文章编号:1001 - 9081(2010)06 - 1495 - 03

传感器网络中基于对偶编码的随机密钥建立算法

成奋华[1,2],周顺先[1],王　雷[1]
(1. 湖南大学 软件学院,长沙 410082; 2. 湖南科技职业学院, 长沙 410004)
(cfh898@163.com)

摘　要:为进一步提高传感器网络节点之间建立直接密钥的概率,降低间接密钥建立过程的通信开销,提高密钥的安全性能,提出了一种新的基于对偶编码的随机密钥建立算法。在新算法中,首先,采用随机数字对节点进行编码;然后,节点之间通过不同位进行第一次通信,并经过三次握手确定最终的密钥参数。理论分析和仿真实验结果表明,与传统的对偶密钥建立算法相比,新算法具有更高的密钥建立概率、密钥安全性能和更低的通信开销。

关键词:传感器网络;对偶编码;随机密钥;密钥安全
中图分类号: TP393　　**文献标志码**:A

Random-key establishment algorithm of pairwise coding for sensor networks

CHENG Fen-hua[1,2], ZHOU Shun-xian[1], WANG Lei[1]
(1. *College of Software, Hunan University, Changsha Hunan* 410082, *China*;
2. *Hunan Science Vocational College, Changsha Hunan* 410004, *China*)

Abstract: In order to further enhance the probability of direct key establishment between nodes in wireless sensor networks, reduce the communication cost of indirect key establishment, and improve the safety performance, a new algorithm for establishing random key based on pairwise coding was proposed. In this new algorithm, first, the nodes were coded with random digit. Then, the first time communication was set up between any two nodes, and the last key's parameter was ensured by thrice handshake. The theoretical analysis and experimental result show that, compared to the traditional algorithm of pairwise key establishment, the new algorithm has higher probability of direct key establishment and key safety, and lower communication costs.

Key words: sensor network; pairwise coding; random key; key safety

0　引言

对偶密钥作为一种基础安全机制,广泛应用于安全通信。但基于传感器节点的资源限制原因,显然公共密钥加密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[1-3]。目前,针对传感器节点的资源限制特性,文献[4]基于密钥预置机制,提出了一种基于概率密钥预置模型。文献[5]对上述思想进行了扩展,提出了 q-composite 密钥预置模型和随机对偶密钥模型。在此基础上,文献[6]基于多项式密钥预置模型[7]给出了一种基于多项式池的密钥预置模型,并提出了随机子集指派和基于超立方体指的密钥预置算法。上述对偶密钥预置模型,虽然有效地提高了传感器网络节点之间的通信安全性,但存在一个共同缺陷: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。

在基于 DNA 模型的对偶密钥建立算法[8]中,利用 DNA 链中寡聚核甘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甘酸对应的编码作为实际对偶密钥。该算法大大提高了直接对偶密钥建立概率。本文在该算法的基础上,综合随机密钥建立的过程,提出了一种新的基于对偶编码的随机密钥建立算法,与 DNA 模型的对偶密钥建立算法相比,新算法具有更高的密钥建立概率和密钥安全性能。

1　基于对偶编码的密钥池生成及密钥预置

1.1　基本概念

定义 1　密钥预置。即在节点部署之前,对节点进行编码并将对应的加密、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时,则称这两个节点之间具有一个对偶密钥。

定义 3　密钥函数。指通信过程中的密钥加密/解密函数 $f(x,y)$,函数满足对称性,即 $f(x,y) = f(y,x)$。

1.2　密钥池生成及密钥预置

为了提高密钥安全性能,结合文献[8]的思想进行密钥池的生成及密钥预置。方法如下。

第 1 步　对 n 个变量对 $(x_1,y_1),(x_2,y_2),(x_3,y_3),\cdots,(x_n,y_n)$ 中的 $2n$ 个变量分别随机赋予一个整数值。用这 n 个变量对构造出 2^n 个长度为 n 的链,其中第一位用 (x_1,y_1) 中的一个变量,第二位用 (x_2,y_2) 中的一个变量,依此类推,第 n 位用 (x_n,y_n) 中的一个变量,并且约定变量 $x_i(1 \leqslant i \leqslant n)$ 用编码 0 表示,变量 $y_i(1 \leqslant i \leqslant n)$ 用编码 1 表示,这样形成了 2^n 个二进制的编码号。

假设有 3 个变量对 $(x_1,y_1),(x_2,y_2),(x_3,y_3)$,则可以构造出 8 个链($2^3 = 8$),各个链的长度均为 3,各链分别为:$x_1x_2x_3$,$x_1x_2y_3$,$x_1y_2x_3$,$x_1y_2y_3$,$y_1x_2x_3$,$y_1x_2y_3$,$y_1y_2x_3$,$y_1y_2y_3$。

收稿日期:2010 - 01 - 06;**修回日期**:2010 - 03 - 17。

作者简介:成奋华(1969 -),男,湖南长沙人,副教授,主要研究方向:计算机网络、软件工程; 周顺先(1968 -),男,湖南邵阳人,副教授,博士,主要研究方向:计算机网络、机器学习; 王雷(1973 -),男,湖南长沙人,副教授,博士,主要研究方向:计算机网络、机器学习、生物计算。

因此，可以将这 8 个链看作 3 个变量对的密钥池，各个链对应的二进制编码为：000、001、010、011、100、101、110、111。

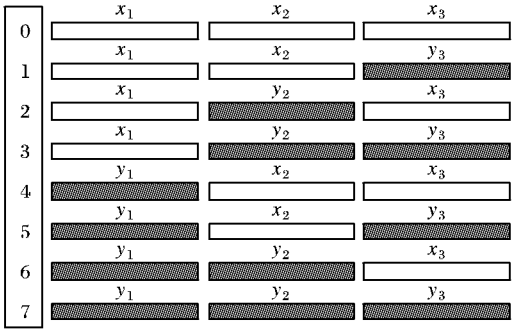

图 1 3 变量对的密钥池示意图

第 2 步 对同一个簇内规模不超过 2^n 的传感器网络中的任意节点 A，从具有 2^n 个不同链的密钥池中随机选择一个链指派给节点 A，并将其二进制的编码作为节点 A 的 ID。节点数与 n 有如下关系：当节点数 T 为 2^m 时（m 为整数），则 n 取值为 m；当节点数 T 满足 $2^m < T \leqslant 2^{m+1}$ 时，n 取值 $m+1$。

2 随机密钥建立算法

假设传感器节点按批次投放，每一批次为一个节点簇，这里先对节点进行如下编码：任意一个节点的编码分为两部分，前面一部分为部署簇编号，后面一部分为簇内编号，分别用二进制表示，字节长度根据簇的多少及每一个簇的大小来决定。比如节点 A 的编号为（0010，001100），则逗号前的编号 0010 代表这是第 2 号簇，而逗号后的编号 001100 则表示这是第 12 号节点，那么节点 A 的编号即为 2 号簇第 12 号节点。算法过程如下。

第 1 步 部署节点，并对节点按以上方式进行编码。

第 2 步 簇间通信路径建立过程。

1）假设同一簇内的节点 A 想和节点 B 通信，则 A 和 B 的簇编号是相同的，不同的是簇内编号，显然这两个编号中必定存在不同的位，从左至右取第一个不同的字节，作为彼此默认的密钥函数 $f(x,y)$ 中的密钥，根据前面密钥池的建立过程可知，这里的 x、y 分别为一个随机数，而不是单纯的 0 和 1。

2）节点 A 生成一个随机数字 t，用默认的对偶密钥函数 $f(x,y)$ 将数字 t 发送给 B，B 收到这个信息后，将 $f(x,y)$ 解密并取得数字 t，同时也生成一个随机数字 m，并将 m 用 $f(t,t)$ 加密后发回给 A。

3）A 收到 B 发回的消息后，如果能用 $f(t,t)$ 解开，则 A 有理由相信这是 B 发回的消息，同时它接收到了 m，倘若不能用 $f(t,t)$ 解开，则拒绝相信这是节点 B 发来的消息。

4）确定之后，A 便将需要发送的消息用 $f(t,m)$ 加密后发送给 B，由此，A 和 B 之间的对偶密钥建立起来，其通信密钥为 $f(t,m)$。

第 3 步 不同的簇之间通信时，由于簇与簇之间的距离往往较大，为了节省传输能耗，将簇内将所有需要传输的数据集中起来，批量传输给另外一个簇。比如簇 A 中节点 a 想和簇 C 中节点 c 通信，建立密钥时使用不同字节作为簇的编号字节，一旦密钥建立起来后，两个簇之间的信息传输都使用这一条路径，进行簇内传输。对于一些不需要及时传输的信息，可以批量传输。

假设同一簇内节点 A 和节点 B 的编号分别为（0011，1010110），（0011，1001101），在节点 A 与 B 之间建立通信路径的过程如下：

1）节点 A 对比自己与节点 B 的编号，发现簇内编号的第 3 位编码不同，于是将这两位编码所对应的随机数字作为初始密钥函数 $f(x,y)$ 的参数，并生成随机数字 t，不妨设 $t=6$，并将之用 $f(x,y)$ 加密后发送出去。

2）节点 B 收到消息后，同样对比节点 A 与自己的编号，获得默认密钥 $f(x,y)$，并用其解密信息，获得数字 t，同时生成随机数 m，不妨设 $m=9$，B 将 m 用 $f(6,6)$ 加密后发送给节点 A。此时 B 节点将解密密钥设置为 $f(6,9)$。

3）节点 A 收到消息后，试图用 $f(6,6)$ 去解密，因为它知道自己之前发送的随机数字为 6，如果能解开，则相信这是 B 发来而不是冒充者；如果不能解密，则拒绝相信。

4）节点 A 确认信息后，获得数字 9，则开始使用密钥 $f(6,9)$，此时节点 A，B 都使用对偶密钥 $f(6,9)$，路径建立。

3 算法性能分析

3.1 新算法与基于 DNA 模型算法的比较

文献[8]提出了一种全新的模型，首先对节点进行编码，编码方式采用 DNA 的脱氧核甘酸链，之后依据脱氧核甘酸链中的相同位来作为对偶密钥的参数来建立密钥路径。对于不能直接建立链路的连接，提出了一种间接链路方法，满足路径建立概率接近 100%。同时，由于采用 DNA 链作为编码参数，大大提高了密钥的安全性能。

本文对文献[8]中基于 DNA 模型的对偶密钥建立算法进行了改进，采用随机数字的方式对节点位进行编码，这样，编码后的节点位就将是一个随机数字，这样可以更大地提高模型的安全性能。同时，在密钥建立过程中也不再是简单的采用节点编码位中的相同位进行直接路径建立，而是首先采用不同位进行第一次通信，之后经过 3 次握手后才确定最终的密钥参数。与基于 DNA 模型的对偶密钥建立算法相比，新算法具有以下主要优点：

1）簇内的任何两个节点之间都能建立直接密钥路径；

2）簇内节点之间的通信具有更高的安全性，由于随机数字的使用，攻击者不可能通过枚举法来破解密钥以获取信息；

3）簇间通信只建立 1 次密钥路径，能大大减少传输能耗。且新算法对于簇与簇之间的通信亦做了相应的链路建立研究。

3.2 节点之间对偶密钥建立概率分析

定理 1 用基于对偶编码的随机密钥算法，同一簇内任意两个节点之间建立直接对偶密钥的概率为 100%。

证明 设共有 N 个节点。对任意节点 A，由于其 ID 的唯一性，则剩余的 $N-1$ 个节点中，任何节点都将存在与节点 A 不相同的位，因此，任意两个节点之间建立直接对偶密钥的概率为 $(N-1)/(N-1)=100\%$。 证毕。

3.3 算法安全性分析

对基于对偶编码的随机密钥算法，其安全性能将大大提高。主要基于算法实施过程中的以下 3 个方面：

1）在通信链路建立之前，两节点之间将会有一次对象验证，这样将会使得信息准确地到达目的地，任何攻击者都不可能伪造身份来进行攻击；

2）由于默认密钥的随机性，使得攻击者很难掌握这个初始密钥；

3）对密钥池采用字符串形式进行编码，相比数字形式的编码，其编码位大大加强，采用计算机枚举也难以破解。

3.4 算法开销分析

1）节点的存储开销。每一个节点的编码位为 n 位随机数

字,故每一个节点共需要 n 位存储开销。

2)通信开销。任意两个节点之间可直接建立链路,设其每一跳的通信开销为 1,则对距离为 L 的任意两节点,其通信开销为 L,故其平均通信开销也为 L。

4　仿真实验

4.1　任意两个节点之间建立直接密钥的概率的仿真实验

在簇内的任意两个节点之间,由于其编码的独特性,必定存在不同位的编码,因此任意两个节点之间建立通信链路的概率为 100%。

4.2　通信开销的仿真实验

对随机密钥模型和 DNA 模型在密钥建立过程中的通信开销仿真实验数据比较如图 2 所示。

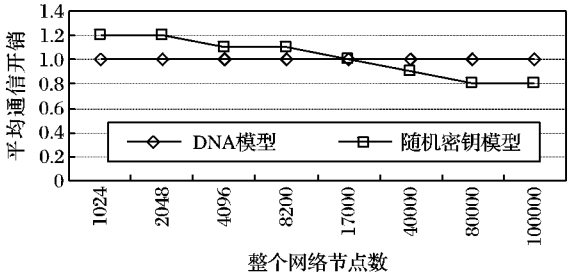

图 2　密钥建立过程通信开销的比较

从图 2 可以看出,当节点数目比较少时,DNA 模型的通信开销小于随机密钥模型,原因在于 DNA 模型中节点之间的密钥路径建立只需要一次通信即可,为了提高安全性能,随机密钥模型在路径建立过程中,不是一次性建立路径,而是通过互相产生随机数字来进行新的密钥生成,在簇中节点之间的第一次通信中,将多进行 2 次通信,相对于其安全性能的提高,簇中节点之间通信开销的少许增加是可以接受的;当节点数目的急剧增加时,随机密钥模型的通信开销小于 DNA 模型,因为随着节点数增加,簇间通信大大增加,随机密钥模型在簇间通信的直接一次路径建立概率得到了提高。

5　结语

在基于DNA模型的对偶密钥建立算法基础上提出了一种新的基于对偶编码的随机密钥建立算法。理论分析和仿真实验结果表明,新算法有效提高了任意两个节点之间直接对偶密钥建立的概率和的安全性能,同时,也在簇与簇之间节点的通信中节省了通信开销。因此,可以认为这是一种性能更好的传感器网络密钥建立算法。

参考文献:

[1] POTTIE G, KAISER W. Wireless sensor networks [J]. Communications of the ACM, 2000, 43(5): 51 – 58.

[2] ESTRIN D, GOVINDAN R, HEIDEMAN J, *et al*. Next century challenges: Scalable coordination in sensor networks [C]// Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking. New York: ACM Press, 1999: 263 – 270.

[3] AKYILDIZ I F, SU W, SANKARASUBRAMANIAM Y, *et al*. A survey on sensor networks [J]. IEEE Communications Magazine, 2002, 40(11): 102 – 114.

[4] 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. New York: ACM press, 2002: 41 – 47.

[5] CHAN H, OERRIG A, SONG D. Random key predistribution schemes for sensor networks [C]// Proceedings of IEEE Symposium on Research in Security and Privacy. Los Alamitos: IEEE Computer Society Press, 2003: 197 – 213.

[6] BLUNDO C, DESANTIS A, KUTTEN S, *et al*. Perfectly secure key distribution for dynamic conferences [C]// Proceedings of the Advances in Cryptology. Berlin: Springer-Verlag, 1993: 471 – 486.

[7] LIU DONGGANG, NING PENG, LI RONGFANG. Establishing pairwise keys in distributed sensor networks [J]. ACM Transactions on Information and System Security, 2004, 20(10): 1 – 35.

[8] 蔡立军, 王雷, 林亚平, 等. 传感器网络中基于 DNA 模型的对偶密钥建立算法研究[J]. 电子学报, 2008, 36(1): 171 – 176.

[9] 胡宇舟, 王雷, 陈治平, 等. 传感器网络中对偶密钥的动态密钥路径建立机制及算法[J]. 通信学报, 2008, 29(2): 52 – 58.

[10] WANG G, CHO G. Compromise-resistant pairwise key establishments for mobile Ad Hoc networks [J]. ETRI Journal, 2006, 28(3): 375 – 378.

(上接第 1485 页)

对于数据的完整度而言,一般情况下会影响数据块的存储转发,所以可以进行适当的修改,以获取更多的稀缺资源。

6　结语

本文结合数据复制,分布式代理存储和服务评价模型等方面的研究成果,提出了一种分布式代理记忆机制。通过对本地策略的设定,可以有效地阻止病毒等服务评价低的文件的传播;对数据分布式代理记忆的信息的动态更新与遗忘,可以减缓数据存储压力,减少带宽需求;当用户只下载不上传时,其余节点无法对其本身节点进行服务评价和代理记忆,熟识度降低后会被列入遗忘节点队列,提供服务也会逐渐减少,这样可以激励用户上传资源。一旦访问节点开始资源搜索时,等同于多个节点提供信息资源,搜索更加便捷,从而传输更加快速;局域网用户访问数据时不需要远距离搜索。对需要保护的数据,用户发布时可将数据安全性划分为隐私、保护和公开 3 个等级以对数据进行安全性约束,当选择隐私级别时,后继节点和邻域节点不进行代理记忆;当用户选择保护时,只有邻域节点代理记忆;在公开级别时默然为节点信息互访不受限制,只根据本地策略进行数据代理记忆。记忆的隐私程度越低,传播程度越广。

参考文献:

[1] 周文莉, 吴晓非. P2P 技术综述[J]. 计算机工程与设计, 2006, 27(1): 76 – 79.

[2] 王意洁, 张小明, 周婧. P2P 系统中数据复制算法研究[J]. 国防科技大学学报, 2007, 29(3): 61 – 70.

[3] 刘翔, 汪海玲. 分布式存储中的一种数据放置策略[J]. 计算机与数字工程, 2009, 37(5): 27 – 29.

[4] 赵恒, 权义宁, 胡予濮. 一种新的 P2P 数据共享解密授权方案[J]. 西安电子科技大学学报: 自然科学版, 2005, 32(5): 781 – 785.

[5] 李佳伦, 谷利泽, 杨义先. 一种新的 P2P 网络的信任管理模型[J]. 北京邮电大学学报, 2009, 32(2): 71 – 74.

[6] 窦文, 王怀民, 贾焰, 等. 构造基于推荐的 Peer-to-Peer 环境下的 Trust 模型[J]. 软件学报, 2004, 15(4): 571 – 583.