新的传感器网络对偶密钥预分配方案

丁晓宇 刘建伟 邵定蓉

(北京航空航天大学 电子信息工程学院, 北京 100191)

摘 要: 提出了一种新的基于超立方体和多项式的对偶密钥预分配方案,此方案以超立方体的维度和传感器节点编码的汉明距离为参数.方案具有如下特性:当任意两个邻居传感器节点间的汉明距离小于预先设定的门限值时,可以直接建立对偶密钥.该方案的创新在于将传感器节点间的汉明距离参数化,解决了以往方案只能在汉明距离为1时才能直接建立对偶密钥的限制,经过安全和性能的分析说明,当汉明距离门限值增大时,方案通过牺牲抗节点俘获能力可以提高直接对偶密钥建立概率,从而节省了对于传感器网络来说十分重要的能量消耗.

关 键 词: 对偶密钥建立;传感器网络;基于超立方体密钥预分配;多项式;汉明距离

中图分类号: TP 393

文献标识码: A **文 章 编 号**: 1001-5965(2009)09-1080-03

New pairwise key predistribution scheme for wireless sensor networks

Ding Xiaoyu Liu Jianwei Shao Dingrong

(School of Electronics and Information Engineering, Beijing University of Aeronautics and Astronautics, Beijing 100191, China)

Abstract: A new hypercube-based key predistribution scheme for establishing pairwise keys between sensor nodes using polynomials, which is parameterized by the dimension of hypercube and the Hamming distance threshold variables was developed. This scheme exhibits a nice property: when the Hamming distance between any two neighboring sensor nodes is less than the pre-defined threshold, the pairwise key can be established directly. The scheme is typical for the innovation that the Hamming distance threshold is parameterized which solves the constraint in previous schemes that any two neighboring nodes can establish pairwise key only when the Hamming distance is one. Extensive performance and security analysis shows that by increasing Hamming distance threshold value, the resilience against node capture attack for higher probability of direct pairwise key establishment can be traded off, so as to save the energy consumption which is the most important issue for sensor networks.

Key words: pairwise key establishment; sensor networks; hypercube-based key predistribution; polynomial; Hamming distance

传感器网络可以在不同的应用场景下使用,如环境监控,军事感测和病人监测等[1].安全问题对于需要可靠、高效的传感器网络通信来说,变得越来越重要,而密钥管理是安全问题的核心.

对偶密钥的建立是最基础的安全服务之一,使得传感器节点间可以利用加密技术实现安全通信.然而,由于传感器节点的资源受限,使得传统的对偶密钥建立技术,如公钥技术[2-3]和在线密钥分配中心(KDC)方案[4]不适用于传感器网络.

本文提出了一种通用的基于超立方体和多项式的对偶密钥建立方案,此方案在传感器节点间汉明距离小于预先设定门限值的情况下,可以直接建立对偶密钥.通过增加汉明距离的限制值,此方案能够获得较高的直接建立对偶密钥概率,从

收稿日期: 2008-07-15

基金项目: 国家863基金资助项目(2006AA01Z422);国家自然科学基金资助项目(60672102)

作者简介: 丁晓宇(1976—),男,河南洛阳人,博士生,ding_xiao_yu@163.com.

而具有较低的通信开销,而这对于传感器网络而言至关重要[5].

1　新的密钥预分配方案

受文献[6]和文献[7－8]方案的启发,本文提出了一种通用的基于超立方体的方案,此方案在节点间的汉明距离低于预设的门限值时,能够直接建立对偶密钥.显然,方案能够提高直接对偶密钥建立的概率,从而减少通信开销,这对于能量受限的无线传感器网络至关重要.

在方案中,用 d 表示预设的汉明距离门限值,用 n 表示超立方体的维度.对偶密钥通过三个阶段建立:安装阶段,对偶密钥发现阶段和路径密钥建立阶段.

1.1　安装阶段

KDC(Key Distribution Center)从多项式池随机选择 $C_n^d \times m^{n-d}$ 个多项式(其中,N 为 WSN(Wireless Sensor Network)网络预期的节点数,$m=\lceil \sqrt[n]{N} \rceil$),利用这些多项式构造超立方体 $P\{p_{(i_1,i_2,\cdots,i_{n-d})}^{(d_1,d_2,\cdots,d_d)}\}$ $(1\leqslant i_1,i_2,\cdots,i_{n-d}\leqslant m, 1\leqslant d_1,d_2,\cdots,d_d\leqslant n)$.然后,KDC 为网络中的每个节点分配一个唯一的坐标.为了简单,把超立方体的节点坐标编码为节点的单值 ID.

对于在坐标 $(j_1,j_2,\cdots,j_n)$ 的传感器节点,KDC 从 P 中选择 C_n^d 个多项式 $\{p_{(j_{t_1},j_{t_2},\cdots,j_{t_{n-d}})}^{(d_1,d_2,\cdots,d_d)}\}$ (其中 $1\leqslant d_1,d_2\cdots,d_d\leqslant n; 1\leqslant j_{t_1},j_{t_2},\cdots,j_{t_{n-d}}\leqslant m$ 并且 $\{d_1,d_2,\cdots,d_d\}\bigcap\{t_1,t_2,\cdots,t_{n-d}\}=\varnothing$),并预加载这些多项式份额到此节点,构成其密钥环.

这个安装过程保证任意两个节点的汉明距离低于 $d+1$ 时,能够有共享的多项式.

1.2　对偶密钥发现阶段

假定传感器网络中任意两个节点 a 和 b 的坐标为 $\{a_1,a_2,\cdots,a_n\}$ 和 $\{b_1,b_2,\cdots,b_n\}$,如果节点 a 想和节点 b 建立对偶密钥,可通过下述方法实现.

首先,节点 a 计算和节点 b 之间的汉明距离,如果汉明距离 $d'\leqslant d$,节点 a 可以根据定理 1 来获得自己和节点 b 的直接对偶密钥.

定理 1　对于网络中任意两个传感器节点 $a\{a_1,a_2,\cdots,a_n\}$ 和 $b\{b_1,b_2,\cdots,b_n\}$,假定两者之间的汉明距离为 d',如果 $d'\leqslant d$,则节点 a 和 b 之间存在直接的对偶密钥.

证明　考虑 $a_t\neq b_t$,当 $1\leqslant t\leqslant d'$;但 $a_t=b_t$,当 $t>d'$.很容易推出多项式

$$p_{(a_{x_1},a_{x_2},\cdots,a_{x_{n-d}})}^{(1,2,\cdots,d',d_{t_2},\cdots,d_{t_{n-d'}})}=p_{(b_{x_1},b_{x_2},\cdots,b_{x_{n-d}})}^{(1,2,\cdots,d',d_{t_2},\cdots,d_{t_{n-d'}})}$$

$(x_1,x_2,\cdots,x_{n-d}>d')$.所以两个节点有 $C_{n-d'}^{d-d'}$ 个共享的多项式,从而可以利用基于多项式的方法直接建立对偶密钥.　　**证毕**

1.3　路径密钥建立阶段

如果 $d'>d$,那么节点 a 可以通过定理 2 建立和节点 b 之间的路径密钥.

定理 2　对于网络中任意两个传感器节点 $a\{a_1,a_2,\cdots,a_n\}$ 和 $b\{b_1,b_2,\cdots,b_n\}$,假定两者之间的汉明距离为 d',如果 $d'>d$,那么节点 a 和 b 之间存在一个路径密钥.

证明　当 $\{a_t\neq b_t\mid 1\leqslant t\leqslant d'\}$ 而 $\{a_t=b_t\mid t>d'\}$.很明显,节点 $a\{a_1,a_2,\cdots,a_n\},\{b_1,b_2,\cdots,b_d,\cdots,a_{d'},\cdots,a_n\},\{b_1,b_2,\cdots,b_{2d},\cdots,a_{d'},\cdots,a_n\},\cdots,\{b_1,b_2,\cdots,b_{d'}\cdots,a_n\}b$ 构成一个节点路径,任意两个邻居节点间的距离低于 $d+1$,　所以由定理 1,很容易知道这些节点中任意两个邻居节点存在直接对偶密钥,并且路径中至少有 $\lceil d'/d\rceil$ 个中间节点.　　**证毕**

2　性能分析

2.1　实用性分析

根据前面的描述和分析,可以很清楚地知道新方案具有以下特性.

性质 1　当不存在错误和俘获节点时,通过新的对偶密钥预分配方案,任意两个节点间能够建立直接对偶密钥的概率为 $p=\dfrac{\sum_{i=1}^{d}C_n^i(m-1)^i}{N-1}$,而 N 是网络中节点的总数.

证明　对于网络中任意节点 $a\{a_1,a_2,\cdots,a_n\}$,根据定理 1,可以和汉明距离 $d'\leqslant d$ 的节点直接建立对偶密钥.当 $d'=1$,很明显存在 $C_n^1(m-1)$ 个节点可以和节点 a 直接建立对偶密钥;当 $d'=2$ 时,存在 $C_n^2(m-1)^2$ 个节点可以和节点 a 直接建立对偶密钥;依次类推,当 $d'=d$ 时,有 $C_n^d(m-1)^d$ 个节点可以和节点 a 直接建立对偶密钥.所以总共有 $\sum_{i=1}^{d}C_n^i(m-1)^i$ 个节点可以和节点 a 直接建立对偶密钥.因为整个网络总共有 N 个节点,所以任意两个节点可以直接建立对偶密钥的概率为 $p=\dfrac{\sum_{i=1}^{d}C_n^i(m-1)^i}{N-1}$.　　**证毕**

利用新的对偶密钥预分配方案,图 1 表示传感器网络中的节点规模 N 取不同的值,当汉明距离门限值 d 为 1 时,任意两个节点直接建立对偶密钥的概率和超立方体的维度 n 的关系.图 2 表

示传感器网络中的节点规模 N 取不同的值，当超立方体的维度 n 为 2 时，任意两个节点直接建立对偶密钥的概率和汉明距离门限值 d 的关系.

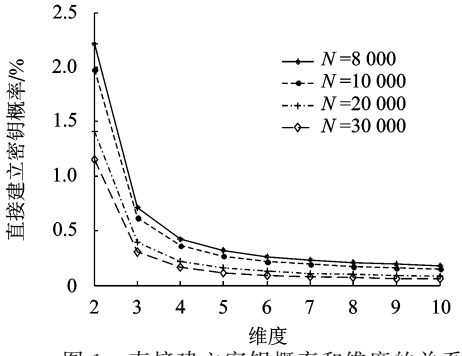

图 1 直接建立密钥概率和维度的关系

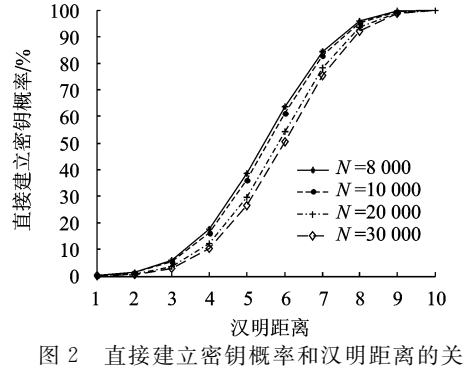

图 2 直接建立密钥概率和汉明距离的关系

从图 1 很容易知道，通过采用新的对偶密钥预分配方案，任意两个节点直接建立对偶密钥的概率随着网络规模的增大而减小，此外，当网络规模一定，超立方体维度增加时，任意两个节点直接建立对偶密钥的概率减小. 从图 2，任意两个节点直接建立对偶密钥的概率随着汉明距离门限值的增大而迅速增加. 而且可以注意到，当 $d=n$ 时，直接建立对偶密钥的概率 $p=1$，即任意两个邻居节点可以直接建立对偶密钥.

2.2 安全性分析

在无线传感器网络，攻击者可以物理俘获一些节点来获取其存储的秘密信息，如通信密钥、关键数据和其它有价值的信息. 节点俘获攻击是无线传感器网络最有威胁的攻击之一.

2.2.1 攻击一对特定节点

首先看攻击一对特定节点. 当攻击者俘获两个相关节点的任意一个时，其特定的直接对偶密钥肯定被攻破. 方案的安全性更关心当攻击者没有攻破相关节点时，攻破对偶密钥的难度和阻止建立对偶密钥的难度.

如果邻居节点 a 和 b 能够直接建立对偶密钥，在没有攻破相关节点的情况下，想要攻破对偶密钥只有攻破其共享的多项式. 这需要攻击者至少俘获 $(t+1)$ 个传感器节点. 即使攻击者成功攻破了多项式，相关的节点仍然可以通过路径密钥建立过程重建对偶密钥. 从路径密钥建立过程看，存在 $C_{n-d'}^{n-d}m^d-2$ 个中间节点可以直接帮助节点 a 和 b 重建对偶密钥. 中间节点的选择如图 3 所示.

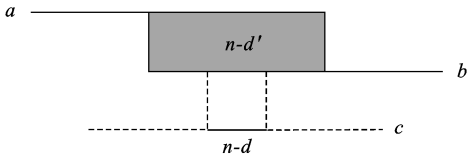

图 3 a 和 b 的汉明距离 $d'\leqslant d$ 的中间节点 c

2.2.2 攻击网络

假设攻击者知道多项式子组分配机制，他能够通过选择一个个特定的传感器节点来攻破多项式，最终攻破整个网络. 假定攻击者正好攻破了 p 中 l 个多项式，则有 $m^d\times l$ 个传感器节点存在至少一个多项式份额被攻破. 而 $m^n-m^d\times l$ 个节点的多项式份额没有被攻破. 根据假设，攻击者正好攻破了 l 个多项式，可知 $m^n-m^d\times l$ 个节点可以建立对偶密钥. 所以，攻击者攻破大约 $(t+1)l$ 个传感器节点(每个多项式为 $t+1$ 个节点)，但是只影响 $m^d\times l$ 个传感器节点的对偶密钥建立，包括被攻破的节点.

假定攻破多项式的概率为 p_c，则至少有一个多项式份额攻破的传感器节点个数最多为 $N'=p_c\times(C_n^d m^{n-d}\times m^d)=p_c\times N\times C_n^d$. 而剩余的 $N-N'$ 个节点没有被攻破的多项式份额. 因此，剩余的 $N-N'$ 个传感器节点可以通过任意共享的多项式直接建立对偶密钥，而非直接建立的对偶密钥则可能受到影响. 他们可能需要选择新的不属于 N' 个俘获节点的替代节点重建对偶密钥.

假定传感器网络的规模为 $N=10\,000$，图 4 表示 p_c 和受影响的节点数目，汉明距离门限值之间的关系. 从图 4 可以看出，当网络规模和攻破的多项式比例一定的情况下，随着汉明距离门限值的增大，受影响的传感器节点的个数也在增加.

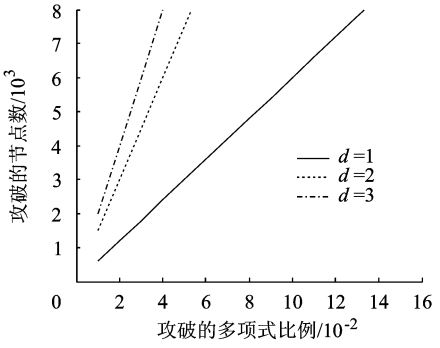

图 4 攻破多项式比例和攻破节点数的关系

(下转第 1087 页)