_b} \\ \mathcal{C}(\tau^*) \leq \tilde{\mathcal{C}} \end{cases} \quad (2)$$

其中, $\mathcal{E}(\tau^*)$ 表示在 τ^* 个时隙内被窃听者窃取的数据消息的比例, 即数据消息窃取率; $\mathcal{R}(\tau^*)$ 表示数据消息投递率, 定义为在 τ^* 个时隙内成功投递至汇聚节点的数据消息比例; $\mathcal{C}(\tau^*)$ 表示单个节点在 τ^* 个时隙内处理一个数据消息的计算开销(以计算复杂度衡量); $\tilde{\mathcal{R}}$ 和 $\tilde{\mathcal{C}}$ 分别表示系统所需的最低数据消息投递率和最大计算开销。

3 问题分析

表1给出了本节所用主要符号的说明。

表1 主要符号说明

Table1 Description of key symbols

参数	描述
$H_k(\tau)$	在第 τ 个相对时隙入度为 k 的信息块持有节点比例
$H(\tau)$	在第 τ 个相对时隙的信息块持有节点比例
$O_k(\tau)$	在第 τ 个相对时隙入度为 k 的普通节点比例
P_d	信息块转发概率
μ	信息块丢弃概率
$\mathcal{R}(\tau)$	在 τ 个时隙内数据消息成功投递的比例(投递率)
$\mathcal{R}_a(\tau)$	在第 τ 个相对时隙成功投递的数据消息比例
$\mathcal{E}(\tau)$	在 τ 个时隙内被窃听者窃取的数据消息比例(窃取率)
$\mathcal{E}_a(\tau)$	在第 τ 个相对时隙被窃听者窃取的数据消息比例
$\mathcal{S}(\tau)$	在 τ 个时隙内节点持有的信息块数
$\mathcal{C}(\tau)$	在 τ 个时隙内的计算开销

对于数据消息 b 的每个信息块, 节点存在以下两种状态。

1) 普通节点: 未持有该信息块(副本)的节点。

2) 信息块持有节点: 已接收并持有该信息块(副本)的节点。

为刻画普通节点与信息块持有节点的比例动态变化, 假设信息块持有节点在每个时隙以转发概率 P_d 转发所持有的信息块, 并以丢弃概率 μ 丢弃所持有的信息块, 则普通节点和信息块持有节点的比例变化可以表示为

$$\begin{cases} H_k(\tau+1) - H_k(\tau) = k \cdot H(\tau) \cdot P_d \cdot O_k(\tau) - \mu \cdot H_k(\tau) \\ H_k(\tau) + O_k(\tau) = 1 \end{cases} \quad (3)$$

其中, 入度 $k \in [1, N-1]$ 且 $H(\tau) = \sum_{k=1}^{N-1} \Pr(k) \cdot H_k(\tau)$ 。由式(3)可以得到式(4)。

$$\begin{aligned} & \Pr(k) \cdot H_k(\tau+1) = \\ & k \cdot P_d \cdot \Pr(k) \cdot [1 - H_k(\tau)] \cdot H(\tau) - \\ & \mu \cdot \Pr(k) \cdot H_k(\tau) + \Pr(k) \cdot H_k(\tau) \end{aligned} \quad (4)$$

则有

$$\begin{aligned} \sum_{k=1}^{N-1} \Pr(k) \cdot H_k(\tau+1) &= H(\tau+1) = \left\{ \beta \cdot P_d \cdot \right. \\ & \left. \sum_{k=1}^{N-1} \Pr(k) \cdot [1 - H_k(\tau)] - \mu + 1 \right\} \cdot H(\tau) \end{aligned} \quad (5)$$

为简化式(5), 不妨令 $\sum_{k=1}^{N-1} k \cdot \Pr(k) \cdot [1 - H_k(\tau)] \approx \beta \cdot \sum_{k=1}^{N-1} \Pr(k) \cdot [1 - H_k(\tau)]$, 其中 β 为可设置的常数, 其设置将在后续小节进行分析。于是, 式(5)可以改写为

$$\begin{aligned} H(\tau+1) &= \left\{ \beta \cdot P_d \cdot \left[\sum_{k=1}^{N-1} \Pr(k) - \right. \right. \\ & \left. \left. \sum_{k=1}^{N-1} \Pr(k) \cdot H_k(\tau) \right] - \mu + 1 \right\} \cdot H(\tau) = \\ & \left\{ \beta \cdot P_d \cdot [1 - H(\tau)] - \mu + 1 \right\} \cdot H(\tau) \end{aligned} \quad (6)$$

由此, 可以得到

$$H(\tau+1) - H(\tau) \approx \frac{dH(\tau)}{d\tau} = (\beta \cdot P_d - \mu) \cdot H(\tau) - \beta \cdot P_d \cdot H(\tau)^2 \quad (7)$$

式(7)是一个伯努利方程, $H(\tau)$ 可以近似表示为

$$\begin{aligned} H(\tau) &\approx \int \beta \cdot P_d \cdot \exp \left[\int (\beta \cdot P_d - \mu) d\tau \right] d\tau = \\ & \frac{\beta \cdot P_d}{\beta \cdot P_d - \mu} \cdot \exp [(\beta \cdot P_d - \mu) \cdot \tau] \end{aligned} \quad (8)$$

3.1 数据消息投递率

当节点均匀分布在水域中时, 节点在移动后仍可近似保持均匀分布。若汇聚节点处于某信息块持有节点的通信范围内, 则该信息块将从持有节点直接转发至汇聚节点。因此, 在第 τ 个相对时隙投递成功率表示为

$$\mathcal{R}_a(\tau) = \binom{n+m}{n} \cdot \left[\frac{4\pi \cdot r_c^3 \cdot N}{3|D|} \cdot Q \cdot H(\tau) \right]^n \quad (9)$$

其中, $\frac{4\pi \cdot r_c^3 \cdot N}{3|\mathbf{D}|} \cdot Q \cdot H(\tau)$ 表示汇聚节点处于信息块持有节点通信范围内的概率, Q 表示一个潜在通信链接的存在概率。 Q 的表达式可由式(1)推导得到。

$$Q = \frac{c_1 \cdot \int_{\Omega_{\min}}^{\Omega_{\max}} \omega^{-\zeta} d\omega}{\Omega_{\max} - \Omega_{\min}} \cdot \frac{\sum_{k=1}^{r_0} [k^3 - (k-1)^3] \cdot (k \cdot r_0)^{-\eta}}{\left(\frac{r_c}{r_0}\right)^3} = \frac{c_1 \cdot (\Omega_{\max}^{1-\zeta} - \Omega_{\min}^{1-\zeta})}{(1-\zeta) \cdot (\Omega_{\max} - \Omega_{\min})} \cdot \frac{\sum_{k=1}^{r_0} (3k^2 - 3k + 1) \cdot (k \cdot r_0)^{-\eta}}{\left(\frac{r_c}{r_0}\right)^3} \quad (10)$$

其中, r_0 表示两个相邻节点之间的最小距离。

此外, 投递率 $\mathcal{R}(\tau) = \mathcal{R}(\tau-1) + \mathcal{R}_a(\tau) \cdot [1 - \mathcal{R}(\tau-1)]$, 即有 $\frac{d\mathcal{R}(\tau)}{d\tau} + \mathcal{R}_a(\tau) \cdot \mathcal{R}(\tau) = \mathcal{R}_a(\tau)$, 因此可以得到

$$\mathcal{R}(\tau) = 1 - c_3 \cdot e^{-\int \mathcal{R}_a(\tau) d\tau} = 1 - c_3 \cdot \exp \left\{ - \binom{n+m}{n} \cdot \left(\frac{4\pi \cdot r_c^3 \cdot N}{3|\mathbf{D}|} \cdot Q \right)^n \cdot \frac{(\beta \cdot P_d)^n \cdot \exp\{(\beta \cdot P_d - \mu) \cdot n \cdot \tau\}}{n \cdot (\beta \cdot P_d - \mu)^{n+1}} \right\} \quad (11)$$

且由于 $\mathcal{R}(0) = 0$, 因此有 $c_3 = \exp \left\{ \binom{n+m}{n} \cdot \left(\frac{4\pi \cdot r_c^3 \cdot N}{3|\mathbf{D}|} \cdot Q \right)^n \cdot \frac{(\beta \cdot P_d)^n}{n \cdot (\beta \cdot P_d - \mu)^{n+1}} \right\}$ 。

$$\left(\frac{4\pi \cdot r_c^3 \cdot N}{3|\mathbf{D}|} \cdot Q \right)^n \cdot \frac{(\beta \cdot P_d)^n}{n \cdot (\beta \cdot P_d - \mu)^{n+1}} \right\}。$$

3.2 数据消息窃取率

当窃听者获取了某数据消息的 n 个不同信息块时, 该数据消息存在被窃取风险。此外, 加密密钥被破译的概率与窃听者已获取的信息块数量相关。类似式(9), 在第 τ 个相对时隙内被窃听者

窃取的数据消息比例可表示为

$$\mathcal{E}_a(\tau) = N_c \cdot \binom{n+m}{n} \cdot \left[\frac{4\pi \cdot r_c^3 \cdot N}{3|\mathbf{D}|} \cdot Q \cdot H(\tau) \right]^n \cdot P_d \cdot p \quad (12)$$

已有 $\frac{d\mathcal{E}(\tau)}{d\tau} + \mathcal{E}_a(\tau) \cdot \mathcal{E}(\tau) = \mathcal{E}_a(\tau)$, 由此得出

$$\mathcal{E}(\tau) = 1 - c_4 \cdot \exp \left\{ - N_c \cdot \binom{n+m}{n} \cdot \left(\frac{4\pi \cdot r_c^3 \cdot N}{3|\mathbf{D}|} \cdot Q \right)^n \cdot P_d \cdot p \cdot \frac{(\beta \cdot P_d)^n \cdot \exp\{(\beta \cdot P_d - \mu) \cdot n \cdot \tau\}}{n \cdot (\beta \cdot P_d - \mu)^{n+1}} \right\} \quad (13)$$

其中 $c_4 = \exp \left\{ N_c \cdot \binom{n+m}{n} \cdot \left(\frac{4\pi \cdot r_c^3 \cdot N}{3|\mathbf{D}|} \cdot Q \right)^n \cdot P_d \cdot p \cdot \frac{(\beta \cdot P_d)^n}{n \cdot (\beta \cdot P_d - \mu)^{n+1}} \right\}$ 。

$$P_d \cdot p \cdot \frac{(\beta \cdot P_d)^n}{n \cdot (\beta \cdot P_d - \mu)^{n+1}} \right\}。$$

3.3 存储限制和计算开销

一个节点在 τ^* 个时隙内所持有的信息块数的数学期望可以表示为

$$E(\tau^*) = N \cdot \rho \cdot (n+m) \cdot \sum_{\tau=0}^{\tau^*-1} H(\tau) \approx N \cdot \rho \cdot (n+m) \cdot \int_0^{\tau^*} H(\tau) d\tau = N \cdot \rho \cdot (n+m) \cdot \frac{\beta \cdot P_d}{(\beta \cdot P_d - \mu)^2} \cdot \left[e^{(\beta \cdot P_d - \mu) \cdot \tau^*} - 1 \right] \quad (14)$$

此外, 对于每个数据消息, 计算开销 $\mathcal{C}(\tau^*)$ 主要产生于编码/解码过程和加密/解密过程。其可表示为

$$\mathcal{C}(\tau^*) = n \cdot m + n^3 \cdot \mathcal{R}(\tau^*) + (m+1) \cdot l_b + \frac{(m+1) \cdot n}{n+m} \cdot l_b \cdot \mathcal{R}(\tau^*) \quad (15)$$

其中, $n \cdot m$ 和 $n^3 \cdot \mathcal{R}(\tau^*)$ 分别表示基于范德蒙矩阵的里德-所罗门纠错码的编码开销和解码开销。

$(m+1) \cdot l_b$ 和 $\frac{(m+1) \cdot n}{n+m} \cdot l_b \cdot \mathcal{R}(\tau^*)$ 分别表示

AES 算法^[27]的加密开销和解密开销。由于 $\frac{1 - \mathcal{R}(\tau)}{c_3} \in [0, 1]$, 式(15)表明通过最小化 P_d 值可以减小 $\mathcal{E}(\tau^*)$, 即降低数据消息窃取率。

3.4 问题推导

根据上述模型可以得到引理1和引理2, 而进一步分析UWSN消息转发问题。

引理1 数据消息投递率的增加会导致数据消息窃取率的增加。

证明 根据式(9)、式(11)、式(12)和式(13), 数据消息窃取率 $\mathcal{E}(\tau)$ 可以表示为

$$\mathcal{E}(\tau) = 1 - c_4 \cdot \exp \left\{ N_e \cdot P_d \cdot p \cdot \ln \left(\frac{1 - \mathcal{R}(\tau)}{c_3} \right) \right\} = 1 - c_4 \cdot \left(\frac{1 - \mathcal{R}(\tau)}{c_3} \right)^{N_e \cdot P_d \cdot p} \quad (16)$$

这表明数据消息投递率的增加会导致数据消息窃取率的增加。

根据引理1, 当获得的数据消息投递率等于所需的最低数据消息投递率 $\tilde{\mathcal{R}}$ 时, 数据消息窃取率可以最小化。

引理2 当 $\beta \cdot P_d$ 值固定时, 数据消息窃取率随 P_d 的减小而降低。

证明 根据引理1可以得到 $\mathcal{R}(\tau^*) = \tilde{\mathcal{R}}$, 因此 $\mathcal{E}(\tau)$ 关于 P_d 的一阶导数可表示为

$$\frac{d\mathcal{E}(\tau^*)}{dP_d} = -c_4 \cdot N_e \cdot p^n \cdot P_d^{n-1} \cdot \ln \left(\frac{1 - \tilde{\mathcal{R}}}{c_3} \right) \cdot \left(\frac{1 - \tilde{\mathcal{R}}}{c_3} \right)^{N_e \cdot (p \cdot P_d)^n} \quad (17)$$

这表明 $\frac{d\mathcal{E}(\tau^*)}{dP_d} < 0$, 即 $\mathcal{E}(\tau)$ 随着 P_d 的减小而降低。

根据引理2的结论, 应设置 $\beta = 1.0$, 则式(2)可简化为

$$\min P_d, \text{ s.t. } \begin{cases} 1 - c_3 \cdot \exp \left\{ -\binom{n+m}{n} \cdot \left(\frac{4\pi \cdot r_c^3 \cdot N}{3|\mathbf{D}|} \cdot Q \right)^n \right. \\ \left. \cdot \frac{P_d^n \cdot \exp \left\{ (P_d - \mu) \cdot n \cdot \tau^* \right\}}{n \cdot (P_d - \mu)^{n+1}} \right\} = \tilde{\mathcal{R}}, \\ N \cdot \rho \cdot (n+m) \cdot \frac{P_d}{(P_d - \mu)^2} \cdot \left[e^{(P_d - \mu) \cdot \tau^*} - 1 \right] \leq \frac{S}{l_b}, \\ n \cdot m + n^3 \cdot \tilde{\mathcal{R}} + (m+1) \cdot l_b + \frac{(m+1) \cdot n}{n+m} \cdot l_b \cdot \tilde{\mathcal{R}} \leq \tilde{C} \end{cases} \quad (18)$$

式(18)表示当 P_d 和 μ 的值满足所需的最低数据消息投递率、节点存储空间限制和计算开销约束时, P_d 应最小化。

4 基于纠删码的UWSN消息转发方法

本节提出了一种基于纠删码的安全消息转发方法 (secure message dissemination approach based on erasure code, SMMDA-EC)。在 SMMDA-EC 中, 每个数据消息被编码为 n 个消息块和 m 个校验块, 然后在其中随机选择 $m+1$ 个信息块进行轻量级加密处理。在每个时隙中, 节点根据预设的转发概率和丢弃概率, 对所持有的信息块执行转发或丢弃操作。

需要注意的是, SMMDA-EC 中所有数据消息

的信息块 (消息块和校验块) 都是以分布式方式进行转发的, 不需要集中式计算和全局信息交互。这一特性使得 SMMDA-EC 的运行开销显著降低。

4.1 SMMDA-EC 的详细描述

假设在第 t 个绝对时隙, 节点 V_s 产生了一个数据消息 $\mathbf{b}$, $\mathbf{b}$ 需从源节点 V_s 转发到汇聚节点 V_d 。UWSN 中所有节点都维护一张关于 $\mathbf{b}$ 的信息块持有列表。表2列出了 SMMDA-EC 描述中的符号及其含义。

SMMDA-EC 主要包括数据消息编码、信息块加密、节点交互、信息块转发和丢弃、信息块持有列表更新和数据消息解码6个主要执行阶段。

阶段 1 数据消息编码。在第 t 个绝对时隙, 源节点 V_s 将数据消息 b 分解和编码为 n 个消息块 $b_1, \dots, b_n$, 然后通过里德-所罗门编码算法生成 m 个校验块 $b_{n+1}, \dots, b_{n+m}$ 。

表 2 SMDA-EC 描述中的符号说明

Table 2 Commonly used symbols and their meanings in SMDA-EC descriptions

符号	含义
$C(i)$	节点 V_i 的坐标
$\mathcal{B}(i)$	V_i 所持有的信息块
$\mathcal{B}_n(i)$	V_i 的邻居节点所持有的信息块
$\mathcal{N}(i)$	V_i 的邻居节点集合
$\mathcal{M}(i, b_k)$	不持有信息块 b_k 的 (V_i 的) 邻居节点集合

阶段 2 信息块加密。从 $n + m$ 个信息块中随机选择 $m + 1$ 个, 并使用 AES 算法对这 $m + 1$ 个信息块进行加密。

阶段 3 节点交互。该阶段由以下两个子阶段组成。

子阶段 3-1 请求。假设在第 $t + \tau - 1$ 个绝对时隙 (其中 $1 \leq \tau \leq \tau^*$), 每个节点 V_i 广播一个包含四元组 ($V_i, t + \tau - 1, C(i), \mathcal{B}(i)$) 的请求报文。同时, V_i 根据接收到的请求报文确定邻居节点集合。

$$\mathcal{N}(i) = \{V_j | d(i, j) \leq r_c\} \quad (19)$$

子阶段 3-2 应答。在接收到来自 V_i 的请求报文后, 每个邻居节点 V_j 会向 V_i 发送一个应答报文作为响应, 该应答报文包含一个四元组 ($V_j, t + \tau - 1, \mathcal{N}(j), \mathcal{B}_n(j)$), 其中 $\mathcal{B}_n(j)$ 表示为:

$$\mathcal{B}_n(j) = \bigcup \{ \mathcal{B}(q) | \forall V_q \in \mathcal{N}(j) \} \quad (20)$$

阶段 4 信息块转发和丢弃。假设 V_i 持有信息块 b_k , 可能接收该信息块的邻居节点集合表示为

$$\mathcal{M}(i, b_k) = \{V_j | \forall V_j \in \mathcal{N}(i) \& b_k \notin \mathcal{B}(j)\} \quad (21)$$

然后, 根据转发概率 P_d 将信息块 b_k 转发给集合 $\mathcal{M}(i, b_k)$ 中的每个节点。此外, V_i 持有的每

个信息块都按丢弃概率 μ 进行丢弃。主动丢弃机制减轻了节点的存储负担, 缓解了节点的存储溢出及无序丢弃问题。

阶段 5 信息块持有列表更新。假设 V_j 已经从 V_i 接收到 b_k 并且丢弃了所持有的另一信息块 $b_{k'}$, 则 V_j 所持有的信息块列表更新为

$$\mathcal{B}(j) \leftarrow \mathcal{B}(j) \cup b_k / b_{k'} \quad (22)$$

阶段 6 数据消息解码。上述阶段 3 到阶段 5 将不断重复, 直到 V_d 已经接收到数据消息 b 的 n 个不同的信息块, 或者转发截止时间 (τ^* 个时隙) 已结束。

当数据消息 b 的 n 个不同的信息块被转发到汇聚节点 V_d 后, 汇聚节点 V_d 首先解密其中的加密块, 然后将这 n 个信息块解码为原始数据消息 b 。此后, V_d 向所有节点广播投递成功通知, 以终止对数据消息 b 的信息块的继续转发。在上述各阶段中, 窃听者可能在一些节点周围移动, 并监听、捕获这些节点转发的信息块。

图 6 所示为数据消息转发示例。在图 6 中, 一个数据消息被编码并加密为 n 个消息块和 m 个校验块, 即图 6 中所示的 $n - 1$ 个未加密信息块和 $m + 1$ 个加密的信息块。3 个窃听者在捕获了若干 (加密的) 信息块后, 可向敌方基地 (具备强大计算与破译能力的舰船或潜艇) 移动, 由敌方基地尝试复原该数据消息。

4.2 SMDA-EC 的复杂度

表 3 给出了 SMDA-EC 的通信复杂度和计算复杂度。

报文/消息交互主要发生在阶段 3 和阶段 4。在阶段 3 中, 每个节点广播一个请求报文, 并向至多 $\left(\frac{4\pi \cdot r_c^3}{3|\mathcal{D}|} \cdot N - 1 \right)$ 个邻居节点发送应答报文, 这表明在最坏情况下交互的报文数量达到 $O(N^2)$ 。在阶段 4 中, 每个节点可能将持有的信息块转发给邻居节点, 转发的信息块 (副本) 总数达到 $\frac{S}{l_b} \cdot N \cdot \left(\frac{4\pi \cdot r_c^3 \cdot N}{3|\mathcal{D}|} - 1 \right)$ 。因此, SMDA-EC 的通信复杂度为 $O(N^2)$ 。

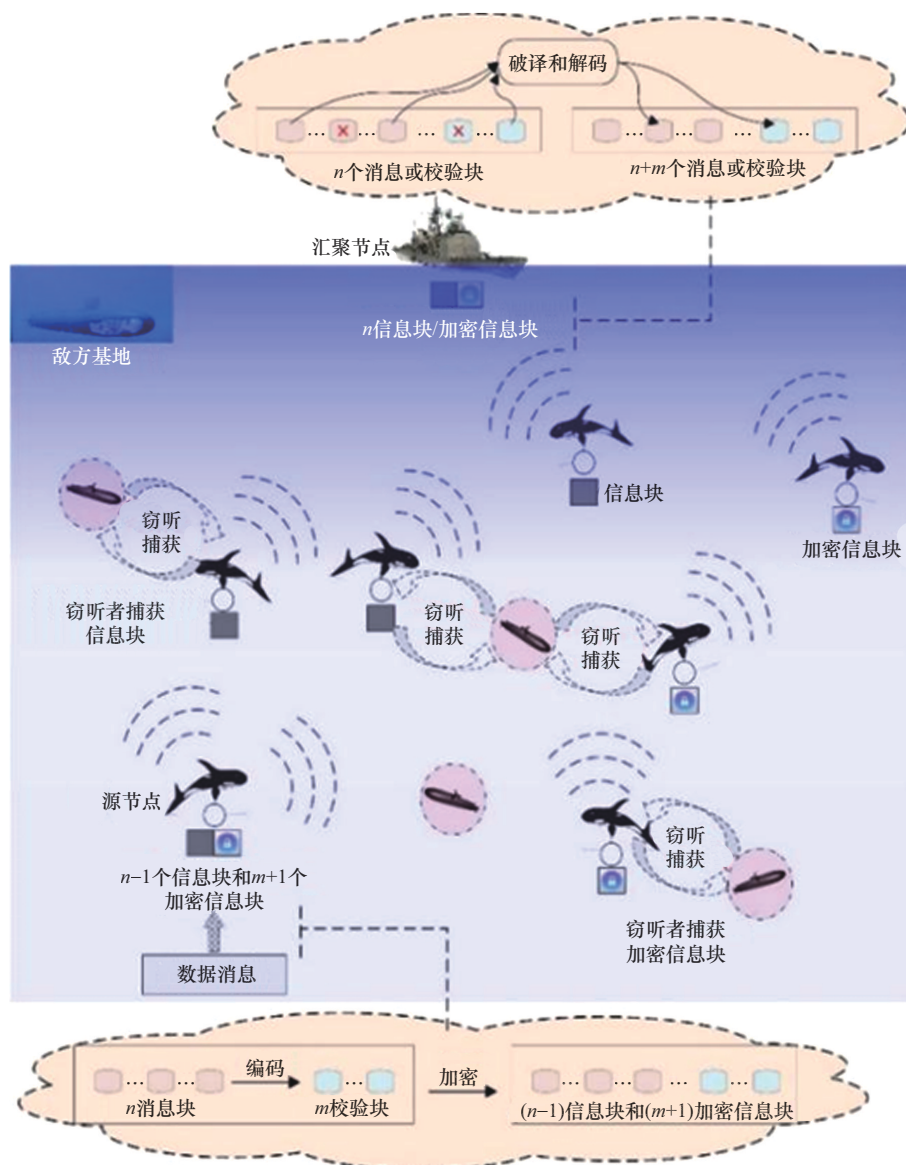


图6 数据消息转发示例

Figure 6 Example of data message disseminating

表3 SMDA-EC的复杂度
Table 3 Complexity of SMDA-EC

阶段	通信复杂度	计算复杂度
1	0	$O(N)$
2	0	$O(N)$
3	$O(N^2)$	$O(N^2)$
4	$O(N^2)$	$O(N)$
5	0	$O(N)$
6	$O(1)$	$O(N)$
总计	$O(N^2)$	$O(N^2)$

SMDA-EC 在各阶段的计算复杂度分析如下：①在阶段1中，每个新数据消息通过里德—所罗门编码算法生成 $n + m$ 个信息块，需执行 $O(n \cdot m \cdot N)$ 次计算，通常 $m < n \ll N$ ，因此计算次数可以表示为 $O(N)$ ；②在阶段2中，每个新数据消息会有 $m + 1$ 个信息块通过 AES 算法进行加密，通常 $m < n \ll N$ ，因此计算次数可以表示为 $O(N)$ ；③在阶段3中，每个节点需确定邻居节点集合和邻居节点所持有的信息块，涉及 $O(N^2)$ 次计算；④在阶段4中，节点执行转发和丢弃所持有的信息块的计算次数为 $O(N)$ ；⑤在

阶段5中, 每个节点可能需要更新所持有信息块的列表, 因此可能存在 $O(N)$ 次更新计算; ⑥在阶段6中, 接收端需要执行 $O(m \cdot N)$ 次计算来解密接收到的信息块, 并需要执行 $O(n^3 \cdot N)$ 次计算来解码复原数据消息。综上, SMDA-EC 的总计算复杂度为 $O(N^2)$ 。

5 仿真实验

在本节中, 通过观察不同参数下 SMDA-EC 的性能变化, 并与 EF、BDCR 和 CAR 等算法进行对比, 评估 SMDA-EC 的性能。主要仿真参数设置见表4, 其中转发概率 P_d 和丢弃概率 μ 通过式(18)计算得到。

表4 主要仿真参数设置
Table 4 Main simulation parameter settings

参数	描述	取值
N	节点数量	800 个
N_e	窃听者数量	5 个
$ D $	节点部署水域大小	$(400 \times 300 \times 50) \text{ m}^3$
S	每个节点的存储空间	1 000 kB
l_b	每个信息块大小	250 B
n	每个数据消息的消息块数	5 个
m	每个数据消息的检验块数	2 个
τ^*	允许转发的时隙数	8 个
r_c	节点通信范围	50 m
r_0	节点之间的最小距离	5 m
ρ	节点在每个时隙产生新数据消息的概率	0.05
c_1	信号不规则公式系数	0.79
ζ	信号不规则公式指数	1.5
η	信号不规则公式指数	2
$\Omega_{\min}$	最小信号不规则性	0.1
$\Omega_{\max}$	最大信号不规则性	0.9
p	窃听者破译加密块的概率	0.1
$\hat{r}$	所需的最低数据消息投递率	0.65
$\hat{c}$	最大计算开销	2 000
T_s	时隙大小	6.02 s

5.1 P_d 和 μ 的设置

基于式(18)得到的转发概率 P_d 和丢弃概率 μ

的计算结果如图7所示, 可以看出 P_d 和 μ 均随 N 的增加呈递减趋势。当 N 增大时, 每个节点的邻域范围内会纳入更多邻居节点, 这将会提高信息块的转发效率; 与此同时, 节点规模的扩大也会导致数据消息生成量增加。为降低节点存储空间溢出风险、避免节点对所持有的信息块的过度丢弃, 应将 P_d 和 μ 设置为较小值。

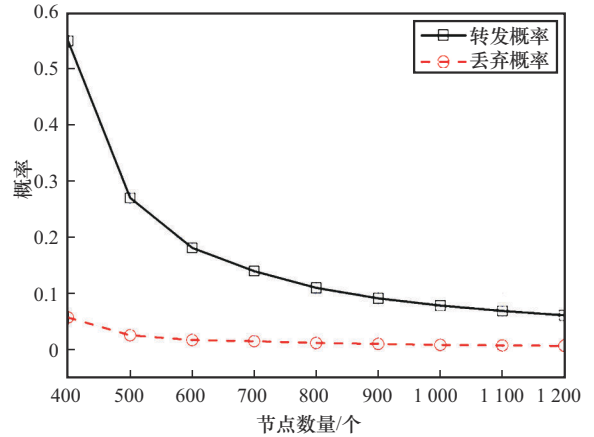


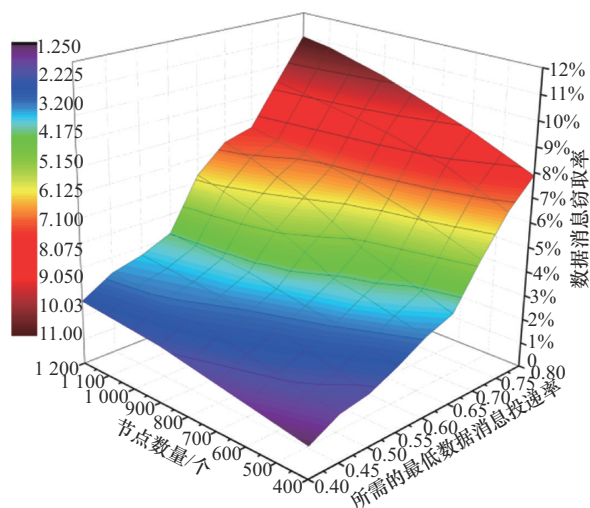
图7 转发概率与丢弃概率

Figure 7 Disseminating probability and discarding probability

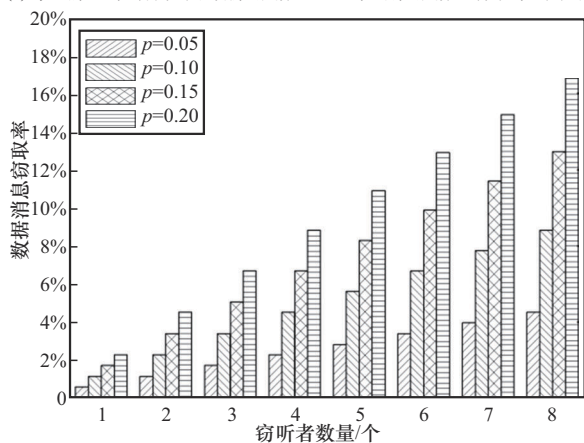
5.2 数据消息窃取率

实验所得的数据消息窃取率如图8所示。在图8(a)中, 数据消息窃取率随着节点数量 N 或 $\hat{r}$ 的增加而增加, 这是由于以下原因: ①当 N 增大时, 节点分布密度提升, 每个窃听者可以同时监听的通信信道数量增加, 导致其捕获的信息块数量显著上升; ②当 $\hat{r}$ 提高时, 系统会通过增大 P_d 加速信息块扩散, 这使得窃听者有更多机会截获转发中的信息块。值得注意的是, 尽管窃取率随 N 增加而增长, 但其增幅很小。这表明 SMDA-EC 对节点规模具有良好的可扩展性, 适合在大规模 UWSN 中部署。

如图8(b)所示, 当窃听者数量 N_e 增加时, 数据消息窃取率呈上升趋势。此外, 窃听者破译概率 p 的提高会直接加剧窃取风险, 这是因为更大的 p 意味着窃听者具有更强的破译能力, 加密信息块更容易被窃听者破译。尽管采用更复杂的加密算法可降低 p 值, 但这会导致计算开销呈指数级增长。因此, 需要在数据消息窃取率和计算开销之间进行权衡, 选择复杂度和保护能力合适的加密方法。



(a) 节点数量和所需的最低数据消息投递率对数据消息窃取率的影响



(b) 窃听器数量和破译概率对数据消息窃取率的影响

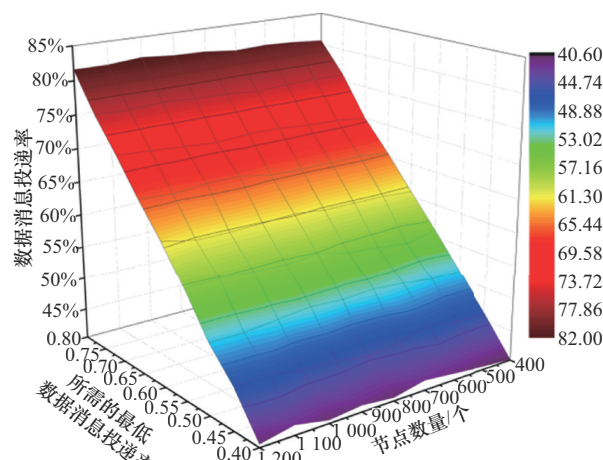
图8 数据消息窃取率

Figure 8 Theft ratio of SMDA-EC

5.3 数据消息投递率、节点存储溢出及计算开销

图9(a)展示了数据消息投递率随 N 和 $\hat{r}$ 的变化规律, 实验结果表明: ①当 $\hat{r}$ 增大时, 数据消息投递率显著提升。这是由于较大的 $\hat{r}$ 会使 P_d 被设置得较大; ②当 $\hat{r}$ 值固定时, 无论 N 如何变化, 数据消息投递率几乎保持不变, 说明SMDA-EC在保证所需的最低数据消息投递率的前提下, 尽可能地降低了数据消息窃取率。

尽管SMDA-EC允许节点主动丢弃所持有的部分信息块, 但节点存储空间溢出问题仍无法完全避免。如图9(b)所示, 节点平均存储溢出数随 N 或 ρ 的增加呈上升趋势。这是因为 N 或 ρ 的增加会造成更多的信息块在UWSN中同时被转发(需要同时转发的数据消息及信息块数量与 N 或 ρ 的值线性相关), 从而会有更多的节点出现存储溢出。



(a) 节点数量和所需的最低数据消息投递率对数据消息投递率的影响

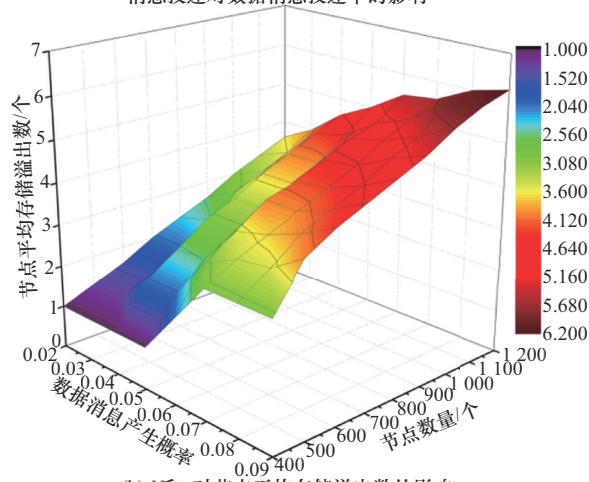
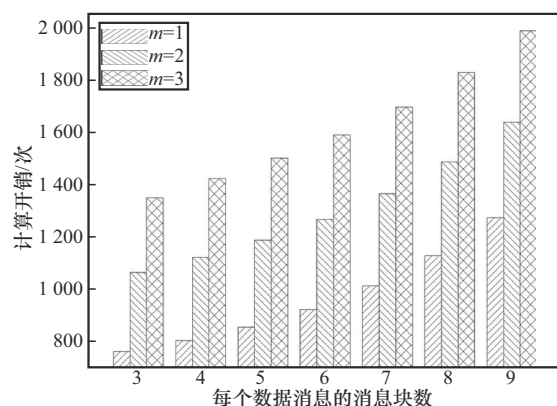
(b) N 和 ρ 对节点平均存储溢出数的影响

图9 数据消息投递率和节点平均存储溢出数

Figure 9 Average value of data message delivery ratio and node storage overflow

此外, 如图10所示, 当设置了较大的 n 或 m 时, 节点计算开销显著增加。以 $n=9$ 、 $m=3$ 为例, 节点计算开销达到1989次操作。

图10 n 和 m 对节点计算开销的影响Figure 10 Computational cost vs. n and m

5.4 算法对比

为进一步评估 SMDA-EC 的性能, 本文基于文献[28]提出的水下移动模型, 将其与 EF、BDCR 和 CAR 算法进行对比分析。实验从数据消息窃取率、投递率、节点平均存储溢出数、平均投递时延 4 个维度展开, 结果如图 11 和图 12 所示。值得注意的是, CAR 虽能通过接触规避抵御窃听, 但其依赖窃听者身份识别。在仿真实验中, 假设 2/3 的窃听者已被 CAR 识别。仿真结果表明, 未被识别的窃听者 (占窃听者总数的 1/3) 仍会显著降低 CAR 的性能。

如图 11(a)所示, SMDA-EC 的数据消息窃取率显著低于其他 3 种算法。这是由于 SMDA-EC 将每个数据消息编码为 $n+m$ 个块, 并对其中 $m+1$ 个块进行了加密, 使得数据消息难以被窃听者捕获和破译, 从而显著降低了数据消息窃取率。

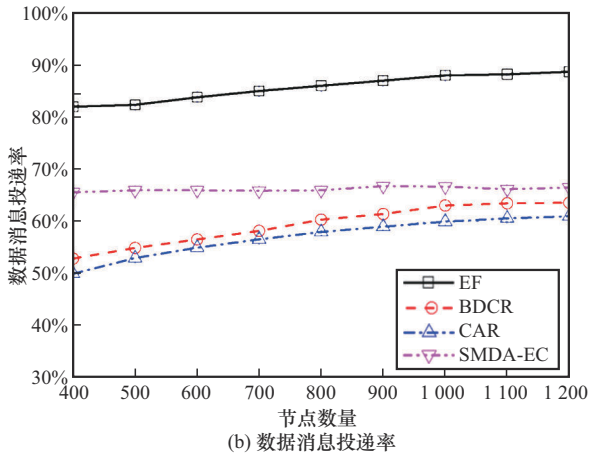
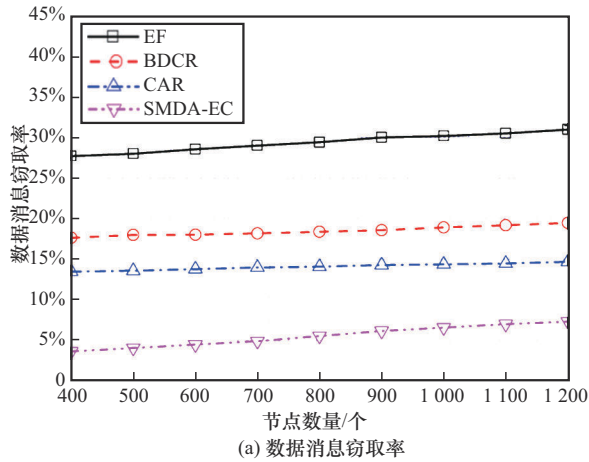


图 11 数据消息投递率与数据消息窃取率的算法比较

Figure 11 Algorithm comparisons of delivery ratio and theft ratio

如图 11(b)所示, 与 BDCR 和 CAR 相比, SMDA-EC 展现出更优的数据消息投递率。尽管 EF 采用洪泛转发方式获得了最佳的数据消息投递率, 但其通信复杂度极高且节点存储溢出问题显著, 如图 12(a)所示。这将导致其在 UWSN 实际应用中不可行, 并且使窃听者可截获更多数据。反观 SMDA-EC, 通过主动丢弃机制动态管理缓存空间, 实现了最低的节点平均存储溢出数。

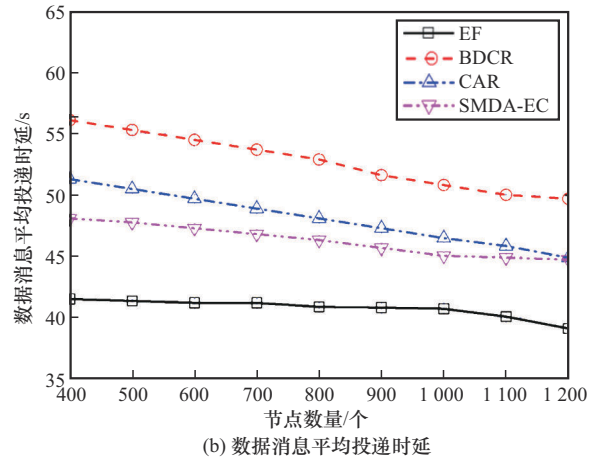
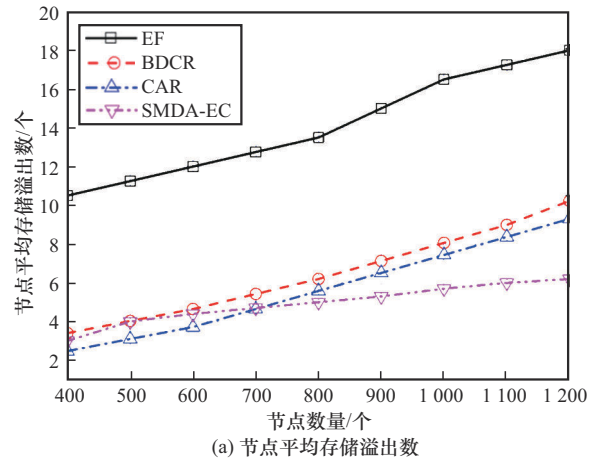


图 12 节点平均存储溢出数和数据消息平均投递时延的算法比较

Figure 12 Algorithm comparisons of average number of storage overflows and average propagation delay

图 12(b)显示这些算法的数据消息平均投递时延随节点数量增加呈下降趋势, 其原因在于每个数据消息的信息块持有节点 (或数据消息持有节点) 在水域中的空间分布更趋均匀, 从而缩短了信息块与汇聚节点的平均距离, 使数据消息能够在更短的时间内被投递到汇聚节点。值得注

意的是, SMDA-EC的转发概率和丢弃概率是在允许转发的时隙数约束下设置的, 因此数据消息平均投递时延受限于预设的允许转发时隙数。

6 可行性分析

本文提出的SMDA-EC方法在真实水下环境中展现出良好的适应性, 尤其在动态水流和多路经衰减等复杂条件下表现出独特优势。

1) 动态水流环境下的鲁棒性。在动态水流环境中, 节点可能会受到洋流和其他动态水流的影响而发生非预期移动。SMDA-EC通过将每个数据消息编码为多个信息块(消息块和校验块), 并在节点间分布式转发这些信息块, 减少了单个节点失效对整个消息转发的影响。即使某些节点因水流移动而暂时丢失链接, 只要汇聚节点最终可以接收到足够数量的有效信息块, 就能够恢复原始数据消息。与此同时, SMDA-EC采用轻量级加密方法对部分信息块进行加密, 减少了计算开销, 使节点能够在资源受限的情况下持续参与消息转发, 即使在动态水流中也能保持较高的计算效率。此外, 信息块以分布式方式转发, 每个节点根据计算出的转发概率和丢弃概率独立操作, 减少了对稳定通信链路的依赖, 提高了系统的鲁棒性。

2) 多路径衰减场景下的容错性。在水下环境中, 声波信号容易受到多路径效应的影响, 出现衰减和失真。SMDA-EC通过引入校验块, 增强了数据的冗余度, 即使部分信息块因多路径衰减而丢失或损坏, 只要汇聚节点接收到足够数量的有效信息块, 就可以通过解码恢复原始数据。此外, SMDA-EC运用里德-所罗门编码算法生成校验块, 这种编码方式具有强大的纠错能力, 能够有效应对多路径衰减引发的错误, 确保数据完整性。

在军事侦察场景中, SMDA-EC凭借高安全性设计为敏感数据提供了多层防护: 通过轻量级加密算法对部分信息块实施加密, 并利用分布式传输将数据分解为多块扩散, 即使敌方截获部分信息, 也难以复原原始数据信息, 从而降低敌方窃取情报的可能性。同时, 纠删码技术赋予系统强大的容错能力, 确保在干扰或节点受损的情况下仍能完成关键信息的传递, 增强了通信的鲁棒

性。此外, 分布式转发机制无须依赖固定路由, 可自适应侦察节点的高频移动特性, 在动态变化的网络拓扑中保持高效的数据传输能力。

在海洋环境监测领域, SMDA-EC也展现出卓越的数据收集与传输能力: 通过分布式转发和存储优化, 减少了单个节点的负担, 同时保证了大规模网络中的数据可靠性。纠删码技术能够有效应对水下复杂信道条件, 提高数据传输的容错率, 非常适合长期部署的监测任务。此外, 主动丢弃策略与轻量级加密的结合, 显著降低了节点的存储和计算开销, 延长了网络生命周期。

7 结束语

本文针对水下UWSN中抵御窃听的消息转发问题展开研究, 提出了SMDA-EC。该方法通过将每个数据消息编码为 n 个消息块和 m 个校验块, 从中选取 $m+1$ 个信息块进行轻量级加密, 并通过建模推导信息块持有节点的转发概率与丢弃概率, 实现了存储受限条件下数据投递率、窃取率和计算开销的多目标优化。仿真结果表明, SMDA-EC在保证所需的最低数据消息投递率和限制节点计算开销的同时, 能够最大限度地降低UWSN的数据消息窃取率。然而, 现有方案在面对智能窃听者时仍存在局限性。例如, 窃听者可能通过篡改或破坏数据消息的部分信息块阻碍数据恢复, 即使汇聚节点收集到该数据消息的 n 个不同信息块, 也可能无法恢复原始数据消息。针对这一挑战, 未来研究计划引入防篡改技术^[29], 通过数字签名或消息认证码为信息块提供完整性校验, 确保接收到的信息块未被篡改。此外, 当前SMDA-EC采用轻量级加密, 未来可结合时变向量(如水下环境噪声^[30])加密机制, 增强加密块的抗破译能力。

参考文献:

- [1] GUAN Q, JI F, LIU Y, et al. Distance-vector-based opportunistic routing for underwater acoustic sensor networks[J]. IEEE Internet of Things Journal, 2019, 6(2): 3831-3839.
- [2] LIU L, XI Z, WU J, et al. Noise-based-protection message dissemination method for insecure opportunistic underwater sensor networks[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 1610-1623.
- [3] DAVIS R, BAUMGARTNER M, COMEAU A, et al. Tracking

- whales on the Scotian Shelf using passive acoustic monitoring on ocean gliders[C]//Proceedings of OCEANS 2016 MTS/IEEE Monterey. Piscataway:IEEE Press, 2016: 1-4.
- [4] FERGUSON B G, LO K W. Acoustic detection, localization, and tracking of tactical autonomous aerial and underwater vehicles[J]. *Journal of the Acoustical Society of America*, 2016, 140(4): 3119-3119.
- [5] WANG Q, DAI H N. On modeling of eavesdropping behavior in underwater acoustic sensor networks[C]//Proceedings of the 18th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM). Piscataway: IEEE Press, 2017: 1-3.
- [6] RANGAPUR I, PRASAD B K S, SURESH R. Design and development of spherical spy robot for surveillance operation[J]. *Procedia Computer Science*, 2020, 171: 1212-1220.
- [7] RAWAT P, SINGH K D, CHAOUCHI H, et al. Wireless sensor networks: a survey on recent developments and potential synergies[J]. *The Journal of Supercomputing*, 2014, 68: 1-48.
- [8] LI F, WU J. LocalCom: a community-based epidemic forwarding scheme in disruption-tolerant networks[C]//Proceedings of the 6th 2009 Annual IEEE Communications Society Conference on Sensor, Mesh and Ad hoc Communications and Networks. Piscataway:IEEE Press, 2009: 1-9.
- [9] ZHANG S, LI D. A beam width and direction concerned routing for underwater acoustic sensor networks[C]//Proceedings of the 9th IEEE International Conference on Mobile Ad-hoc and Sensor Networks. Piscataway:IEEE Press, 2013: 17-24.
- [10] MIR M Y, HU C L. Exploiting mobile contact patterns for message forwarding in mobile opportunistic networks[C]//Proceedings of 2020 IEEE Wireless Communications and Networking Conference (WCNC). Piscataway:IEEE Press, 2020: 1-7.
- [11] DENG Q, OUYANG Y, TIAN S, et al. Early wake-up ahead node for fast code dissemination in wireless sensor networks[J]. *IEEE Transactions on Vehicular Technology*, 2021, 70(4): 3877-3890.
- [12] QURESHI T N, JAVAID N. Enhanced adaptive geographic opportunistic routing with interference avoidance assisted with mobile sinks for underwater wireless sensor network[C]//Proceedings of 2018 International Conference on Frontiers of Information Technology (FIT). Piscataway:IEEE Press, 2018: 367-372.
- [13] FAHEEM M, NGADI M A, GUNGOR V C. Energy efficient multi-objective evolutionary routing scheme for reliable data gathering in Internet of underwater acoustic sensor networks[J]. *Ad Hoc Networks*, 2019, 93: 101912.
- [14] ASHRAF S, GAO M, CHEN Z, et al. CED-OR based opportunistic routing mechanism for underwater wireless sensor networks[J]. *Wireless Personal Communications*, 2022, 125(1): 487-511.
- [15] OSUKI T, SAKAI K, FUKUMOTO S. Contact avoidance routing in delay tolerant networks[C]//Proceedings of IEEE INFOCOM 2017-IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2017: 1-9.
- [16] SALMAN T, JAIN R, GUPTA L. A reputation management framework for knowledge-based and probabilistic blockchains[C]//Proceedings of 2019 IEEE International Conference on Blockchain. Piscataway:IEEE Press, 2019: 520-527.
- [17] ARAI H, ARAI M. Erasure-code-based DTN multi-path routing for contact avoidance[C]//Proceedings of the 22nd IEEE Pacific Rim International Symposium on Dependable Computing (PRDC). Piscataway:IEEE Press, 2017: 215-216.
- [18] KOU Z, WANG C, LEI M. Multipath routing with erasure coding in underwater delay tolerant sensor networks[C]//Proceedings of the 92nd IEEE Vehicular Technology Conference (VTC2020-Fall). Piscataway:IEEE Press, 2020: 1-5.
- [19] TAN H, CHOI D, KIM P, et al. Secure certificateless authentication and road message dissemination protocol in VANETs[J]. *Wireless Communications and Mobile Computing*, 2018, 2018(1): 7978027.
- [20] CHEN J, MAO G, LI C, et al. A topological approach to secure message dissemination in vehicular networks[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2019, 21(1): 135-148.
- [21] PARANJOTHI A, KHAN M S, ZEADALLY S, et al. GSTR: secure multi-hop message dissemination in connected vehicles using social trust model[J]. *Internet of Things*, 2019, 7: 100071.
- [22] LIU L, ZHANG H, WU J, et al. Message piece dissemination approach for opportunistic underwater sensor network invaded by underwater spy-robots[J]. *Software: Practice and Experience*, 2022, 52(5): 1242-1261.
- [23] ZHOU G, HE T, KRISHNAMURTHY S, et al. Models and solutions for radio irregularity in wireless sensor networks[J]. *ACM Transactions on Sensor Networks (TOSN)*, 2006, 2(2): 221-262.
- [24] HUSSAIN M, TRIGONI N. Distributed localization in cluttered underwater environments[C]//Proceedings of the 5th International Workshop on Underwater Networks. New York: ACM Press, 2010: 1-8.
- [25] LIU L, WANG P, WANG R. Propagation control of data forwarding in opportunistic underwater sensor networks[J]. *Computer Networks*, 2017, 114: 80-94.
- [26] NASRI N, ANDRIEUX L, KACHOURI A, et al. Efficient encoding and decoding schemes for wireless underwater communication systems[C]//Proceedings of 2010 7th International Multi-Conference on Systems, Signals and Devices. Piscataway: IEEE Press, 2010: 1-6.
- [27] MASOUMI M, REZAYATI M H. Novel approach to protect advanced encryption standard algorithm implementation against differential electromagnetic and power analysis[J]. *IEEE Transactions on Information Forensics and Security*, 2014, 10(2): 256-265.
- [28] LIU L, WANG R, WU J. A time-inhomogeneous Markov chain and its distributed solution for message dissemination in OUSNs[J]. *Journal of Parallel and Distributed Computing*, 2019, 130: 179-192.
- [29] VASILE D C, SVASTA P. Protecting the secrets: advanced technique for active tamper detection systems[C]//Proceedings of the 25th IEEE International Symposium for Design and Technology in Electronic Packaging (SIITME). Piscataway: IEEE Press, 2019: 212-215.
- [30] BETKE K, SCHULTZ-VON GLAHN M, MATUSCHEK R. Underwater noise emissions from offshore wind turbines[C]//Proceedings of the Joint Congress CFA/DAGA'04. Strasbourg: CFA, 2004: 591-592.

[作者简介]



严翔渝（2000-），男，江苏常州人，南京邮电大学硕士生，主要研究方向为水下传感器网络。



吴洲（2004-），男，江苏丹阳人，主要研究方向为移动网络、深度学习技术。



张文哲（2000-），男，内蒙古锡林浩特人，南京邮电大学硕士生，主要研究方向为无人机网络和拓扑修复。



刘林峰（1981-），男，江苏丹阳人，博士，南京邮电大学教授、博士生导师，主要研究方向为移动计算、水下传感器网络、机器学习。