面向异质感知网络的水声 MAC 层信任评估与协同防御机制

朱荣鑫[1]，唐智超[1]，程亮亮[2]，黄向党[1]，羊秋玲[1]
（1.海南大学计算机科学与技术学院，海南 海口 570100；2.格罗宁根大学科学与工程学部，格罗宁根 9747AG）

摘要：动态异构感知网络中的末梢节点受算力、能量和带宽约束，难以承载重型密码学机制；同时，不可靠链路易使信道异常与恶意行为相互混淆，导致 MAC 层安全防护不足。针对上述问题，本文提出一种反馈驱动的 MAC 层信任评估与协同防御机制。该机制将 ACK/NACK 反馈重构为零成本信任原语，利用 Dempster-Shafer 证据理论融合通信状态、环境扰动和剩余能量等多源证据，并通过显式不确定性建模降低信道波动引发的误判。在防御层，机制根据可疑节点的接收方或发送方角色，分别触发向量转发路由绕行或备用信道隔离，形成“检测—角色判别—防御执行”的闭环。该框架不依赖特定物理层，并以水声传感器网络为典型场景，结合 Bellhop 声场建模与 α-稳态噪声进行实例化。仿真结果表明，所提机制在检测精度、数据投递和吞吐性能方面均优于代表性基线；小规模湖试进一步验证了 ACK/NACK 驱动信任评估在真实多径水声信道中的可行性。

关键词：零信任；MAC 层信任评估；D-S 证据理论；感知协同防御；水声传感器网络；轻量级安全
中图分类号：TP393
文献标志码：A

MAC-Layer Trust Evaluation and Cooperative Defense for Heterogeneous Sensing Networks: An Underwater Acoustic Instantiation

ZHU Rongxin[1], TANG Zhichao[1], CHENG Liangliang[2], HUANG Xiangdang[1], YANG Qiuling[1]
1. School of Computer Science and Technology, Hainan University, Haikou 570100, China
2. Faculty of Science and Engineering, University of Groningen, Groningen 9747AG, The Netherlands

Abstract: Terminal nodes in dynamic heterogeneous sensing networks are constrained by computation, energy, and bandwidth, making heavy cryptographic mechanisms difficult to deploy. Meanwhile, unreliable links may obscure the boundary between channel anomalies and malicious behaviors, leaving MAC-layer security insufficiently addressed. To address this issue, this paper proposes a feedback-driven MAC-layer trust evaluation and cooperative defense mechanism. The proposed mechanism reconstructs ACK/NACK feedback as a zero-cost trust primitive, and employs Dempster-Shafer evidence theory to fuse multi-source evidence from communication status, environmental disturbance, and residual energy. Explicit uncertainty modeling is further introduced to reduce misjudgment caused by channel fluctuation. At the defense layer, the mechanism differentiates the role of a suspicious node as either a receiver or a sender, and accordingly triggers vector-based forwarding rerouting or spare data channel isolation, forming a closed loop of trust evaluation, role identification, and defense execution. The framework is independent of a specific physical layer, and is instantiated in underwater acoustic sensor networks by combining Bellhop-based acoustic field modeling with α-stable noise.

收稿日期：XXXX–XX–XX；修回日期：XXXX–XX–XX
通信作者：羊秋玲，qlyang@hainanu.edu.cn
基金项目：国家自然科学基金资助项目（No.62362026）；海南省重点资助项目（No.ZDYF2023GXJS158）；海南省院士创新平台专项研究基金（No.YSPTZX202314）
Foundation Items：The National Natural Science Foundation of China (No.62362026), the Key Project of Hainan Province (No. ZDYF2023GXJS158), the specific research fund of The Innovation Platform for Academicians of Hainan Province (No. YSPTZX202314)

Simulation results show that the proposed mechanism outperforms representative baselines in detection accuracy, packet delivery, and throughput. A small-scale lake trial further verifies the feasibility of ACK/NACK-driven trust evaluation in real multipath underwater acoustic channels.

Key words: zero trust, MAC-layer trust assessment, Dempster--Shafer evidence theory, aware cooperative defense, underwater acoustic sensor networks, lightweight security

0 引言

随着物联网、云边端协同计算与下一代无线通信技术的发展，网络末梢正在连接大量类型、协议和能力差异显著的异质感知终端[1]。这些终端承担环境监测[2]、工业控制[3]、交通感知[4]和海洋观测[5]等任务，但普遍面临链路不稳定、带宽稀缺、能量受限和身份基础设施薄弱等问题[6-7]。零信任（Zero-Trust）作为NIST SP 800-207 等标准所定义的“永不信任、持续验证”安全范式[8]，正在成为应对此类开放、动态、可被任意节点接入的网络的主流选择。然而现有零信任体系高度依赖完备的身份基础设施与重型密码学，恰恰是上述资源受限末梢节点最难承载的部分。在身份层难以到位时，行为侧持续验证便成为零信任在末梢落地的唯一可行路径，而MAC层因直接决定信道接入、重传与控制反馈，是行为侧最早、最稳定、最低开销的可观测信号源[9-10]。

更进一步，MAC层的ACK/NACK反馈在任何竞争型或调度型协议中都已被传输，只不过其语义长期被局限为通信成功/失败确认。本文将这一信号**重构为零成本的信任原语（trust primitive）**——每一次ACK/NACK都是一次邻居行为的隐式投票，无需任何额外控制开销即可作为持续行为验证的最小单元。这一观察为资源受限异质感知网络提供了一条不同于身份驱动零信任的反馈驱动零信任路径。为验证该路径的可行性，我们选取约束最为极端的水声传感器网络（Underwater Acoustic Sensor Networks, UASNs）作为实例化对象。

UASNs把上述约束推到了极限。水声链路可用带宽仅为数千赫兹，传播时延可达秒级，信道受多径扩展、时变衰落与非高斯脉冲噪声影响显著，节点能量补给极度困难[11]；网络又常由浮标、潜标、自主水下航行器（Autonomous Underwater Vehicle, AUV）与海床节点协同组成，节点算力、协议栈和物理层各不相同。这种“节点能力+协议栈+物理层”三重异构性使任何依赖统一身份层或重型密码学的方案难以在UASNs中保持一致语义，因此UASNs既是检验反馈驱动零信任的代表性极端场景，也是本文方法的实例化对象。

然而现有研究在MAC层信任化上仍存在两道缺口。其一，MAC协议主要围绕长传播时延、低带宽与信道竞争优化吞吐量、冲突与能效[12-13]，普遍默认节点行为可信；信任评估虽已用于异常节点识别[14]、Dempster-Shafer（D-S）证据理论也适合处理不确定与冲突证据[15]，但绝大多数机制位于网络层或应用层，与MAC层的ACK/NACK反馈、接入控制和信道切换动作没有交汇—这导致面对选择性拒绝服务（Selective denial-of-service, SDoS）、洪泛与开-关攻击时无法形成“检测-缓解”闭环。其二，恶意节点在通信中可同时扮演接收方与发送方两种角色：作为接收方时表现为被动丢弃，需通过路由绕行规避[16-17]；作为发送方时表现为主动占用信道，需通过信道隔离遏制[18]。当前防御方案普遍采用单一动作（仅切路由或仅切信道），与攻击的角色异质性不匹配，因而难以在混合攻击场景下取得最优效果。例如，仅依赖路由绕行可缓解恶意接收方造成的选择性丢包，但无法抑制恶意发送方通过洪泛方式持续占用主数据信道；相反，仅依赖信道隔离也难以恢复由恶意接收方破坏的多跳转发路径。角色推断因此应当与信任检测共同构成MAC层信任控制平面的两根支柱。

针对资源受限异质感知终端中身份基础设施薄弱、持续验证开销高和防御动作难以落地等问题，本文提出一种反馈驱动的 MAC 层信任控制平面，并以水声传感器网络为典型场景进行实例化与验证。主要贡献如下：

1）提出反馈驱动的 MAC 层信任评估机制。将 ACK/NACK 反馈由传统的传输确认信号扩展为零成本信任原语，构建融合通信状态、环境扰动、能量变化和邻居推荐的模糊—D-S 证据融合模型，实现低开销的行为侧持续验证。

2）设计角色感知的协同防御策略。根据可疑节点在通信中的接收方或发送方角色，分别触发路

由绕行或备用信道隔离，形成“信任评估—角色判别—防御执行”的 MAC 层闭环控制机制。

3）完成水声场景下的建模与验证。面向复杂水声信道，结合 Bellhop 声场建模与非稳态噪声构造证据输入，并通过仿真、消融和湖试验证所提机制在检测性能、网络传输性能和实际可行性方面的有效性。

1　相关工作

现有工作大体沿三条路径展开：一是面向长时延、低带宽和共享信道竞争的MAC协议优化，二是面向异常节点识别的行为信任评估，三是面向开放网络的零信任持续验证。三类研究分别改善了通信效率、安全判别和体系化访问控制，但在资源受限异质感知终端中仍缺少可直接落到MAC层的轻量级闭环机制。

1.1　水声与低功耗MAC协议

面向水声及低功耗无线网络的MAC研究长期围绕长传播时延、低带宽和共享信道竞争展开。早期竞争型协议以ALOHA[19]、slotted ALOHA[20]和Slotted FAMA[21]为代表，通过退避、时隙化或RTS/CTS握手降低碰撞；随后MC-UWMAC[22]、GO-MAC[23]和DC-MAC[24]等方法进一步引入多信道、地理信息或博弈建模，以提高吞吐量和信道利用率。无竞争型协议则通过确定性调度减少冲突，如PLSS[25]、DR-DLMA[26]和HN-MAC[27]分别从帧内预测、强化学习时隙分配和非正交多址角度提高资源利用率。已有综述亦指出，水声MAC的核心难点在于传播时延、隐藏终端、能量预算和拓扑动态之间的耦合[28]。然而，上述研究主要服务于接入效率，通常默认节点遵循协议，不区分链路失效与蓄意攻击，因而难以直接处理选择性丢包、洪泛占信道和开-关规避等对抗行为。

1.2　行为信任与证据融合

信任评估研究主要关注在不确定观测下识别异常节点。基于规则的模型利用云理论[29]、隐马尔可夫模型[30]、直接/间接信任融合[31]或争端仲裁机制[32]描述信任演化；数据驱动模型则引入SVM[33]、决策树[34]和LSTM[35]等方法提升复杂攻击场景下的识别能力。Dempster-Shafer证据理论能够显式表达不确定质量并融合冲突证据[15]，适合水声链路中“信道异常”与“恶意行为”并存的场景。现有机制证明了行为信任在恶意节点检测中的价值，但多数运行于网络层或应用层，依赖转发统计、路由历史或集中式特征汇聚，既未充分利用ACK/NACK等MAC层原生反馈，也难以把检测结果立即转化为信道切换、路由绕行等MAC层缓解动作。

1.3　零信任与MAC层安全

零信任体系强调“永不信任、持续验证”，并通过身份、设备状态、行为上下文和策略引擎持续收缩访问面[36-37]。这一思想与异质感知网络的开放接入和动态拓扑高度契合，但标准零信任架构通常假定较完备的身份基础设施、策略控制点和日志采集能力，难以直接部署在算力、能量和带宽均受限的末梢节点上。因此，资源受限场景更需要从已有协议反馈中抽取低成本行为证据。本文在上述三类工作的基础上：将ACK/NACK重构为MAC层信任原语，并把信任融合、角色推断与向量转发（Vector-Based Forwarding, VBF）/备用数据信道（Spare Data Channel, SDC）防御动作统一到同一控制平面中，从而形成可执行的“检测-缓解”闭环。

2　系统模型与设计原则

2.1　应用场景与设计原则

本文面向由资源受限异质感知终端构成的多跳子网。异质性体现在节点能力、协议栈和物理层三个层面：同一网络中可同时存在低端 MCU、能量采集节点、AUV、浮标和海床节点，不同节点在算力、存储、接入协议、调制方式和工作频段上均可能不同。尽管形态各异，这类终端在MAC层面临共同瓶颈：链路质量高度波动，丢包原因难以区分；可用带宽与能量预算有限，额外安全开销必须严格受控；身份基础设施薄弱，难以依赖重型认证和密钥管理。基于此，本文框架遵循轻量化、自适应、容错和可移植四项原则，即单帧信任更新保持常数级开销，控制语义控制在比特级；信任值变化可直接触发路由或信道调整；冲突证据下保留不确定性而非强制二元判决；证据源、信道模型和防御动作均以接口形式与具体场景解耦。

2.2　威胁模型

本文考虑协议知情但能力受限的内部攻击者。攻击者可控制不超过$\rho_{\max}$比例的节点（实验中最高取0.4），掌握合法MAC协议格式并发送符合规范

的数据帧或控制帧，但不能破解物理层加密、伪造时间戳或发起女巫攻击。其目标是降低投递率、消耗带宽和能量，并尽可能规避行为检测。围绕MAC层最具代表性的对抗行为，本文重点评估三类攻击：恶意接收方以概率p_{drop}选择性丢弃数据包，恶意发送方以高于正常速率的流量注入伪造帧（Flooding），以及攻击者在正常与异常状态之间周期切换（On-off）。

2.3　信任表示与冲突处理

水声链路中，ACK 超时既可能源于恶意丢弃，也可能来自多径衰落、突发噪声或隐藏终端竞争。为避免把不完整观测过早压缩为二元判决，本文采用Dempster-Shafer（D-S）证据理论表示信任状态。设假设空间为$\Theta=\{T,\neg T\}$，分别表示可信与不可信；基本概率赋值m将观测支持分配到$\{T\}$、$\{\neg T\}$和$\{T,\neg T\}$三类焦元。其中$m(\{T,\neg T\})$表示不确定质量，用于承载ACK缺失、环境扰动或证据冲突带来的模糊性。

当存在多个证据源时，Dempster组合规则将它们聚合为：

$$m(C)=\frac{1}{1-K}\sum_{A\cap B=C}m_1(A)m_2(B) \tag{1}$$

其中K为冲突系数。当K接近1时，Dempster规则会放大冲突证据；本文采用阈值截断策略，当融合冲突超过$K_{\max}$时保留上一窗口信任值，避免高冲突时信任值震荡。

需要指出的是，水声信道的大传播时延和多径扩展可能导致 ACK/NACK 反馈延迟或短时缺失。为避免单帧反馈异常引起信任值振荡，本文并不直接基于单次 ACK 超时进行二元判决，而是在观测窗口内统计 ACK/NACK 行为，并结合环境、能量和推荐证据进行 D-S 融合。当通信证据与环境证据存在较大冲突时，异常观测优先转化为不确定质量；若冲突系数超过阈值，则保留上一窗口信任值，从而抑制由时延波动和信道异常引起的频繁判决切换。同时，当连续窗口内不确定性较高或信任值波动较大时，系统自适应延长观测窗口，以获得更稳定的行为判断。

2.4　水声信道实例化

水声信道具有强多径、强时变和非高斯噪声特性，简单几何损耗模型难以反映近岸浅海传播。本文采用Bellhop射线追踪模型[38]为节点对生成信道冲激响应（Channel Impulse Response, CIR），并用对称α-稳态分布刻画船舶、生物和环境扰动引起的脉冲噪声。给定海域几何、声速剖面、海面/海底反射参数及节点位置后，Bellhop输出P条到达路径的复振幅a_p与时延τ_p，节点n_i到n_j的CIR写为

$$h_{ij}(t)=\sum_{p=1}^{P}a_p(t)\delta(t-\tau_p(t)) \tag{2}$$

接收端据此合成期望信号、并发干扰与噪声，进一步得到有效 SINR：

$$\mathrm{SINR}_{ij}=10\log_{10}\frac{P_s\sum_p|a_p^{(ij)}|^2}{\sum_{k\in\mathcal{I}}P_k\sum_p|a_p^{(kj)}|^2+\sigma_n^2B_w} \tag{3}$$

其中$\mathcal{I}$为并发干扰集合，σ_n^2为截断意义下的噪声有效功率，B_w为接收带宽。若有效SINR低于解调门限，该帧计为失败；局部噪声尺度和干扰能量同时进入后续环境证据建模。

3　MAC层信任控制框架

MAC层信任控制框架由三部分构成：ACK/NACK驱动的信任更新、基于角色的防御动作选择，以及面向水声信道的证据映射。

3.1　总体结构

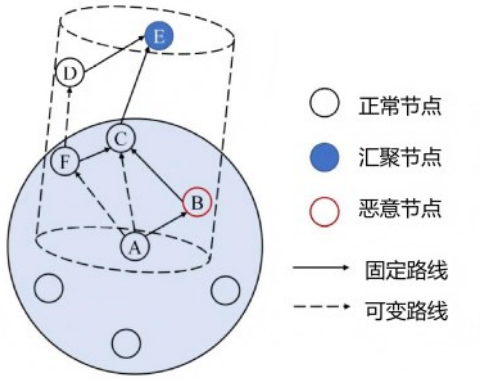

图1　固定路径路由示意及当节点B表现为恶意行为时的脆弱性示意图

通信最初遵循最短路径的固定路由策略。图1给出了角色攻击的基本动机：路径A→B→C→E中若节点B是恶意节点，它既可作为接收方破坏上游投递，也可作为发送方干扰下游接入；因此防御动作必须区分节点在通信中的角色，而不能只给出单一惩罚策略。

框架在每个节点维护邻居信任表。每一帧通信完成后，节点根据ACK/NACK反馈及环境、能量、

推荐等证据更新相邻节点的基本概率赋值（Basic Probability Assignment, BPA）；当信任值低于阈值时，控制平面根据可疑节点在最近窗口内的发送/接收角色选择VBF或SDC。该流程只要求三类接口：证据源可归一化到[0, 1]，每帧可获得ACK/NACK反馈，帧结构可承载少量控制语义。因此，除水声网络外，其他感知网络也可通过替换证据源实现迁移。

3.1.1　模糊信任表示

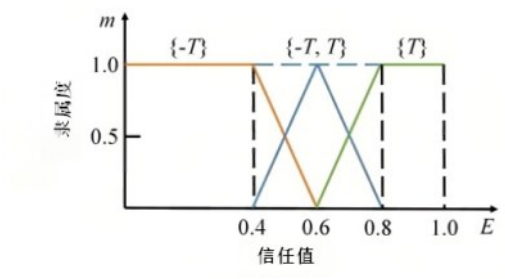

图2　描述节点信任等级模糊子集的隶属函数示意图

模糊集合用于把连续证据值映射为可信、不可信和不确定三类质量。如图2所示，归一化输入x经隶属函数得到$\mu_T(x)$、$\mu_D(x)$和$\mu_U(x)$，并进一步形成BPA：

$$m_{sub}(\{T\}) = \mu_T(x),$$

$$m_{sub}(\{\neg T\}) = \mu_D(x), \tag{4}$$

$$m_{sub}(\{T,\neg T\}) = \mu_U(x).$$

由此，链路波动或证据不足不会被直接归入可信/不可信，而是进入不确定质量。

3.1.2　D-S多源融合

如图3所示，本文将本地环境/能量证据形成的主观信任m_S、ACK/NACK与频率统计形成的证据信任m_{EV}、邻居广播形成的推荐信任m_R进行迭代融合：

$$m_{12} = m_S \oplus m_{EV}, m_{123} = m_{12} \oplus m_R \tag{5}$$

按上式迭代展开后，即可得到节点n_j在三源焦元$A,B,C \subseteq \Theta$下的最终融合信任度；三源迭代后的总冲突系数记为K_{123}。当$K_{123} \geqslant K_{\max}$时，按§2.3的截断策略保留旧信任值不更新。

3.1.3　决策制定

最终决策比较$m(\{T\})$与$m(\{\neg T\})$。若可信质量占优，则继续观察；否则判定节点可疑并触发防御。

不确定质量用于调节观测窗口：当连续窗口内不确定性过高或可信质量波动过大时，窗口由T_w延长至$2T_w$，

以覆盖开-关攻击的完整周期，避免短时正常行为掩盖长期恶意模式。

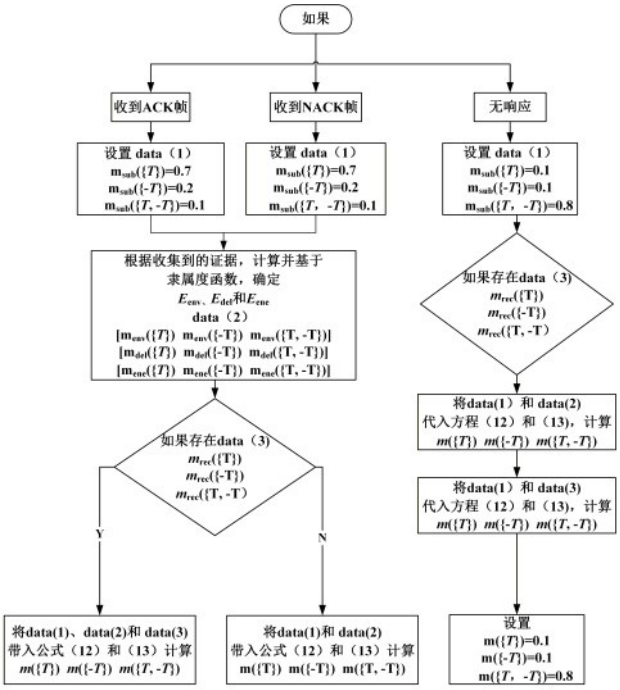

图3　利用ACK/NACK反馈和推荐证据进行多源信任融合的过程

3.2　角色感知协同防御

一旦节点被判定可疑，防御动作由其通信角色决

定。若可疑节点主要作为下一跳接收方出现，威胁通常表现为选择性丢包，应通过VBF绕行；若可疑节点主要作为发送方出现，威胁通常表现为洪泛或冲突制造，应通过SDC隔离。表1给出两类动作的触发特征与回退条件。

3.2.1　针对恶意接收者的路由切换机制

当下一跳节点表现为恶意接收方时，发送节点将数据帧中的VBF标志置1，使下一跳地址字段暂时失效，并通过推荐字段广播检测事件。路径附近节点据此反馈本地信任信息，发送方选择信任得分最高的候选节点作为替代下一跳；路由恢复稳定

后，VBF 标志清零并回到固定路由。图 4 展示绕行路径如何避开恶意接收方。

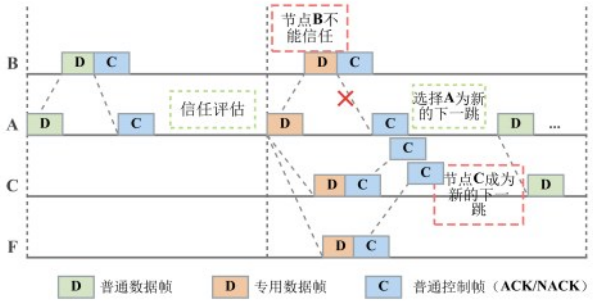

图 4　基于信任的 VBF 路由切换示例，用于绕过低信任接收节点

3.2.2　针对恶意发送节点的多信道隔离机制

对恶意发送方，仅丢弃其数据帧不足以阻止其占用信道。框架将频谱划分为控制信道、常规数据信道和备用数据信道 SDC，并在控制帧中嵌入 SDC 标志。

标志激活后，可疑发送方被限制到备用信道，合法节点继续在常规数据信道传输，从而降低洪泛对主数据通道的影响。图 5 展示隔离前后的通信关系。

3.3　水声场景证据建模

为保证信任评估的可靠性，本节给出水声场景下的多类证据来源。本文采用三类反映外部条件与节点行为的证据：环境证据、通信证据与剩余能量证据。

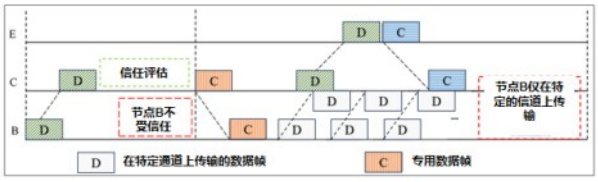

图 5　通过备用数据信道隔离恶意发送节点的结构示意

a) **环境证据** 水声信道条件极不稳定，噪声与干扰水平随时间与空间变化显著。为降低误检率，本文引入环境证据，以区分由环境噪声变化引起的非恶意异常。节点 n_i 与节点 n_j 之间的证据定义为：

$$E_{env}(i \to j) = \frac{1}{1 + \alpha |N(i) - N(j)|} \tag{6}$$

其中 α 是缩放参数，i 和 j 分别为发送节点和接收节点的索引；$N(i)$ 与 $N(j)$ 分别表示节点 n_i 与 n_j 周围的局部噪声功率密度，由局部噪声尺度与并发干扰能量共同估计得到。

b) **通信证据** 通信行为为节点的可靠性提供直接指标。本文考虑两个方面：

交付率证据，代表传输可靠性（采用 Beta(1,1) 先验下的拉普拉斯平滑以处理小样本）：

$$E_{del}(i \to j) = \frac{v_1 + 1}{v_1 + v_2 + 2} \tag{7}$$

其中 v_1 表示观测窗口内节点 n_i 到节点 n_j 的成功帧数量，包括收到确认帧或确认已送达的数据包，v_2 表示观测窗口内节点 n_i 到节点 n_j 的失败帧或未被确认帧数量。

频率证据，反映异常活动水平（用于识别洪泛模式）：

$$\begin{aligned} E_{fre}(i \to j) &= 1 - \left| \frac{F(j) - \bar{F}}{\bar{F}} \right| \\ \bar{F} &= \frac{1}{K} \sum_{m=1}^{K} F(m), \quad F(m) = \frac{n_{send}^{(m)}}{T_{record}} \end{aligned} \tag{8}$$

其中 $\bar{F}$ 表示节点 n_i 的 K 个邻居节点的平均通信频率，$n_{send}^{(m)}$ 是邻居 m 在观测窗口 T_{record} 内发送的帧数。当 $\bar{F} \to 0$ 时（如低负载场景），公式退化处理为 $E_{fre} = 1$，避免数值不稳定。

c）剩余能量证据 水声节点能量补给极为困难，能量显著下降的节点更易出现数据包丢失或间歇性离网，其行为可能被误判为恶意操作。为避免此类误判：

$$E_{ene}(i \to j) = 1 - \frac{|En(i) - En(j)|}{En(i) + En(j)} \tag{9}$$

其中 $En(i)$ 与 $En(j)$ 分别表示节点 n_i 与 n_j 的剩余能量。该指标确保低能量影响能够与有意的恶意行为有效区分开来。

d）推荐证据 为支撑§3.1 D-S 融合中第三个

表 1　　**接收方与发送方恶意角色的触发特征、缓解动作与回退条件**

恶意节点角色	攻击类型	检测特征	防御动作	回退条件	控制开销
接收节点	SDoS（被动）	投递率证据骤降	VBF 路由切换	信任恢复至 $m(\{T\})>0.6$	1bit/帧
发送节点	洪泛（主动）	频率证据+通信证据	SDC 信道隔离	5 个观测窗口正常	1bit/帧

BPA 输入m_R，本文引入推荐证据E_{rec}：节点n_i通过周期性广播向邻居发布其对共同邻居n_j的本地信任值$\tau_{k\to j}\in[0,1]$，由邻居$n_k\in\mathcal{N}(i)\cap\mathcal{N}(j)$收集后取加权平均：

$$E_{rec}(i\to j)=\frac{\sum_{k\in\mathcal{N}(i)\cap\mathcal{N}(j)} w_k\tau_{k\to j}}{\sum_{k\in\mathcal{N}(i)\cap\mathcal{N}(j)} w_k} \tag{10}$$

其中权重$w_k=\tau_{i\to k}$由本节点对推荐者n_k的现有信任值给出，从而抑制恶意推荐者影响（共谋抑制）。当$\mathcal{N}(i)\cap\mathcal{N}(j)=\varnothing$时退化为$E_{rec}=0.5$（不确定先验）。$E_{rec}$与前三类证据共同经§3.1.1 模糊隶属映射后参与D-S融合：环境与能量证据合并入主观分支m_S，通信证据合并入证据分支m_{EV}，推荐证据单独构成m_R。

上述四类证据经§3.1.1 的模糊隶属映射后，按§3.1 的 D-S 规则融合为最终信任值。

3.4　复杂度与开销分析

框架的主要计算开销来自 BPA 构造和 D-S 融合。设每条链路使用q类证据源、节点平均邻居数为K，则单帧BPA构造复杂度为$O(q)$，D-S融合在二元假设空间内为常数级，角色判断与动作选择同样为$O(1)$；仅在VBF路由重选时需要遍历邻居信任表，复杂度为$O(K)$。空间上，每个节点维护$O(K)$规模的邻居信任表，每条记录保存可信、不可信、不确定质量和时间戳，约为十余字节。通信上，VBF 与 SDC 仅需在数据帧或控制帧中增加比特级标志位。

4　实验结果与分析

本节从仿真与湖试两方面验证所提框架。仿真用于评估检测性能、网络收益和机制贡献；湖试用于检验 ACK/NACK 驱动信任评估在真实多径水声信道下的可行性。

4.1　实验环境设置

仿真在 1000m × 800 m × 600 m 三维水声区域中进行，部署 11 个发射节点和 6 个观测/汇聚节点；其中一定比例节点执行 SDoS、Flooding 或 On-off 攻击，另随机选取 2 个节点作为低端能力受限终端，以检验异构条件下的可部署性。底层 MAC 采用 ALOHA，数据帧和 ACK 帧大小分别为 185 字节和 5 字节；发射流量服从 Poisson 过程，归一化业务负载G在$[0.05,0.5]$内扫描，基准值为 0.2。物理层采用扩频通信，载波频率 10 kHz、带宽 400 Hz、采样率 50 kHz；CIR 由 Bellhop 生成，背景噪声采用对称α-稳态分布（实验中$\alpha=1.8$）。每组配置重复不少于 30 次，报告均值及 95% 置信区间。

为保证对比的可解释性，本文选取 GHL-SAR、SEECR 和 GEDAR 作为代表性基线。其中，GHL-SAR 为基于学习的安全自适应路由方法，SEECR 为安全能效协作路由方法，GEDAR 为地理机会路由与深度调整方法。

上述基线主要工作在网络层或路由层，未显式构建基于 ACK/NACK 的 MAC 层信任闭环，也未区分恶意节点的接收方/发送方角色。因此，本文将其用于评估所提 MAC 层信任评估与角色感知协同防御机制的增益。为保证公平性，所有基线与本文方法共享相同拓扑、信道实例、MAC 协议、帧大小、恶意比例、随机种子和重复次数，差异主要体现在路由/安全决策机制及是否引入 MAC 层信任评估与角色感知防御。

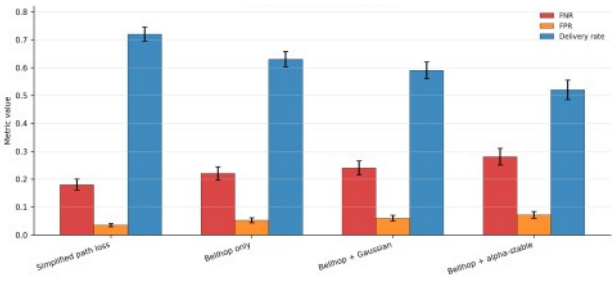

图6　不同信道与噪声建模假设下的FNR、FPR与投递率对比

4.2　信道建模有效性

信道模型决定 ACK/NACK 观测的可靠性，也直接影响信任评估结论。图 6 比较了简化路径损耗、Bellhop only、Bellhop+Gaussian 与 Bellhop+α-stable 四种设置。简化模型得到的 FNR/FPR 和投递率分别为 0.18/0.035 和 0.72，明显偏乐观；加入 Bellhop 多径后，时延扩展和路径衰落增加检测不确定性；进一步加入α-稳态噪声后，FNR/FPR 上升至 0.28/0.072，投递率降至 0.52。该结果表明，若忽略多径和脉冲噪声，将低估水声环境下信任评估的难度。因此后续实验均采用 Bellhop+α-stable 作为默认信道实例。

4.3　检测准确率

本组实验考察不同恶意节点比例和业务负载下的检测稳定性。恶意节点比例取约 9%、18% 和

27%，以FNR和FPR衡量漏检与误检。

图7显示，在负载升高和恶意节点比例增加时，FNR总体保持在0.4以下，FPR维持在约0.05的低水平。低负载高恶意比例下FNR略有上升，原因在于可用ACK/NACK样本较少；随着观测样本增加，多源证据融合能够抑制单一ACK失败带来的误判。该结果说明，保留不确定性质量和跨证据融合有助于稳定检测，具体贡献在§4.5中进一步拆解。

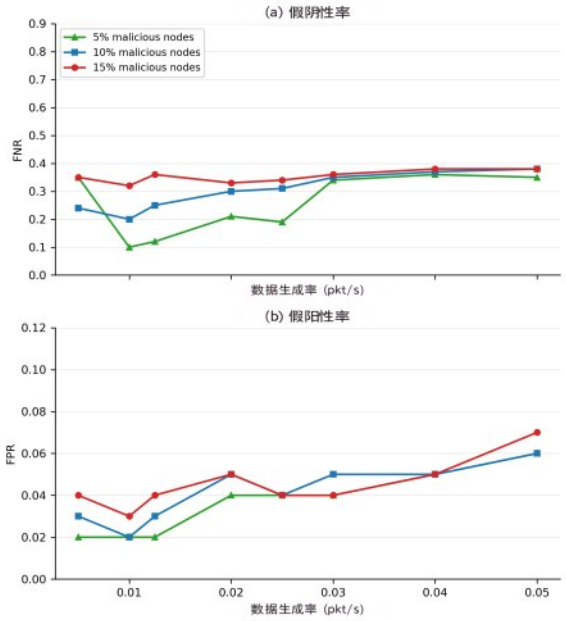

图7　不同恶意节点比例与业务负载下的检测性能：(a)漏检率FNR；(b)误检率FPR

4.4　网络性能

本节比较投递率和能耗。第一组实验固定11个发射节点并扫描G，第二组固定G=0.2并改变节点密度，恶意节点比例约为18%。

图8表明，随着负载或节点密度增加，所有方法的投递率均因ALOHA冲突和水声多径干扰而下降；但本文方法在恶意场景下始终高于GEDAR、GHL-SAR和SEECR。需要指出，无恶意场景的投递率并不接近100%，其主要原因是水声多径深衰落、脉冲噪声、隐藏终端与ACK时延竞争共同构成了物理和协议基线损失，而非安全机制开销。

图9显示，本文方法在负载增加时能够维持更高吞吐量，在节点密度提高时也比基线具有更平缓的退化趋势。其原因在于VBF绕行减少了恶意接收方造成的路径中断，SDC隔离降低了恶意发送方对主数据信道的占用。

4.5　消融实验与开销分析

1） 信任侧消融

图10合并展示模型层面与证据层面的消融结果。模型层面对比ACK-only、Weighted-sum、去除不确定性质量的D-S、去除推荐证据的D-S与完整D-S；证据层面采用“留一”方式剔除环境、通信、能量、推荐四类证据。

ACK-only在多径衰落、脉冲噪声和临时干扰下易把信道异常误判为恶意，FNR/FPR分别为0.31/0.105；Weighted-sum与去不确定性D-S虽利用更多证据源，但前者缺乏冲突建模，后者过早硬判决。完整D-S模型将FNR/FPR降至0.14/0.042，F1提升至0.91。证据留一结果进一步表明，通信证据对降低漏检贡献最大，推荐证据主要抑制误报和共谋推荐，环境与能量证据则改善误判恢复时间。

2） 防御侧消融与开销

图11给出No-defense、Detection-only、+VBF、

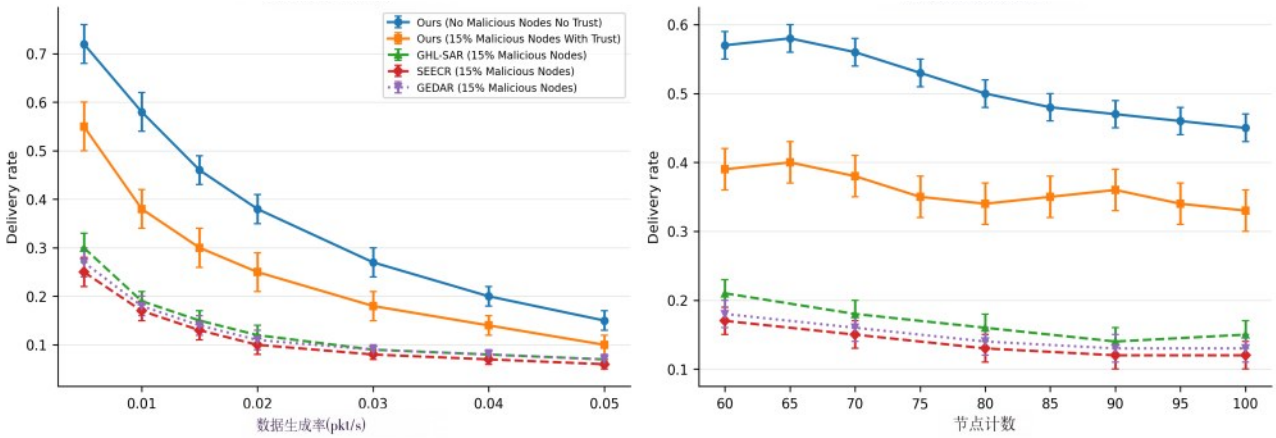

图8　数据帧投递率对比：(a)随业务负载G变化；(b)随节点密度变化

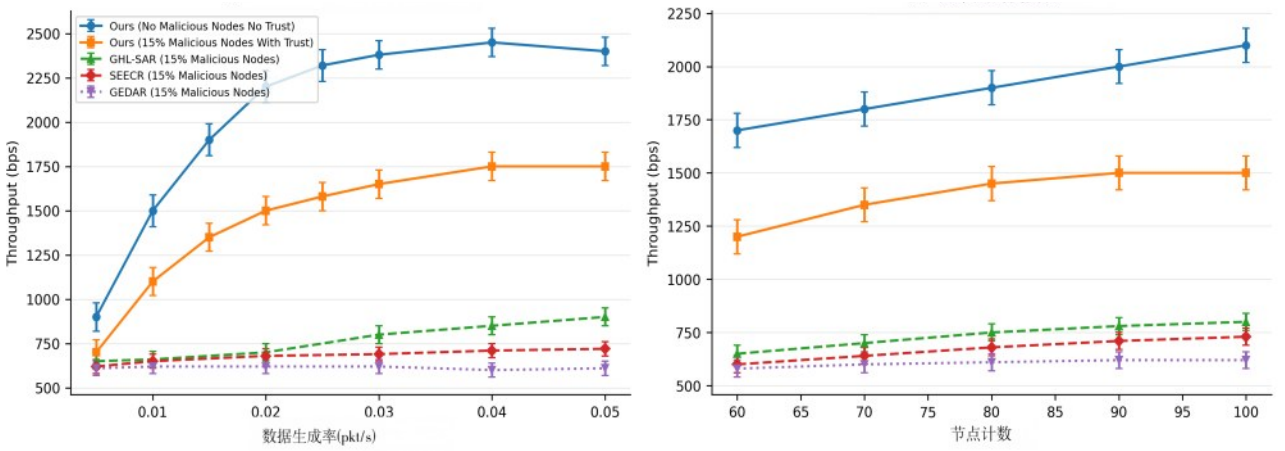

图 9　网络吞吐量对比：(a)随归一化负载 G 变化；(b)随节点密度变化

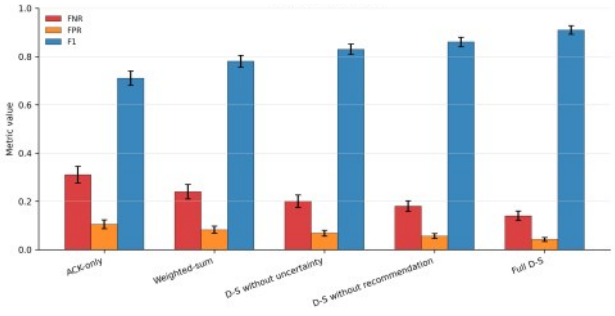

图 10　信任侧消融结果：ACK-only、Weighted-sum、无不确定性 D-S、无推荐 D-S 与完整 D-S 在 FNR、FPR 和 F1 上的对比

+SDC 和+VBF&SDC 五组对比，并进一步分解每成功包能耗。

无防御时，混合攻击使投递率降至 0.34、吞吐量降至 720bps、每成功包能耗升至 10.8J；仅检测无法绕过恶意接收方或抑制恶意发送方占信道。单独启用 VBF 或 SDC 只能缓解对应角色攻击；二者联合后，投递率升至 0.68、吞吐量升至 1510bps、每成功包能耗降至 4.9J。能耗分解表明，联合防御主要通过减少重传节省能量，VBF/SDC 切换带来的额外开销远小于其节省的失败传输能耗。实测开销也保持在轻量级：单次信任更新时间约 0.18ms，每邻居表项约 16bytes，控制语义不超过 2bit/帧。

此外，实验表明推荐证据采用信任加权后，在坏推荐者比例升高时 FPR 和 FNR 的增长均显著低于等权推荐；角色推断在 SDoS-only、Flooding-only 和混合攻击下保持较高对角占比，说明 VBF/SDC 的动作选择具有可靠基础；T_0 与 $K_{\max}$ 的二维扫描显示(0.55, 0.90)附近取得较优检测—投递折中；简单自适应攻击者通过下调 p_{drop} 虽能延缓检测，但攻击强度也随之下降；节点移动速度升至 2m/s 时性能缓慢退化，在典型 AUV 速度范围内仍保持可接受水平。

4.6　湖试验证

为进一步验证所提框架在真实场景下的可行性，本文于 2025 年 1 月在校内湖开展了湖试。部署了三个通信节点，每节点都标定了坐标。整个系统架构包括一个锚节点和两个使用水声信道进行通信的附加节点。该设置在硬件最少的条件下，对真实环境下的信任评估框架进行了原型验证。受硬件规模限制，湖试不引入物理层恶意节点，而在软件层模拟 SDoS 行为：在两个附加节点中随机指定一个为“软件恶意节点”，对到达的上行数据帧以 p_{drop}=0.5 的概率主动丢弃且不返回 ACK，其余行为与正常节点一致；信任评估模块据此累积失败帧观测，用于检验 ACK/NACK 驱动的 D-S 融合在真实多径 CIR 下能否捕捉到该模拟攻击。

实验所使用的设备为自主研发的水声调制解调器，工作频段 21-27kHz，标称带宽 2-3kHz。仿真侧重大规模可扩展性与基线对照，湖试侧重 ACK/NACK 反馈在真实多径 CIR 下的可用性，因此本文不做跨设置的绝对值横向对比。调制解调器配备线性调频同步起始码和 OFDM 探测信号块；消息信号采用 QPSK 调制和低密度奇偶校验信道编码以提高可靠性。所收集的数据，包括信道脉冲响应 CIR 和 ACK/NACK 反馈信息，被用于评估所提出的信任评估框架。

收集到的 ACK/NACK 记录被映射为证据值，并使用所提的 D-S 融合机制处理。图 12 展示了 ACK 成功率与所得信任值之间的相关关系。可以观察到，信任评估框架能够适应信道质量和节点行

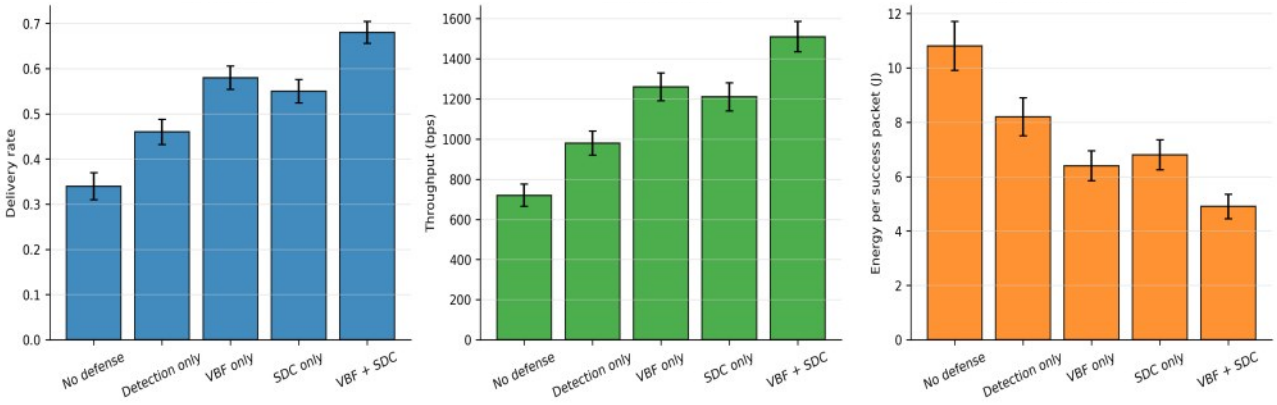

图 11　防御侧消融与能耗分解：No-defense、Detection-only、+VBF、+SDC 与+VBF\&SDC 五组下的投递率、吞吐量和每成功包能耗

为的变化：对协作节点保持较高信任度，对不可靠或模拟恶意的节点降低信任值。这些结果验证了基于 ACK/NACK 的证据融合方案在实际水下环境下的有效性。

为进一步把湖试结果从“静态散点”升级为“时间因果序列”，本节将同一段湖试日志按时间窗口对齐 ACK 成功率、融合后信任值与 CIR 主径能量三条曲线（图 13）。

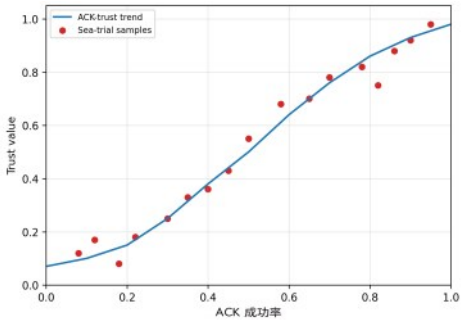

图 12　湖试 ACK 成功率与融合信任值的相关关系，用于验证 ACK/NACK 反馈可作为 MAC 层信任原语

可观察到：(i)在 $t \in [120,300]$s 的“软件恶意”窗口内，CIR 主径能量本身仅有约 6dB 的自然下降，但 ACK 成功率与信任值同步下降至 ~0.46 与 ~0.28，幅度显著超出 CIR 衰落能解释的范围，这说明信任值的下降并非由信道恶化所致，而由模拟攻击行为导致；(ii)信任值的下降相对 ACK 成功率呈现轻微时间提前（约 10-20s），反映 D-S 融合借助环境与能量证据形成先兆，先于 ACK 显式失败便已开始降低对该节点的信任度。该早期预警的特性验证了不确定性质量在真实信道下的工程价值。

受硬件条件与部署规模限制，多跳路由切换、多信道隔离、多节点协同检测等机制仍需在更大规模海试中进一步验证。

5　结论

本文面向资源受限异质感知终端提出一种 MAC 层信任评估与协同防御机制。该机制将 ACK/NACK 反馈重构为零成本信任原语，通过模糊—D-S 融合综合通信、环境、能量和推荐证据，并利用不确定性质量缓解信道异常与恶意行为的混淆；在防御层，根据可疑节点的接收/发送角色分别触发 VBF 路由绕行或 SDC 信道隔离，从而把信任判断转化为 MAC 层可执行动作。

仿真结果表明，完整 D-S 融合模型能够降低漏检率和误检率，并提升综合识别性能；在混合攻击场景下，VBF 与 SDC 协同防御可提高数据投递率和吞吐量，同时降低单位成功投递能耗。信道敏感性实验表明，简化路径损耗模型会低估复杂水声信道下的检测难度。小规模湖试进一步验证了 ACK/NACK 驱动信任评估在真实多径水声信道中的可行性。上述结果说明，该反馈驱动的 MAC 层信任控制平面能够以低开销方式支撑可执行的协同防御。

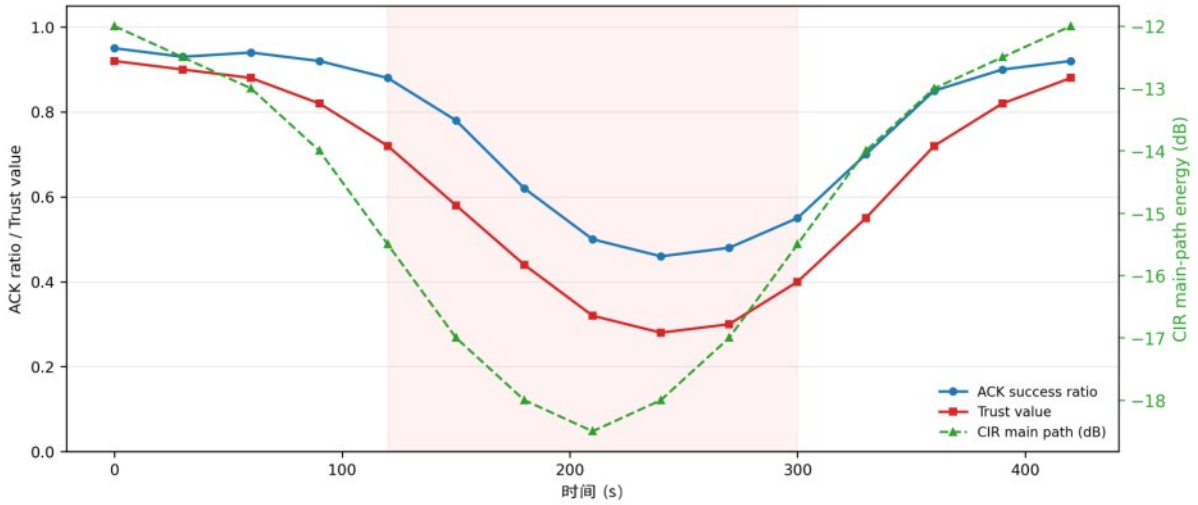

图 13　湖试日志时间序列对齐结果:粉色阴影为软件模拟SDoS窗口;ACK成功率、融合信任值与CIR主径能量同步呈现,用于区分信道波动与模拟攻击行为

参 考 文 献:

[1] 袁子淇, 孙庆赟, 周号益, 朱祖坤, 李建欣. MNDetector:基于多层网络的异常访问检测方法[J]. 计算机研究与发展, 2025, 62(3): 765-778.
Yuan Ziqi, Sun Qingyun, Zhou Haoyi, Zhu Zukun, Li Jianxin. MNDetector: Anomaly Access Detection Method Based on MultiplexNetwork [J]. Journal of Computer Research and Development, 2025, 62(3): 765-778.

[2] Fan Rong, Jin Zhigang, Su Yishan. A novel pas sive localization scheme of underwater non-cooperative targets based on weak-control auvs. IEEE Transactions on Wireless Communications, 2024, 23(8): 9129 – 9143.

[3] Jiang Shengming. On securing underwater acoustic networks: A survey. IEEE Communications Surveys & Tutorials, 2018, 21(1):729 – 752.

[4] Wei Xiaohui, Guo Hao, Wang Xingwang, et al. Reliable data collection techniques in underwater wireless sensor networks: A survey. IEEE Communications Surveys & Tutorials, 2021, 24(1):404 – 431.

[5] 黄沛烁,王易因,关新平,等.面向水声传感网的自主水下航行器辅助定位动态路径规划[J].电子与信息学报,2022,44(06):1927-1936.
Huang Peishuo, Wang Yixin, Guan Xinping, et al. Autonomous Underwater Vehicle-Assisted Dynamic Path Planning for Autonomous Underwater Sensor Networks [J]. Journal of Electronics & Information Technology, 2022, 44(06): 1927-1936.

[6] Song Yujae. Underwater acoustic sensor networks with cost efficiency for internet of underwater things. IEEE Transactions on Industrial Electronics, 2020, 68(2):1707 – 1716.

[7] 金志刚,梁嘉伟,羊秋玲.融合深度调整和自适应转发的水声网络机会路由[J].电子与信息学报,2024,46(01):49-57.
Jin Zhigang, Liang Jiawei, Yang Qiuling. Opportunistic Routing in-Underwater Acoustic Networks Based on Deep Adjustment and Adaptive Forwarding [J]. Journal of Electronics and Information Technology, 2024, 46(01): 49-57

[8] 肖警续,郭渊博,常朝稳等.基于SDN的物联网边缘节点间数据流零信任管理[J].通信学报,2024,45(07):101-116. DOI：10.11959/j.issn.1000-436x.2024060.
XIAO Jingxu,GUO Yuanbo,CHANG Chaowen,et al.Zero trust management of data flow between IoT edge nodes based on SDN[J].Journal on Communications,2024,45(07):101-116.

[9] Dong Wei, Yang Qiuling, Chen Yanxia, et al. RHNE-MAC: Random handshake MAC protocol based on Nash equilibrium for underwater wireless sensor networks[J]. IEEE Sensors Journal, 2021, 21(18): 21090-21098.

[10] Wang Shidu, Zhao Danfeng. A power control based handshake-competition MAC protocol for underwater acoustic networks[C]//2020 IEEE International Conference on Artificial Intelligence and Information Systems (ICAIIS). IEEE, 2020: 665-669.

[11] 羊秋玲,唐智超,朱荣鑫等.水下无线传感器网络节点定位方案综述[J].通信学报,2025,46(08):225-240. DOI：10.11959/j.issn.1000-436x.2025141.
YANG Qiuling,TANG Zhichao,ZHU Rongxin,et al.Survey of node localization scheme in underwater wireless sensor network[J].Journal on Communications, 2025, 46(08): 225-240. DOI： 10.11959/j. issn. 1000-436x.2025141.

[12] Liu Meiyan, Zhuo Xiaoxiao, Yuan Yufan, et al. Adaptive scheduling MAC protocol in underwater acoustic broadcast communications for AUV formation[J]. IEEE Internet of Things Journal, 2022, 10(8): 6887-6901.

[13] Roy A, Sarma N. A synchronous duty-cycled reservation based MAC protocol for underwater wireless sensor networks[J]. Digital Communications and Networks, 2021, 7(3): 385-398.

[14] 秦丹阳,贾爽,杨松祥,等.基于信任感知的无线传感器网络安全路由机制研究[J].通信学报,2017,38(10):60-70.
Qin Danyang, Jia Shuang, Yang Songxiang, et al. Research on Security Routing Mechanism for Wireless Sensor Networks Based onTrust Perception [J]. Journal of Communications, 2017, 38(10): 60-70.

[15] Zhao Kaiyi, Li Li, Chen Zeqiu, et al. A survey: Optimization and applications of evidence fusion algorithm based on Dempster – Shafer theory[J]. Applied Soft Computing, 2022, 124: 109075.

[16] Huan Xintao, Kim Kyeong Soo, Zhang Junqing. NISA: Node identification and spoofing attack detection based on clock features and radio information for wireless sensor networks[J]. IEEE Transactions on

Communications, 2021, 69(7): 4691-4703.

[17] Li Yue, Liu Yingjian, Yin,Haoyu, et al. Trident: Defensing synergetic denial-of-service attacks in underwater named data networking[J]. IEEE Internet of Things Journal, 2023, 10(23): 20633-20648.

[18] Saeed K, Khalil W, Ahmed S, et al. SEECR: Secure energy efficient and cooperative routing protocol for underwater wireless sensor networks[J]. IEEE Access, 2020, 8: 107419-107433.

[19] Koseoglu M, Karasan E, Chen Lin. Cross-layer energy minimization for underwater ALOHA networks[J]. IEEE Systems Journal, 2015, 11 (2): 551-561.

[20] Syed A A, Ye Wei, Heidemann J, et al. Understanding spatio-temporal uncertainty in medium access with ALOHA protocols[C]//Proceedings of the 2nd Workshop on Underwater Networks. 2007: 41-48.

[21] Molins M, Stojanovic M. Slotted FAMA: a MAC protocol for underwater acoustic networks[C]//OCEANS 2006-Asia Pacific. IEEE, 2006: 1-7.

[22] Multi-Channel M. Collision avoidance energy efficient Multi-Channel MAC protocol for UnderWater acoustic sensor networks[J]. IEEE Trans. Mobile Comput, 2019, 1(8): 10.

[23] Guo Jiani, Song Shanshan, Liu Jun, et al. An efficient geo-routing-aware MAC protocol based on OFDM for underwater acoustic networks[J]. IEEE Internet of Things Journal, 2023, 10(11): 9809-9822.

[24] Zhu Rongxin, Liu Li, Li Pengcheng, et al. DC-MAC: A delay-aware and collision-free MAC protocol based on game theory for underwater wireless sensor networks[J]. IEEE Sensors Journal, 2024, 24(5): 6930-6941.

[25] Liu Meiyan, Zhuo Xiaoxiao, Wei Yan, et al. Packet-level slot scheduling MAC protocol in underwater acoustic sensor networks[J]. IEEE Internet of Things Journal, 2021, 8(11): 8990-9004.

[26] Ye Xiaowen and Fu Liqun. Deep reinforcement learning based MAC protocol for underwater acoustic networks[C]//Proceedings of the 14th International Conference on Underwater Networks & Systems. 2019: 1-5.

[27] Guo Jiani, Song Shanshan, Liu Jun, et al. A hybrid NOMA-based MAC protocol for underwater acoustic networks[J]. IEEE/ACM Transactions on Networking, 2023, 32(2): 1187-1200.

[28] Qiu Tianyou, Li Yiping, and Feng Xisheng . Distributed channel sensing MAC protocol for multi-UUV underwater acoustic network[J]. IEEE Internet of Things Journal, 2024, 11(9): 16119-16133.

[29] Jiang Jinfang, Han Guangjie, Shu Lei , et al. A trust model based on cloud theory in underwater acoustic sensor networks[J]. IEEE Transactions on Industrial Informatics, 2015, 13(1): 342-350.

[30] Signori A, Campagnaro F, Nissen I, et al. Channel-based trust model for security in underwater acoustic networks[J]. IEEE Internet of Things Journal, 2022, 9(20): 20479-20491.

[31] Zhu Rongxin, Boukerche Azzedine, Huang Xiangdang, et al. DESLR: Energy-efficient and secure layered routing based on channel-aware trust model for UASNs[J]. Computer Networks, 2023, 234: 109939.

[32] Jiang Jinfang, Hua Shanshan, Han Guangjie, et al. Controversy-adjudication-based trust management mechanism in the internet of underwater things[J]. IEEE Internet of Things Journal, 2022, 10(3): 2603-2614.

[33] Han Guangjie, He Yu, Jiang Jinfang, et al. A synergetic trust model based on SVM in underwater acoustic sensor networks[J]. IEEE transactions on vehicular technology, 2019, 68(11): 11239-11247.

[34] Jiang Jinfang, Zhu Xinyu, Han Guangjie, et al. A dynamic trust evaluation and update mechanism based on C4.5 decision tree in underwater wireless sensor networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(8): 9031-9040.

[35] Du Jiaxin, Han Guangjie, Lin Chuan, et al. LTrust: An adaptive trust model based on LSTM for underwater acoustic sensor networks[J]. IEEE Transactions on Wireless Communications, 2022, 21(9): 7314-7328.

[36] Mehreen Tahir, Tanjila Mawla, Feras Awaysheh, Sadi Alawadi, Maanak Gupta, and Muhammad Intizar Ali. Securefedprom: A zero-trust federated learning approach with multi-criteria client selection. IEEE Journal on Selected Areas in Communications, 2025, 43(6): 2025-2041.

[37] Kai Li, Conggai Li, Xin Yuan, Shenghong Li, Sai Zou, Syed So-hail Ahmed, Wei Ni, Dusit Niyato, Abbas Jamalipour, Falko Dressler, et al. Zero-trust foundation models: A new paradigm for secure and collaborative artificial intelligence for internet of things. IEEE Internet of Things Journal, 2025, 12(2): 46269-46293.

[38] Shehwar D E, Gul S, Zafar M U, et al. Acoustic wave analysis in deep sea and shallow water using bellhop tool[C]//2021 OES China Ocean Acoustics (COA). IEEE, 2021: 331-334.