软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2014,25(Suppl.(1)):39−46

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于量子隐形传态的水下传感器网络分级加密通信协议*

马鸿洋[1,2], 范兴奎[2], 王淑梅[2], 董玉民[2]

[1](中国海洋大学 信息科学与工程学院,山东 青岛 266100)

[2](青岛理工大学 理学院,山东 青岛 266033)

通讯作者: 马鸿洋, E-mail: hongyang_ma@aliyun.com

摘 要: 针对水下传感器网络中通信信息安全性与水声信道通信特性的不足,提出了一种基于量子隐形传态的水下传感器网络分级加密通信协议.一级在水面基站与自由水下航行器之间,采用量子隐形传态实现两者之间共享量子密钥,利用纠缠关联空间非定域性保证其通信信息安全性;二级在水下节点到水下自由航行器之间,采用对称加密算法实现两者之间信息的加密传输,利用对称加密快捷的优点提高其通信信息效率.分别对量子攻击、经典攻击及通信效率这 3 个方面进行了分析,证明该协议能有效防止量子态截获、重构、替换等攻击.

关键词: 水下传感器;量子隐形传态;量子通信;安全

中文引用格式: 马鸿洋,范兴奎,王淑梅,董玉民.基于量子隐形传态的水下传感器网络分级加密通信协议.软件学报,2014,25(Suppl.(1)):39−46. http://www.jos.org.cn/1000-9825/14005.htm

英文引用格式: Ma HY, Fan XK, Wang SM, Dong YM. Secure hierarchical hybrid encryption communication protocol based on quantum teleportation for underwater sensor networks. Ruan Jian Xue Bao/Journal of Software, 2014,25(Suppl.(1)):39−46 (in Chinese). http://www.jos.org.cn/1000-9825/14005.htm

Secure Hierarchical Hybrid Encryption Communication Protocol Based on Quantum Teleportation for Underwater Sensor Networks

MA Hong-Yang[1,2], FAN Xing-Kui[2], WANG Shu-Mei[2], DONG Yu-Min[2]

[1](College of Information Science and Engineering, Ocean University of China, Qingdao 266100, China)

[2](School of Sciences, Qingdao Technological University, Qingdao 266033, China)

Corresponding author: MA Hong-Yang, E-mail: hongyang_ma@aliyun.com

Abstract: In order to overcome the shortcomings of underwater sensor network communication security and the characteristics of the underwater acoustic communication channel, this paper proposes a secure hierarchical hybrid encryption communication protocol based on quantum teleportation for underwater sensor network. For the first layer in the communication of the surface station and autonomous underwater vehicle (AUV), the method achieves shared key transmission in the onshore sink and AUV by the application of quantum teleportation to ensure the security of the communication information by quantum nonlocality. For the second layer in the AUV and UW-sensor, it attains the underwater node to the autonomous underwater vehicle transmission information encryption using symmetric encryption algorithms to improve the efficiency of the communication by using the symmetric key. The paper analyzes quantum attack, classical attack and communication efficiency, and the proposed protocol can effectively prevent quantum intercepted attack, quantum reconstructive attack and quantum replacement attack.

Key words: underwater sensor network; quantum teleportation; quantum communication; security

水下传感器网络(underwater wireless sensor network)[1−6]是由数量众多水下节点通过声波通信方式所构成分布式自组织通信网,在海洋数据收集、水面环境监测、水下目标探索等方面具有广阔的应用前景.

* 基金项目: 国家自然科学基金(61173056, 11304174); 山东省高等学校科技计划(J11LG07); 青岛市科技计划基础研究项目(12-1-4-4-(6)-JCH)

收稿时间: 2014-05-10; 定稿时间: 2014-08-26

由于水下传感器网络的数据传输模式和水声信道所独有的特性(带宽受限、高时延、背景噪声大、多径效应、多普勒频散、时空高度变化等),表现出很多不同于陆地无线传感器网络的特点.由于海水复杂的物理条件,陆地无线传感器网络安全技术无法有效地移植应用到水下通信网络中,水下传感器网络安全技术研究仍处于起步阶段.文献[7]首先分析水下传感网络在通信过程中的威胁、攻击等安全问题,进一步提出了跨层次、高能效、自适应水下传感器网络安全架构模型.文献[8]针对水下传感器网络中非法锚节点定位的不足,提出了一种基于信任过滤方法的水下节点安全定位通信协议,仿真表明其对于定位精准度和安全性都有较大的提高.

为了适应水下传感器网络未来安全的发展需要,其安全技术必须在技术与理论方面有所突破,现在水下传感器网络采用的安全手段均是基于传统信息加密的复杂算法,需要采用新的技术与理论来增强其安全性.量子密钥是新兴安全加密技术,对信息加密不再依靠经典加密技术的复杂算法,而是依靠量子物理奇特性质——纠缠关联空间非定域性.量子密钥是目前公认的信息加密的终极保障手段,可提供理论上较高安全密钥分配方案.将量子密钥和水下传感器网络融合,构建新的加密通信协议是未来的发展趋势.其中,国外研究理论与实验成果层出不穷[9,10].文献[11]提出了基于量子隐形传态自组织通信网络路由通信方案,计算纠缠对的数目为路由度量值,利用量子纠缠和两端同时逼近的思路,实现任意两个通信节点的信息传输.文献[12]等提出了基于量子纠缠的跨中心三方通信安全通信协议,分析了协议的安全性,并证明了其有较高的通信效率,能够进一步扩展到多方量子通信.

本文提出了基于量子隐形传态的水下传感器网络分级混合加密协议,纠缠关联空间非定域性是水下传输的保证,能够最大限度地满足水下传感器安全通信的需求.本文第 1 节介绍水下传感器网络与量子隐形传态的相关知识.第 2 节阐述基于量子隐形传态的分级混合加密通信协议.第 3 节对通信协议安全性理论分析.第 4 节是结束语.

1 水下传感器网络与量子隐形传态的相关知识

1.1 水下传感器网络的相关知识

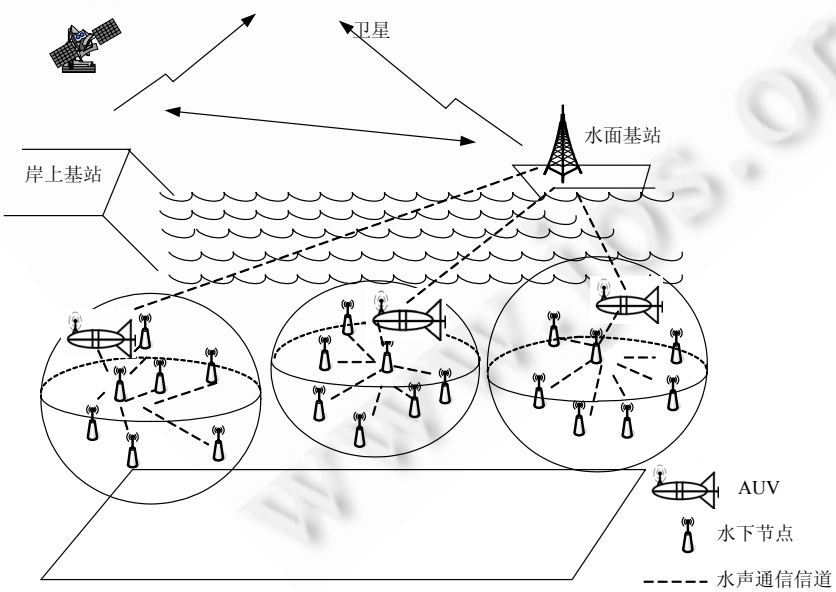

图 1 水下传感器网络混合三维动态网络模型

水下传感器网络通信设备:水下节点、水下自由航行器(autonomous underwater vehicle,简称 AUV)、水面基站、岸上基站等.其中,水下节点将采集的温度、密度、盐度、酸度等数据,通过 AUV 发送给水面基站,再通过无线电通信发送给岸上基站.

水下传感器网络的通信模型:静态网络模型、二维动态网络模型、三维动态网络模型、混合三维动态网络模型.其中,静态网络是水下节点部署在确定位置,而且无法移动;二维动态网络结构是水下节点锚在海底,可以有限区域的活动;三维动态网络结构是水下节点能够悬浮在水中不同深度;混合三维动态网络是水下节点相对静止,但 AUV 可以在较大区域内活动,如图 1 所示.

水下传感器网络通信的特点是:无线电磁波在海水中传播时能量衰减严重,而声波在海水中传播时衰减较小,能够传输较远的距离,目前水下节点与 AUV 之间,AUV 与水面基站之间主要采用声波通信方式.

1.2 量子隐形传态的参考模型

假设一定距离的甲、乙方,甲方拥有 qubit *a*,qubit *b*,乙方拥有 qubit *c*.其中,qubit *a* 表达式:$|\psi\rangle_a=\alpha|0\rangle_a+\beta|1\rangle_a$,$\alpha$ 与 β 之间关系满足 $|\alpha|^2+|\beta|^2=1$. 甲方拟将 qubit *a* 发送给乙方,步骤如下:

(1) 双方事先建立量子通信信道,即 qubit *b*,qubit *c* 构建一对纠缠的 qubit,其量子状态的表达式:

$$|\Phi\rangle^+=\frac{1}{\sqrt{2}}\left(|0\rangle_b|0\rangle_c+|1\rangle_b|1\rangle_c\right) \tag{1}$$

(2) 双方共同拥有的 qubit *a*,qubit *b*,qubit *b*,其构建的量子态为

$$\left(\alpha|0\rangle_a+\beta|1\rangle_a\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle_b|0\rangle_c+|1\rangle_b|1\rangle_c\right) \tag{2}$$

(3) 甲方对 qubit *a*,qubit *b* 进行 Bell 基测量,则式(2)变换为

$$\frac{1}{2}\left[\,|\Phi^+\rangle_{ab}\left(\alpha|0\rangle_c+\beta|1\rangle_c\right)+|\Phi^-\rangle_{ab}\left(\alpha|0\rangle_c-\beta|1\rangle_c\right)\,\right]+\frac{1}{2}\left[\,|\Psi^+\rangle_{ab}\left(\beta|0\rangle_c+\alpha|1\rangle_c\right)-|\Psi^-\rangle_{ab}\left(\beta|0\rangle_c-\alpha|1\rangle_c\right)\,\right] \tag{3}$$

其中,$|\Phi^\pm\rangle=\frac{1}{\sqrt{2}}\left(|00\rangle\pm|11\rangle\right)$,$|\Psi^\pm\rangle=\frac{1}{\sqrt{2}}\left(|01\rangle\pm|10\rangle\right)$,称为 Bell 基.

(4) 甲方随之通过量子通信信道,将测量信息发送给乙方.

(5) 乙方根据接受的测量信息选择合适的 Pauli 门处理信息,从而获得甲方传输的量子信息.例如,当甲方测量信息是 $|\Phi^+\rangle_{ab}$ 时,乙方应用 I 变换,获得甲方传输的量子信息;当甲方测量信息是 $|\Phi^-\rangle_{ab}$ 时,乙方应用 Z 变换,获得甲方传输的量子信息;当甲方测量信息是 $|\Psi^+\rangle_{ab}$ 时,乙方应用 X 变换,获得甲方传输量子信息;当甲方测量信息是 $|\Psi^-\rangle_{ab}$ 时,乙方应用–iY 变换,获得甲方传输的量子信息,见文献[13].其中,Pauli 门表达式为

$$I=\begin{bmatrix}1&0\\0&1\end{bmatrix},\ Z=\begin{bmatrix}1&0\\0&-1\end{bmatrix},\ X=\begin{bmatrix}0&1\\1&0\end{bmatrix},\ Y=\begin{bmatrix}0&-i\\i&0\end{bmatrix} \tag{4}$$

分析整个量子信息传输过程可知,甲方不用知晓乙方的具体地理位置,只要两方事先共享 qubit 对即可;该过程具有一定保密性,只有共享 qubit 对的乙方才能准确的恢复传输的量子信息.通过分析可知,量子隐形传态的优点有利于其在水下通信协议中实施.

2 基于量子隐形传态水下传感器网络分级混合加密协议

本协议所采用的通信模型为混合三维动态网络的改进模型,定义为基于量子隐形传态的水下传感器网络通信模型,如图 2 所示.该模型既考虑水下声波通信的要求,具备较好的传感器布放策略,满足水下节点获得最佳感知效果和通信覆盖率的需求,又考虑量子通信的要求,能实施量子隐形传态的通信,水面基站、AUV 能实现对量子态的发送、测量.其中,假设水面基站为可信方.

2.1 系统初始化

水下传感网有 3 个簇,每个簇由簇主节点、簇从节点组成,如图 2 所示.

簇主节点由能量充足、计算能力强的 AUV 担当,内置标识号 ID=0,负责量子纠缠态的制备,路由的生成、维护、信道分配等等;在离开水面基站下水之前,与水面基站共享 *N* 对量子纠缠态,*N*=64,其表达式为 $Q=\{|q_1\rangle,|q_2\rangle,...,|q_N\rangle\}$,其中,$|q_i\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle_b^i|1\rangle_c^i-|1\rangle_b^i|0\rangle_c^i\right)$,这样,水面基站拥有 qubit *b*,AUV 拥有 qubit *c*.

簇从节点由 *m* 个水下节点担任,内置标识号 *ID*=1,2,…,*m*,负责数据的采集、上传.对于水下节点 d_j 投放下水之前,水面基站预先放置分组密码 K_j (64 位),因分组密码是对称加密算法,对于加密和解密有较快的速度,并能减少水下节点存储空间的占用量.在水面基站中存在一个 64 位密钥库 *j*=1,2,…,*m*.每个水下节点初始 64 位密

钥均不同,这样可以避免某个水下节点被俘获后密钥的泄露,并且该密钥库在 AUV 上也配备.本协议对水下布网有较高要求,是水下密集传感器网络,需要随机投放大量的水下节点(包括冗余节点),而且水下节点之间至少被 1 个邻居水下节点所探测到,并能通过多跳模式互相声学通信;水下节点之间通信损耗与距离、频率等均有关系.

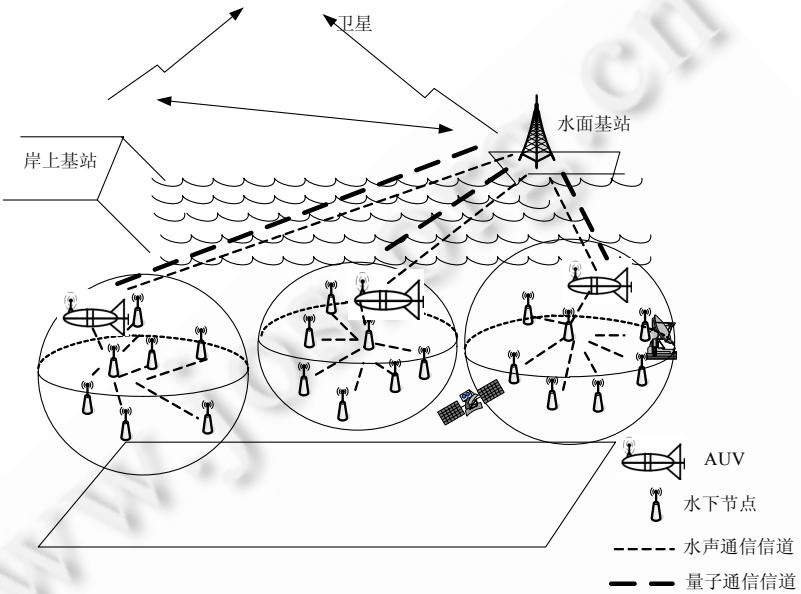

图 2 基于量子隐形传态的水下传感器网络通信模型

水面基站、AUV、水下节点三者之间的通信所使用的信道有量子通信信道与水声通信信道,量子通信信道是传输量子态的物理通路,用粗虚线表示;水声通信信道是使用声波传输“0”、“1”码的物理通路,用细虚线表示,水面基站与 AUV 采用量子隐形传态中的经典信息的传输采用声波通信,水下节点到 AUV 之间通信采用声波通信.

2.2 水面基站与自由水下航行器共享量子密钥

水面基站发送 N 个量子比特流作为与 AUV 的共享密钥,其中,第 i 个 qubit 表达式为 $|\psi\rangle_i=\alpha_i|0\rangle_a^i+\beta_i|1\rangle_a^i$,满足 $|\alpha_i|^2+|\beta_i|^2=1, i=1,\ldots,N, N=64$, 水面基站拥有 qubit a.

Qubit a,b,c 组成的量子态为式(2),其变形式为

$$|\Omega_i\rangle_{abc}=\frac{1}{2}\Big[\,|\Phi^+\rangle_{ab}\left(\alpha|0\rangle_c+\beta|1\rangle_c\right)+|\Phi^-\rangle_{ab}\left(\alpha|0\rangle_c-\beta|1\rangle_c\right)\Big]+\frac{1}{2}\Big[\,|\Psi^+\rangle_{ab}\left(\beta|0\rangle_c+\alpha|1\rangle_c\right)-|\Psi^-\rangle_{ab}\left(\beta|0\rangle_c-\alpha|1\rangle_c\right)\Big] \tag{5}$$

当水面基站测量信息 $|\Phi^+\rangle_{ab}$ 时,利用水声通信信道告知 AUV,则 AUV 应用 I 变换,获得水面基站传输过来的量子信息;同理,当水面基站测量信息 $|\Phi^-\rangle_{ab}$ 时,AUV 应用 Z 变换,获得传输过来的量子信息;当水面基站测量信息 $|\Psi^+\rangle_{ab}$ 时,AUV 应用 X 变换,获得传输过来的量子信息;当水面基站测量信息 $|\Psi^-\rangle_{ab}$ 时,AUV 应用–iY 变换,获得传输过来的量子信息.这样,根据纠缠关联空间非定域性,水面基站和 AUV 不需要获得之间的地理位置信息,却能利用量子纠缠对获得共享的 64 位密钥.

为了减轻下一步计算的复杂度,本协议没有采用 128 位密钥的模式.在实际的系统中,量子态采用的 Bell 测

量也有局限性,实际上只能区分 3 个 Bell 态,测量效率仅为 3/4,因此,在实际协议中使用 64 个纠缠对是远远不够的.假设纠缠对的正确率为 τ,则实际的纠缠对数量为 $\frac{64}{\tau}\times\frac{4}{3}$.

2.3 自由水下航行器生成水下网络拓扑结构

AUV 接受到 64 位密钥后,用密钥加密广播信息,利用自身携带的垂直收发器、水平收发器告知水下节点启动,并准备生成通信网络的拓扑结构.

水下节点 d_j 收到广播后根据事先与水面基站共享的密钥解密,并用密钥加密广播信息,其中包含 ID 及其他信息(节点之间的相对深度与距离、能量的数值).

AUV 接受并解密广播信息,构建路由表.该表包含周围水下节点的信息.对于密码解密错误的节点,将其 ID 列入黑名单.如果解密成功,则向该水下节点 d_j 回复应答信息,并携带一个伪随机数 R_j.

2.4 水下节点与AUV通信加密

水下节点 d_j 接受应答信息和伪随机数 R_j 后,用密钥 K_j 与伪随机数 R_j 对其采集到数据 M 进行分组加密,得到密文信息 C:$C=E_{K_j}(M|R_j)$.水下节点与 AUV 的通信是声信号,虽然声信号在海里传播时存在反射、折射、声影区等很多不足,但声信号在海水里有较为稳定的传播速度(大约为 1 530 m/s),所以传播时延是稳定和可计算的,这对于水下通信虽然不是最优方案却是可行方案.AUV 收到密文信息 C 后,进行逆向解密,$M=D_{K_j}(C|R_j)$,随之得到水下节点采集到数据.

2.5 AUV与水面基站通信加密

AUV 收集到簇内水下节点的信息,分组处理发送给水面基站,因此两者之间的通信安全特别重要.在这部分没有采用对称加密方案,因为对称加密易于被截获破解,会危及整个网络的安全.所以,这一部分的密钥是利用与水面基站共享的量子密钥加密,并上传到水面基站.

2.6 动态添加水下节点

假设水面基站又投放了一个水下节点,该节点在水中稳定后,需要将其采集的数据发送给水面基站,需要申请加入已有的网络.

水下节点广播请求信息,信息中包含自身 ID 及其他信息.该信息用与水面基站初始的对称密钥加密.AUV 接受到其请求信息后,根据 ID 号查询自身的密钥库,读取对应的密钥,再利用该密钥解密信息,如果解密成功,则该水下节点是合法节点,发送同意其加入的信息,并更新自身路由表.如果信息有异,则将其 ID 列入黑名单.

3 协议安全与通信效率分析

该协议存在的攻击有量子技术的攻击、经典技术的攻击,下面分别进行分析.

3.1 量子技术的攻击分析

(1) 窃听者截获 qubit a,b,c 共享态 $|\Omega_i\rangle_{abc}$.

根据式(5)可知水面基站的测量量子态有 4 种情况:$\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle)_{ab}$,$\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle)_{ab}$.窃听者要获得水面基站测量的准确信息,其概率只有 $p_1=\frac{1}{4}$.而本协议要求传输 64 次,所以窃听者获得准确信息的概率为 p_1^{64},并且在实际的测量设备中,测试次数还要远远大于 64,所以窃听者获得密钥的概率很低(接近是 0).

(2) 窃听者重构量子态,组建新的 GHZ 态.

窃听者、水面基站、AUV 构建由 qubit E,S,D 组成的 GHZ 态,其表达式:$|\psi\rangle=\frac{1}{\sqrt{2}}(|000\rangle-|111\rangle)_{SDE}$,见文献

[14].窃听者在 64 个量子比特中任意截取一个量子态,表达式为 $\left(\alpha_i|0\rangle+\beta_i|1\rangle\right)_a$, 则 4 个 qubit 构建的系统为

$$\begin{aligned}|\Omega\rangle_{aSDE}&=\left(\alpha_i|0\rangle+\beta_i|1\rangle\right)_a\otimes\frac{1}{\sqrt{2}}\left(|000\rangle-|111\rangle\right)_{SDE}\\&=\frac{1}{2}\Big[\ |\Psi^-\rangle_{aS}\left(-\beta_i|00\rangle_{DE}-\alpha_i|11\rangle_{DE}\right)+|\Psi^+\rangle_{aS}\left(\beta_i|00\rangle_{DE}-\alpha_i|11\rangle_{DE}\right)\Big]+\\&\quad\frac{1}{2}\Big[\ |\Phi^-\rangle_{aS}\left(\alpha_i|00\rangle_{DE}+\beta_i|11\rangle_{DE}\right)+|\Phi^+\rangle_{aS}\left(\alpha_i|00\rangle_{DE}-\beta_i|11\rangle_{DE}\right)\Big]\end{aligned}\tag{6}$$

由式(6)可知,水面基站使用 Bell 测量,AUV 与窃听者读取的量子态存在 4 种情况:

$$-\beta_i|00\rangle_{DE}-\alpha_i|11\rangle_{DE},\ \beta_i|00\rangle_{DE}-\alpha_i|11\rangle_{DE},\ \alpha_i|00\rangle_{DE}+\beta_i|11\rangle_{DE},\ \alpha_i|00\rangle_{DE}-\beta_i|11\rangle_{DE}.$$

窃听者获准确量子态信息的概率 $p_2=\frac{1}{4}$, 而且进一步获得传输的量子态必须在测量基 $\frac{|0\rangle\pm|1\rangle}{\sqrt{2}}$ 帮助下实现, 这一步采用正确测量基的概率 $p_3=\frac{1}{2}$, 见文献[15].所以,窃听者获得一个准确量子态的概率是 $p_4=p_2\times p_3$, 概率非常低.

(3) 窃听者替换量子态.

窃听者制备另外一组量子纠缠对,分别表示为 qubit a_1,b_1;窃听者能截获水面基站发送给 AUV 的 qubit b,并将 qubit b_1 发送给 AUV,这样替换了 AUV 本应获得的量子态,而水面基站、AUV 均不知道.但是 qubit a 与 qubit b_1 没有纠缠内在关系,在测量时通过关联性就可以知道该量子态被替换,所以窃听者替换量子态是不行的.

3.2 经典技术的攻击分析

(1) 该协议为分级密钥管理体系,水面基站与自由水下航行器采用量子隐形传态共享量子密钥,利用纠缠关联空间非定域性提高通信的安全性;水下节点到自由水下航行器利用预制的密钥对称加密,有效地提高通信效率.这种分级体系增强了网络的安全性,即使攻击者破解了某个水下节点,影响到与 AUV 的通信,但是 AUV 与水面基站的通信是通过量子密钥来加密实现的,其安全性有较强的保证.

(2) 在该协议中,每个水下节点通过水面基站预先分配一个共享密钥,用于合法身份的确认,保证了通信的安全性.当身份确认后,其会话密钥采用伪随机数协商生成,降低了密钥泄露的风险,增强了安全性.其中,水面基站为可信方,它与水下节点的预分配密钥是安全的.

3.3 通信效率分析

考虑到分级混合加密协议中系统初始化阶段,水下节点 $d_j(j=1,2,...,m)$ 到 AUV 之间的通信采用声波传速,可假设 AUV 生成水下网络拓扑结构以及水下节点与 AUV 通信加密一共所需要的时间为 T_1.海水中声通信的实际带宽是有限的,在 100 m~1×10^6 m 通信距离内,带宽在 1×10^5 Hz~1×10^3 Hz,本文设定是较为理想的直线传播,发散面是一个球面(不考虑反射、折射、柱面波形式).在水面基站与自由水下航行器共享量子密钥过程中,水面基站对 N=64 个量子比特密钥预处理时间为 $T_2=t_d$, 而在系统初始化阶段,本文设定系统可同时做好量子比特密钥的预处理,所以在计算这部分的通信时间延时可取 $T_2=0$.

水面基站将其量子比特依次发送一个水下自由航行器 A_v,A_v 是在 3 个簇的簇首中任选 ($v\in1,2,3$), 每个发送时延为 t_a; 从水面基站到水下自由航行器 A_v, 量子比特传播时延为 t_q; 水面基站将测量信息告知 AUV 时传播时延 t_p, 该信号通过声信号传输,通信时延较长. A_v 接收一个量子比特所需处理时间为 t_{pr}. 考虑各个 A_v 对信息处理能力的差异,处理时间 $t_{pr}=\max\{t_{prj}\}(v\in1,2,3)$, 其中包括不同量子门操作时间. A_v 发送确认帧 ACK 告知 AUV, ACK 发送时延为 t_b, 传播时延为 t_p.

该阶段成功发送一个量子比特所需时间 t_f(其中因量子隐形传态的瞬时性 t_q=0) 为

$$\begin{aligned}t_f&=t_a+t_q+t_p+t_{pr}+t_b+t_p\\&=t_a+t_b+2t_p+t_{pr}\end{aligned}\tag{7}$$

若不考虑 64 个量子比特通信时间重叠,则成功发送 64 个量子比特所需的时间 T(在该部分通信时间中 $t_p \neq 0$, 而且 t_p 是较大的数值)为

$$T = T_1 + 64\left(t_a + t_b + 2t_p + t_{pr}\right) \tag{8}$$

若考虑 64 个量子比特通信时间重叠,则存在传输时间的重叠,假设传输时间重叠 β,$0 \leqslant \beta < 1$, 则成功发送 64 个量子比特所需要的时间为 $T_f = T - \beta T$. 另外,设每个一个量子比特传输过程中出错及丢失概率均为 p,则发送 64 个量子比特通信时间为

$$T_3 = 64T_f + 64T_f \sum_{i=1}^{64} p^i.$$

由于测量设备等问题,在实际协议中需要构建的纠缠对会远远大于 64.在分级混合加密协议的情况下,正确传送一个量子比特所需的平均时间为

$$t_{av} = \frac{T_3}{64} = \frac{T(1-\beta)}{1-p} \tag{9}$$

在水面基站与自由水下航行器共享量子密钥过程中,量子密钥通信的最大吞吐量为

$$\lambda_{\max} = \frac{1}{t_{av}} = \frac{1-p}{T(1-\beta)} \tag{10}$$

所以,根据式(10)可知,要提高信道的吞吐量,在量子比特传输过程中出错及丢失概率是定值的情况下,需要增加 β 的数值.

4 结束语

本文提出了一种基于量子隐形传态的水下传感器网络分级加密通信协议.该协议分为水面基站与自由水下航行器之间,水下节点到自主水下航行器之间两级通信,其中,对于水面基站与自由水下航行器采用量子隐形传态共享量子密钥,利用纠缠关联空间非定域性提高通信的安全性;对于水下节点到自主水下航行器,利用对称加密算法提高通信的效率.本文仅从理论部分进行讨论,对其实验部分的研究还需继续深入.

References:

[1] Ren Y, Zadorozhny VI, Oleshchuk VA, Li FY. A novel approach to trust management in unattended wireless sensor networks. IEEE Trans. on Mobile Computing, 2014,13(7):1409−1423.

[2] Chao CM, Wang YZ, Lu MW. Multiple-Rendezvous multichannel MAC protocol design for underwater sensor networks. IEEE Trans. on Systems, Man, and Cybernetics: Systems, 2013,43(1):128−138.

[3] Zennaro D, Ahmad A, Vangelista L, Serpedin E, Nounou H, Nounou M. Network-Wide clock synchronization via message passing with exponentially distributed link delays. IEEE Trans. on Communications, 2013,61(5):2012−2024.

[4] Peng J, Hong CJ, Liu T, Zhang YY. Strategy of routing based on layered for underwater wireless sensor networks. Journal on Communications, 2014,35(6):25−31 (in Chinese with English abstract).

[5] Guo ZW, Luo HJ, Hong F, Yang M, Ni MX. Current progress and research issues in underwater sensor networks. Journal of Computer of Computer Research and Development, 2010,47(3):377−389 (in Chinese with English abstract).

[6] Hong L, Hong F, Li ZB, Guo ZW. CT-TDMA: Efficient TDMA protocol for underwater sensor networks. Journal on Communications, 2012,33(2):163−174 (in Chinese with English abstract).

[7] Wei ZQ, Yang G, Cong YP. Security of underwater sensor networks. Chinese Journal of Computers, 2012,35(8):1594−1606 (in Chinese with English abstract).

[8] Zhang Y, Jin ZG, Luo YM, Du XJ. Node secure localization algorithm in underwater sensor network based on trust mechanism. Journal of Computer Applications, 2013,33(5):1208−1211 (in Chinese with English abstract).

[9] Fang J, Huang P, Zeng GH. Multichannel parallel continuous-variable quantum key distribution with Gaussian modulation. Physical Review A, 2014,89:022315.

[10] Lim CCW, Curty M, Walenta N, Xu FH, Zbinden H. Concise security bounds for practical decoy-state quantum key distribution. Physical Review A, 2014,89(2):022307.

[11] Yu XT, Xu J, Zhang ZC. The routing protocol for wireless and hoc quantum communication network based on quantum teleportation. Acta Physica Sinica, 2012,61(22):0220303 (in Chinese with English abstract).

[12] Zhou NR, Cheng HL, Gong LH. Three-Party quantum network communication protocols based on quantum teleportation. Int'l Journal of Theoretical Physics. 2014,53(4):1387−1403.

[13] Bennett CH. Quantum cryptography using any two nonorthogonal states. Physical Review Letters, 1992,68(21):3121−3124.

[14] Greenberger DM, Horne MA, Shimony A, Zeilinger A. Bell's theorem without inequalities. American Journal of Physics, 1990,58 (12):1131−1143.

[15] Ma HY, Chen BQ, Guo ZW,Li HS. Development of quantum network based on multiparty quantum secret sharing. Canadian Journal of Physics, 2008,86(9):1097−1101.

附中文参考文献:

[4] 彭舰,洪昌建,刘唐,张云勇.基于分层的水下传感器网络路由策略.通信学报,2014,35(6):25−31.

[5] 郭忠文,罗汉江.洪锋,杨猛,倪明选.水下传感器网络的研究进展.计算机研究与发展,2010,47(3):377−389.

[6] 洪璐,洪锋,李正宝,郭忠文.CT-TDMA:水下传感器网络高效 TDMA 协议.通信学报,2012,33(2):163−174.

[7] 魏志强,杨光,丛艳平.水下传感器网络安全研究.计算机学报,2012,35(8):1594−1606.

[8] 张尧,金志刚,罗咏梅,杜秀娟.基于信任机制的水下传感器网络节点安全定位算法.计算机应用,2013,33(5):1208−1211.

[11] 余旭涛,徐进,张在琛.基于量子远程传态的无线自组织量子通信网络路由协议.物理学报,2012,61(22):220303.

马鸿洋(1976－),男,山东即墨人,博士,副教授,主要研究领域为量子信息安全,无线网络,信息论.
E-mail: hongyang_ma@aliyun.com

王淑梅(1975－),女,副教授,主要研究领域为无线网络,信息论.
E-mail: smw6@qtech.edu.cn

范兴奎(1970－),男,博士,副教授,主要研究领域为无线网络,信息论.
E-mail: fanxingkui@126.com

董玉民(1966－),男,博士,教授,主要研究领域为量子通信网络,人工智能.
E-mail: dym@qtech.edu.cn