基于簇的三维水声传感器网络的密钥管理方案

黄 彬 刘广钟 徐 明
(上海海事大学信息工程学院 上海 201306)

摘 要 在基于簇的三维水声传感器网络中,将布置区域划分为多个正方体的簇空间。在簇头节点间,提出通过相对坐标位置产生节点间的验证对称密钥;在簇内节点间,提出通过改进的对称多项式方法产生节点间的验证对称密钥。网络中的节点进行通信交流时都是采用基于对称矩阵的通信对称密钥,实现节点间的通信全连通。相比于传统的传感器网络密钥管理方案,本方案能够实现节点撤销和密钥更新,具有较高的可扩展性、可靠性和较低的开销。由于事先采用了轻量级节点认证机制,本方案能够很好地抵御节点间信息交流时的DoS攻击,特别是汇聚攻击。由于采用了三维密钥,本方案比单一的单向哈希链方法能更加有效地抵御簇头节点妥协。

关键词 三维密钥,单向哈希链,对称矩阵,验证密钥,通信密钥
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.11.042

Key Management Scheme for Three-dimensional Acoustic Sensor Network Based on Cluster

HUANG Bin LIU Guang-zhong XU Ming
(School of Information Engineering, Shanghai University of Maritime, Shanghai 201306, China)

Abstract In the three-dimensional acoustic sensor network based on cluster, the decorated area is divided into multiple rooms which are cubes. Among cluster head nodes, the symmetric key is generated to verify nodes by relative coordinates. Between nodes within the cluster, the symmetric key is generated to verify nodes by modified symmetric polynomials. When the nodes communicate in the network, they generate symmetric key which is used to communicate by symmetric matrices. It realizes complete connection in communication. Compared with the previous key management scheme for sensor network, this scheme can realize node revocation and key update, and it has high scalability, reliability and low cost. This scheme can also effectively resist DoS attack especially gather attack between nodes' communication because of first lightweight node authentication mechanism. Compared with one-way hash method, this scheme can more efficiently resist cluster head compromise because of three-dimensional key.

Keywords Three-dimensional key, One-way hash chain, Symmetric matrix, Verification key, Communication key

1 引言

近年来,随着水声传感网技术的发展,水声传感器网络的应用越来越广泛。水声传感器网络凭借其分布性、低成本等优点被广泛应用于海洋监测、污染监控、资源开采、海难搜救等众多领域[1]。但是,由于水声传感器网络中自身受限的计算、通信、存储等能力的硬件限制和水声通道高延迟、低带宽、多路径等特性,水声传感器网络容易受到攻击,因此对水声传感器网络安全问题的研究是必不可少的。水声传感器网络中的节点大多被部署在无人照看的不确定区域[2],信息的传输极其容易被非法者窃取,采用安全的密码技术是水声传感器网络安全的重要部分,所以安全的密钥管理方案是至关重要的。由于硬件和组网技术等的不成熟,水声传感器网络中有关安全的研究多处于理论研究和仿真阶段,尤其是密钥管理的研究还没有完备的体系,水声传感器网络中的密钥管理一般都是基于无线传感器网络中的密钥管理体系。因此从现有的无线传感器网络的密钥管理出发,提出水声传感器网络中的密钥管理方案。在现有的无线传感器网络的密钥管理方案[3,4]中,对其根据网络结构划分为分布式密钥管理和层次式密钥管理,根据节点的密钥分配方法划分为随机密钥管理方案和确定密钥管理方案。在几种典型的无线传感器网络密钥管理的方案和协议中,Eschenauer 和 Gligor 提出的随机密钥预分配方案[5]是最常用的密钥管理方案,后续的很多方案都是在E-G方案的基础上发展来的,它们分别从共享密钥阈值、密钥池结构、密钥预分配策略、密钥路径建立方法等方面提高随机密钥预分配方案的性能。比如,Chan 等人提出的 q-

到稿日期:2015-09-13 返修日期:2015-11-29 本文受国家自然科学基金项目(61202370),上海市教委科研创新项目(14YZ110),中国博士后科学基金资助项目(2014M561512)资助。

黄 彬(1991-),男,硕士生,主要研究方向为传感器网络安全,E-mail:hb1451568552@sina.com;刘广钟(1962-),男,教授,博士生导师,主要研究方向为分布式数据库、分布式人工智能、计算机网络技术、网格计算、CIMS技术、物流信息化技术等;徐 明(1977-),男,博士,副教授,主要研究方向为水声传感器网络、道路网络、智能信息处理。

composite 随机密钥预分配方案[11]就是在 E-G 方案的基础上由相邻节点共享一个密钥扩展到共享 q 个密钥得到的。除此外，Blom 提出的基于对称矩阵的单密钥空间方案[6]以及 Blundo 提出的基于对称多项式的随机密钥预分配方案[7]等都是在 E-G 方案框架的基础上进行改进或扩展得到的。上述随机密钥预分配方案使得密钥的分配具有盲目性，节点中可能存在一些没用的密钥而浪费存储空间。本文方案在 E-G 方案的基础上通过融合 E-G 方案的后续改进方案和单向哈希链等方法而得到。该方案虽然参考了上述随机密钥预分配的方法，但它不是一个随机密钥预分配方案，而是融合了确定密钥和随机密钥两种方案。

因为水声传感器网络的环境更加恶劣，对每一节点都进行同等的要求是不现实的，出于节能和高效的考虑，多采用分簇的层次式网络拓扑结构和对称密钥体系。所以本方案采用基于簇的三维空间层次式网络结构，重点对簇头节点进行严格的控制和管理。在无线传感器网络中，相比于叶子节点，簇头节点的计算、通信、存储等能力是较高的。所以本方案在簇头节点间采用较复杂的单向哈希函数链[8]来得到簇头节点间的三维对称密钥，该密钥用来对节点进行验证。在簇内节点间，本方案采用轻量级的改进对称多项式来产生节点间的对称密钥以对节点间进行验证。整个网络中的节点在通过验证后都是采用基于对称矩阵的密钥交换方式来得到节点间交流的对称密钥。

本文第 2 节介绍了所提方案中基于簇的三维空间网络模型；第 3 节具体描述了所提方案中采用的密钥管理方法；第 4 节从可扩展性、密钥连接性、抗毁性、开销、抵御 DoS 攻击等方面对该方案的安全和性能进行分析；最后对该方案进行了总结。

2 网络模型

从实际考虑出发，水声传感器网络一般被布置在水下空间，所以本方案采用基于簇的三维空间水声传感器网络模型，被布置空间事先被划分为多个正方体区域，每个区域代表一个簇(见图 1)，每一簇都有自己的相对坐标位置。为了保证相邻簇的簇头能够进行通信交流，本方案采取以下步骤布置整个基于簇的三维空间水声传感器网络。

步骤 1　由于水声传感器网络自身环境的影响，簇头节点可能在自身簇区域中产生偏移，考虑到相邻簇的簇头通信的最坏情况(簇头节点相离最远)，簇头 A 和簇头 B 此时的距离最远，如图 2 所示。假设簇头的通信半径是 R，正方体区域的边长是 a，那么

$$|AB|=2R=2\sqrt{a^2+a^2+a^2}\rightarrow a=\frac{\sqrt{3}}{3}R \tag{1}$$

通过以上方式，本方案可以确定每簇区域的规模大小。

步骤 2　当方案确定了整个布置空间的分簇情况后，为每簇中的正方体区域分配一个簇头节点，簇头节点中预装载了网络所有者分配的系统参数。

步骤 3　当所有的簇头节点都布置完成后，传感器节点被布置到网络空间中，传感器节点中预装载了网络所有者分配的系统参数。

上述过程中，各节点中的具体操作过程将在第 3 节中具体阐述。

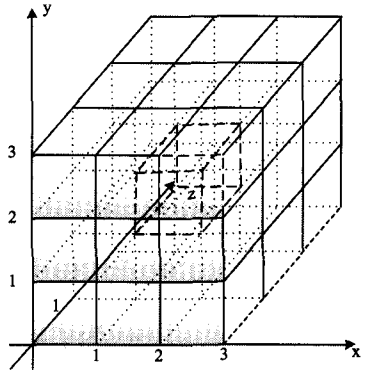


图 1　基于簇的节点三维空间分布图

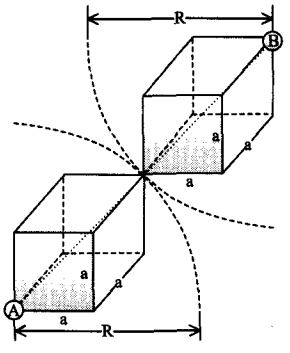
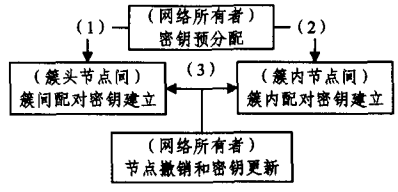


图 2　相邻簇头节点距离最远的情况

3 方案原理

所提出的密钥管理方案由密钥预分配、簇间配对密钥建立、簇内配对密钥建立 3 部分组成。由于水声传感器网络中水下环境、水声信道的特性和水下通信网络的拓扑特性，又增加了节点撤销和密钥更新这一部分。图 3 示出了上述 4 个部分在整个网络中的关系



(1) 分配系统公共参数与簇头节点自身参数
(2) 分配系统公共参数与簇间节点自身参数
(3) 更新节点新的自身参数

图 3　密钥管理方案中各阶段的部分关系

3.1 密钥预分配

在整个网络布置前，网络所有者事先选择一个对称矩阵密钥池 A。

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{pmatrix}_{m\times m} \tag{2}$$

其中，$a_{ij}=a_{ji}(1\leqslant i,j\leqslant m)$，$m$ 的取值根据簇的规模决定。

基站在网络布置前被预装载了系统参数$\{K,k\}$和其他参数。其中 K 是基站与簇头节点进行单向通信交流的对称密钥，k 是基站与叶子节点进行单向通信交流的对称密钥。

簇头节点在布置前被预转载了系统公共参数$\{H_1, H_2, H_3, K\}$，对于每一个不同的簇头节点 i，除了具有系统公共参数外还预装载了自身参数：

$$\{ID_{CH_i}, f_i(ID_{CH_i}, y), (x_i, y_i, z_i), \Delta_i, k_{i1}, k_{i2}, k_{i3}, a_i, p\} \tag{3}$$

其中，H_1, H_2, H_3 是便于计算的单向哈希函数，K 是基站与所有簇头节点进行单向通信交流的对称密钥，ID_{CH_i} 是簇头节点独一无二的身份标识，$f_i(ID_{CH_i}, y)$ 是由对称多项式 $f_i(x, y)$ 和簇头 ID 产生的。

$$f_i(x,y)=\sum_{i=0}^{t}\sum_{j=0}^{t}a_{ij}x^iy^j \tag{4}$$

其中，$a_{ij}=a_{ji}$ 的取值决定了方案的安全性。(x_i, y_i, z_i) 是簇头节点的相对坐标位置且坐标值都是整数，Δ_i 是多项式的偏移量，$\{k_{i1}, k_{i2}, k_{i3}\}$ 是网络所有者分配给簇头节点的认证密钥（网络所有者产生密钥的方式如算法 1 所示），a_i 是网络所有者从对称矩阵密钥池 A_i 中选取后分配给簇头节点的密钥链（网络所有者选取密钥链的方式如算法 2 所示），p 是簇头节点取模后的身份标识。

$$p=ID_{CH_i} \bmod m+1 \tag{5}$$

算法 1 三维密钥的产生

输入：网络所有者的种子密钥 τ，簇头节点 i 的身份标识 ID_{CH_i}，簇头节点 i 的相对坐标位置$\{x_i, y_i, z_i\}$，单向哈希函数$\{H_1, H_2, H_3\}$，整个网络的预估簇数量 n

输出：簇头节点的三维密钥$\{k_{i1}, k_{i2}, k_{i3}\}$

1. 网络所有者根据簇头节点 i 的相对坐标$\{x_i, y_i, z_i\}$计算出三维密钥$\{k_{i1}, k_{i2}, k_{i3}\}$。
2. 计算 $k_{i1}=H_1^{[x_i \bmod n]}(\tau)$。
3. 计算 $k_{i2}=H_2^{[(n-y_i) \bmod n]}(\tau)$。
4. 计算 $k_{i3}=H_1^{[(\frac{n}{2}+z_i) \bmod n]}(\tau)$。
5. 簇头节点在内存中存储三维密钥$\{k_{i1}, k_{i2}, k_{i3}\}$。

算法 2 节点密钥链的产生

输入：对称矩阵密钥池 A，簇头节点的身份标识 ID_{CH_i}，单向哈希函数 H_1

输出：簇头节点 i 的密钥链 a_i

1. 簇头节点计算 $d=ID_{CH_j} \bmod m+1$。
2. $$A_i=H_1^d(A)=\begin{pmatrix} H_1^d(a_{11}) & H_1^d(a_{12}) & \cdots & H_1^d(a_{1m}) \\ H_1^d(a_{21}) & H_1^d(a_{22}) & \cdots & H_1^d(a_{2m}) \\ \vdots & \vdots & \ddots & \vdots \\ H_1^d(a_{m1}) & H_1^d(a_{m2}) & \cdots & H_1^d(a_{mm}) \end{pmatrix}_{m\times m}$$
3. 网络所有者根据得到的 d 值选取对称矩阵密钥池 A_i 的第 d 行作为簇头节点 i 的密钥链 a_i。

$$a_i=(H_1^d(a_{i1}), H_1^d(a_{i2}), \cdots, H_1^d(a_{im}))$$

在以簇头节点 i 为首的簇中，叶子节点 i_1 在布置前被预装载系统参数：

$$\{ID_{LN_{i_1}}, f_i(ID_{LN_{i_1}}, y), \Delta_i, k, a_{i_1}\} \tag{6}$$

其中，$ID_{LN_{i_1}}$ 是叶子节点独一无二的身份标识，$f_i(ID_{LN_{i_1}}, y)$ 是由对称多项式 $f_i(x, y)$ 和叶子节点 ID 产生的，Δ_i 是多项式的偏移量，k 是基站与叶子节点进行单向通信交流的对称密钥，a_{i_1} 是网络所有者从对称矩阵密钥池 A_i 中选取后分配给叶子节点的密钥链（它的选取过程可参照算法 2）。

$$p=ID_{LN_{i_1}} \bmod m+1 \tag{7}$$

3.2 簇间配对密钥建立

当簇 i 与簇 j 之间的簇头节点进行信息交流时，簇头节点间首先建立验证对称密钥用于验证双方相互的通信请求。簇头节点 j 通过算法 3 建立验证对称密钥 k_{j-i}^1。只有簇头节点间通过了相互间的验证，它们才进行进一步的信息交流。因为簇头节点的安全性在整个网络中是至关重要的，同时也为了充分利用簇头节点中预存储的 A_i，所以本方案还将用密钥链 A_i 为簇头节点 j 产生与簇头节点 i 进行信息交流的通信对称密钥 k_{j-i}^2。通信对称密钥 k_{j-i}^2 的具体产生过程参见算法 4。通过算法 3 和算法 4，簇头节点 j 就可以得到双对称密钥 $k_{j-i}=\{k_{j-i}^1, k_{j-i}^2\}$。该双对称密钥产生过程中的信息交流如图 4 所示。同理，簇头节点 i 采用同样的方式产生验证对称密钥 k_{j-i}^1 和通信对称密钥 k_{j-i}^2。通过这种方式，该簇头节点就可以验证周围簇头并安全地进行信息交流。

算法 3 簇间验证对称密钥的产生

输入：簇头节点 i 的相对坐标位置(x_i, y_i, z_i)，三维密钥$\{k_{i1}, k_{i2}, k_{i3}\}$，簇头节点 j 的相对坐标位置$(x_j, y_j, z_j)$，三维密钥$\{k_{j1}, k_{j2}, k_{j3}\}$，单向哈希函数$\{H_1, H_2, H_3\}$

输出：验证对称密钥 k_{j-i}^1 与取模后身份标识的映射表

1. if $x_i > x_j$
2. $k_{1_{j-i}}=H_1^{x_i-x_j}(k_{j1})$
3. else $k_{1_{j-i}}=k_{j1}$
4. if $y_i \geqslant y_j$
5. $k_{2_{j-i}}=k_{j2}$
6. else $k_{1_{j-i}}=H_2^{x_i-x_j}(k_{j2})$
7. if $z_i > z_j$
8. $k_{3_{j-i}}=H_3^{z_i-z_j}(k_{j3})$
9. else $k_{3_{j-i}}=k_{j3}$
10. $k_{j-i}^1=k_{1_{j-i}} \oplus k_{2_{j-i}} \oplus k_{3_{j-i}}$
11. 簇头节点 j 在内存中存储簇头节点 i 取模后的身份标识与验证对称密钥 k_{j-i}^1 的映射表。

算法 4 簇间通信对称密钥的产生

输入：簇头节点 j 进行身份标识 ID_{CH_j} 得到的 d_j，a_j，簇头节点 i 取模后的身份标识 p

输出：簇头节点 j 产生与簇头节点 i 之间进行信息交流的通信对称密钥 K_{j-i}^2 与簇头节点 i 取模后身份标识的映射表

1. 簇头节点 j 接收到簇头节点 i 取模后的身份标识 p 后得到 $d_i=p$。
2. 簇头节点 j 从 a_j 中取出 a_{jp}。
3. if $d_i \leqslant d_j$
4. $K_{j-i}^2=a_{jp}$
5. else $K_{j-i}^2=H_1^{d_i-d_j}(a_{jp})$
6. 簇头节点 j 在内存中存储簇头节点 i 取模后的身份标识和通信对称密钥 k_{j-i}^2 的映射表。

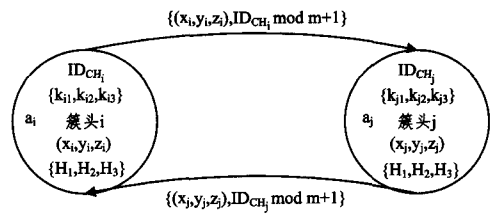


图 4 簇头节点间验证对称密钥产生过程中的信息交流

3.3 簇内配对密钥建立

当每个簇中的叶子节点被布置到相应区域后，为了和相

邻节点形成双对称密钥 K_{i-i_1}，节点间的信息交流过程如图 5 所示。簇头节点 i 与叶子节点 i_1 建立双对称密钥 K_{i-i_1} 的方式如算法 5 所示。当簇头节点在叶子节点的通信范围时，叶子节点直接将用于产生密钥的信息发送给簇头节点。当簇头节点不在叶子节点的通信范围时，叶子节点通过相邻节点间接将用于产生密钥的信息发送给簇头节点。由于叶子节点肯定在簇头节点的通信范围内，因此所有叶子节点可以直接接收簇头节点发送的用于产生密钥的信息，该对称密钥的产生过程与算法 5 类似，这里不再详述。

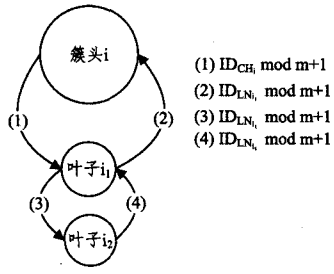


图 5　簇内节点间产生对称密钥过程中的信息交流

算法 5　双对称密钥的产生

输入：簇头节点的身份标识 ID_{CH_i}，$f_i(ID_{CH_i}, y)$，Δ_i，A_i，叶子节点 i_1 取模后的身份标识 p

输出：簇头节点 i 产生与叶子节点 i_1 之间进行信息交流的双对称密钥 K_{i-i_1} 与叶子节点取模后身份标识的映射表

1. 簇头节点接收到叶子节点的身份标识 p 后，产生双对称密钥。
2. 簇头节点从 A_i 中取出 a_{ip} 作为验证对称密钥 $K^1_{i-i_1}$。
3. 计算 $f=f_i(ID_{CH_i} \bmod m+1, p)+\Delta_i$。
4. 簇头节点将 f 的值作为通信对称密钥 $K^2_{i-i_1}$。
5. 令 $K_{i-i_1}=\{K^1_{i-i_1}, K^2_{i-i_1}\}$。
6. 簇头节点 i 在内存中存储叶子节点 i_1 取模后的身份标识和双对称密钥 K_{i-i_1} 的映射表。

在双对称密钥 K_{i-i_1} 中，$K^1_{i-i_1}$ 用于信息交流前的节点验证，只有验证通过后节点间才用密钥 $K^2_{i-i_1}$ 进行信息交流。

通过算法 5，不管是簇头节点还是叶子节点，它们的内存中都存储了在本簇中与自己相邻节点取模后的身份标识和双对称密钥的映射表。当簇头节点周围不同的相邻节点对自身 ID 取模运算得到的值相同时，簇头节点只需存储一个取模后的身份标识与双对称密钥的映射。通过这样的方式，该节点即可以通过采用对称密钥加密的方式与周围节点进行安全的信息交流。

3.4　节点撤销和密钥更新

当网络所有者通过已有的方案[9]检测到有节点妥协时，整个网络就通过更新对称多项式的偏移量来实现验证密钥的更新，从而实现节点的撤销。

3.4.1　被妥协的节点是叶子节点

当簇头节点 i 所在的簇中有叶子节点 i_1 被妥协时，基站向所有节点广播节点撤销密钥更新信息：

$$\{ID_{CH_{i_1}}, ID_{LN_{i_1}}, E_k(f(x) \| tag)\} \tag{8}$$

其中，ID_{CH_i} 是簇头节点的身份标识，Δ_i' 是新的多项式偏移量，E_k 是采用密钥 k 的对称加密操作，tag 是节点妥协标识（当 $tag=1$ 时，表示妥协的节点是叶子节点；当 $tag=0$ 时，表示妥协的节点是簇头节点）。$f(x)$ 是多项式的一般形式。

$$f(x)=\sum_{x\neq LN_{i_1}}(x-ID_{CH_i})(x-ID_{LN_{i_1}})\cdots(x-ID_{LN_{i_j}})+\Delta_i' \tag{9}$$

当所有叶子节点接收到密钥更新消息，随后节点先通过簇头节点 ID_{CH_i} 判断是否属于该簇。只有属于该簇的节点才用密钥 k 解密 $E_k(\Delta_i')$ 得到 $f(x)$。令 x 的值为自身 ID，随后节点就可以得到新的多项式偏移量 Δ_i'，节点将 Δ_i' 作为基站与叶子节点进行单向通信交流时新的对称密钥 k'。但是妥协节点得不到 Δ_i'，这是因为在 $f(x)$ 中，妥协节点的 $(x-ID_{CH_i})\cdots(x-ID_{LN_{i_j}})$ 不为 0。簇中没有被妥协的节点根据 $ID_{LN_{i_1}}$ 判断妥协节点是否是自己的邻居节点。若是邻居节点，则将节点内存中存储的与妥协节点的对称密钥映射表去除。簇头节点采用以上同样的方式进行操作，但是它们接收到的节点撤销密钥更新信息为：

$$\{ID_{CH_i}, ID_{LN_{i_1}}, E_k(f(x) \| tag)\} \tag{10}$$

其中，tag 为 1，这里不再详述。通过这样的方式就实现了节点的撤销和密钥的更新。

3.4.2　被妥协的节点是簇头节点

由于簇头节点在整个过程中是至关重要的，因此采用双对称加密方式来确保它的安全性。但是簇头节点也是可能被妥协的。下面考虑簇头节点被妥协的情况。

当簇头节点 i 被妥协时，基站选择簇 i 中计算和通信能力较强的叶子节点 i_1 作为临时簇头。基站向所有节点广播节点撤销密钥更新信息：

$$\{ID_{CH_i}, ID_{LN_{i_1}}, E_k(\Delta_i' \| tag)\} \tag{11}$$

其中，tag 为 0，表示该信息是簇头节点妥协。

簇 i 中的叶子节点接收到该信息后就可以对其进行解密并更新多项式偏移量，从而实现密钥更新。通过节点中已经存在的对称矩阵密钥链和对称多项式，新的簇头 i_1 就可以和叶子节点形成新的双对称密钥。

当然上述的信息对于簇头节点是无法解密的，被妥协的簇头节点无法更新。对于周围簇头节点的更新，基站向簇头节点广播临时通话密钥 $\{ID_{CH_i}, g(x)\}$，其中 $g(x)$ 是多项式的一般形式。

$$g(x)=\sum_{x\neq CH_i}(x-ID_{CH_1})\cdots(x-ID_{CH_{i-1}})(x-ID_{CH_{i+1}})\cdots(x-ID_{CH_n})+P \tag{12}$$

被妥协簇头节点 i 的周围簇接收到该信息后先从内存中去除与簇头节点 i 建立的对称密钥映射表，再令 x 为自己的 ID 就可以得到临时会话密钥 P，然而簇头节点 i 无法得到会话密钥 P，这是因为 $(ID_{CH_i}-ID_{CH_1})\cdots(ID_{CH_i}-ID_{CH_n})$ 不为 0。基站通过会话密钥 P 向周围簇发送信息 $E_P(ID_{LN_{i_1}})$，周围簇头收到信息解密后与新的簇头通过已经存储的对称矩阵密钥链实现对称密钥的建立。在这个过程中，被妥协的簇头节点是无法进行的。通过这样的方式即可实现簇头节点的撤销和新簇头的建立。

4　性能分析

4.1　抵抗节点妥协的网络弹性

当某一簇中的叶子节点被妥协后，非法者就得到了该节

点的所有信息。密钥链和对称多项式的泄漏不会影响其他节点安全，至多影响妥协节点与自己周围节点的通信。该方案采用了节点撤销和密钥更新机制，被妥协的节点会被撤销，其它安全节点会更新自己的对称多项式和密钥 k。

当某一簇中的簇头节点被妥协后，非法者就得到了该节点的所有信息。$\{k_1,k_2,k_3\}$的泄漏只会影响与周围节点的通信。如算法 3 所示，本方案采用三组哈希函数链操作，其它簇头的密钥无法得到。如果非法者想要破解密钥，就必须妥协分别包含 $H_1(\tau),H_2(\tau),H_3(\tau)$的 3 个特定簇头节点。假设网络中的簇头节点总数为 n，3 个特定簇头节点被妥协的概率为 P，则

$$P=\frac{1}{\binom{n}{3}}=\frac{6}{n(n-1)(n-2)} \tag{13}$$

由式(13)可以看出，随着节点总数 n 的增大，3 个特定节点同时被妥协的概率越小。

由 3.4.2 节可知，通过节点撤销和密钥更新机制，妥协的簇头节点会被检测到，新的临时簇头节点将产生。通过这样的方式，网络所有者就可以有充足的时间去重置簇头节点，并且不影响整个网络的工作。

4.2 安全连通性

在本方案中，任意通信范围内相邻的节点间都可以建立对称密钥。在基于密钥池的随机密钥预分配方案和 q-Composite 随机密钥预分配方案中，由经典的随机图理论[10]可知，节点的度 d 与网络中的节点总数 n 有如下关系：

$$d=\frac{n-1}{n}(\ln n-\ln(-\ln P_m)) \tag{14}$$

其中，P_m 是网络要求的全网连通率。

如果节点所期望的邻居节点数为 $n'(n'\ll n)$，则两个相邻节点之间共享密钥的概率为 P。

$$P=1-\frac{((N-k)!)^2}{(N-2k)!\ N!} \tag{15}$$

其中，N 是密钥池中的密钥总数，k 为每个节点从密钥池中选择的密钥个数。

由式(15)可以看出，网络中要想达到高的连通率，每个节点需要存储的密钥数量相对较多。所以与随机密钥预分配的方案相比，本方案实现了 100% 的连通，任意两个通信范围内的节点都可以建立验证对称密钥和通信对称密钥。在任意两个节点间的验证对称密钥中，对于簇头节点而言，任意两个相邻簇头节点的基于哈希函数得到的三维密钥$\{k_1,k_2,k_3\}$是不同的。对于簇中节点而言，任意相邻节点形成的基于对称多项式的密钥 K^2_{i-i1} 是不同的。通过这样的方式，整个网络就实现了安全的连通。

4.3 开销分析

本方案中簇头节点间和簇内节点间的信息交流密钥采用的都是基于对称矩阵的对称密钥。在同一数量级的网络规模下，随着网络中节点总数的增多，节点中存储的密钥链的大小是不变的。虽然这种方式导致随着网络规模的增大，任意两个节点间的通信密钥重复率也在上升，但是本方案采用了节点间的验证机制，任意两个节点间的验证密钥是不同的，这在一定程度上弥补了通信密钥重复的缺陷。在式(14)、式(15)分析的基础上，假设节点总数为 N 的网络中节点平均度为 $\sqrt{N}$，随机密钥方案的连通率 p 为 0.33(这是因为当传感器网络中的安全连通率达到 0.33 时，两相连节点至多需要 3 跳就可以建立对称密钥[11])。通过计算分析，对本方案和现有方案的网络规模和内存开销关系进行了对比，描述了在相同叶子节点数的情况下，采用本方案与 E-G 随机密钥预分配方案、q-composite 方案在节点对称密钥存储开销方面的对比，如图 6 所示。由图 6 可以看出，在同一数量级的网络规模下，随着网络规模的不断扩大，所提方案相比其他两种方案在节点对称密钥存储上的开销增长缓慢。而其他两种方案在节点对称密钥存储上的开销是随着网络规模线性增加的。所以在相同的网络环境下，相比于传统的随机密钥管理方案，本文的密钥管理方案由于密钥存储的内存较小，密钥被浪费的概率也相对较小。

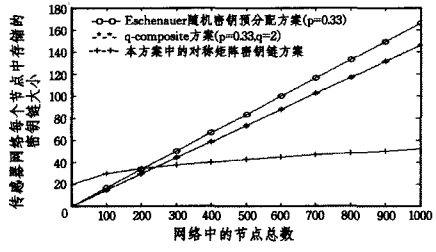


图 6 网络规模和节点密钥内存开销

在节点间建立对称密钥时，本方案只需要进行简单的取模运算和哈希操作(当节点是簇头节点时)或取模运算和四则运算(当节点是簇内节点时)。在本方案中，节点对称密钥的建立只需接收相邻节点取模后的身份标识，没有其他通信开销，这在能量消耗上是相对较低的。假设簇头节点平均要与 d 个邻居簇头节点建立对称密钥，簇内节点的平均邻居节点数为 c，S 表示发送一次消息的通信开销，R 表示接收一次消息的通信开销，u 表示产生对称密钥过程中哈希操作的计算开销，v 表示产生对称密钥过程中取模运算的计算开销，f 表示取模后的身份标识代入对称多项式的计算开销，g 表示利用更新对称多项式的计算开销，E、D 分别表示加密和解密信息的计算开销。表 1 列出了本方案中的计算和通信开销。

表 1 通信开销和计算开销

		通信开销	计算开销
验证密钥对的建立	簇间	d(S+R)	du
	簇内	c(S+R)	cf
通信密钥对的建立	簇间	d(S+R)	dv+0.5du
	簇内	0	cv
簇内节点被撤销	基站	S	E
	簇头	R	0
	簇内安全节点	R	D
	簇外安全节点	R	0
簇头节点被撤销	基站	2S	2E
	新簇头	(c+d)(S+R)	d(u+v)+0.5du+c(f+v)
	邻居簇头	2R+S	f+D+0.5du+d(u+v)
	簇内叶子节点	R	D
	簇外叶子节点	R	0
	其它节点	R	0

由表 1 可以看出，在簇内节点中，节点只需进行一次发送和接收操作就可以实现验证对称密钥和通信对称密钥的建

立，这减少了通信的开销。当簇内节点被撤销时，基站只进行一次发送操作，其它节点只进行一次接收操作，这样的通信开销是很小的。因为各节点间交换的只是取模后的节点标识，所以节点周围的不同相邻节点的身份标识经过取模运算后可能得到相同的结果，这时节点只需进行一次计算。所以表1中的计算开销是最坏情况下的结果，真实的计算开销不高于表1中的计算开销。

4.4 可扩展性

当有新的叶子节点需要加入网络时，网络所有者根据节点要分配到的簇信息只需给新节点预装载系统参数$\{ID_{LN_j}, f_i(ID_{LN_j}, y), k, a_j\}$。新加入的节点进入簇后通过自身系统参数就可以与周围的节点建立通信需要的对称密钥。当有新的簇头节点需要加入网络时，网络所有者根据新簇头节点要加入的相对坐标位置(x_i, y_i, z_i)给其分配密钥$\{k_1, k_2, k_3\}$和其它系统参数。通过这样的方式，新簇头节点可以与周围簇头建立对称密钥，并且后续加入的叶子节点也可以与簇头节点建立对称密钥。

4.5 抵御 DoS 攻击

本方案在任意两个节点间进行信息交流前会进行一次基于验证对称密钥的验证过程。在验证过程中，若有一方是非法的，则无法得到验证的对称密钥，从而无法通过另一方的验证。在进行验证之前，可以先用验证对称密钥进行轻量级的验证。所有节点在网络布置前已经存储了一个计算简单的单向哈希函数 H_2。轻量级的验证过程如下。

(1)当被验证的节点是簇间节点时，假设簇头节点 i 验证簇头节点 j 的合法性。被验证的簇头节点 j 根据验证对称密钥 k_{j-i}^1 产生轻量级的验证码 MAC。

$$MAC=H_2(k_{j-i}^1) \tag{16}$$

簇头节点 i 接收到簇头节点 j 的验证码 MAC 后，就可以根据自己的验证对称密钥 k_{j-i}^1 来判断簇头节点 j 的合法性。

$$MAC \overset{?}{\Leftrightarrow} H_2(k_{j-i}^1) \tag{17}$$

(2)当被验证的节点是簇内节点时，轻量级的验证过程与上述方法类似，这里不再详述。

由于这种轻量级验证方式的计算、通信、存储的代价是相对较小的，即使有大量的请求需要被验证，节点只需进行简单的哈希运算就可以很快判断请求节点的合法性。因此该轻量级的节点先验证方案可以对非法者的恶意 DoS 攻击，尤其是汇聚攻击起到很好的防范作用。

结束语 本文在基于簇的三维空间水声传感器网络的环境下，综合了现有的传感器网络对称密钥方案，提出了一种双对称密钥的密钥管理方案。在簇头节点间，该方案采用了基于相对三维坐标位置的验证对称密钥和基于对称矩阵的通信对称密钥。在簇内节点间，本方案采用了基于改进对称多项式的验证对称密钥和基于对称矩阵的通信密钥。该方案中的节点间在进行信息交流时，节点双方交换的不是节点的真实身份标识，而是经过取模运算后的身份标识，有效地隐藏了节点的真实身份，具有匿名性。当现有的网络检测方法发现妥协节点后，该方案可以实现妥协节点的撤销和密钥更新，能够抵御节点妥协。在性能方面，该方案实现了安全的网络全连通，具有较高的可扩展性和可靠性。与已有的方案相比，本方案的存储开销相对较低。在同一数量级的节点总数情况下，本方案中基于对称矩阵通信密钥方式的每个节点的密钥链长度是不变的。另外，节点轻量级先认证机制使得本方案能够有效地抵御 DoS 攻击。

参 考 文 献

[1] Heidemann J, Ye W, Wills J, et al. Research challenges and applications for underwater sensor networking[C]// Proceedings of the Wireless Communication and Networking Conference. Las Vegas, NV, USA, 2006, 1: 228-235

[2] Wei Zhi-qiang, Yang Guang, Cong Yan-ping. Underwater sensor network security research[J]. Chinese Journal of Computer, 2012, 8(35): 1594-1606(in Chinese)
魏志强，杨光，丛艳平. 水下传感器网络安全研究[J]. 计算机学报，2012，8(35)：1594-1606

[3] Su Zhong, Lin Chuang, Feng Fu-jun. Wireless sensor network key management scheme and protocol [J]. Chinese Journal of Software, 2007, 5(18): 1218-1231(in Chinese)
苏忠，林闯，封富君. 无线传感器网络密钥管理的方案和协议[J]. 软件学报，2007，5(18)：1218-1231

[4] Xiao Y, Rayi V K, Sun B, et al. A survey of key management schemes in wireless sensor networks [J]. Computer Communications, 2007, 30(11/12): 2314-2341

[5] Eschenauer L, Gligor V. A key management scheme for distributed sensor networks [C]// Proc. of the 9th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2002: 41-47

[6] Blom R. An optimal class of symmetric key generation systems [C]// Beth T, Cot N, Ingemarsson I, eds. Proc. of the EUROCRYPT'84. New York: Springer-Verlag, 1984: 335-338

[7] Blundo C, Santis A D, Herzberg A, et al. Perfectly secure key distribution for dynamic conferences [J]. Information and Computation, 1998, 146(1): 1-23

[8] Su Zhong, Lin Chuang, Ren Feng-yuan. A preassigned hair schene in Wireless sensor network about the random key based on the hash chain[J]. Chinese Journal of Computer, 2009, 32(1): 30-41(in Chinese)
苏忠，林闯，任丰原. 无线传感器网络中基于散列链的随机密钥预分发方案[J]. 计算机学报，2009，32(1)：30-41

[9] Perrig A, Stankovic J, Wagner D. Security in wireless sensor networks [J]. Communications of the ACM, 2004, 47(6): 53-57

[10] Bollobas B, Fflton W, Katok A, et al. Rand Graphs [M]. Cambridge: Cambridge University Press, 2001: 160-200

[11] Chan H, Perri G A, Song D. Random key pre-distribution schemes for sensor networks[C]// IEEE Symposium in Security and Privacy. Berkeley, California: IEEE Computer Society, 2003: 197-205