Journal of Computer Applications
计算机应用,2013,33(5):1208 - 1211
ISSN 1001-9081
CODEN JYIIDU
2013-05-01
http://www.joca.cn

文章编号:1001 - 9081(2013)05 - 1208 - 04
doi:10.3724/SP.J.1087.2013.01208

基于信任机制的水下传感器网络节点安全定位算法

张　尧[1],金志刚[1*],罗咏梅[2],杜秀娟[3]
(1.天津大学 电子信息工程学院,天津 300072;　2.天津大学 计算机科学与技术学院,天津 300072;
3.青海师范大学 计算机学院,西宁 810008)
(*通信作者电子邮箱 zgjin@tju.edu.cn)

摘　要:为了及时检测出水下传感器网络(UWSN)定位系统中的恶意锚节点,提出一种基于信任机制的节点安全定位算法。算法结合簇结构和信任机制,根据锚节点提供的位置信息采用 Beta 分布作出初步信任评价,并可根据需要调整信任更新权重。为了降低了水声信道的不稳定性对信任评价过程的影响,同时识别恶意锚节点的信任欺骗行为,提出信任过滤机制(TFM),对直接信任值进行差异量化,由簇头节点决定各锚节点是否可信。仿真结果表明所提算法适用于水下传感器网络,并且能够及时识别恶意锚节点,在定位系统的精确度和安全性方面都有很大提升。

关键词:水下传感器网络;安全定位;节点捕获;入侵检测;信任机制
中图分类号:TP393　　**文献标志码**:A

Node secure localization algorithm in underwater sensor network based on trust mechanism

ZHANG Yao[1], JIN Zhigang[1*], LUO Yongmei[2], DU Xiujuan[3]
(1. *School of Electronic and Information Engineering, Tianjin University, Tianjin* 300072, *China*;
2. *School of Computer Science and Technology, Tianjin University, Tianjin* 300072, *China*;
3. *School of Computer, Qinghai Normal University, Xining Qinghai* 810008, *China*)

Abstract: A new security localization algorithm based on trust mechanism was proposed to recognize the malicious beacon nodes timely in UnderWater Sensor Network (UWSN). According to the location information offered by the beacon nodes and combining cluster structure with trust mechanism, this algorithm used Beta distribution to form the initial trust value and the trust update weight could be set as required. In order to reduce the influence of the instability of underwater acoustic channel on the trust evaluation process, meanwhile, recognize the trust cheating of malicious beacon nodes, this algorithm proposed a mechanism named TFM (Trust Filter Mechanism), which calculated and quantized the trust value, and let the cluster head node decide whether each beacon node was credible or not. The results of simulation prove that the proposed algorithm is suitable for UWSNs and it can recognize malicious beacon nodes timely, and the accuracy and security of localization system are greatly improved.

Key words: UnderWater Sensor Network (UWSN); secure localization; node capture; intrusion detection; trust mechanism

0　引言

水下传感器网络(UnderWater Sensor Network,UWSN)节点定位技术的研究是一项理论和实践相结合的研究工作,由于无线电在水中衰减较快,UWSN 多采用声音作为通信媒介[1]。现有的 UWSN 定位算法可以分为距离无关(Range-free)算法和距离相关(Range-based)算法两大类[2],其中距离无关算法只能提供“粗精度”的节点定位,而对于大多数的 UWSN 应用需要精度较高的定位(如目标跟踪、潜艇探测等),因此多采用距离相关算法。总的来说,目前关于水下传感器网络中定位算法[3-7]的研究通常假设网络环境是安全可信的,忽略了开放性的网络结构以及物理信道对于定位安全的威胁。

然而,水下传感器网络的开放性和无人看守使得节点的定位过程极易受到来自敌方的恶意攻击,锚节点随时面临被捕获的危险,被捕获后形成的恶意节点可以得知网络密钥,发起多种恶意攻击,给出错误位置信息等[8],严重威胁定位系统的安全。

传统的密码体制对捕获攻击没有很好的对策,因此采取信任机制作为网络安全的一道屏障,通过对节点进行信任评价来识别网络中的恶意节点[9-10]。针对无线传感器网络(Wireless Sensor Network,WSN)中锚节点在定位过程中容易被捕获的威胁,Srinivasan 等[11]提出了一种基于分布式声誉机制的锚节点信任模型(Distributed Reputation-based Beacon Trust System,DRBTS),优点是算法简洁有效,不足之处为锚节点声誉更新算法过于简单,鲁棒性及精确度都较差。凌远景等[12]提出一种基于声誉机制的传感器网络安全定位算法,该算法结合分簇结构和声誉机制,投票机制采用的是大多数原则,算法简单易行。

但由于海水的流动、不同层次水面的反射以及不同深度

收稿日期:2012-11-19;**修回日期**:2012-12-18。
基金项目:国家自然科学基金资助项目(61162003,61202379);青海省科技项目(2012-Z-902)。
作者简介:张尧(1990 -),女,安徽合肥人,硕士研究生,主要研究方向:水下传感器网络安全;　金志刚(1972 -),男,上海人,教授,博士生导师,主要研究方向:计算机网络及信息安全;　罗咏梅(1974 -),重庆人,工程师,硕士,主要研究方向:网络信息系统;　杜秀娟(1970 -),女,河北藁城人,教授,博士,主要研究方向:无线网络、网络与信息安全。

的水下声速的不同,水下的声音通信与陆地无线电通信大不相同,存在严重的多普勒频移、长延时、低带宽等特点[13],这些因素对水下节点的定位算法精度和通信成功率会造成很大影响,因此以上算法在进行信任评价的过程中容易造成误判,导致检测成功率降低。

本文在文献[13]的基础上,结合距离界定技术[8]和 Beta 分布,初步得到锚节点的直接信任值。为了消除水下环境对信任评价过程的影响,同时检测出信任欺骗的恶意节点,提出信任过滤机制(Trust Filter Mechanism,TFM),针对同一锚节点的所有直接信任值进行差异量化,以锚节点给出的直接信任值的差异作为进一步筛选的依据。由簇头节点进行综合得到锚节点的全局信任值,并将全局信任值高于信任阈值节点放入可信节点列表中,可信节点列表仅在簇头节点间保存和传播,具有较好的安全性。

1　距离相关定位算法及安全挑战

1.1　水声通信的特点

由于无线射频信号(Radio Frequency)在水中有非常高的衰减率,因此利用卫星在水下实现类似全球定位系统(Global Positioning System,GPS)的定位系统并不可行。对比无线电波,声波在水中具有良好的传播特征,因此成为更加适合的水下通信载体。和陆地上的无线信道相比,水声信道具有如下几个特点:

1) 信号延时长(秒级)且不稳定;

2) 带宽窄(只有几百 kHz);

3) 具有严重多径效应、多普勒频移以及相位和幅度的震荡等信道特征;

4) 信道特征受到复杂海洋环境的影响,难以估计。

1.2　距离相关定位算法

在距离相关定位算法中,节点首先使用测距技术来估算它和锚节点之间的距离或夹角,然后再通过距离相关算法计算未知节点的位置。常用算法包括三边测量(trilateration)、三角测量(triangulation)或极大似然估计(multilateration)等[2]。

主要的测距技术包括到达角度(Angle of Arrival, AoA)、接收信号强度指示(Received Signal Strength Indicator,RSSI)、到达时间(Time of Arrival, ToA)和到达时间差(Time Difference of Arrival,TDoA)。这些技术在陆上无线传感器网络的节点定位技术中得到了广泛应用,但是水声信道的特征对这些测距技术的应用产生了许多不利的影响。

1.3　安全挑战

针对距离相关定位算法的攻击主要发生在位置关系的测量与估算阶段,攻击的目标通常是锚节点或传输信标报文的无线链路[8]。由于锚节点在距离相关定位算法中的重要地位以及水下环境的开放性,针对锚节点的捕获攻击对整个定位系统的安全具有很大威胁。

被捕获后形成的恶意锚节点的行为主要有两类[15],一类是直接恶意行为,包括给出虚假位置信息、在利用测量呼叫-应答报文往返时间计算节点间距离的 ToA/TDoA 定位技术中,提前或者延迟发送响应报文以达到虚减或虚增节点距离的目的等;另一类是间接恶意行为,指通过故意降低正常锚节点的信任值或者提高恶意锚节点信任值影响网络正常运行,即信任欺骗行为[14]。

通常信任机制在检测恶意节点时没有考虑第二类行为[9-10],而这类行为往往对于信任决策的正确性有很大影响,需要引起足够的重视。

2　基于信任机制的水下传感器节点安全定位

本文引入信任机制的主要目的是:1) 把恶意锚节点从系统中检测孤立出来;2) 通过信任机制使得普通传感器节点根据簇头节点判断后选择可信度高的锚节点来实现自身定位,提高定位的准确性和安全性。

基于信任机制的安全定位算法流程如图 1 所示,普通传感器节点根据簇头节点的判断选择可信列表中的锚节点实现自身定位,可信节点列表仅在簇头节点间保存和传播,具有较好的安全性。

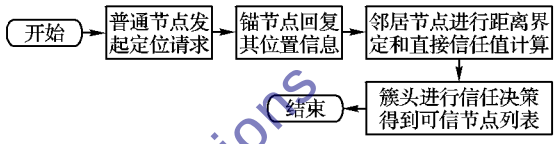

图 1　基于信任机制的安全定位算法流程示意图

2.1　距离界定和直接信任值计算

2.1.1　距离界定

假设锚节点 i 已知自身位置坐标(x,y),监听到锚节点 j 广播其自身位置信息为(x',y')后,使用响应报文中的坐标计算两点间的距离并与测量距离进行比较,如式(1)所示,以判断误差是否在允许的范围之内。如果超过了最大测距误差,则表明 j 节点有可能发送了虚假的信标节点位置信息。

但是正如前文提到,水下环境复杂多变,定位误差超过阈值有可能是因为外界环境导致,因此不能以此为单纯信任评价标准,故引入信任过滤机制,后面会详细描述。

$$\left| \sqrt{(x-x')^2+(y-y')^2} - d \right| \geqslant \theta_{th} \tag{1}$$

其中:d 为测量距离,θ_{th} 为最大测距误差。

2.1.2　直接信任值计算

根据距离界定情况用 s 和 f 表示一次观察的结果,其中 $s=1$ 表示该次广播的位置信息是准确的,认为节点 i 和节点 j 交互成功,否则 $f=1$,TR_{ij} 表示由节点 i 评价节点 j 得到的直接信任值。根据贝叶斯理论,节点 i 和节点 j 交互成功的概率密度函数可以用 Beta 分布函数表示如下:

$$f_{p|\alpha,\beta} = \frac{1}{B_{\alpha,\beta}} p^{\alpha-1}(1-p)^{\beta-1};\ 0 \leqslant p \leqslant 1, \alpha > 0, \beta > 0 \tag{2}$$

其中:$B_{\alpha,\beta} = \int_0^1 x^{\alpha-1}(1-x)^{\beta-1}\,dx$,并且

$$B_{\alpha,\beta} = \frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)} \tag{3}$$

将式(3)代入式(2)可得:

$$f_{p|\alpha,\beta} = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1} \tag{4}$$

其中:$\Gamma(\cdot)$ 为 Gamma 函数,$\alpha = s+1$,$\beta = f+1$。

节点 i 对节点 j 的信任评价就是与节点 j 交互成功的概率,因此节点 i 对节点 j 的直接信任值 TR_{ij} 就是 Beta 分布的期望值:

$$TR_{ij} = E(p) = \alpha/(\alpha+\beta) \tag{5}$$

又因为 $\alpha = s + 1, \beta = f + 1$，所以式(5)又可以表示为

$$TR_{ij} = E(p) = (s+1)/(s+f+2) \tag{6}$$

由式(6)可以看出，节点 i 和节点 j 交互成功的概率与参数 p 无关，而与 s 和 f 值紧密相关。当 $s = f$ 时，$TR_{ij} = 0.5$，此时信息熵最大，因此节点 i 很难决定节点 j 的可信度；当 $s > f$ 时，$TR_{ij} > 0.5$，表明节点 j 可信度较高，TR_{ij} 值越高，节点 j 的可信度越高；当 $s < f$ 时，结论正相反。

2.2 直接信任值的更新

为了保证直接信任值及时准确地更新，新的信任值由过去的信任值和最近的交互记录决定，通过对二者设置不同的权重可以实现不同的目的。

在本文中，信任更新的权重是根据最近的交互记录动态 Δs 和 Δf 选择的。在 t_{n+1} 时刻，节点 i 利用近期信任证据对 t_n 时刻的历史信任证据 s_n 和 f_n 进行更新，得到 t_{n+1} 时刻的信任证据 s_{n+1} 和 f_{n+1}，如式(7)所示：

$$\begin{cases} s_{n+1} = (1-\omega_{new}) \cdot s_n + \omega_{new} \cdot \Delta s \\ f_{n+1} = (1-\omega_{new}) \cdot f_n + \omega_{new} \cdot \Delta f \end{cases} \tag{7}$$

其中 ω_{new} 为信任更新权重，根据式(8)动态选择其大小。

$$\omega_{new} = \begin{cases} \omega_h, & \Delta s < \Delta f \\ \omega_l, & \Delta s \geqslant \Delta f \end{cases} \tag{8}$$

从式(7)、式(8)中可以看出，当近期交互成功率较高时，ω_{new} 取值为 $\omega_h (0.5 \leqslant \omega_h < 1)$，即过去的信任值为主，更新值为辅，目的为防止恶意节点通过伪装和欺骗快速提升自己的信任值；当近期交互成功率较低时，ω_{new} 取值为 $\omega_l (0 < \omega_l \leqslant 0.5)$，即过去的信任值为辅，更新值为主，目的是实现对恶意行为的惩罚。

2.3 信任分级和信任过滤机制

正如前文提到，由于水下环境较为复杂，定位误差较大，单纯根据锚节点提供的位置信息很难判定节点是否可信，并且单纯根据直接信任值高低决定节点可信无法抵御恶意节点的信任欺骗行为。因此，本文提出信任过滤机制，通过判断节点间的信任值差异来排除外界因素对信任评价的影响，同时识别信任欺骗行为，使评价结果更准确。在 TFM 中，设评价节点为 i，被评价节点为 j，TR_{ij} 表示节点 i 对节点 j 的直接信任值，TR_j 表示节点 j 的全局信任值。将直接信任值划分为 5 个等级，映射关系如表 1 所示。TR_j 的计算方法如式(9)所示，其中 A 代表对节点 j 进行信任评价的节点集合。

$$TR_j = \sum_{i \in A} (R_i \times TR_{ij}) \Big/ \sum_{i \in A} R_i \tag{9}$$

表 1 信任值分级

直接信任值	信任等级 R_i
(0,0.2]	1
(0.2,0.4]	2
(0.4,0.6]	3
(0.6,0.8]	4
(0.8,1)	5

正如前文提到，直接信任值的高低并不能直接代表节点的可信度，故引入矛盾因子 C_i：

$$C_i = \frac{1}{|A|} \sum_{i \in A} d(TR_{ij}, TR_j) \tag{10}$$

其中：A 表示对节点 j 进行信任评价的节点集合，$d(\cdot,\cdot)$ 是用距离来衡量差异。图 2 所示为迭代过程，其中 C_{imax} 代表所有节点矛盾因子的最大值，C_{th} 代表矛盾阈值。矛盾因子最大的节点将被标记，如果其矛盾因子大于阈值 C_{th}，则拉入黑名单，并取消其下一轮评价资格。每一轮迭代完成后，在没有被拉入黑名单的节点中重新计算 TR_j 的值，进入第二次迭代，依次进行下去，当所有评价节点的矛盾因子值都低于阈值时，停止迭代。

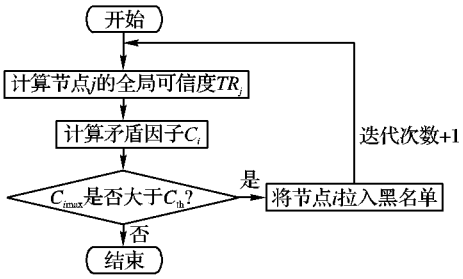

图 2 TFM 迭代过程

2.4 簇头节点的判断策略

本文簇头节点的判断策略基于以下假设前提：1）由于具体的分簇及簇头选取策略不在本文研究范围内，假设传感器网络中一定范围内簇头节点已经存在；2）簇头节点是由能量充足、计算能力强大的锚节点担任的，并假设其可信。

图 3 所示为簇头节点的决策流程。锚节点在互相进行信任评价时，将评价结果以信任条目形式发送给簇头节点，信任条目形式为〈*Source_ID*, *Dest_ID*, TR_{ij}〉，其中 *Source_ID* 代表信任评价者，*Dest_ID* 代表被评价者，并假设节点 ID 为全网唯一，T 代表信任阈值。簇头收集小范围内锚节点的信任条目后进行信任过滤，得到可信节点列表，并选择其中信任值高的锚节点广播给普通传感器节点。可信节点列表仅在簇头节点内保存并传播，具有较好的安全性。簇头节点对其传播范围内普通传感器节点的定位情况进行汇总，同时监督传感器节点的定位情况，从而达到更好的定位效果，并在很大程度上缓解了对水面基站的依赖。

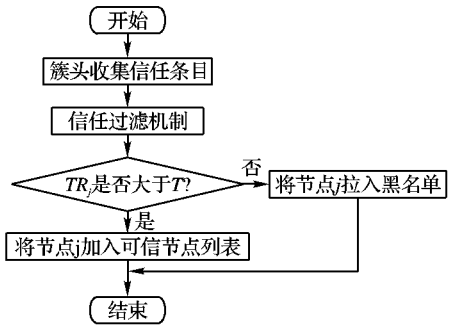

图 3 簇头节点的决策流程

3 仿真结果和性能分析

为了评估本文方案的性能，分别采用基于 NS-2 的 Aquasim[16] 和 Matlab 进行仿真和性能测试。实验场景设置如下：100 个节点随机分布在 100 m × 100 m 的监测区域，其中锚节点数目为 20。节点通信半径为 25 m。信任更新周期为10 s，矛盾阈值 C_{th} 设为 0.07，信任阈值 T 为 0.7。仿真时长为 500 s，同时为了得到更加客观的仿真结果，重复运行 1 000 次并统计结果。

实验中将锚节点分为恶意节点和诚实节点，W 为恶意锚节点数在总节点数中所占比例。恶意节点从 $t = 0$ 开始实行第 1.3 节中的两类攻击行为，并且同一恶意节点只进行一类恶

意攻击;诚实节点在所有交互周期中很少有欺骗行为。

算法的安全性通过恶意锚节点检测成功率和定位误差来衡量。检测成功率同时也反映了漏报率和误检率,检测成功率越高,代表漏报率和误检率越低,检测方法越可靠。定位误差定义为待定位节点经定位算法的估计坐标与其实际坐标位置间的距离与节点的通信半径值的比值。

图 4 所示为本文方案与文献[12]方案在不同 W 值下对锚节点捕获攻击的检测成功率的对比。可以看出针对不同的 W 值,本文方案的检测成功率最终都能够达到 90% 左右,而文献[12]方案的检测成功率受到恶意节点比例影响很大,从 W = 10% 时的80% 左右到 W = 20% 时的55% 左右,最后到 W = 30% 时的不到 40%。这是由于在文献[12]方案中,没有考虑到节点的低信任值可能是由于恶意节点的恶意诽谤,高信任值可能来自恶意推荐,同时,由于水下环境的影响,可能造成较大的定位误差,因此仅根据锚节点发送的位置信息进行信任评价结果不够准确;并且随着恶意节点比例的增加,漏报率和误检率越高,检测成功率也就越低。而在本文方案中采用了信任过滤机制,大大消除了恶意诽谤及恶劣信道的影响,因此检测成功率几乎不受恶意节点比例的影响,检测效果较好。

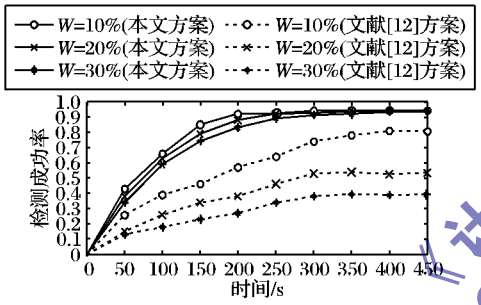

图 4　检测成功率对比

图 5 所示为不同 W 值下应用不同方案以及无信任方案的系统相对定位误差对比。随着恶意锚节点比例的增加,系统相对定位误差不可避免地增大。但在相同的恶意锚节点比例下,本文方案与文献[12]方案相比,相对定位误差可以降低 25% ~33%,且较稳定。这是由于算法引入信任过滤机制,很大程度上提高了恶意锚节点检测的准确率,从而提高了定位精度。应用本文方案后,与无信任方案相比,在恶意锚节点比例较高情况下可以将相对定位误差降低 50% 左右。可以看出,应用本文方案后,通过及时识别被捕获锚节点,过滤错误位置信息,大大提高了定位系统的安全性和鲁棒性。

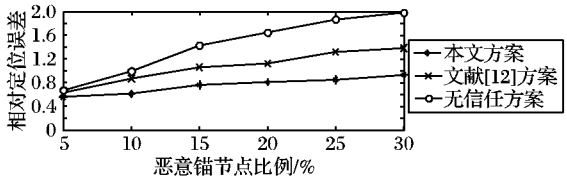

图 5　恶意锚节点比例对相对定位误差的影响

4　结语

不同于以往的定位算法往往假设锚节点全部可信,本文提出了一种基于信任机制的水下传感器网络节点安全定位算法,主要是针对恶意锚节点的检测。该算法中根据锚节点提供的位置信息,采用 Beta 分布对锚节点的信任值进行初步计算,计算方法简单有效,并通过信任过滤机制减少了恶劣水下环境对信任评价准确度的影响,能有效抵御信任欺骗行为。同时,簇头节点对其传播范围内普通传感器节点的定位情况进行汇总,同时监督传感器节点的定位情况,达到更好的定位效果,在很大程度上缓解了对水面基站的依赖,提高了定位的精度及系统鲁棒性。在系统中存在恶意锚节点的情况下,仍能保证较低的定位误差。在未来的工作中,将讨论定位安全算法和分簇结构的高能效结合,并且考虑引入节点移动对定位安全算法的影响。

参考文献:

[1] 李淑秋, 李启虎, 张春华. 水下声学传感器网络的发展和应用[J]. 物理, 2006, 35(11): 945 – 952.

[2] 黎作鹏, 蔡绍滨, 张菁, 等. 水声传感器网络节点定位技术综述[J]. 小型微型计算机系统, 2012, 33(3): 442 – 447.

[3] CHENG X Z, SHU H N, LIANG Q L, *et al*. Silent positioning in underwater acoustic sensor networks[J]. IEEE Transactions on Vehicular Technology, 2008, 57(3): 1756 – 1766.

[4] KIM E, LEE S, KIM C, *et al*. Long-range beacons on sea surface based 3D-localization for underwater sensor networks[C] // Proceedings of the 5th International Conference on Mobile Ad-Hoc and Sensor Networks. Piscataway: IEEE, 2009: 102 – 107.

[5] EROL M, VIERA L F M, GERLA M. Localization with Dive'N'rise (DNR) beacons for underwater acoustic sensor networks [C] // WuWNet '07: The Second ACM International Workshop on Underwater Networks. New York: ACM, 2007: 97 – 100.

[6] EROL M, VIEIRA L F, GERLA M. AUV-aided localization for underwater sensor networks[C] // Proceedings of International Conference on Wireless Algorithms, Systems and Applications. Piscataway: IEEE, 2007: 44 – 54.

[7] LUO H-J, ZHAO Y-Y, GUO Z-W. UDB: using directional beacons for localization in underwater sensor network[C] // Proceedings of the 14th IEEE International Conference on Parallel and Distributed Systems. Piscataway: IEEE, 2008: 551 – 556.

[8] 曹晓梅, 俞波, 陈贵海, 等. 传感器网络节点定位系统安全性研究[J]. 软件学报, 2008, 19(4): 869 – 877.

[9] BAO F Y, CHEN I-R, CHANG M J. Trust-based intrusion detection in wireless sensor networks[C] // Proceedings of 2011 IEEE International Conference on Communications. Piscataway: IEEE, 2011: 1 – 6.

[10] 康松林, 王彦东, 李慧. 信任模型在无线传感器网络入侵检测中的应用[J]. 计算机工程与应用, 2012, 48(5): 89 – 92.

[11] SRINIVASAN A, TEITELBAUM J, WU J. DRBTS: Distributed reputation-based beacon trust system [C] // Proceedings of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing. Piscataway: IEEE, 2006: 277 – 283.

[12] 凌远景, 叶阿勇, 许力, 等. 基于声誉机制的传感器网络节点安全定位算法[J]. 计算机应用, 2012, 32(1): 70 – 73.

[13] URICK R J. Principles of underwater sound [M]. New York: McGraw-Hill, 1983.

[14] 荆琦, 唐礼勇, 陈钟. 无线传感器网络中的信任管理[J]. 软件学报, 2008, 19(7): 1716 – 1730.

[15] CONG Y P, YANG G, WEI Z Q, *et al*. Security in underwater sensor network[C] // Proceedings of 2010 International Conference on Communications and Mobile Computing. Piscataway: IEEE, 2010: 162 – 168.

[16] XIE P. Aqua-Sim: An NS-2 based simulator for underwater sensor networks[C] // OCEANS 2009: MTS/IEEE Biloxi-Marine Technology for Our Future: Global and Local Challenges. Piscataway: IEEE, 2009: 26 – 29.