传感器网络中基于 DNA 模型的对偶密钥建立算法研究

蔡立军[1,2], 王 雷[1,2], 林亚平[1,2], 李小龙[2]
(1. 湖南大学软件学院, 湖南长沙 410082; 2. 湖南大学计算机与通信学院, 湖南长沙 410082)

摘 要: 在 KDC(Key Distribution Center) 和 DNA 多样性的基础上, 提出了一种用于密钥预置的 DNA 模型及其密钥预置(Key Predistribution) 机制, 然后, 在结合密钥池(Key Pool) 加密技术优点的基础上, 提出了一种传感器网络中基于 DNA 模型的新对偶密钥建立算法. 新算法利用 DNA 链中寡聚核苷酸编码特性进行密钥预置, 任意节点对之间以 DNA 链进行信息交换, 而以 DNA 链中包含的某段寡聚核苷酸对应的编码作为实际对偶密钥. 理论与实验分析表明, 与基于多项式、多项式池的密钥预置模型的对偶密钥建立算法相比, 新算法具有更好的安全性能, 更低的通信开销、以及更高的直接对偶密钥建立概率. 因此, 是一种更适合传感器网络特点的新型高效对偶密钥建立算法.

关键词: 对偶密钥; 传感器网络; 密钥池; 密钥预置; DNA 模型
中图分类号: TP391 文献标识码: A 文章编号: 0372-2112 (2008) 01-0171-06

Researches on DNA Model Based Algorithm of Establishment of Pairwise Key for Sensor Networks

CAI Li-jun[1,2], WANG Lei[1,2], LIN Ya-ping[1,2], LI Xiao-long[2]
(1. *College of Software, Hunan University, Changsha, Hunan 410082, China;*
2. *College of Computer and Communication, Hunan University, Changsha, Hunan 410082, China*)

Abstract: On the basis of KDC (key distribution center) and diversity of DNA molecules, an innovative DNA model for key predistribution and key predistribution scheme based on the new DNA model are proposed. And in addition, by combing with the good characteristics of key pool, a novel DNA model based pairwise key establishment algorithm is presented for distributed sensor networks, which uses characteristics of the code of oligonucleotides in DNA strands for key predistribution, and in which, any pair of nodes exchange DNA strands information and use the code of some oligonucleotide in the DNA strand as their actual pairwise key. Theoretical and experimental analyses show that, compared with those previous well-known polynomial-based and polynomial pool-based key predistribution models and pairwise key establishment algorithms, the newly proposed algorithm has better security, lower communication costs and higher probability of direct pairwise key establishment. So, it is a better and more efficient new pairwise key establishment algorithm suitable for distributed sensor networks.

Key words: pairwise key; sensor networks; key pool; key predistribution; DNA model gene clustering

1 引言

集传感、数据处理及网络通信功能于一体的无线集成网络传感器[1], 由于具有体积小、便宜及彼此之间可在近距离内进行无线通信等良好特性, 在环境与军事监控、地震与气候预测、地下及空间探索等许多方面得到广泛应用. 并被认为是本世纪的一项具有挑战性的研究课题[2]. 作为一种新型的无线自组(Ad hoc) 网络[3], 与传统的移动 Ad hoc 网络节点相比, 传感器网络节点都很小, 主要通过电池驱动, 且它们之间通过无线链路进行通信. 因此, 传感器节点的存储、能量、处理能力等资源非常有限.

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[4~7]. 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, 从而有效保障其通信的安全性. 但基于前述传感器节点的资源限制原因, 显然公共密钥加密、KDC(Key Distribution Center) 等传统的对偶密钥建立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.

考虑传感器网络资源限制的特点, 2002 年

收稿日期: 2005-06-30; 修回日期: 2007-08-23
基金项目: 湖南省自然科学基金(No. 06JJ20049, No. 07JJ5085)

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

Eeschnaure 和 Gligor[8] 基于密钥预置(Key Predistribution)机制,提出了一种基于概率密钥预置(Probabilistic Key Predistribution)模型的传感器网络对偶密钥建立算法.其主要思想是让每个传感器节点在其被部署之前从密钥池(Key Pool)中随机选择一组密钥,使得任意两个传感器节点在一定概率上具有至少一个共同密钥.2003 年,Chan 等[9]对上述思想进行了扩展,提出两种新的密钥预置模型:t-composite 密钥预置模型和随机对偶密钥模型.其中 t-composite 密钥预置模型同样利用密钥池进行密钥选择,但要求两个节点从它们共同拥有的至少 t 个预置密钥中计算出其对偶密钥;而随机对偶密钥模型则是随机成对选择传感器节点,然后为每对节点随机分配一个唯一的对偶密钥.分析表明,t-composite 密钥预置模型和随机对偶密钥模型均可有效提高概率密钥预置模型的安全性.2004 年,Liu 等[10]又对上述方法进行了改进,并基于多项式密钥预置模型[11],给出了一种基于多项式池的密钥预置(Polynomial Pool-based Key Predistribution)模型,并提出两种新的密钥预置算法:随机子集指派(Random Subset Assignment)和基于超立方体指派(Hypercube-based Assignment)密钥预置算法.

在以上几种密钥预置模型中,q-composite 密钥预置模型和概率密钥预置模型的缺陷是:当小部分的节点被俘后,将会对很大部分的对偶密钥造成影响.而随机对偶密钥模型虽然没有上述缺陷,但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较好地克服了上述两种缺陷,但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,而其提出的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建立直接对偶密钥的概率,有效降低间接密钥建立过程的通信开销,本文结合 DNA 的多样性和密钥池(Key Pool)加密技术的优点,在 KDC 密钥预置模型基础上,提出了一种用于密钥预置的 DNA 模型,并基于新的 DNA 模型提出了一种新型密钥预置(Key Predistribution)机制,然后,在结合密钥池加密技术的优点的基础上,提出了一种传感器网络中基于 DNA 模型的新对偶密钥算法.新算法利用 DNA 链中寡聚核苷酸编码的特性进行密钥预置,任意传感器节点对之间以 DNA 链中的一段寡聚核苷酸编码作为对偶密钥.理论与实验分析表明,新算法具有更好的安全性能、更低的通信开销、以及更高的直接对偶密钥建立概率.

2 预备知识

2.1 基本概念

定义 1(密钥预置) 即在节点部署之前,将对应的加密、解密算法预先植入到节点之中.

定义 2(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 3(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, …, A_{k-1}, A_k,使得任意节点对 A_i, A_{i+1} 之间至少存在一个对偶密钥,其中 $0 \leqslant i \leqslant k-1$,则称 A_0 和 A_k 之间存在密钥路径.

2.2 DNA 模型[12, 13]

DNA 是一种高分子化合物,组成它的基本单位是脱氧核苷酸,每个脱氧核苷酸由一分子磷酸,一分子脱氧核糖和一分子含氮碱基组成.含氮碱基有四种,即腺嘌呤(A),鸟嘌呤(G),胞嘧啶(C)和胸腺嘧啶(T).DNA 不仅具有一定的化学组成,还具有规则的双螺旋结构.这一结构的主要特点是:(1) DNA 分子是由两条平行的脱氧核苷酸链盘旋而成,这两条脱氧核苷酸链互为对方的补链;(2) DNA 分子中的脱氧核糖和磷酸交替连接,排列在外侧;(3) 两条平行脱氧核苷酸链上的碱基通过氢键连接,形成碱基对.碱基对的配对方式有一定的规律,即嘌呤与嘧啶配对,而且腺嘌呤(A)一定与胸腺嘧啶(T)配对,鸟嘌呤(G)一定与胞嘧啶(C)配对.组成 DNA 的碱基虽然只有 A、T、G、C 这 4 种,碱基对的配对方式只有两种,但由于碱基对具有多种不同的序列,因而构成了 DNA 分子的多样性.

2.3 相关工作[8~10]

(1)传感器网络中基于多项式模型的密钥预置.

在基于多项式模型的密钥预置算法中,首先密钥设置机(Key Setup Server)在有限域 F_q 上生成一个二元 t 次多项式 $f(x, y) = \sum_{i,j=0}^{t} a_{ij} x^i y^j$,其中 $f(x, y)$ 满足对称特性,即 $f(x, y) = f(y, x)$.每个节点根据自己唯一的 ID 值计算与其他节点之间的共享密钥对 $f(\mathrm{ID}, \mathrm{ID}')$.然后,该模型要求节点保存一个二元 t 次多项式 $f(\mathrm{ID}, y)$,并与其他节点通过该多项式建立共享密钥对.文献[12]证明,当被俘获节点不超过 t 时不会泄露任何信息.

(2)传感器网络中基于多项式池模型的密钥预置.

前述基于多项式模型的密钥预置算法最多只能容许 t 个节点被俘获,且节点的存储开销与 t 的大小成正比,而传感器节点的存储能力非常有限,因此导致 t 的值也只能很小.但传感器网络的规模经常较大,如果要在很多节点被俘获的情况下,仍能保障整个网络中通

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

信的安全, 则小的 t 值显然不够, 这样就构成了一个矛盾. 为了解决上述问题, 2004 年 Liu 等[10]提出了一种基于多项式池的密钥预置模型. 该模型结合了基于多项式模型的密钥预置模型和密钥池(Key Pool)的优点, 其对偶密钥建立过程分为以下三个步骤: (1)多项式密钥池的生成与密钥预置; (2)直接密钥建立; (3)间接密钥建立.

多项式密钥池的生成与密钥预置: 主要是随机生成一个有限域 F_q 上度数为 t 的的二元多项式集合(池) F, 并给每个多项式指定一个唯一 ID. 然后, 选择一个多项式子集 $F_i \in F$, 并将 F_i 中所有多项式的在节点 i 的分量均指派给节点 i.

直接密钥建立: 如果节点 i 需要和节点 j 之间建立对偶密钥, 若节点 i, j 存在一个共同的二元多项式的分量, 则它们之间可类似 2.2 节中描述的基于多项式模型的密钥预置算法一样直接建立对偶密钥.

间接密钥建立: 如果节点 i 和节点 j 之间不存在对偶密钥, 则首先需要找到一条满足定义 3 中条件的密钥路径(Key Path), 然后让节点 i 和节点 j 之间通过该密钥路径来进行密文传递.

文献[10]提出了两种新的密钥预置算法: 随机子集指派(Random Subset Assignment)和基于超立方体指派(Hypercube-based Assignment)的密钥预置算法. 其主要思想分别是:

随机子集指派密钥预置算法是在多项式密钥池的生成过程中, 随机选择一个多项式子集 $F_i \in F$, 并将 F_i 中所有多项式的在节点 i 的分量均指派给节点 i. 显然, 利用该算法, 将无法保障节点 i 和节点 j 之间不存在对偶密钥时, 节点 i 和节点 j 之间能建立一条有效的密钥路径.

基于超立方体指派的密钥预置算法是在多项式密钥池的生成过程中, 基于超立方体模型进行二元多项式密钥池的生成, 并依据超立方体节点 ID 进行多项式子集的指派. 这样将使得在假定任意节点可与其他节点进行直接通信的前提下, 可保障节点 i 和节点 j 之间不存在对偶密钥时, 节点 i 和节点 j 之间一定能建立一条有效的密钥路径.

显然, 上述两种密钥预置算法均存在缺陷: (1)节点在对偶密钥建立过程中交换的均为密钥明文信息, 从而导致密钥信息容易被中途截获, 因此算法的安全性能不高; (2)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(Key Path), 而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, 从而导致节点在建立路径密钥过程中的通信开销大.

为了进一步提高节点之间直接建立对偶密钥的概率, 有效降低建立路径密钥的通信开销, 并在此基础上进一步研究出一种适合传感器网络特点的绝对安全的密钥预置及对偶密钥建立机制, 本文结合 DNA 的多样性和密钥池加密技术的优点, 在 KDC 密钥预置模型基础上, 提出了一种用于密钥预置的 DNA 模型, 并基于新的 DNA 模型提出了一种新型密钥预置机制, 然后, 在结合密钥池加密技术的优点的基础上, 提出了一种传感器网络中基于 DNA 模型的新对偶密钥算法. 在随后的第 3 节和第 4 节中给出了新算法的详细描述. 其中, 第 3 节给出了基于 DNA 模型的新型密钥预置机制及其对偶密钥算法的具体描述; 第 4 节对新算法的可行性、开销、以及安全性进行了论证.

3　基于 DNA 模型的对偶密钥建立算法

为了克服基于多项式及多项式池模型的密钥预置算法的缺陷, 本文结合 DNA 的多样性和密钥池加密技术的优点, 并在 KDC 密钥预置模型基础上, 提出了一种基于 DNA 模型的新型密钥预置机制及其对偶密钥算法. 新算法主要包括以下三个过程: (1) 多项式密钥池的生成与密钥预置; (2) 直接密钥建立; (3) 间接密钥建立.

3.1　DNA 密钥池的生成与密钥预置

步骤 **1**　对 n 个变量 $x_1, x_2, \cdots, x_n$, 首先合成 $2n$ 种短的寡聚核苷酸, 将它们分为 2 组, 第 1 组的 n 种寡聚核苷酸分别表示变量 $x_1, x_2, \cdots, x_n$; 第 2 组的 n 种寡聚核苷酸分别表示变量 $\bar{x}_1, \bar{x}_2, \cdots, \bar{x}_n$; 然后, 利用此两组 $2n$ 种寡聚核苷酸构造 DNA 链, 构造出此 $2n$ 种寡聚核苷酸的不同的 $2n$ 个组合, 每个组合包含 n 个变量所对应的寡聚核苷酸, 利用杂交的方法把它们连接成 2^n 个不同的 DNA 链; 对 n 个变量 $x_1, x_2, \cdots, x_n$, 我们选择 2 种互异颜色分别表示下标为奇数和下标为偶数的变量, 而对任意变量 x_i, 我们选择两种不同灰度分别表示 x_i 和 $\bar{x}_i$. 将生成的 2^n 个不同的 DNA 链看作密钥池.

例如: 对 3 个变量 x, y, z, 首先构造 $2^* 3 (= 6)$ 种短的寡聚核苷酸, 将它们分为 2 组, 第 1 组的 3 种寡聚核苷酸分别表示变量 x, y, z; 第 2 组的 3 种寡聚核苷酸分别表示变量 $\bar{x}, \bar{y}, \bar{z}$; 我们可选择图 1 所示的 6 种短的寡聚核苷酸.

x: AACCTGGT;　y: ACCATAGC;　z: AGAGTCTC

$\bar{x}$: CCAAGTTG;　$\bar{y}$: GTTGGGGT;　$\bar{z}$: AGCTTGCA

x': TTGGACCA;　y': TGGTATCG;　z': TCTCAGAG

$\bar{x}'$: GGTTCAAC;　$\bar{y}'$: CAACCCAA;　$\bar{z}'$: TCGAACGT

图 1　6 种短的寡聚核苷酸编码示意图

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

然后, 用此 6 种短寡聚核苷酸 $x, y, z, \bar{x}, \bar{y}, \bar{z}$ 杂交组合成 $2^3(=8)$ 个互异的 DNA 链, 并如图 2 所示. 其中, 对任意变量 x_i, 我们选择两种不同灰度分别表示 x_i 和 $\bar{x}_i$.

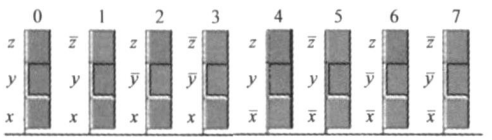

图 2 8 个互异的 DNA 链

由于每个 DNA 链均具有 n 个段, 而每个段包含两级灰度, 我们用 0, 1 表示此两级灰度. 为了进一步简化 DNA 链表示的复杂度, 我们限定 n 个变量 $x_1, x_2, \cdots, x_n$ 的取值为 0; $\bar{x}_1, \bar{x}_2, \cdots, \bar{x}_n$ 的取值为 1. 则对规模不超过 $2n$ 的传感器网络中的任意节点, 我们可用 n 维 0– 1 向量来表示其对应的 DNA 链.

例如: 图 2 中编号为 0~ 7 的 DNA 链可简单表示为: 0(000), 1(001), 2(010), 3(011), 4(100), 5(101), 6(110), 7(111).

步骤 **2** 对规模不超过 $2n$ 的传感器网络中的任意节点A, 我们从具有 $2n$ 个不同的 DNA 链的密钥池中随机选择一条 DNA 链指派给节点 A, 并将该 DNA 链对应的 n 维 0– 1 向量作为节点 A 的 ID.

3.2 直接密钥建立

假定传感器网络中的任意节点 A 均可与其他节点之间进行直接通信, 则节点 A 可依据以下方法生成与任意目的节点 B 之间的对偶密钥:

节点 A 按照从左到右顺序依次比对其自身与节点 B 的 ID, 若发现在某位上两者的值相同, 则选择该段对应的寡聚核苷酸编码作为其与节点 B 之间的对偶密钥. 而节点 B 同样可依据节点 A 的 ID 来判定其与节点 A 之间的对偶密钥.

例如: 假定节点 A 对应的 DNA 链为图 2 中的第 0 条DNA 链, 节点 B 对应的 DNA 链为图 2 中的第 4 条 DNA 链, 则节点 A 与节点 B 可选择其 DNA 链中第 2 段对应的寡聚核苷酸编码 ACCATAGC 作为它们之间的对偶密钥.

综上所述, 我们可给出节点 A 与节点 B 之间的直接对偶密钥建立算法 Direct_ Key_ Establishment_ Algorithm() 具体如下:

步骤 **1** 按照从左到右的顺序依次对比节点 A 与节点 B 的 ID; 若第 i 位相同, 则转步骤 2, 否则转步骤 3;

步骤 **2** 选择 DNA 链中第 i 段对应的寡聚核苷酸编码作为对偶密钥. 算法终止.

步骤 **3** 启动 3.3 节中的密钥路径建立算法.

3.3 间接密钥建立

若节点 A 与节点 B 的 ID 中所有位的值均不相同, 则节点 A 与节点 B 之间可按照如下方法建立间接对偶密钥:

节点 A 找到任意其它节点 C, 显然节点 A 与节点 C 之间具有直接对偶密钥, 而节点 B 与节点 C 之间也具有直接对偶密钥, 即 $A \leftrightarrow C \leftrightarrow B$ 为节点 A 与节点 B 之间的一条密钥路径.

例如: 假定节点 A 对应的 DNA 链为图 2 中的第 3 条 DNA 链, 节点 B 对应的 DNA 链为图 2 中的第 4 条 DNA 链, 则节点 A 与节点 B 之间通过图 2 中的其它任意 DNA 链对应的节点构成一条密钥路径.

综上所述, 我们可给出节点 A 与节点 B 之间的间接对偶密钥建立算法 Indirect_ Key_ Establishment_ Algorithm() 具体如下:

步骤 **1** 节点 A 找到任意其它节点 C.

步骤 **2** 节点 A 启动算法 Direct_ Key_ Establishment_ Algorithm(), 建立与节点 C 之间的直接对偶密钥.

节点 C 启动算法 Direct_ Key_ Establishment_ Algorithm(), 建立与节点 B 之间的直接对偶密钥. 算法终止.

4 算法分析

4.1 算法可行性分析

定理 **1** 对规模为 $2n-1< N \leqslant 2n$ 的传感器网络, 采用基于 DNA 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 $P_{\mathrm{DNA}} \approx 100\%$.

证明 对任意节点 $A(a_1, a_2, \cdots, a_n)$, $a_i \in \{0, 1\}$, 与 A 的 ID 至少存在一位相同的其他节点 ID 共有 $2n-2$ 个. 即, 在其余 $2n-1$ 个节点中, 与 A 有直接对偶密钥的节点共有 $2n-2$ 个. 因此, 任意两个节点之间建立直接对偶密钥的概率 $P_{\mathrm{DNA}}=(N-2)/(N-1)\,100\%$.

例如: 对具有 $N=10000$ 个节点的传感器网络, 经计算可知 $n=14$. 由定理 1 可知, 采用基于 DNA 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为 $P_{\mathrm{DNA}} \approx 100\%$. 而依据文献[10]中 5.3 节的性能分析可知, 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, 任意两个节点之间建立直接对偶密钥的概率为 $P_{\mathrm{H}} \approx 0.14\%$. 由此可知, 新算法具有更强的可行性. 结合定理 1 及文献[11], 我们进而可证得下述定理 2 成立.

定理 **2** 假定采用基于 DNA 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为 P_{DNA}, 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, 任意两个节点之间建立直接对偶密钥的概率为 P_{H}, 则 $P_{\mathrm{DNA}} \gg P_{\mathrm{H}}$.

证明 假定网络总节点数为 $2n-1< N \leqslant 2n$, 则依

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

据文献[10]中 5.3 节的性能分析, $P_H \approx \frac{n}{N-1}$. 再结合定理 1 显然有: $\lim_{n\to\infty}\frac{P_H}{P_{DNA}} = \lim_{n\to\infty}\frac{n}{2^n-2} = 0$. 即定理的结论成立.

图 3 给出了基于 DNA 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.

4.2 算法安全性分析

对基于 DNA 模型的对偶密钥建立算法, 由于传感器节点之间交换的是 DNA 链信息, 而它们之间采用的对偶密钥为某段 DNA 链对应的寡聚核苷酸编码. 如果寡聚核苷酸采用 128 位编码, 则寡聚核苷酸的总量可达 4^{128}种, 显然以目前超级计算机的计算能力是无法破解寡聚核苷酸编码的. 因此, 基于 DNA 模型的对偶密钥建立算法建立的对偶密钥是绝对安全的.

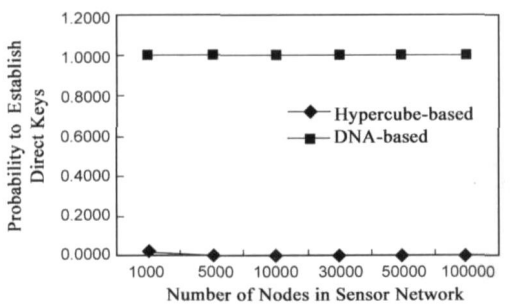

图 3　DNA-based 与 Hypercube-based 算法的直接密钥建立概率比较

4.3 算法开销分析

(1) 节点的存储开销

任意节点 $A(a_1, a_2, \cdots, a_n)$, $a_i \in \{0, 1\}$, 需要存储其 ID 信息共 n bits.

节点 A 还需存储与其 ID 对应的寡聚核苷酸编码信息, 假如采用 128 位编码, 则其所需要的存储开销为 $128n$ bits.

由以上分析可知, 传感器网络中任意节点的存储开销为 $129n$ bits.

(2) 节点的通信开销

在传感器网络中, 任意两个节点之间间接对偶密钥的建立过程实质上是一个利用单播消息传递建立路由的过程, 因此将产生通信开销. 假定任意节点均可与其他节点进行直接通信, 且每跳(Hop)的通信开销为 1, 则对距离为 L 的任意节点A、B, 可在 A、B 之间建立长度为L 的最短密钥路径, 即所要的通信开销最小为 L.

由定理 1 可知, 基于 DNA 模型的密钥建立算法的直接对偶密钥建立概率接近 100%. 因此, 基于 DNA 模型的对偶密钥建立算法的平均通信开销为 $L = 1$.

推论 **1**　采用基于 DNA 模型的新型密钥预置机制及其对偶密钥算法的平均通信开销, 远小于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的平均通信开销.

证明　假定网络总节点数为 $2n-1 < N \leqslant 2n$, 则依据文献[10]中 5.4 节的通信开销分析, 易知定理的结论成立.

图 4 给出了基于 DNA 模型的对偶密钥建立算法的平均通信开销与基于超立方体模型的对偶密钥建立算法的平均通信开销的对比数据.

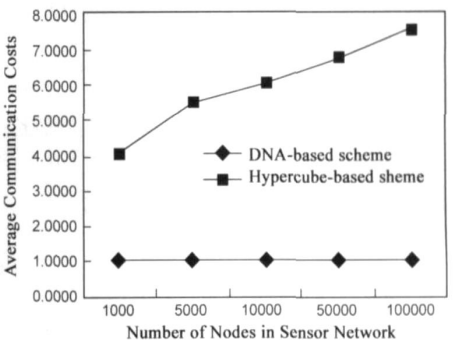

图 4　DNA-based 与 Hypercube-based 算法的平均通信开销比较

5　结论

提出了一种用于密钥预置的 DNA 模型, 并基于新的 DNA 模型提出了一种新型密钥预置(Key Predistribution)机制, 然后, 在结合 DNA 分子的多样性和密钥池(Key Pool)加密技术各自优点的基础上, 提出了一种传感器网络中的新对偶密钥建立算法. 与基于多项式池的密钥预置模型的对偶密钥建立算法相比, 新算法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, 达到 100%, 且具有更低的通信开销, 以及绝对的安全性能. 因此, 是一种更适合传感器网络特点的高效对偶密钥建立算法.

参考文献:

[1] G Pottie, W Kaiser. Wireless sensor networks[J]. Communications of the ACM, 2000, 43(5): 51-58.

[2] Estrin D, Govindan R, Heideman J, Kumar S. Next century challenges: scalable coordination in sensor networks[A]. Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking[C]. Seattle, Washington, USA: ACM Press, 1999. 263-270.

[3] 林亚平, 王雷. 传感器网络中一种基于位置信息的分布式数据汇聚层次路由算法[J]. 电子学报, 2004, 32(11): 1801-1805.
Lin Yaping, Wang Lei. A distributed data centric clustering hierarchical routing algorithm for sensor networks[J]. Acta Electronica Sinica, 2004, 32(11): 1801-1805. (in Chinese)

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

[4] Liu D, Ning P. Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks[A]. In Proceedings of the 10th Annual Network and Distributed System Security Symposium[C]. San Diego: ACM Press, 2003, 263-276.

[5] Karlof C, Wangner D. Secure routing in wireless sensor networks: attacks and countermeasures[A]. In Proceedings of 1st IEEE International Workshop on Sensor Networks Protocols and Application[C]. IEEE Press, 2003. 113-127.

[6] Pietro R D, Mancini L V, Mei A. Random key assignment for secure wireless sensor networks[A]. In 2003 ACM Workshop on Security in Ad Hoc and Sensor Networks[C]. New York, NY, USA: ACM Press, 2003. 62-71.

[7] Du W, Deng J, Han Y S, et al. A pairwise key predistribution scheme for wireless sensor networks[A]. In Proceedings of 10th ACM Conference on Computer and Communication Security[C]. Washington: ACM Press, 2003. 42-51.

[8] Eeschnaure L, Gligor V D. A key-management scheme for distributed sensor networks[A]. In Proceedings of the 9th ACM Coference on Computer and Communication Security[C]. Washington: ACM Press, 2002, 41-47.

[9] Chan H, Oerrig A, Song D. Random Key Predistribution Schemes for Sensor Networks[A]. In IEEE Symposium on Research in Security and Privacy[C]. IEEE Press, 2003. 197-213.

[10] Donggang Liu, Peng Ning, Rongfang Li. Establishing pairwise keys in distributed sensor networks[J]. ACM Transactions on Information and System Security, 2005, 8(1): 41-77.

[11] Blundo C, Desantis A, Kutten S, et al. Perfectly secure key distribution for dynamic conferences[A]. In Advances in Cryptology-CRYPTO'92[C]. Berlin: Springer-Verlag, 1993. 471-486.

[12] Lipton R. Using DNA to solve NP-complete problems[J]. Science, 1995, 268(4): 542-545.

[13] Frank G, Makiko F. Carter B. Making DNA add[J]. Science, 1996, 273(7): 220-223.

作者简介:

蔡立军 男, 1964 年 12 月出生于湖南常德, 1986 年毕业于华中科技大学计算机系, 现为湖南大学教授、博士. 主要从事机器学习、计算机网络、基因分类等方面的研究工作.
E-mail: ljcai@hnu.cn

王 雷 男, 1973 年 7 月出生于湖南长沙, 博士, 副教授. 主要研究方向为计算机网络、机器学习、生物计算.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net