水下无线传感器网络安全研究综述

苏毅珊[①] 张贺贺[①] 张 瑞[①②] 马素雅[①] 范 榕[①] 付晓梅[③] 金志刚*[①]

[①](天津大学电气自动化与信息工程学院 天津 300072)

[②](天津中德应用技术大学软件与通信学院 天津 300350)

[③](天津大学海洋科学与技术学院 天津 300072)

摘 要：水下无线传感器网络(UWSNs)广泛应用于如灾害预警、资源勘探等各种领域，然而易受到恶意攻击，迫切需要发展能够适应其通信带宽窄、传播时延长、时空不确定性严重等特性的安全机制。首先，该文从水下无线传感器网络的特性及安全需求入手，对其面临的安全威胁进行了分析。然后，对水下无线传感器网络中的加密、认证、信任管理、入侵检测、安全定位、安全同步和安全路由各类安全机制进行了综述。最后，对水下无线传感器网络安全研究中面临的缺少实际测试及相关数据集等挑战以及利用网络特性发展安全机制的未来研究方向进行了探讨。

关键词：水下无线传感器网络；网络安全；恶意攻击；安全技术

中图分类号：TN915.08; TP393 **文献标识码**：A **文章编号**：1009-5896(2023)03-1121-13

DOI: 10.11999/JEIT211576

Review of Security for Underwater Wireless Sensor Networks

SU Yishan[①] ZHANG Hehe[①] ZHANG Rui[①②] MA Suya[①]
FAN Rong[①] FU Xiaomei[③] JIN Zhigang[①]

[①](*School of Electrical and Information Engineering, Tianjin University, Tianjin* 300072, *China*)

[②](*School of Marine Science and Technology, Tianjin Sino-German University of Applied Sciences, Tianjin* 300350, *China*)

[③](*School of Marine Science and Technology, Tianjin University, Tianjin* 300072, *China*)

Abstract: Underwater Wireless Sensor Networks (UWSNs) are widely used in disaster warning, resource exploration and other fields. However, UWSNs are vulnerable to malicious attacks. Therefore, it is urgent to develop a security mechanism that can adapt to its characteristics, e.g. communication band width, propagation time extension, and severe spatio-temporal uncertainty. First, based on the analysis of the characteristics and security requirements of UWSNs, the security threats UWSNs face are discussed in this paper. Then, the security mechanisms of UWSNs are summarized, including encryption, authentication, trust management, intrusion detection, secure location, secure synchronization and secure routing. Finally, the challenges of lack of practical tests and relevant data sets in the security research of UWSNs are discussed, as well as the future research direction of developing security mechanism based on network characteristics.

Key words: Underwater Wireless Sensor Networks (UWSNs); Network security; Malicious attacks; Security technology

1 引言

水下无线传感器网络 (Underwater Wireless Sensor Networks, UWSNs)主要由地面基站、水面汇聚节点和水下传感器节点组成，可完成海洋监测、资源勘探等军民应用[1]，是各国开发、利用海洋资源的重要技术。由于电磁波与光波在水下衰减较大，采用水声通信作为水下远距离通信的主要手段。UWSNs作为无线传感器网络的分支，面临着信道开放及无人监管的问题。开放的水声传播环境使保密水声通信面临严峻挑战。恶意节点可以对广播信道中的消息进行窃听、拦截、修改、重放，或者注入虚假消息破坏网络中的数据完整性和正确性。由

收稿日期：2021-12-27；改回日期：2022-05-12；网络出版：2022-06-13
*通信作者： 金志刚 zgjin@tju.edu.cn
基金项目：国家自然科学基金(62171310, 52171337)
Foundation Items: The National Natural Science Foundation of China (62171310, 52171337)

于水下部署的网络缺乏监管，网络面临着入侵发现困难的问题。然而，相比于无线电通信，水声通信中存在着严重的时空不确定性。节点位置受风浪、洋流等因素的影响剧烈变化，从而导致网络中报文冲突造成丢包的概率增加。并且，水声信道还具有严重的多径、多普勒效应、高传输损耗及高环境噪声，也在一定程度上造成了高误码和高丢包[2,3]。此外，电磁波信道具有较为精确描述的经典模型，而水声信道中缺乏适用于不同环境下的通用信道模型，难以对误码和丢包情况进行准确评估。上述各问题使UWSNs一定程度上难以区分水下环境造成的误码和丢包与攻击者的恶意篡改、丢包行为。

此外，UWSNs的硬件资源包括能量、计算和存储能力严重受限，且由电池供电[4]的传感器不便进行充电或更换。这些限制使现有很多成熟的无线传感器网络 (Wireless Sensor Networks, WSNs)安全机制无法直接应用于UWSNs中。能耗的限制和水声远距离通信的不可靠性使多跳协作通信在UWSNs中具有更大吸引力。多跳通信依赖于节点的转发机制以及节点间的高度合作，这为网络层中的多种攻击，如选择性转发、女巫攻击等提供了实施条件。综上，如何在水下通信技术不断发展，安全威胁不断演进的形势下保障UWSNs的安全，受到越来越多的重视。本文从UWSNs的特性和安全需求入手对其面临的恶意攻击以及相关的安全机制进行了分析。

2 UWSNs的特性

2.1 UWSNs的网络结构及其网络特性

UWSNs节点间的通信主要有3种拓扑结构：集中式、分布式和分层式。

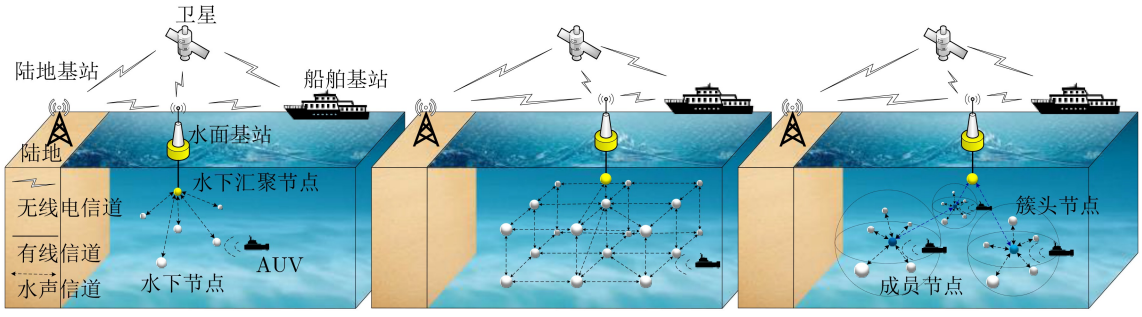
集中式网络结构示例如图1(a)。集中式网络指每个节点都有一条链路与汇聚节点相连。集中式结构简单、便于维护、易于实现。缺点是网络覆盖范围小，可靠性低。一旦中心节点出现故障，将导致整个网络瘫痪。此外，部署在中心节点附近的恶意节点可以通过窃听获取网络的所有信息，也可以采取干扰等拒绝服务攻击，破坏网络服务，致使整个网络瘫痪。

分布式网络的结构示例如图1(b)。分布式网络中每个节点身份平等，源节点和目的节点间可经由多条路径进行通信，实现流量平衡、减少网络拥塞、提高整体可靠性。少量恶意节点的存在难以对整个网络安全造成威胁，此外通过安全路由协议，可在节点间建立安全的路由来进行数据传输。然而出于对节点的移动性以及安全性的考虑，UWSNs的路由信息需要动态维护，过多的维护路由控制信息会增加路由开销和能量消耗。

分层式网络结构示例如图1(c)。分层式网络中，簇头节点的能耗高于成员节点，通常由簇内各节点轮流当选以平衡节点能耗、延长网络寿命。分层式网络的优点在于扩展性好，网络规模不受限制，可通过增加簇的数量来提高网络容量。分层式中的簇头节点是一个簇的中心节点，攻击单个簇头节点虽无法致使整个网络瘫痪，但会影响该簇的正常通信。簇头节点的轮换机制可减小此类影响，一定程度上提高了安全性。

UWSNs的网络特性：

(1) 严重受限的硬件资源。水下传感器节点成本昂贵，部署稀疏，节点间距离可达数千米至数十千米[5]，导致其收发功率远高于陆地无线网络。例如，对于ZigBee，它大约是10 mW和10～1000 mW的无线网络。然而，UWSNs中的发送功率通常需要几十瓦。对于相同的网络安全通信开销，UWSNs会消耗更多的能量。能源限制使UWSNs不能直接运用无线电网络的安全机制，UWSNs既要避免过分追求安全性而忽略开销和能源问题，减少网络寿命；也要避免过分追求节能而忽略安全问题，以耗尽关键节点能量为目的的恶意攻击可使水下网络节点能量比无线电网络更快耗尽，破坏网络服务。因



(a) 集中式结构 (b) 分布式结构 (c) 分层式结构

图 1 UWSNs的网络结构

此，应尽可能在减少安全通信开销的前提下保证网络安全，实现两者平衡。

(2) 不安全的网络环境。水下传感器节点部署在无人值守的开放环境中，易受船舶、海洋生物的撞击，或被污垢腐蚀造成节点失效。除了物理损坏，开放的声传播环境使恶意节点可通过监听信号流量确定关键节点位置进行攻击，也可窃听、拦截数据消息，或在信道中注入噪声等信号对正常通信进行干扰。此外，伪装成合法节点的恶意节点通过发动拒绝服务攻击，对网络的定位、同步、路由具有严重威胁。所以，UWSNs需要考虑安全性问题，避免其在遇到安全威胁和恶意攻击后瘫痪。

(3) 动态的网络拓扑。水下传感器节点通过水面浮标投放至不同深度，或通过不同长度的锚链系在海底的锚定，实现3维静态部署。不同于陆地传感器节点的固定性，在洋流、潮汐的作用下，多数水下传感器节点在其相对位置上具有一定动态位移。如图2所示，S_1是节点未受到洋流影响时的位置，S_2是节点S_1受到洋流$\boldsymbol{F}_c$漂移后的位置。水下传感器节点以锚为中心、系绳为半径在半球上运动，并且运动模型在一定的时空范围内保持一致性[6]。

2.2 水声信道特性

不可靠的水声信道被公认为是当今最难使用的通信媒介之一。首先，水声传播速度约为1.5×10^3 m/s，比陆地空气中的无线电传播速度(3×10^8 m/s)低5个数量级。水声传播的高时延超过了卫星无线电通信中的对应值，并且受水下温度、盐度和深度的影响而动态变化。其次，水声信道的可用带宽极其有限，传输距离在1～10 km的系统，带宽约为10 kHz；传输距离为0.1～1 km的水声通信系统的带宽为20～50 kHz；若使网络的通信带宽达到100 kHz及以上，通信距离只有几十米。此外，水下环境中更为显著的传输损耗、环境噪声、多径效应、多普勒频移等问题，导致水声通信具有高误码率和高丢包率。以下是对水声信道几个特性的介绍：

(1) 传输损耗。传输损耗包括吸收损耗和几何扩散损耗。信号的吸收损耗指水声信号的部分声能在传输过程中转换为热能被吸收，造成信号强度不断减弱，取决于频率。信号的几何扩散损耗随着距离的增加而增加，与频率无关。当前常用的信道模型只考虑大尺度效应。以信号散射为例的小尺度信道特征信息是信号变化的主要因素，通常表现为随机变化。小尺度衰落系数可由下式定义[7]

$$\gamma_p(f,t)=\frac{1}{h_p}\sum_i h_{p,i}\mathrm{e}^{-\mathrm{j}2\pi f\delta\tau_{p,i}(t)} \tag{1}$$

其中，$h_{p,i}$为路径内增益，$\tau_{p,i}=\tau_p+\delta\tau_{p,i}$为路径内延迟。由于散射场中散射点的位置随机，因此增益$h_{p,i}$和延迟$\tau_{p,i}$都为随机值。

对于传输频率为f的信号，若存在多条传输路径$p=0,1,\cdots,N_p$，滤波效果对于所有路径都是相同的，由函数$\bar{H}_0(f)$描述。对于路径p，时变信道传输函数可表示为

$$H(f,t)=\bar{H}_0(f)\sum_p h_p\tilde{\gamma}_p(f,t)\mathrm{e}^{-\mathrm{j}2\pi f\tau_p} \tag{2}$$

其中，$\tilde{\gamma}_p(f,t)=\gamma_p(f,t)\mathrm{e}^{\mathrm{j}2\pi a_p ft}$，$h_p$为路径增益，$\tau_p$为传播延迟，$a_p$为多普勒扩展因子。

(2) 环境噪声。水声传播环境中的多种环境噪声容易造成声信号的失真，主要包括3种噪声：海洋背景噪声、水下自主航行器的自噪声和间歇性的场地噪声(如，冰裂、地震)。强级别的噪声会使通信链路完全中断，一般噪声也会导致通信误码率和丢包率的上升。按照影响不同频段声学通信可将环境噪声分为4种类型：(a) 湍流噪声(N_t，小于10 Hz)；(b) 运输噪声(N_s, 10～100 Hz)；(c) 风噪声(N_w, 100 Hz～100 kHz)；(d) 热噪声(N_th, 大于100 kHz)[8]。

(3) 多径效应。水下多径的形成受两类因素影响：声音在表面、底部和任何物体上的反射及在水中的折射。声的折射是由于水声声速受水的温度、盐度和压力影响并随深度与位置变化，根据斯涅尔定律，声向传播速度低的区域弯曲。在经反射和折射产生的无限多信号中损耗大的信号会被丢弃，只留下有限数量的有效路径[9]，每条路径充当一个低通滤波器，影响接收信号振幅。

(4) 多普勒效应。发射和接收节点的运动会对信道响应造成额外影响，即多普勒效应导致的频率偏移(发射和接收的频率之差)和额外的频率扩展。多普勒效应的幅度和收发相对速度v与声速c的比值$a=v/\mathrm{c}$成正比[10]。与电磁波速度相比，声速低了5个数量级，所以因节点运动引起的声信号的多普勒失真非常严重。除了水下自主航行器的移动，节点也会随波浪、洋流等漂移，即水下无线传感器节点始终处于运动状态。

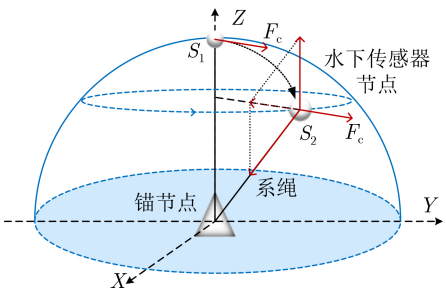


图 2 水下传感器节点的移动模型

上述水声信道的特性为通过时延、误码率、丢包率等表现区分合法节点的异常行为及攻击者的恶意行为带来了挑战。水下传感器节点成本高，因此网络对攻击节点和通信异常节点的响应有所不同。对攻击节点的处理包括逻辑删除和物理移除[11]。逻辑删除指对网络重新设置密钥，而无需破解网络密钥即可阻塞网络的攻击者(如干扰攻击)需被物理移除。对于信道异常导致行为异常的合法节点，网络通常令其休眠一段时间，避免频繁的链路中断造成过多的通信开销。此外，逻辑删除需要占用一定的网络资源，水下的物理移除也需付出一定的额外成本，所以安全机制需要对攻击者和通信异常节点做出准确判断，避免付出不必要的代价。

3 UWSNs面临的挑战

3.1 物理层

(1) 窃听 (Eavesdroping)攻击。恶意节点无需主动发送、截获或转发消息，只需保持监听状态，监听并窃取信道中的数据包信息，或通过分析通信流量确定节点身份和位置，然后配合主动攻击危害网络。被动攻击不会对网络的通信活动造成异常影响，因此难以被检测到，所以应对被动攻击的主要方法是预防而非检测。

当前主要通过加密机制应对窃听节点窃取重要信息。文献[12]对水声网络中的窃听攻击存在概率进行了研究，作者提出水声网络中的窃听概率很大程度上取决于由声信号频率、扩频因子和发射节点与窃听节点之间的距离表征的水声信道，并建立了一个分析模型研究在考虑水声信道条件的情况下网络中窃听攻击的存在概率。基于此，只需要对易受窃听攻击的区域或方向的通信进行加密，大大降低安全成本。然而，该文只建立了一个相对简单的分析框架，实际的水声信道更为复杂，未来研究应当考虑更多的水声信道特征。

(2) 拥塞 (Jamming)攻击。在物理层的干扰攻击中，恶意节点向信道中以某种攻击模式(持续、随机、反应式)发送噪声或发送无用信号占用通信信道，干扰其他节点正常数据转发。UWSNs多为分层式网络结构，若恶意节点干扰到簇头节点、基站等关键节点，将导致整个网络瘫痪。此外，干扰攻击者无需获取密钥等认证信息侵入网络，且无需特殊硬件要求，发动攻击成本低。UWSNs中采用扩频、多径路由、睡眠-唤醒等机制防御干扰攻击。

文献[13]分析了UWSNs面临干扰攻击的脆弱性，并利用不同的基于多频移键控(Multi-Frequency Shift Keying, MFSK)的声学调制解调器进行湖试干扰实验。作者测量了无干扰机的正常网络条件下和有干扰机的网络条件下的平均包传递率 (Packet Delivery Ratio, PDR)、包发送率 (Packet Send Ratio, PSR)和网络吞吐量 (network ThroughPut, TP)，并改变了攻击模式，实验结果见表1。通过实验结果可以得出以下结论：首先，增强的白噪声无法干扰网络，因为白噪声干扰下的网络性能与正常运行期间大致相同。其次，持续的和反应性的干扰表现最好。然而，反应式攻击模型更节能，因为不需要持续发射信号阻塞网络。第三，虽然干扰可以阻止接收端接收数据包，但无法阻止网络实际发送数据包。此外，作者进一步实验表明对传输信号的头部进行干扰更加有效。鉴于此，可以针对信号头部对干扰的容忍度较低这一特点来设计更加高效和低能耗的干扰方案。

文献[14]测试分析了LinkQuest, AquaSeNT和Benthos调制解调器的干扰，产生了连续单频、扫频和正弦调制脉冲3类干扰信号，并使用了持续攻击和针对性攻击两类方案。其中，几类干扰方案示例如图3。该文重点在于通过分析不同调制解调器发送的信号，设计最为高效的干扰方案。

以上探讨了一些UWSNs中物理层干扰方案的实际测验，此外研究人员也就如何抵抗干扰展开了研究。文献[15]利用多径路由的冗余性避免了数据包在强干扰下的过度丢失。与静态及单路径路由相比，该方案提高了包含检测信息的数据包被及时发送到接收器的成功率。与泛洪路由相比，该方案有效降低了传输开销。

3.2 数据链路层

(1) 碰撞 (Collision)攻击。某些媒体访问控制(Media Access Control, MAC)协议通过载波监听与邻居节点协商占用信道，在发生信道冲突后，发送节点通常退避重传。恶意节点通过窃听合法节点的请求发送 (Request To Send, RTS)或允许发送(Clear To Send, CTS)包，重复发送窃听的RTS/CTS帧，占用通信信道，造成网络中的信号冲突，导致UWSNs的吞吐量及数据包的平均时延性能下降。可通过设计冲突检测机制，减少数据冲

表 1 网络性能[13]

攻击	PDR(%)	PSR(%)	TP(bit/s)
无攻击	100	100	140.0660
持续干扰	0	100	0
随机干扰	54	100	30.0900
反应式	0	100	0
白噪声	100	100	139.8205

突，或通过节点协作通信来提高通信成功率，减小碰撞攻击对通信质量的影响。

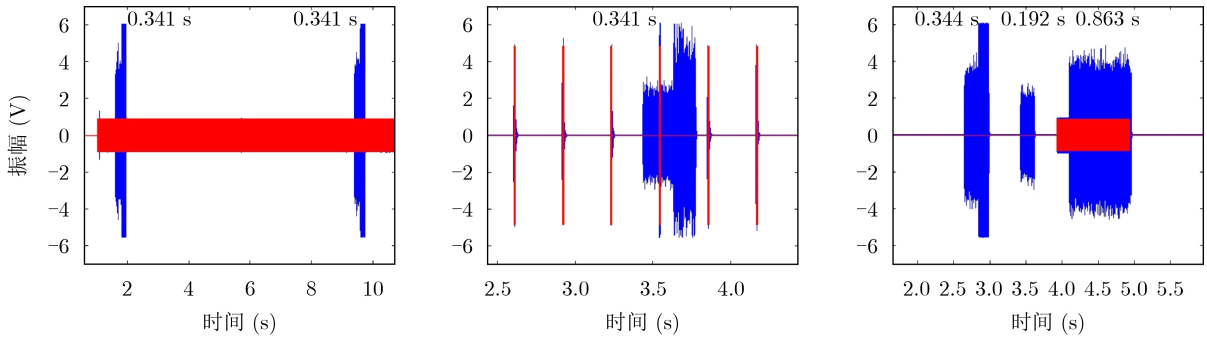
(2) 耗尽 (Exhausting)攻击。传感器网络中的耗尽攻击针对水下无线传感器节点收发功率大且电池无法更换充电的特点，不以耗尽计算或存储资源为目标，而是通过发送请求或重传请求使目标节点持续发送消息，无法进入休眠状态，导致目标节点能量快速耗尽。部分节点甚至一个关键节点能量的耗尽可能使整个网络无法继续工作，严重威胁网络寿命。

(3) 重放 (Replay)攻击。恶意节点窃取消息后再将消息重发给接收节点，通常用以身份认证，破坏认证正确性。恶意节点也可在拦截消息后，延迟发送给接收节点，使接收节点得到错误的传播时延和接收信号强度，对一些定位、同步协议造成影响。文献[16]研究了4种不同的重放攻击，将非法数据包注入网络，填充节点媒体访问控制的队列，使网络饱和。该文也提出了在数据链路层和路由层增加一个安全层，基于时间和生成的节点地址信息通过哈希函数计算出唯一的数据包标识符，验证数据包的新鲜度。

(4) 网络分配矢量 (Network Allocation Vector, NAV)干扰。RTS/CTS握手协议包含NAV信息，恶意节点可通过伪造或修改NAV后周期性发送RTS/CTS帧，使合法节点不断退避，从而使合法节点接入信道的时延增加、网络吞吐量降低。文献[17]利用目的地址分别为1～5的5个通信机和1个干扰机在湖中进行了实验，数据链路层采用了避免冲突的多路访问协议，路由层采取静态路由，考察了NAV干扰对UWSNs的丢包率及吞吐量的影响情况。实验结果如图4所示，图中T表示RTS的发送周期，d表示目的地址，目的地址为6表示节点没有针对性干扰网络中某合法节点。由图4(a)、图4(b)可知，NAV干扰下的网络丢包率为44.26%，网络吞吐量从1.83 bit/s变为1.05 bit/s，下降了45%。图4(c)表明，干扰某个网络中存在的目的地址或减少RTS的发送周期可对网络吞吐量造成更大的负面影响。实验结果表明NAV干扰对UWSNs的通信效果具有一定威胁。

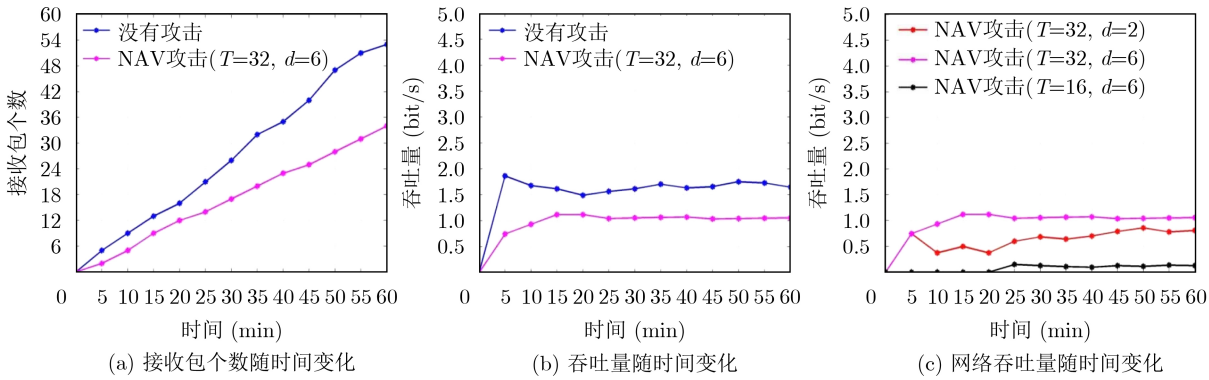
3.3 网络层

(1) 选择性转发 (Selective Forwarding)。在选择性转发攻击中，恶意节点拒绝转发某些敏感消息并丢弃它们，从而降低网络的数据投递率，破坏数据完整性。拒绝转发所有消息的攻击称为黑洞攻击，但黑洞攻击者的恶意行为明显，更容易被检测出并隔离出网络。此外，水声信道异常导致的丢包一定程度上掩盖了选择性转发行为，加大了对其的检测难度。



(a) 持续干扰　(b) 持续脉冲干扰　(c) 对数据包的针对干扰

图 3 对LinkQuest调制解调器的几种干扰方案[14]

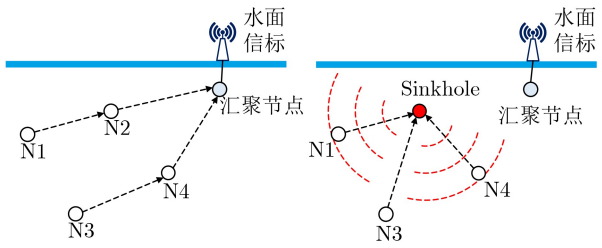


(a) 接收包个数随时间变化　(b) 吞吐量随时间变化　(c) 网络吞吐量随时间变化

图 4 NAV干扰攻击对网络性能的影响[17]

(2) 槽洞 (Sinkhole)攻击。UWSNs中的路由协议多重视能量均衡，常常优先选择剩余能量高的节点作为下一跳节点。槽洞攻击者可谎报剩余能量或声称自己距接收节点最近，从而将自己伪装成路由的最优下一跳，尽可能吸引更多流量。如图5(a)为正常情况下的路由路径，图5(b)是节点N2被捕获成为槽洞节点后的路由路径。槽洞攻击通常和其他攻击如篡改、选择性转发或黑洞攻击等结合，对网络造成更大威胁。

(3) 虫洞 (Wormhole)攻击。在虫洞攻击中，两个及以上的恶意节点通过一条长距离低延迟链路(水上射频信道、有线信道)形成隧道，一个节点将接收到的消息通过隧道在另一个节点重放。由于UWSNs对能耗的限制，许多传感器网络服务都试图通过最小化某些预定义的路由度量，如跳数、延迟，来优化性能。虫洞隧道可以有效减少路由跳数，对于基于距离向量的机会路由协议倾向于选择该条路径将数据传输至目的节点。靠近源节点一端的虫洞攻击者相当于一个槽洞攻击者，吸引大量流量后与共谋端联合发动其他攻击，将服务质量降至最低，对网络造成更大影响。水下虫洞隧道的两种形式如图6，其中，图6(a)是两个低成本虫洞节点通过有线信道连接水面设备后通过无线电信道形成低延迟链路；图6(b)是两个虫洞节点直接通过有线信道连接。图6(c)是干扰或重放攻击与低延迟的虫洞隧道相结合。在该混合攻击中，虫洞的接收方在接收到合法发送者的消息后通过有线信道迅速通知虫洞作为干扰节点的另一端对该消息进行干扰，成功阻塞网络。低延迟的虫洞隧道为干扰器提供了一定的处理时间，无需持续性干扰，使其能够更为准确高效地拥塞网络，降低能耗。文献[18]研究了基于方位测量技术的水声通信网络虫洞攻击检测算法，通过方位或距离异常值判断虫洞攻击是否存在。然而水下网络定位会产生一定的通信开销，通过定位的方式检测虫洞是低效的。因此，有效对抗UWSNs中的虫洞攻击是一个具有挑战性的问题。

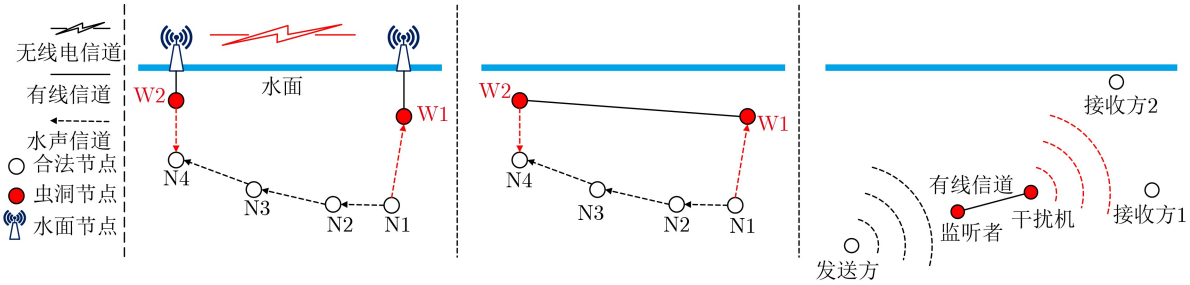


(a) 节点均合法时的路由　(b) 存在Sinkhole攻击时的路由

图 5 UWSNs中的Sinkhole攻击

(4) 女巫 (Sybil)攻击。女巫节点可以通过编造或者窃取正常节点身份以多个身份同时出现在网络中，降低多径路由、拓扑维护的容错性。女巫节点也可在被逻辑隔离出网络后，通过新的身份重新加入网络，利用多个身份轮流加入网络[19]。女巫攻击节点可以通过广播消息误导接收节点以为自己有实际并不存在的邻居，方便女巫节点截获被误导节点的数据信息。女巫节点也可以向源节点提供虚假的坐标信息，破坏网络的定位服务。与其他形式的恶意攻击相比，女巫攻击很少需要与其他节点合作且资源需求较小[20]，因此它经常出现在UWSNs中。文献[21]提出了一种基于节点状态信息的检测方案，信标节点通过通信频率与列表中记录的剩余能量之间的关系来判断是否存在女巫节点。然而水下环境的波动致使通信链路的不稳定引起的重传等问题会带来额外的能量消耗，可能会导致合法节点被误判为女巫节点。

(5) Hello泛洪 (Flood)攻击。在一些UWSNs路由协议中，节点通常会广播Hello消息向邻居节点通知自身的存在，接收到Hello消息的节点将发送节点作为自己通信范围内的邻居节点。发动Hello泛洪的恶意节点通过增大发射功率重播合法的Hello消息从而吸引一些节点将其通信范围外的合法节点当作自己路由的下一跳，增加了这些节点的丢包率和能耗。Hello泛洪攻击会影响依靠邻居节点间的信息交互进行拓扑维护或流量控制的协议。



(a) 通过水上无线电信道建立虫洞隧道　(b) 通过水下有线信道建立虫洞隧道　(c) 虫洞攻击与干扰攻击的结合

图 6 UWSNs中的虫洞攻击

3.4 传输层

UWSNs面临的传输层攻击主要为去同步 (Desynchronizing)攻击。去同步攻击指攻击者将伪造了序号或控制标志的数据包发送给网络的一端或两端，从而影响节点间的传输工作。例如当节点为建立连接发送一个需确认的包后，去同步攻击使该节点无法正确接收与之匹配的确认包，因此尝试重新传输该包。若该攻击有效存在一定时间，频繁的同步恢复不仅会耗尽节点能量，还会额外占用一定的带宽资源，对UWSNs具有一定威胁。此外，去同步攻击对UWSNs中时间同步的准确性和计划事件的效率具有巨大影响。由于水下节点无法使用全球定位系统，时间同步服务是UWSNs的技术重点及难点。将去同步攻击与对节点测距和传输往返时间有影响的虫洞、女巫或重放攻击相结合，会加剧对整个网络通信与协作的破坏。

3.5 应用层

应用层的安全威胁与实际应用相关，UWSNs的应用多以数据为中心，用户往往更关注数据的正确性。篡改攻击通过窃听或拦截数据包对数据进行恶意篡改，然后重新注入网络，旨在破坏数据的完整性、正确性、实时性。此外，上述各层中的攻击也会间接影响UWSNs的应用安全，例如虫洞或重放攻击对定位的影响。众所周知，定位是UWSNs中的一个重难点，许多军民应用需要传感器节点的位置信息，而虫洞或重放攻击可影响基于测距的定位算法，导致定位产生错误结果，从而给用户带来错误的数据信息。

4 UWSNs的安全机制

为满足UWSNs的安全需求，见表2，以及解决UWSNs面临的安全威胁，研究人员为UWSNs提出了包括加密、认证、信任模型、入侵检测、安全定位、安全同步及安全路由协议等安全机制。加密和认证主要为防止外部节点的恶意侵入；信任管理和入侵检测机制主要应对通过伪造合法身份信息成功侵入网络内部后进行攻击的恶意节点；安全定位、安全同步、安全路由针对协议加入合适的安全技术，使传感器网络可以解决对协议具有恶劣影响的攻击，提高协议的安全性。

4.1 加密和认证机制

加密机制在确保信息安全方面具有重要作用。加密使敏感信息能够在信道开放的UWSNs中安全存储或传送，避免信息被非法用户或恶意攻击者读取或篡改。然而，由于严重受限的水声信道可用带宽以及较高的收发功率，使数据包长度显著增加的加密机制不适用于UWSNs。文献[22]提出了一种基于混沌理论的轻量级8轮迭代分组密码算法，采用逻辑映射进行置换，并通过改变迭代轮数来增加密钥空间。该算法降低了加密成本，平衡了安全性与通信开销，具有更高的能量效率。

此外，随着量子计算机的出现，基于量子密钥分发的加密机制会受到威胁。因此，研究人员对利用两个合法节点间的信道特性生成密钥的方案进行了研究，此类方案对于水声信道具有明显时空不确定性的UWSNs具有一定的优越性。文献[23]利用水声信道多径的幅值和时延值来生成加密密钥，并通过仿真和实验结果验证了基于水声信道冲激响应生成加密密钥的可行性，为水声隐蔽通信提供了加密支持。

认证机制可判断身份未知节点的合法性。不同于静态WSNs，节点的主动与被动移动使UWSNs经常出现新节点的加入或旧节点的重新加入。开放的水声信道使恶意节点可通过伪造合法消息或合法身份侵入UWSNs。认证机制可确认请求加入网络的节点身份合法性，有效防止恶意节点的入侵。文献[24]提出了一种水声网络协同消息认证方法。该方法利用水声信道的强空间依赖性和时不变性(在较小的时间及空间变化下，两节点间信道特征分布可近似为静态，但在不同空间上区别较大)计算决策值对相关节点执行认证。该操作由一组分布的可信节点协同执行，汇聚节点通过融合可信节点所提供的决策值来确定节点的合法性。

4.2 信任管理机制

信任管理是一种新颖的安全机制，信任模型是其核心内容。信任模型为每个水下传感器节点赋予

表 2　UWSNs中的安全需求

安全需求	目标
数据保密性	防止敏感信息在开放水声信道中被恶意节点窃取
数据完整性	确保接收端能够获取完整正确有效的数据、控制及调度等信息
数据新鲜性	确保数据为最新的，而不被恶意节点故意延迟重放
网络可用性	UWSNs的重要服务需要在网络中存在攻击或某些节点故障后仍然可用
入侵检测和隔离	对于成功破解身份认证信息伪装为合法节点的恶意节点，UWSNs应当能够准确识别其恶意行为并对其进行有效隔离，防止其对网络产生长期的负面影响

信任值，其他节点确认其可信后再与其进行协同工作。信任模型可应用于路由协议、定位和同步等协议中，增强协议的安全性。不同于认证机制，信任模型通常周期性工作，通过节点多方面表现收集信任证据并计算其可信度。信任模型可以有效响应内部攻击，提高网络安全性。近期，为解决UWSNs中内部攻击问题，研究人员开始对信任模型进行大量研究。信任模型框架如图7所示。信任模型主要由3部分组成：信任证据收集、信任值计算和信任值更新。

(1) 信任证据的收集基于恶意节点与正常节点在行为表现上的区别。例如邻居节点接收Hello泛洪攻击者的信号强度过高；拒绝服务 (Denial of Service, DoS)攻击者频繁工作会产生大量能耗；选择性转发、黑洞攻击者的包转发率低于正常节点。信任模型要根据恶意节点的行为和表现选择合理有效的信任证据。

文献[25]根据UWSNs潜在的攻击威胁的行为特性提出了3类信任证据，分别是通信信任、数据信任和能耗信任。(a) 将节点n_i与其各个邻居节点的交互情况作为信任证据是由于多种攻击如，选择性转发、黑洞攻击或碰撞攻击会导致一定的失败交互。通信信任T_i^c可由下式计算

$$T_i^c = \mathrm{E}(\mathrm{Beta}(a+1, b+1)) = \frac{a+1}{a+b+2} \tag{3}$$

其中，a和b分别表示成功的交互次数和失败的交互次数，E代表期望值。(b) 由于UWSNs是以数据为中心的网络，用户更关注数据的正确性，所以使用数据信任表示传感器节点内的数据一致性和数据差异性，用以识别产生虚假或潜在篡改数据的恶意节点。(c) 将剩余能量作为信任证据是由于UWSNs中节点的通信能耗较大，发动攻击的节点能耗与正常节点有很大区别。例如黑洞攻击的能耗低于正常节点，而女巫攻击、干扰攻击的能耗高于正常节点。能耗信任T_i^{e}可由式(4)定义。

$$T_i^{\mathrm{e}} = \frac{E_{\mathrm{re}}}{E} \tag{4}$$

其中，E_{re}是一个节点的剩余能量值，E是初始能量值。

此外，不同于陆地WSNs，恶劣的水下环境引起的通信、能量和数据的波动很容易被误认为是异常行为，导致合法节点被误判为恶意节点。例如为了全面衡量水下节点的信任度，文献[25]还考虑了环境信任度T_i^{EN}，它由水声信道中噪声的功率谱密度表示。

(2) 计算信任度的方法，包括贝叶斯理论、D-S证据理论、加权平均、机器学习等。文献[25]利用将通信信任、数据信任、能源信任及环境信任集成的信任数据集，通过孤立森林算法计算信任值来评估传感器节点上的可信度，以检测潜在的异常节点。孤立森林算法属于无监督学习算法，无需预先定义恶意攻击进行模拟训练，在动态多变的水下环境具有一定的优越性。并且孤立森林算法适用于包含少量负样本的不平衡数据集，符合UWSNs中恶意节点通常处于少数的特点。此外，信任具有不确定性，传感器节点间的信任关系是模糊和随机的。现有的一些方法将信任量化为一个确定的实数，不足以用来表示信任关系。文献[26]采取了将信任证据模糊化的方法，认为信任证据的值$T \in [0, 0.4)$时为低信任，$T \in [0.4, 0.6)$时为中信任，$T \in [0.6, 1]$时为高信任。将所有信任证据模糊化后，采用C4.5决策树对信任度进行分类，以判断节点的合法性，而不再继续计算节点的综合信任值。

(3) 信任值更新也是信任模型必不可少的一部分。攻击者的攻击模式多变，可随时切换。当恶意节点将选择性转发攻击切换为篡改攻击，节点的异

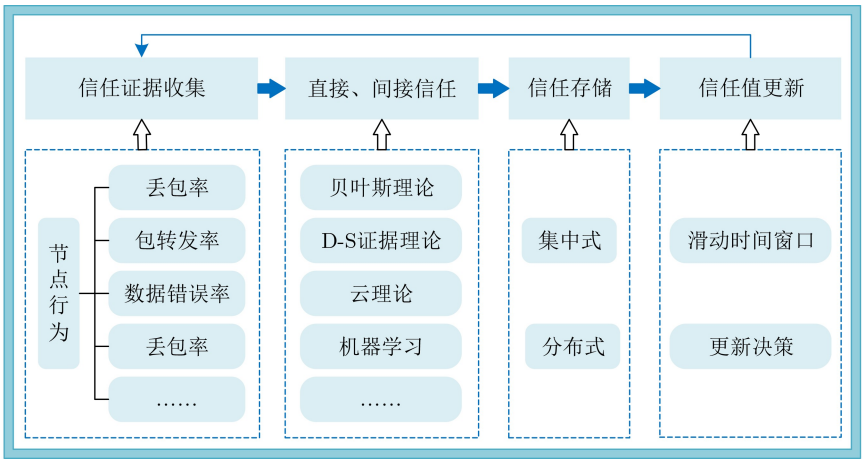


图 7 信任模型框架

常表现不再是高丢包率、低转发率，历史证据将无法真实反映节点当前攻击类型，造成信任评估的不准确。此外，由于UWSNs的时空多变性，合法节点在传播环境异常时同样具有高丢包率、高误码率，所以信任模型要考虑环境因素对节点的影响，使信任评估更加准确。文献[27]设计了一个环境模型量化水下波动对节点数据的影响，提出了一种基于强化学习的信任更新机制，以抵抗不断变化的攻击模式，同时实现有效的信任更新。

4.3 入侵检测机制

加密和认证机制可有效预防UWSNs的外部攻击，然而一旦传感器节点遭到破坏，其所有相关机密将会公开于攻击者，使得基于加密和认证机制变得无效。入侵检测系统作为第2道防护墙，可以有效解决预防机制无效问题，帮助识别恶意的内部入侵活动。一个完整的入侵检测系统包括4步：监控、分析、检测、响应。无线传感器网络中的入侵检测的分类如图8所示。入侵检测技术根据原理主要分为两类：异常检测和特征检测。异常检测通过发现与预期表现或正常行为不相符的事件检测恶意节点，根据算法可将基于异常的入侵检测分为如图8的类型。特征检测通过与预先定义的攻击特征相匹配，从而识别出入侵网络的攻击。异常检测无法确定具体的入侵方式，对网络环境的适应性相对较弱并且缺乏精确的判定，特别是对于UWSNs复杂多变的环境，常会出现将正常节点误判为恶意节点的情况。特征检测相较于异常检测，可以更准确地识别出已经预先定义好的攻击类型，但是无法检测出系统未知的攻击，并且特征库中存储的攻击类型越多，检测速度也会越低。将两种检测机制相结合的混合检测方式，可以更加全面准确高效地做出判断，但是系统也会更加复杂，增加能耗和开销。

由于UWSNs的特点和限制，考虑检测准确性的同时也要考虑检测系统的通信、内存、能量资源的消耗问题，针对UWSNs的实际应用需求设计入侵检测系统。众多应用，如水下环境检测需要传感器节点的位置信息，文献[28]为保证UWSNs的节点定位安全提出了异常检测方案以检测错误的位置信息。该方案针对UWSNs的计算和存储能力受限问题，分别为传感器节点和锚节点设计了单独的检测方法。其中，传感器节点中通过自回归预测检测锚节点所发数据包的异常，锚节点通过模糊逻辑监测传感器节点发送的每个数据包的异常指数，并存储可信节点的位置信息。此外，UWSNs中的入侵检测需要克服检测速度、自适应能力以及合适的检测指标选择这些技术难点以提高检测准确率。由于UWSNs较高的发送接收功率，只追求高检测成功率而忽略检测速率会使传感器节点的能量在耗尽攻击下快速耗尽。水下环境的动态变化特别是强噪声的出现会使传感器节点的通信行为出现异常，因此需要入侵检测机制对环境的变化具有一定自适应能力，从而降低误检率。现有的一些入侵检测机制见表3。

4.4 安全定位和同步协议

在无法使用GPS的UWSNs中，水声信道的高延迟和时空不确定性，使定位和时间同步研究成为一个巨大的挑战。上述攻击中的虫洞、女巫和重放攻击可以通过改变数据包的端到端时延和接收端的接收信号强度，使接收节点对上一跳发送节点的距离和时钟判断产生巨大偏差，严重影响网络的定位和时间同步。

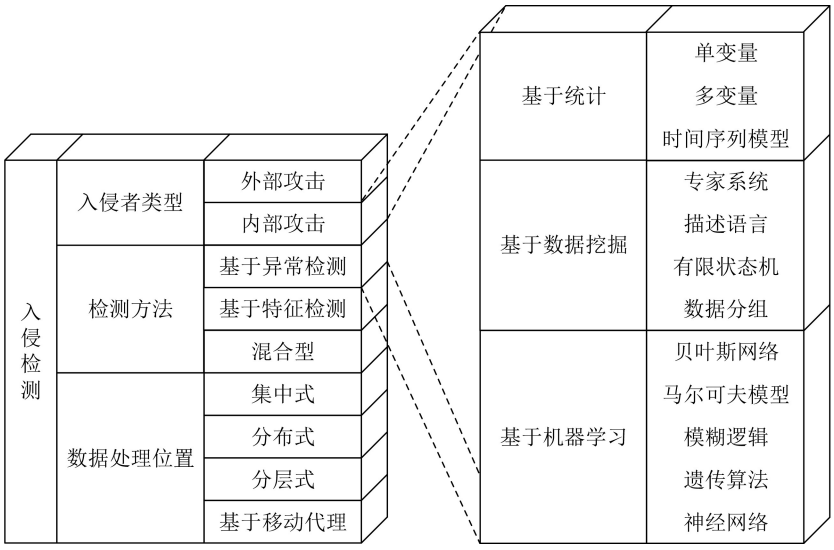


图 8 入侵检测系统及基于异常检测的分类

UWSNs的许多重要应用，如目标跟踪和监控，需要传感器节点的位置信息；事件的时间戳、分布式数据融合等需要网络实现时间同步。目前大量针对如何提高定位和同步精度的研究取得了一定的进展，但只有少量研究考虑了定位和同步的可靠性与安全性。除了通过加密技术对定位和同步信息进行加密抵御外部攻击以外，可通过信任管理[35]或入侵检测机制识别内部攻击者，隔离内部攻击者注入的虚假、错误信息。或通过研究安全的定位和同步机制，提高对攻击的容忍度，保证UWSNs中存在攻击时的准确定位和同步。文献[36]需要具有精确时间同步的一对传感器节点利用到达时间差 (Time Difference of Arrival, TDOA)进行定位，说明了去同步攻击对定位的严重影响，并证明了残差分析不能检测和识别去同步攻击。此外，该文提出了一种对去同步攻击具有一定鲁棒性的两步TDOA定位技术，结果表明该方法可以识别被扰乱的网络时间同步，获得修正的未知位置估计。表4列举了一些UWSNs中的安全定位和安全同步协议。

4.5 安全路由协议

安全路由涉及两个方面：安全路由和安全数据转发。安全路由指网络在建立或更新路由时，节点间相互合作，共享正确的状态等信息从而建立高效的路由，保证网络的连通性和能效性。安全数据转发指路由建立后，防止数据被路径上的节点恶意篡改、丢弃。

根据路由协议所采用的核心安全策略，可以将它们分为以下几类[42]：

(1) 基于反馈信息的安全路由协议。节点通过反馈信息如传播时延、信任度、剩余能量等选择安全、低能耗的路径作为路由。文献[43]基于最新的机会路由策略，提出了遇到路由空洞时向上一跳节点反馈空洞警示包，通知其寻找其他可靠路由从而避免空洞的方法。该方案与处理通信空洞的现有技术相比，更易于实现且具有更小开销和延迟，可有效抵御黑洞攻击，提高数据传输的安全性。

(2) 基于地理位置的安全路由协议。网络层攻击中的女巫、虫洞攻击节点具有不合理的位置信息，地理位置信息对检测这类攻击具有重要作用。文献[44]通过估计两个合法邻居的水声信号到达方向判断相对位置来发现虫洞。此外该安全路由协议加入了认证机制确保节点发现安全邻居。该方案与基本的邻居发现和信道感知路由协议相比，提升了故障检测、能量消耗和开销方面的性能。

(3) 基于密码算法的安全路由协议。加密机制可以防止敏感信息泄露；认证机制一定程度上可避免恶意节点侵入网络内部。文献[43]将一种简单、轻量的强加密算法集成到路由协议中，对感应和收集的数据包进行加密，使数据包只能被接收方解密，防止数据的泄露。这对于需要高保密性的军事应用具有重要意义。

(4) 基于多路径传输的安全路由协议。多路径

表 3 陆地和水下无线传感器网络中的入侵检测机制

检测方法	针对的攻击	网络类型	评价
不完全信息随机博弈论[29]	未指定攻击类型	WSNs	该法用于优化IDS的资源分配，需要传感器节点数量具有一定冗余，不适用于节点稀疏分布的UWSNs
二元逻辑回归[30]	网络层攻击	WSNs	该法需要训练建立回归模型。训练阶段需要模拟无攻击存在的真实环境，对于UWSNs具有一定的挑战
扩展卡尔曼滤波[31]	虚假数据注入	WSNs	该法依赖于WSNs节点间观测数据的高度时空相关性，不适用于具有时空不确定性且节点稀疏分布的UWSNs
加权信任管理[32]	内部攻击	WSNs	适用于UWSNs；基于加权算法的方法，经验权重和信任阈值的确定具有一定主观性
对特定包的行为分析[33]	恶意丢包、篡改	UWSNs	未考虑环境因素导致的丢包行为
利用往返时间异常特点[34]	虫洞攻击	UWSNs	对网络结构具有一定要求，且未考虑信道时空不确定性

表 4 UWSNs中安全定位、同步协议

文献	协议类型	协议机制
一种基于信任模型的水下无线传感器网络协同安全定位算法[35]	安全定位	基于信任模型识别并隔离恶意丢弃、修改定位信息节点
一种新的协同定位测量信息异常检测方法[37]	安全定位	基于自适应神经模糊推理系统检测异常的声距信息，保证测距信息准确
水下传感器网络异步定位的隐私保护解决方案[38]	安全定位	避免位置信息的泄露
基于证据理论的水下传感器网络安全距离定位[39]	安全定位	基于信任模型，选择最可信的节点进行定位
一种基于集群的水下无线传感器网络安全同步协议[40]	安全同步	基于中心超椭球支持向量机检测异常端到端时延
水声网络中带异常点检测的垂直和水平同步服务[41]	安全同步	基于关联检测和统计信誉检测离群时间戳，识别内部攻击节点

路由不仅可以提高数据消息的成功投递率，还可以对路径上的恶意节点进行判别。文献[45]提出了一种协作路由协议，当源节点到目的节点不可直达或链路中断时，通过多个中继节点进行转发。目的节点对多条路径数据传输行为进行对比分析，实现对常见的主动路由攻击(如黑洞攻击、篡改)的检测和隔离。该文所提方案与基于深度信息的路由协议(Depth-Based Routing, DBR)的优化算法对节点存活数、传输损耗、吞吐量、能耗率、端到端时延进行性能分析对比，结果表明攻击会显著降低DBR优化算法的性能，而对该文所提路由方案几乎没有影响。

(5) 基于分层式结构的安全路由协议。分层式UWSNs在平衡能耗、扩展拓扑方面有一定的优势。基于分层式结构的路由协议通常将水下传感器节点分为簇头节点和成员节点，其中，路由的建立主要通过各个簇头节点进行交互[46]，因此簇头节点的安全性对基于分层式结构的路由性能具有重要影响。

5　结束语

针对水声信道条件恶劣、硬件资源受限、通信能耗大等特性以及UWSNs的应用背景，本文论述了安全机制对于UWSNs 的重要性，重点研究了典型攻击的工作特点，并讨论了如何结合UWSNs的特性设计合适的信任模型、入侵检测等安全机制。

现有研究多数没有在实际的水下环境中进行测试，绝大多数停留在理论方案。由于UWSNs的特性，特别是复杂多变的水声信道难以通过仿真软件有效建模，仍需要真实环境测试以实现有效验证。此外，需要对水下无线传感器网络系统进行安全分析跟踪，建立一个具有攻击节点样本存在的数据集。现有基于机器学习算法中的分类算法构建的信任模型和入侵检测模型，需要通过数据集训练出有效的分类器，用以区分合法节点和恶意节点，所以迫切需要建立一个在真实水下环境中获取的具有恶意节点样本存在的UWSNs数据集，这对于未来建立能够有效保护UWSNs的安全系统具有重要意义。另外，UWSNs的一些特性也给攻击者带来了挑战，可以在加强UWSNs的安全性时加以利用，例如水声信道的长传播时延，使窃听者无法迅速获取消息，为通过中继节点在不影响目的节点接收的情况下对窃听者进行干扰提供了可能。

综上，UWSNs的安全研究仍处于起步阶段，也需要更多的水池、湖试、海试实验验证方案有效性，需要进行更多适合UWSNs的防窃听、抗干扰、入侵检测等安全机制的研究，并且对于具有一定安全需求的UWSNs，还需研究通过各层之间的高效协作以最小化资源消耗的安全框架。此外，UWSNs的应用领域非常广泛，各个应用对安全的需求也各不相同，因此要更为实际地考虑具体的应用场景进行安全方案的设计。

参 考 文 献

[1] CUI Junhong, KONG Jiejun, GERLA M, *et al*. The challenges of building mobile underwater wireless networks for aquatic applications[J]. *IEEE Network*, 2006, 20(3): 12–18. doi: 10.1109/MNET.2006.1637927.

[2] DEMIRORS E, SKLIVANITIS G, SANTAGATI G E, *et al*. Design of a software-defined underwater acoustic modem with real-time physical layer adaptation capabilities[C]. The International Conference on Underwater Networks & Systems, Rome, Italy, 2014: 25. doi: 10.1145/2671490.2674473.

[3] YAN Hai, WAN Lei, ZHOU Shengli, *et al*. DSP based receiver implementation for OFDM acoustic modems[J]. *Physical Communication*, 2012, 5(1): 22–32. doi: 10.1016/j.phycom.2011.09.001.

[4] AKYILDIZ I F and WANG Xudong. A survey on wireless mesh networks[J]. *IEEE Communications Magazine*, 2005, 43(9): S23–S30. doi: 10.1109/MCOM.2005.1509968.

[5] FREITAG L, GRUND M, SINGH S, *et al*. The WHOI micro-modem: An acoustic communications and navigation system for multiple platforms[C]. OCEANS 2005 MTS/IEEE, Washington, USA, 2005: 1086–1092. doi: 10.1109/OCEANS.2005.1639901.

[6] ZHANG Wenbo, HAN Guangjie, WANG Xin, *et al*. A node location algorithm based on node movement prediction in underwater acoustic sensor networks[J]. *IEEE Transactions on Vehicular Technology*, 2020, 69(3): 3166–3178. doi: 10.1109/TVT.2019.2963406.

[7] QARABAQI P and STOJANOVIC M. Statistical characterization and computationally efficient modeling of a class of underwater acoustic communication channels[J]. *IEEE Journal of Oceanic Engineering*, 2013, 38(4): 701–717. doi: 10.1109/JOE.2013.2278787.

[8] STOJANOVIC M. On the relationship between capacity and distance in an underwater acoustic communication channel[J]. *ACM SIGMOBILE Mobile Computing and Communications Review*, 2007, 11(4): 34–43. doi: 10.1145/1347364.1347373.

[9] STOJANOVIC M and PREISIG J. Underwater acoustic communication channels: Propagation models and statistical characterization[J]. *IEEE Communications Magazine*, 2009, 47(1): 84–89. doi: 10.1109/MCOM.2009.4752682.

[10] LI Baosheng, ZHOU Shengli, STOJANOVIC M, *et al*. Multicarrier communication over underwater acoustic channels with nonuniform doppler shifts[J]. *IEEE Journal of Oceanic Engineering*, 2008, 33(2): 198–209. doi: 10.1109/JOE.2008.920471.

[11] JIANG Shengming. On securing underwater acoustic networks: A survey[J]. *IEEE Communications Surveys & Tutorials*, 2019, 21(1): 729–752. doi: 10.1109/COMST.2018.2864127.

[12] WANG Qiu, DAI Hongning, LI Xuran, *et al*. Eavesdropping attacks in underwater acoustic networks[C]. The 10th International Conference on Information, Communications and Signal Processing (ICICS), Singapore, 2015: 1–5. doi: 10.1109/ICICS.2015.7459921.

[13] ZUBA M, SHI Zhijie, PENG Zheng, *et al*. Vulnerabilities of underwater acoustic networks to denial-of-service jamming attacks[J]. *Security and Communication Networks*, 2015, 8(16): 2635–2645. doi: 10.1002/sec.507.

[14] SAMIR M, KOWALSKI M, ZHOU Shengli, *et al*. An experimental study of effective jamming in underwater acoustic links[C]. The 11th International Conference on Mobile Ad Hoc and Sensor Systems, Philadelphia, USA, 2014: 737–742. doi: 10.1109/MASS.2014.80.

[15] GOETZ M, AZAD S, CASARI P, *et al*. Jamming-resistant multi-path routing for reliable intruder detection in underwater networks[C]. The Sixth ACM International Workshop on Underwater Networks, Seattle, USA, 2011: 10. doi: 10.1145/2076569.2076579.

[16] CAMPAGNARO F, TRONCHIN D, SIGNORI A, *et al*. Replay-attack countermeasures for underwater acoustic networks[C]. The Global Oceans 2020: Singapore – U. S. Gulf Coast, Biloxi, USA, 2020: 1–9. doi: 10.1109/IEEECONF38699.2020.9389259.

[17] 张俊清. 水声网络协议干扰技术研究[D]. [硕士论文], 中国舰船研究院, 2017.
ZHANG Junqing. Research on protocol interferences against underwater acoustic network[D]. [Master dissertation], China Ship Research and Development Academy, 2017.

[18] ZHANG Junqing, ZHANG Gangqiang, and LIU Junkai. Wormhole attack detecting in underwater acoustic communication networks[C]. 2021 OES China Ocean Acoustics (COA), Harbin, China, 2021: 647–650. doi: 10.1109/COA50123.2021.9519987.

[19] LI Hong, HE Yunhua, CHENG Xiuzhen, *et al*. Security and privacy in localization for underwater sensor networks[J]. *IEEE Communications Magazine*, 2015, 53(11): 56–62. doi: 10.1109/MCOM.2015.7321972.

[20] SU Zhong, LIN Chuang, REN Fengyuan, *et al*. Security mechanisms analysis of wireless sensor networks specific routing attacks[C]. 2006 First International Symposium on Pervasive Computing and Applications, Urumqi, China, 2006: 579–584. doi: 10.1109/SPCA.2006.297488.

[21] LI Xun, HAN Guangjie, QIAN Aihua, *et al*. Detecting sybil attack based on state information in underwater wireless sensor networks[C]. The 21st International Conference on Software, Telecommunications and Computer Networks, Split, Croatia, 2013: 1–5. doi: 10.1109/SoftCOM.2013.6671865.

[22] PENG Chunyan, DU Xiujuan, LI Keqin, *et al*. An ultra-lightweight encryption scheme in underwater acoustic networks[J]. *Journal of Sensors*, 2016, 2016: 8763528. doi: 10.1155/2016/8763528.

[23] 刘俊凯, 董阳泽, 张刚强. 隐蔽通信中基于水声信道的密钥生成技术[J]. 应用声学, 2019, 38(4): 681–687. doi: 10.11684/j.issn.1000-310X.2019.04.027.
LIU Junkai, DONG Yangze, and ZHANG Gangqiang. Key generation technology based on underwater acoustic channel estimation in covert communication[J]. *Journal of Applied Acoustics*, 2019, 38(4): 681–687. doi: 10.11684/j.issn.1000-310X.2019.04.027.

[24] DIAMANT R, CASARI P, and TOMASIN S. Cooperative authentication in underwater acoustic sensor networks[J]. *IEEE Transactions on Wireless Communications*, 2019, 18(2): 954–968. doi: 10.1109/TWC.2018.2886896.

[25] DU Jiaxin, HAN Guangjie, LIN Chuan, *et al*. ITrust: An anomaly-resilient trust model based on isolation forest for underwater acoustic sensor networks[J]. *IEEE Transactions on Mobile Computing*, 2022, 21(5): 1684–1696. doi: 10.1109/TMC.2020.3028369.

[26] 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. doi: 10.1109/TVT.2020.2999566.

[27] HE Yu, HAN Guangjie, JIANG Jinfang, *et al*. A trust update mechanism based on reinforcement learning in underwater acoustic sensor networks[J]. *IEEE Transactions on Mobile Computing*, 2022, 21(3): 811–821. doi: 10.1109/TMC.2020.3020313.

[28] DAS A P, THAMPI S M, and LLORET J. Anomaly detection in UASN localization based on time series analysis and fuzzy logic[J]. *Mobile Networks and Applications*, 2020, 25(1): 55–67. doi: 10.1007/s11036-018-1192-y.

[29] MOOSAVI H and BUI F M. A game-theoretic framework for robust optimal intrusion detection in wireless sensor networks[J]. *IEEE Transactions on Information Forensics and Security*, 2014, 9(9): 1367–1379. doi: 10.1109/TIFS.2014.2332816.

[30] IOANNOU C, VASSILIOU V, and SERGIOU C. An intrusion detection system for wireless sensor networks[C].

The 24th International Conference on Telecommunications (ICT), Limassol, Cyprus, 2017: 1–5. doi: 10.1109/ICT.2017.7998271.

[31] SUN Bo, SHAN Xuemei, WU Kui, *et al*. Anomaly detection based secure in-network aggregation for wireless sensor networks[J]. *IEEE Systems Journal*, 2013, 7(1): 13–25. doi: 10.1109/JSYST.2012.2223531.

[32] BAO Fenye, CHEN I R, CHANG M, *et al*. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection[J]. *IEEE Transactions on Network and Service Management*, 2012, 9(2): 169–183. doi: 10.1109/TCOMM.2012.031912.110179.

[33] DARGAHI T, JAVADI H H S, and SHAFIEI H. Securing underwater sensor networks against routing attacks[J]. *Wireless Personal Communications*, 2017, 96(2): 2585–2602. doi: 10.1007/s11277-017-4313-1.

[34] MURGOD T R and SUNDARAM S M. Cluster based detection and reduction techniques to identify wormhole attacks in underwater wireless sensor networks[J]. *International Journal of Advanced Computer Science and Applications* (*IJACSA*), 2020, 11(7): 58–63. doi: 10.14569/IJACSA.2020.0110708.

[35] HAN Guangjie, LIU Li, JIANG Jinfang, *et al*. A collaborative secure localization algorithm based on trust model in underwater wireless sensor networks[J]. *Sensors*, 2016, 16(2): 229. doi: 10.3390/s16020229.

[36] DELCOURT M and LE BOUDEC J Y. TDOA source-localization technique robust to time-synchronization attacks[J]. *IEEE Transactions on Information Forensics and Security*, 2020, 16: 4249–4264. doi: 10.1109/tifs.2020.3001741.

[37] XU Bo, LI Shengxin, RAZZAQI A A, *et al*. A novel measurement information anomaly detection method for cooperative localization[J]. *IEEE Transactions on Instrumentation and Measurement*, 2021, 70: 3516918. doi: 10.1109/TIM.2021.3077981.

[38] ZHAO Haiyan, YAN Jing, LUO Xiaoyuan, *et al*. Privacy preserving solution for the asynchronous localization of underwater sensor networks[J]. *IEEE/CAA Journal of Automatica Sinica*, 2020, 7(6): 1511–1527. doi: 10.1109/JAS.2020.1003312.

[39] MISRA S, OJHA T, and MADHUSOODHANAN P. SecRET: Secure range-based localization with evidence theory for underwater sensor networks[J]. *ACM Transactions on Autonomous and Adaptive Systems*, 2020, 15(1): 2. doi: 10.1145/3431390.

[40] XU Ming, LIU Guangzhong, ZHU Daqi, *et al*. A cluster-based secure synchronization protocol for underwater wireless sensor networks[J]. *International Journal of Distributed Sensor Networks*, 2014, 10(4): 398610. doi: 10.1155/2014/398610.

[41] HU Fei, MALKAWI Y, KUMAR S, *et al*. Vertical and horizontal synchronization services with outlier detection in underwater acoustic networks[J]. *Wireless Communications and Mobile Computing*, 2008, 8(9): 1165–1181. doi: 10.1002/wcm.559.

[42] 李挺, 冯勇. 无线传感器网络安全路由研究综述[J]. 计算机应用研究, 2012, 29(12): 4412–4419. doi: 10.3969/j.issn.1001-3695.2012.12.003.

LI Ting and FENG Yong. Survey on secure routing research in wireless sensor networks[J]. *Application Research of Computers*, 2012, 29(12): 4412–4419. doi: 10.3969/j.issn.1001-3695.2012.12.003.

[43] MENON V, MIDHUNCHAKKARAVARTHY D, JOHN S, *et al*. A secure and energy-efficient opportunistic routing protocol with void avoidance for underwater acoustic sensor networks[J]. *Turkish Journal of Electrical Engineering and Computer Sciences*, 2020, 28(4): 2303–2315. doi: 10.3906/elk-2001-51.

[44] BHARAMAGOUDRA M R and MANVI S S. Agent-based secure routing for underwater acoustic sensor networks[J]. *International Journal of Communication Systems*, 2017, 30(13): e3281. doi: 10.1002/dac.3281.

[45] 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. doi: 10.1109/ACCESS.2020.3000863.

[46] NGUYEN N T, LE T T T, NGUYEN H H, *et al*. Energy-efficient clustering multi-hop routing protocol in a UWSN[J]. *Sensors*, 2021, 21(2): 627. doi: 10.3390/s21020627.

苏毅珊：男，博士，副教授，研究方向为计算机网络与传感器网络、水声通信与水下网络等.

张贺贺：女，硕士生，研究方向为水下无线传感器网络安全等.

张　瑞：男，博士，副教授，研究方向为水下网络等.

马素雅：女，硕士，研究方向为水下无线传感器网络安全等.

范　榕：女，博士生，研究方向为物理层通信和水下传感器网络安全等.

付晓梅：女，博士，教授，研究方向为声呐信号处理、水下通信与导航、信息安全等.

金志刚：男，博士，教授，研究方向为无线网络与网络安全、水下通信与网络、智能电网与能源互联网等.

责任编辑：马秀强