第33卷 第10期 计 算 机 工 程 2007年5月
Vol.33 No.10 Computer Engineering May 2007
·博士论文· 文章编号：1000—3428(2007)10—0001—03 文献标识码：A 中图分类号：TP393

基于层次超立方体模型的对偶密钥预置算法

王 雷[1,2]，陈治平[1,2]
(1. 福建工程学院计算机与信息科学系，福州 350014；2. 清华大学计算机科学与技术系，北京 100084)

摘 要：通过所建立对偶密钥，传感器网络节点之间可使用加密技术进行通信，从而保障了通信的安全性。在KDC和基于多项式池的密钥预置模型基础上，提出了一种用于密钥预置的层次超立方体模型及其密钥预置算法。理论与实验分析表明，与基于多项式和基于多项式池的对偶密钥预置算法相比，该算法具有更好的安全性能与更高的对偶密钥建立概率。

关键词：对偶密钥；传感器网络；密钥池；密钥预置；H2模型

Pairwise Key Predistribution Algorithm Based on Hierarchical Hypercube Model

WANG Lei[1,2], CHEN Zhiping[1,2]
(1. Department of Computer and Information Science, Fujian University of Technology, Fuzhou 350014;
2. Department of Computer Science & Technology, Tsinghua University, Beijing 100084)

【Abstract】 Security schemes of pairwise key establishment, which enable sensors to communicate with each other securely, play a fundamental role in research on security issue in wireless sensor networks. A general framework for key predistribution named H2 (Hierarchical Hypercube) is presented, based on the idea of key distribution center and polynomial pool schemes. Theoretic analysis and experimental figures show that the new algorithm has better security performance and provides higher possibilities for sensors to establish pairwise key, compared with previous related works such as polynomial and polynomial pool-based pairwise key predistribution algorithms.

【Key words】 Pairwise key; Sensor networks; Key pool; Key predistribution; H2 model

1 概述

在敌意环境下，安全认证、密钥管理等安全手段对传感器节点之间通信的安全性具有重要意义[1,2]。对偶密钥作为一种基础安全机制，可使得传感器节点之间利用加密技术进行通信，从而可有效保障其通信的安全性。但由于传感器节点的资源限制原因[3,4]，显然公共密钥加密、KDC(Key Distribution Center)等传统技术并不适合传感器网络节点之间的对偶密钥建立，因此，有必要研究适合传感器网络特点的新的对偶密钥建立算法。

考虑传感器网络的资源限制特点，2002年Eeschnaure和Gligor[5]基于密钥预置机制，提出了一种基于概率密钥预置模型的传感器网络对偶密钥建立算法。2003年，Chan等[6]对上述思想进行了扩展，提出了两种新的密钥预置模型：即t-composite密钥预置模型和随机对偶密钥模型。2004年，Liu等[7]又对上述方法进行了改进，并基于多项式密钥预置模型[8]，给出了一种基于多项式池的密钥预置模型，并提出了两种新的密钥预置算法：即随机子集指派和基于超立方体指派的密钥预置算法。

在以上几种密钥预置模型中，q-composite置模型的缺陷是当小部分的节点妥协时，将会对很大部分的对偶密钥造成影响。随机对偶密钥模型的缺陷是：若要让任意两个节点之间均具有一个对偶密钥，则其对节点的存储要求过大，这与传感器网络的资源限制矛盾。基于多项式池的密钥预置模型中，当两个节点之间不存在对偶密钥时，其提出的随机子集指派密钥预置算法无法保障在这两个节点之间建立一条密钥路径，基于超立方体指派的密钥预置算法虽然能保障密钥路径的建立，但节点之间直接建立对偶密钥的概率低，从而导致节点在间接密钥建立过程的通信开销大。

为了进一步提高节点之间直接建立对偶密钥的概率，有效降低间接密钥建立过程的通信开销，本文结合基于多项式密钥和密钥池加密技术的优点，并在KDC和多项式池的密钥预置模型基础上，提出了一种用于密钥预置的H2模型及其密钥预置算法。新算法利用H2模型中节点编码的特性进行密钥预置，理论与实验分析表明，与基于多项式的密钥预置模型，以及基于多项式池的密钥预置模型的对偶密钥预置算法相比，新算法具有更好的安全性能，因此，它是一种适合传感器网络特点的高效对偶密钥预置算法。

2 预备知识

定义1 对偶密钥 当任意两个节点具有某个共同的密钥E时，则称这两个节点之间具有一个对偶密钥E。

定义2 密钥路径 当两个节点A_0，A_k之间不具备对偶密钥时，若存在这样一条路径$A_0, A_1, A_2, \ldots, A_{k-1}, A_k$，使得任意节点对$A_i$，$A_j$之间至少存在一个对偶密钥，其中$0\le i\le k-1$，$1\le j\le k$。

定义3 n维超立方体互联网络[9,10] n维超立方体网络

基金项目：福建省青年科技人才创新基金资助项目(2005J051)；福建省自然科学基金资助项目(A0510024)
作者简介：王 雷(1973－)，男，副教授、博士后，主研方向：计算机网络，机器学习；陈治平，副教授、博士后
收稿日期：2006-06-25 **E-mail：**13308404743@hn165.com

Hn(简称为n–cube)是具有下述性质的一种网络拓扑结构：(1)它由 2^n个结点和$n\cdot 2^{n-1}$条边构成；(2)每一个结点可由一个不相同的n位二进制串$b_1b_2\ldots b_n$进行编号；(3)结点编号的规则为：当且仅当Hn中两个结点的二进制串恰有一位不同时，两个结点是相邻的，即这两个结点之间有一条边相连。

图 1 所示为一个 4 维超立方体网络的拓扑结构，图中共有 2^4=16 个节点和 $4\cdot 2^{4-1}$=32 条边，节点的编号为 0000~1111。

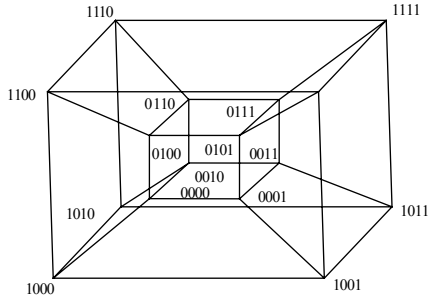

图 1 四维超立方体互联网络的拓扑结构

3 H2 (Hierarchical Hypercube)模型

定义 4 H2 模型 假设有 2^n个节点，则n维H2 模型H2(n)的构造算法如下：

(1)每 $2^{\lceil n/2\rceil}$个节点连接成一个$\lceil n/2\rceil$维超立方体：在每个$\lceil n/2\rceil$维超立方体中，各节点按 $\underbrace{00\ldots0}_{\lceil n/2\rceil}$ ~ $\underbrace{11\ldots1}_{\lceil n/2\rceil}$进行编号(称为内超立方体节点编号)，于是共得到 $2^{\lfloor n/2\rfloor}$个这样的$\lceil n/2\rceil$维超立方体。其中$\lfloor\ \rfloor$为向下取整符，$\lceil\ \rceil$为向上取整符。

(2)将这 $\lfloor n/2\rfloor$个$\lceil n/2\rceil$维超立方体按 $\underbrace{00\ldots0}_{\lfloor n/2\rfloor}$ ~ $\underbrace{11\ldots1}_{\lfloor n/2\rfloor}$进行编号(称为外超立方体节点编号)，并按如下方法连接成$\lfloor n/2\rfloor$维超立方体：在编号为 $\underbrace{00\ldots0}_{\lfloor n/2\rfloor}$ ~ $\underbrace{11\ldots1}_{\lfloor n/2\rfloor}$的这 $2^{\lfloor n/2\rfloor}$个$\lceil n/2\rceil$维超立方体中,具有相同内超立方体节点编号的节点连接成一个$\lfloor n/2\rfloor$维超立方体。

(3)H2(n)的编码：H2(n)采用如下的编码方式，每个节点由两部分(r, h)决定，其中 r 为外超立方体节点编号，$\underbrace{00\ldots0}_{\lfloor n/2\rfloor}\le r\le\underbrace{11\ldots1}_{\lfloor n/2\rfloor}$；h 为内超立方体节点编号，$\underbrace{00\ldots0}_{\lceil n/2\rceil}\le h\le\underbrace{11\ldots1}_{\lceil n/2\rceil}$。

4 基于 H2 密钥预置机制的对偶密钥算法

假定传感器网络包含 $2^{n-1}<N\le 2^n$个节点。算法首先生成一个n维H2(n)，并按如下方法生成多项式密钥池，并为传感器网络中的各个节点进行密钥预置。

(1)密钥设置机随机生成一个有限域F_q上具有$n*2^n$个度数为t的二元多项式的二元多项式池：

$$F=\{\ f^{i}_{<i_1,i_2,\ldots,\ i_{\lfloor n/2\rfloor-1}>}(x,y),\ f^{j}_{<j_1,j_2,\ldots,\ j_{\lceil n/2\rceil-1}>}(x,y)\mid 0\le i_1\le i_2\le\ldots\le i_{\lfloor n/2\rfloor-1}\le 1,\ 1\le i\le\lfloor n/2\rfloor,\ 0\le j_1\le j_2\le\ldots\le j_{\lceil n/2\rceil-1}\le 1,\ 1\le j\le\lceil n/2\rceil\}$$

(2)算法为 H2(n)中属于第 $(i_1,i_2,\ldots,\ i_{\lfloor n/2\rfloor})$ 个$\lceil n/2\rceil$维超立方体的每个维度 j 指派 $2^{\lceil n/2\rceil-1}$ 个二元多项式：

$$\{\ f^{j}_{<j_1,j_2,\ldots,\ j_{\lceil n/2\rceil-1}>}(x,y)\mid 0\le j_1\le j_2\le\ldots\le j_{\lceil n/2\rceil}\le 1\ \},$$

其中，$1\le j\le\lceil n/2\rceil$。

(3)算法为 H2(n)中属于第 $(j_1,j_2,\ldots,\ j_{\lceil n/2\rceil})$ 个$\lfloor n/2\rfloor$维超立方体的每个维度 i 指派 $2^{\lfloor n/2\rfloor-1}$ 个二元多项式：

$$\{\ f^{i}_{<i_1,i_2,\ldots,\ i_{\lfloor n/2\rfloor-1}>}(x,y)\mid 0\le i_1\le i_2\le\ldots\le i_{\lfloor n/2\rfloor-1}\le 1\},$$

其中，$1\le i\le\lfloor n/2\rfloor$。

(4)算法将以下 n 个多项式的分量：

$$\{\ f^{1}_{<j_2,\ldots,\ j_{\lceil n/2\rceil}>}(x,y),\ f^{2}_{<j_1,j_3,\ldots,\ j_{\lceil n/2\rceil}>}(x,y),\ldots,\ f^{\lceil n/2\rceil}_{<j_1,j_2,\ldots,\ j_{\lceil n/2\rceil-1}>}(x,y)\}\ \cup\ \{\ f^{1}_{<i_2,i_3,\ldots,\ i_{\lfloor n/2\rfloor}>}(x,y),\ f^{2}_{<i_1,i_3,\ldots,\ i_{\lfloor n/2\rfloor}>}(x,y),\ldots,\ f^{\lfloor n/2\rfloor}_{<i_1,i_2,\ldots,\ i_{\lfloor n/2\rfloor-1}>}(x,y)\}$$

指派给 H2(n)中的任意节点：

$$((i_1,i_2,\ldots,\ i_{\lfloor n/2\rfloor}),(j_1,j_2,\ldots,\ j_{\lceil n/2\rceil}))$$

(5)密钥设置机在 n 维空间上，按从小到大的顺序，为每个传感器节点 A 连续指派一个唯一序列：

$$((i_1,i_2,\ldots,\ i_{\lfloor n/2\rfloor}),\ (j_1,j_2,\ldots,\ j_{\lceil n/2\rceil}))$$

作为其 ID，其中，$0\le i_1\le i_2\le\ldots\le i_{\lfloor n/2\rfloor}\le 1$，$0\le j_1\le j_2\le\ldots\le j_{\lceil n/2\rceil}\le 1$。

(6)密钥设置机预置密钥：

$$F_A=\{\ f^{1}_{<j_2,\ldots,\ j_{\lceil n/2\rceil}>}(j_1,y),\ f^{2}_{<j_1,j_3,\ldots,\ j_{\lceil n/2\rceil}>}(j_2,y),\ldots,\ f^{\lceil n/2\rceil}_{<j_1,j_2,\ldots,\ j_{\lceil n/2\rceil-1}>}(j_{\lceil n/2\rceil},y)\}\ \cup\ \{\ f^{1}_{<i_2,\ldots,\ i_{\lfloor n/2\rfloor}>}(i_1,y),\ f^{2}_{<i_1,i_3,\ldots,\ i_{\lfloor n/2\rfloor}>}(i_2,y),\ldots,\ f^{\lfloor n/2\rfloor}_{<i_1,i_2,\ldots,\ i_{\lfloor n/2\rfloor-1}>}(i_{\lfloor n/2\rfloor},y)\}$$

及 A 的 ID 给节点 A。

5 算法分析

5.1 可行性分析

定理 1 采用基于H2 模型的新型密钥预置机制及其对偶密钥算法，任意两个节点之间建立直接对偶密钥的概率 $P_{H2}\approx(2^{\lfloor n/2\rfloor}+2^{\lceil n/2\rceil})/(N-1)$。

证明 由于算法对任意节点 $A((i_1,i_2,\ldots,i_{\lfloor n/2\rfloor}),(j_1,j_2,\ldots,j_{\lceil n/2\rceil}))$的预置密钥为$F_A=\{\ f^{1}_{<j_2,\ldots,\ j_{\lceil n/2\rceil}>}(j_1,y),\ f^{2}_{<j_1,j_3,\ldots,\ j_{\lceil n/2\rceil}>}(j_2,y),\ldots,\ f^{\lceil n/2\rceil}_{<j_1,j_2,\ldots,\ j_{\lceil n/2\rceil-1}>}(j_{\lceil n/2\rceil},y)\}\ \cup\ \{\ f^{1}_{<i_2,\ldots,\ i_{\lfloor n/2\rfloor}>}(i_1,y),\ f^{2}_{<i_1,i_3,\ldots,\ i_{\lfloor n/2\rfloor}>}(i_2,y),\ldots,\ f^{\lfloor n/2\rfloor}_{<i_1,i_2,\ldots,\ i_{\lfloor n/2\rfloor-1}>}(i_{\lfloor n/2\rfloor},y)\}$。显然，与A有直接对偶密钥的节点共有 $2^{\lfloor n/2\rfloor}+2^{\lceil n/2\rceil}$个。而网络总节点数为 $2^{n-1}<N\le 2^n$，因此，$P_{H2}\approx(2^{\lfloor n/2\rfloor}+2^{\lceil n/2\rceil})/(N-1)$。

图 2 给出了基于 H2 模型的新型密钥预置机制及其对偶密钥算法，与基于超立方体模型的密钥预置机制及其对偶密钥算法的直接密钥建立概率对比数据。

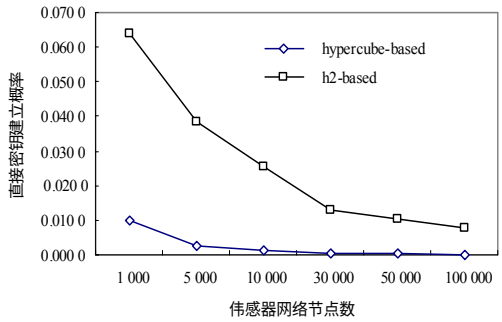

图 2 H2-based 与 Hypercube-based 算法直接密钥建立的概率比较

定理 2 假定采用基于H2 模型的新型密钥预置机制及其对偶密钥算法，任意 2 个节点之间建立直接对偶密钥的概率为P_{H2}，而采用基于超立方体模型的密钥预置机制及其对偶密

钥算法，任意 2 个节点之间建立直接对偶密钥的概率为P_H，则$P_{H2}>>P_H$。

证明 假定网络总节点数为 $2^{n-1}< N \le 2^n$，则依据性能分析，$P_H \approx \frac{n}{N-1}$。显然有

$$\lim_{n\to\infty}\frac{P_H}{P_{H2}}=\lim_{n\to\infty}\frac{n}{2^{\lfloor n/2\rfloor}+2^{\lceil n/2\rceil}}=0$$

定理的结论成立。

5.2 存储开销分析

定理 3 采用基于 H2 模型的对偶密钥预置算法，与采用基于超立方体模型的对偶密钥预置算法，具有相同的存储开销。

证明

(1) 任意节点 $A((i_1,i_2,\ldots,i_{\lfloor n/2\rfloor}),(j_1,j_2,\ldots,j_{\lceil n/2\rceil}))$ 需要存储域 q 上的 n 个度数为 t 的二元多项式，因此其所需要的存储开销为 n(t+1)log q bit。

(2)为了保障密钥的安全性，对任意二元多项式 f(x,y)，节点 $A((i_1,i_2,\ldots,i_{\lfloor n/2\rfloor}),(j_1,j_2,\ldots,j_{\lceil n/2\rceil}))$还需存储所有能够利用 f(x,y)与之建立直接对偶密钥的妥协节点的 ID 信息。由于二元多项式 f(x,y)的度数为 t，因此多余 t+1 个能够利用 f(x,y)与 A 建立直接对偶密钥的节点妥协时，f(x,y)将被破译。因此，对任意二元多项式 f(x,y)，节点 A 最多只需要存储 t 个能够利用 f(x,y)与之建立直接对偶密钥的妥协节点的 ID 信息。另外，由于节点的 ID 为一个 n 维的 0-1 向量，因此易知节点 A 只需要确定妥协节点 ID 的哪一位与之互异，即可判定该节点是否妥协节点，因此其所需要的存储开销为 nt bit。

(3)任意节点 $A((i_1,i_2,\ldots,i_{\lfloor n/2\rfloor}),(j_1,j_2,\ldots,j_{\lceil n/2\rceil}))$ 还需要存储自己的节点 ID，共需要存储开销为 n bits。

由以上(1)、(2)、(3)的分析可知，采用基于 H2 模型的对偶密钥预置算法，任意节点的存储开销为 n(t+1)log q+nt+n= n(t+1)log 2q bits。

假定网络总节点数为 $2^{n-1}< N \le 2^n$，则依据存储开销分析，易知定理的结论成立。

5.3 安全性分析

当部分传感器节点妥协时，基于 H2 密钥预置机制的强容错性，源节点可以通过寻找替代密钥路径来重建与目的节点之间的新对偶密钥。

由第 4 节可知，二元多项式池F中共有$n*2^n$个度数为t的二元多项式，即$|F|=n*2^n$；而每个传感器节点包含n个不同的二元多项式分量；因此，对任意传感器节点，其包含给定二元多项式f的分量的概率为$n/|F|$。假定传感器网络的总节点数为 $2^{n-1}< N \le 2^n$，网络中妥协节点数为 N_c，则在 N_c 个妥协节点中恰好包含i个f的分量的概率为

$$P_i=\frac{N_c!}{(N_c-i)!\,i!}\left(\frac{n}{|F|}\right)^i\left(1-\frac{n}{|F|}\right)^{N_c-i}$$

由于攻击者要破解 f 需要至少妥协个 t+1 节点，因此，给定二元多项式 f 的妥协概率为

$$P_c=1-\sum_{i=0}^{t}P_i$$

由H2 模型的特性易知，当某个二元多项式f妥协时，非妥协传感器节点之间的链路妥协概率可估算为：$P_{link}=P_c\times P_{H2}$。由定理 1 可知，任意 2 个节点之间建立直接对偶密钥的概率为P_{H2}，故建立间接对偶密钥的概率为 $1-P_{H2}$。从而任意 2 个非妥协传感器节点之间的直接对偶密钥妥协概率可估算为：$P_{H2}\times P_c$；而它们之间的间接对偶密钥妥协概率可估算为

$$(1-P_{H2})[1-(1-\frac{N_c}{N})\times(1-P_c)^2]$$

因此，任意两个非妥协传感器节点之间的(直接或间接)对偶密钥妥协概率为

$$P_{key}=P_{H2}\times P_c+(1-P_{H2})[1-(1-\frac{N_c}{N})\times(1-P_c)^2]$$

图 3 给出了传感器网络规模 N=30 000，二元多项式度数 t=2 时，采用基于 H2 模型的对偶密钥预置算法与基于超立方体模型的对偶密钥预置算法，任意两个非妥协传感器节点之间的(直接或间接)对偶密钥妥协的概率与网络中妥协节点比例之间的关系对比数据。

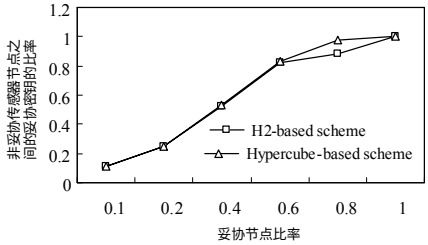

图 3 基于 H2-based 与 Hypercube-based 算法的对偶密钥妥协概率与妥协节点比例对比

显然，由图 3 可知，在传感器网络规模及妥协节点比例相同时，基于 H2 模型的的对偶密钥预置算法中，任意两个非妥协传感器节点之间的(直接或间接)对偶密钥妥协的概率，要低于基于超立方体模型的对偶密钥预置算法中的对偶密钥妥协概率。

6 结论

本文提出了一种用于对偶密钥预置的 H2 模型及其密钥预置算法，与基于多项式池的密钥预置模型的对偶密钥预置算法相比，新算法在相同存储的条件下，有效提高了任意两个传感器网络节点之间直接对偶密钥建立的概率，且具有良好的安全性能。因此，它是一种适合传感器网络特点的高效对偶密钥预置算法。

参考文献

1 Liu D, Ning P. Efficient Distribution of Key Chain Commitments for Broadcast Authentication in Distributed Sensor Networks[C]// Proceedings of the 10th Annual Network and Distributed System Security Symposium. 2003.

2 Wang Lei, Chen Zhiping. Researches on Scheme of Pairwise Key Establishment for Distributed Sensor Networks[C]//Proceedings of the 1st ACM Workshop on Wireless Multimedia Networking and Performance Modeling. 2005.

3 任丰原, 黄海宁, 林　闯. 无线传感器网络[J]. 软件学报, 2003, 14(7): 1282-1291.

4 林亚平, 王　雷, 陈治平. 传感器网络中一种分布式数据汇聚层次路由算法[J]. 电子学报, 2004, 32(11): 1801-1805.

5 Eeschnaure L, Gligor V D. A Key-management Scheme for Distributed Sensor Networks[C]//Proceedings of the 9th ACM Conference on Computer and Communication Security. 2002.

(下转第 43 页)