一种基于 ID 的传感器网络密钥管理方案

章 睿 刘吉强 赵 佳
(北京交通大学信息安全体系结构研究中心 北京 100044)

摘 要：对偶密钥的建立是无线传感器网络的安全基础，它使得节点之间能够进行安全通信。但是由于节点资源的限制，传统的密钥管理方法在传感器网络中并不适用。在分析了现有密钥预分配协议的前提下，该文提出一种新的基于 ID 的密钥预分配协议。此协议用计算和比较散列值的方式替代广播方式协商密钥，减少了传感器节点大量的通信消耗。然后，分析了所提出方案的安全性、通信量和计算量，并和已有协议进行了比较。结果表明本文的方法不仅能保证安全性，而且节约了大量通信资源。

关键词：无线传感器网络；对偶密钥；哈希算法
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1009-5896(2009)04-0929-04

An ID-based Key Pre-distribution Scheme for Wireless Sensor Networks

Zhang Rui Liu Ji-qiang Zhao Jia
(*Research Center of Information Security Architecture*, *Beijing Jiaotong University*, *Beijing* 100044, *China*)

Abstract: Pairwise key establishment is a fundamental security service in sensor networks. It enables sensor nodes to communicate securely with each other using cryptographic techniques. However, due to the resource constraints on sensors, it is infeasible to use traditional key management techniques. To facilitate the study of novel pairwise key predistribution techniques, this paper presents a new framework for establishing pairwise keys between sensors on the basis of an ID-based key predistribution protocol. In this paper key agreement uses hash calculation and comparison instead of broadcasting; it reduces communication consumption on sensors. This paper then analyses the security and overhead and compares with previous schemes. The results show our scheme is superior to the existing approaches, and it can save communication resources.

Key words: Wireless Sensor Networks (WSN); Pairwise key; Hash algorithm

1 引言

无线传感器网络(Wireless Sensor Network，WSN)是由大量的微型传感器节点组成，通过无线通信方式形成的一个多跳的自组织网络系统，其目的是协作地感知、采集和处理网络覆盖区域中被感知对象的信息，并发送给观察者。传感器网络被用在敌对环境中时，安全变得尤为重要。但是受到传感器节点由电池供电，有限的计算能力和通信能力的限制，传统网络的加密方案以及相应的密钥管理机制无法适用于无线传感器网络。如何在传感器网络节点间建立安全通信，即如何进行合理的密钥分发和管理并且有效地减少节点的资源消耗成为传感器网络设计中一个非常热门的问题。

1989 年，Tatebayashi 等人较早考虑了移动环境中资源有限设备的密钥分发问题[1]。Eschenauer 和 Gligor 提出基本概率论的密钥预分配协议[2]。Chan，Perrig 等人将这个观点进行了改进，提出 q 复合度的密钥预分配协议和随机对偶密钥协议[3]。之后，Du，Liu 等又提出多重空间的密钥预分配协议[4,5]。近几年，又提出一些新的密钥分配方案[6−8]，这些方案提高了无线传感器网络的安全性和鲁棒性，但是由于计算复杂性和能量消耗的增加，使得这些方案在实际中难于实现。文献[9, 10]提出密钥管理方案中满足操作需求与满足安全需求同样重要。并且由于传感器节点的绝大部分能量消耗在无线通信模块上[11]，因此降低传感器节点间的通信量从而降低能量消耗是本文提出方案的一个主要目标。

本文提出一种适用于大中型无线传感器网络的基于 ID 的对偶密钥预分配方案，此方案中各节点不需要广播自己的密钥列表来获取共享密钥，各节点自身决定通信路径，从而节约了大量通信资源。

本文的剩余部分组织如下：第 2 部分提出了我们设计的基于 ID 的密钥管理方案；在第 3 部分给出了所提出方案的性能分析，安全分析并与已有类似方案的性能比较；第 4 部分给出了总结。

2 基于 ID 的密钥管理方案

基于 ID 的密钥管理方案包括 3 个阶段：密钥预分配，直接建立安全链路和间接建立安全链路。

2007-12-31 收到，2008-07-31 改回
国家 973 规划项目(2007CB307101)，国家 863 计划项目(2007AA01Z410，2007AA01Z177)和北京交通大学校基金(K08J0030)资助课题

2.1 密钥预分配

密钥预分配阶段是一个离线的密钥预分配过程。设在整个传感器网络中存在 N 个节点，每个节点具有唯一的标识 $\mathrm{ID}_u, u=1,2,\cdots,N$，所有的节点标识形成的集合记为 $D=\{\mathrm{ID}_u, u=1,2,\cdots,N\}$，单向函数 $H: D\to\{0,1\}^{l\times n}$。在密钥分发服务器上产生一个容量为 $m\times n$ 的密钥池 $\boldsymbol{S}$，其中 $m=2^l$，$l,n\in Z^+$。为便于叙述，可以认为密钥池中的密钥是以矩阵的形式存放，即 $\boldsymbol{S}=\begin{pmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ k_{21} & \ddots & & k_{2n} \\ \vdots & & \ddots & \vdots \\ k_{m1} & k_{m2} & \cdots & k_{mn} \end{pmatrix}_{m\times n}$，并以每个密钥在矩阵中所处的行列坐标作为密钥唯一的标识，分别记为 $11,12,\cdots,1n,21,\cdots,mn$。

对每个传感器节点 $\mathrm{ID}_u(u=1,2,\cdots,N)$，密钥分发服务器按照如下步骤操作：

(1)计算散列值 $H(\mathrm{ID}_u)=B_1B_2\cdots B_n$，其中 $B_i(i=1,\cdots,n)$ 是长度为 l 的二进制串；

(2)对每一个 $B_i(i=1,\cdots,n)$，从矩阵 $\boldsymbol{S}$ 的第 i 列中取出第 j_i 个密钥作为传感器节点 ID_u 的一个密钥 $k_{j_i i}$，其中 j_i 为 B_i 的十进制形式。所有密钥 $k_{j_1 1},k_{j_2 2},\cdots,k_{j_n n}$ 组成传感器节点 ID_u 的密钥环。

2.2 直接安全链路的建立

直接建立安全链路是通过发现共享密钥来实现的，假设两个传感器节点间至少需要 $t\geq 1$ 个共享密钥才能建立安全链路。在无线传感器网络初始化时，每个节点 $\mathrm{ID}_u(u=1,2,\cdots,N)$ 按照如下步骤计算出在通信范围内的邻近节点是否和自己有共享密钥。

(1)节点 ID_u 计算节点 ID_v 的散列值 $H(\mathrm{ID}_v)=B_1^vB_2^v\cdots B_n^v$；

(2)计算 $H(\mathrm{ID}_v)\oplus H(\mathrm{ID}_u)=B_1^vB_2^v\cdots B_n^v\oplus B_1^uB_2^u\cdots B_n^u=B_1^{uv}B_2^{uv}\cdots B_n^{uv}$，此处 $\oplus$ 为逐位异或运算；

(3)检查 $B_1^{uv},B_2^{uv},\cdots,B_n^{uv}$ 中是否为 0，若存在 $q(\geq t)$ 个 $B_i^{uv}=0$，即存在 q 个共享密钥，则转向第(4)步，否则终止；

(4)不妨设有 $B_1^{uv}=B_2^{uv}=\cdots=B_q^{uv}=0$，且 B_i^u 对应的十进制数为 j_i。节点 ID_u 计算会话密钥 $K_{uv}=\mathrm{hash}(k_{j_1 1}\,\|\,k_{j_2 2}\,\|\cdots\|\,k_{j_q q}), t\leq q\leq n$。

2.3 间接安全链路的建立

若两个节点没有共享密钥，或共享密钥数少于 t，就需要间接建立对偶密钥来进行通信。由于密钥预分配算法是公开和确定的，并且在此方案中，只要各节点知道邻近节点的ID，源节点通过简单的计算，就能知道经由哪些节点能和目标节点建立通信，哪一条路径是最短最方便的。设节点 ID_u 和节点 ID_v 之间无法直接建立安全链路，两节点可以重复上述直接安全链路的建立步骤寻找中间节点 ID_x，并通过两次安全通信达到信息传递的目的。

显然，此方案可以随意增加节点，密钥分发服务器按照所增加节点的ID为节点分发相应密钥。而在删除某节点时，每个节点只需计算出被删除节点的散列值并删除相应的共享密钥即可。

3 协议分析

与文献[2, 5]类似，任意两个传感器节点之间恰有 i 个共享密钥的概率为

$$p(i)=\frac{C_n^i(m-1)^{n-i}}{m^n} \tag{1}$$

任意两个节点之间至少有 t 个共享密钥的概率为

$$p=1-(p(0)+p(1)+\cdots+p(t-1))=1-\sum_{i=0}^{t-1}p(i) \tag{2}$$

由式(2)可知，若 m 值不变，随着 n 的值变大，p 值也相应增大。由式(2)计算得，当 $m=128,n=256,t=1$ 时，p 的值高达将近 90%，$t=3$ 时，p 仍然有 30%多。

表 1 中将本文的方法和 q 复合度密钥预分配方法[3]中任两节点间至少有 q 个共享密钥的概率进行了比较。从表中数据分析，选择相近 m 和 n 的值能得到较理想的概率值，此概率值与使用 q 复合度密钥预分配方法得到的概率值相近。

表 1 本文的基于 ID 密钥预分配方案与 q 复合度密钥预分配方案的共享密钥概率比较

	本文基于 ID 的方案		文献[3]中 q-复合度方案	
	m=128 n=128	m =256 n =256	m =128 $\lvert S\rvert$ =16384	m =256 $\lvert S\rvert$ =65536
t=1 (q=1)	0.63356	0.63244	0.635	0.63356
t=2 (q=2)	0.26424	0.26424	0.26423	0.26424
t=3 (q=3)	0.07958	0.07994	0.07885	0.07958

3.1 网络连通性分析

根据以上分析，任意两个节点能直接建立安全链路的概率可由式(2)计算得出。为表示方便，记两节点间能直接建立安全链路，即“单跳”的概率为 p_1，两节点通过一个中间节点建立安全链路，即“两跳”的概率为 p_2。设每个节点有 d 个邻居节点，对每个邻居节点而言，它可以直接与源节点 ID_u 和目标节点 ID_v 建立安全链路的概率是 p_1^2。因此，节点 ID_u 和 ID_v 能通过“单跳”或“两跳”建立通信的概率 $p_{1,2}$ 为：

$$p_{1,2}=1-(1-p_1)(1-p_1^2)^d \tag{3}$$

显然，概率 $p_{1,2}$ 随着概率 p_1 的增加而增加，而增加的幅度随邻居节点的个数 d 的增加而变大。根据式(3)可以计算出，在通信范围内的任意两个节点能直接或间接(“两跳”)建立安全链路的概率高达 90%以上。

3.2 安全性分析

对于此方案，攻击者可能发起两种攻击：

(1)攻击者的目标是单个或一对特定的传感器节点。攻击

者可能试图捕获这个节点的所有密钥；或试图捕获两个节点之间的共享密钥，获得两个节点的通信内容。

(2)攻击者的目标是破坏整个网络，从而降低节点间建立对偶密钥的概率或增加建立对偶密钥的消耗。

3.2.1 对于单个或一对特定传感器节点的攻击　此方案中，攻击者可以通过捕获其他节点来获得某一特定节点的所有密钥，从而获得该节点与其他节点的通信密钥。假设已有 k 个节点被捕获，计算攻击者能获得某一个节点 ID_u 的所有密钥的概率。把 k 个节点中包含节点 ID_u 的所有密钥的概率记为 p_s：

$$p_s = \left(1-\left(\frac{m-1}{m}\right)^k\right)^n \tag{4}$$

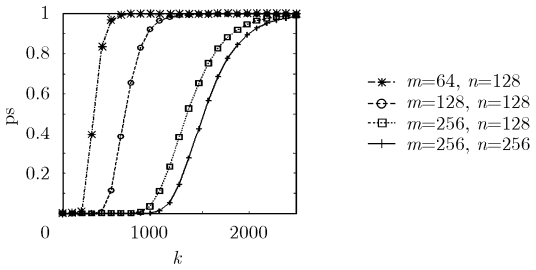

图 1 从捕获的 k 个节点中获得一个节点所有密钥的概率

假设节点 ID_u 和节点 ID_v 能直接建立安全链路，在 ID_u 和 ID_v 都没有被捕获的情况下，攻击者只有获得了 ID_u 和 ID_v 的所有共享密钥，才能知道 ID_u 和 ID_v 的通信密钥。攻击者能从 k 个已捕获的节点中获得其他任意两个能建立安全链路的节点之间通信密钥的概率 p_c 如式(5)所示。且由式(5)可知，t 越大，需要捕获的节点数越多。

$$p_c = \sum_{i=t}^{n}\left(1-\left(\frac{m-1}{m}\right)^k\right)^i \frac{p(i)}{p} \tag{5}$$

3.2.2 对于整个网络的攻击　理论上攻击者可以通过捕获一定数量的节点来获得密钥池中的所有密钥，从而破坏整个传感器网络。

计算已有 k 个节点被捕获的情况下，攻击者能获得密钥池中所有密钥的概率 p_p。当 k 个节点中的所有密钥都不重复时，k 的值即为 m。所以攻击者要获得密钥池中的所有密钥至少要捕获 m 个节点。设 $S(k,m)$ 为第 2 类 Stirling 数，则攻击者能获得密钥池中所有密钥的概率 p_p 如等式(6)所示：

当 $k \geq m$ 时

$$p_p = \left(\frac{S(k,m)m!}{m^k}\right)^n \tag{6}$$

当 m 和 n 的值都取 128 时，$k=m$ 的情况下，$p_p \approx 3.1648\mathrm{e}-530$。可见 k 个节点中的所有密钥都不重复且正好覆盖密钥池中所有密钥的概率是可忽略的。当给定 m 和 n 的值时，k 的取值越大，攻击者获得密钥池中所有密钥的概率越大。当 $k=1000$，$m=n=128$ 时，$p_p \approx 0.0016$。攻击者捕获所有节点的概率仍然是一个很小的值。可见，攻击者通过这种方法捕获密钥池中的所有密钥是不可行的。

3.2.3 与现有方法的比较　该方案与基本概率论的密钥预分配协议[2]、q 复合度密钥预分配协议[3]进行比较如图 2 所示。

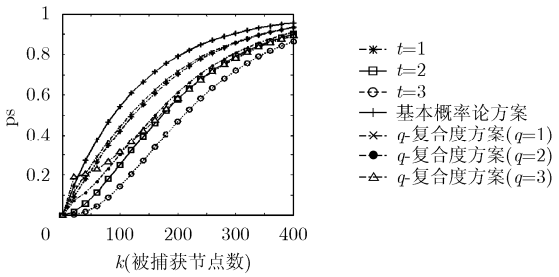

图 2 被捕获节点数与剩余节点的通信被捕获概率的关系

假设每个节点都存储 128 个密钥，密钥池大小 $|S|=128\times128=16384$。由图 2 可知，这个密钥预分配方案的安全性明显高于基本概率论的密钥预分配方案。当 t 的值取 2 和 3 时，此方案比 q 复合度的密钥预分配方案更安全。

3.3 通信量分析

在无线传感器网络中，通信是最大的资源消耗者[11]，本文采用的方案最大的好处是减少广播通信的次数，每个节点通过计算得到通信密钥，且可以自由选择通信路径，从而大大减少了通信量，节约了资源，延长传感器节点的存在周期。

设网络中有 N 个节点，每个节点的通信范围内有 d 个邻居节点，两个节点之间可以直接建立安全链路的概率为 p，即每个节点可以和 $\overline{d} \approx dp$ 个邻居节点直接建立安全链路。

在无线传感器网络初始化阶段，每个节点都向所有邻居节点广播加密的包含密钥信息的列表 α，$E_{K_i}(\alpha), i=1,\cdots,k$，$k$ 是每个节点包含的密钥数。只有与该节点有共享密钥的节点才能解密广播的列表，从而找到两者之间的共享密钥。即每个节点需要加密 k 次。若加密后的信息长度为 l bit，那么，整个网络中至少需要广播的信息量为 $l\times k\times N$ bit。

当两个节点没有共享密钥时，需要建立间接密钥路径。在大部分的现有方法中，源节点事先不知道和目标节点建立对偶密钥的路径。假设节点 ID_u 要和节点 ID_v 通信，当它们之间只有一个中间节点(“两跳”)时，至少需要通信 $\overline{d}+1$ 次；当它们之间有两个中间节点(“三跳”)时，至少需要通信 $\overline{d}^2+1$ 次。相应地，加密和解密的次数和通信次数一样。而使用本文的方法，根据 2.1 节的分析，“两跳”时，只需要通信两次；“三跳”时，只需要通信三次；以此类推，“n 跳”时，通信 n 次。因此，加密、解密的次数也随着通信次数而大幅度减少。

3.4 计算量分析

此方法中，每个节点必须计算邻近节点的散列值来获得共享密钥。若某节点希望与所有通信范围内的邻近节点都能通信，那么需要分别计算 d 个邻居节点的散列值并与自己的比较，对于其中的 $d-\overline{d}$ 个不能直接建立安全链路节点，只

需要重复比较从而发现间接链路即可。

4 结束语

本文提出了一种新的基于 ID 的密钥预分配方案，这个方案较现有方案有以下几个明显的优点：(1)不需要通过广播来发现共享密钥，大大减少了节点之间的通信量，同时减少了资源的消耗量，延长了节点的存在周期。(2)间接建立对偶密钥阶段，源节点能通过计算获得通信路径，并选择一条最适合的路径进行通信。(3)能够方便地动态增加和删除节点。需要增加或删除传感器节点时，只需通知通信范围内的各个节点增加或删除节点的 ID 即可。通过对此方案的具体分析发现，这个方法在保证一定概率的网络连通性的情况下，仍然具有较好的安全性。在传感器节点的计算能力范围内，用计算的方法替代广播获取共享密钥，使网络通信量大大降低，也使得网络的安全性进一步加强。

参 考 文 献

[1] Tatebayashi M, Matsuzaki N, and Newman D B Jr. Key distribution protocol for digital mobile communication systems[C]. Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, California, United States, USA, August 20-24, 1989, Lecture Notes in Computer Science, Vol. 435: 324–334.

[2] Eschenauer L and Gligor V D. A key-management scheme for distributed sensor networks[C]. Proceedings of the 9th ACM conference on Computer and communications security, Washington, DC, USA, November 17-21, 2002: 41–47.

[3] Chan H, Perrig A, and Song D. Random key predistribution schemes for sensor networks[C]. Proceedings of the IEEE Syrup. on Research in Security and Privacy, Berkeley, CA, USA, May 11-14 2003: 197–213.

[4] Du W, Deng J, Han Y S, and Varshney P K. A pairwise key pre-distribution scheme for wireless sensor networks[C]. Proceedings of the 10th ACM Conference on Computer and Communications Security, Washington, DC, USA, October 27-30, 2003: 42–51.

[5] Liu D G, Ning P, and Li R F. Establishing pairwise keys in distributed sensor networks[J]. *ACM Trans. on Information and System Security*, 2005, 8(2): 41–77.

[6] Hussain S, Kausar F, and Masood A. An efficient key distribution scheme for heterogeneous sensor networks[C]. Proceedings of the 2007 international conference on Wireless communications and mobile computing, Honolulu, Hawaii, USA, August 12-16, 2007: 388–392.

[7] Younis M F, Ghumman K, and Eltoweissy M. Location-aware combinatorial key management scheme for clustered sensor networks[J]. *IEEE Trans. on Parallel and Distrib*, 2006, 17(8): 865–882.

[8] 杨庚, 王江涛, 程宏兵, 容淳铭. 基于身份加密的无线传感器网络密钥分配方法[J]. 电子学报, 2007, 35(1): 180–184.
Yang Geng, Wang Jiang-tao, Cheng Hong-bing, and Rong Chun-ming. A key establish scheme for WSN based on IBE and Diffie-Hellman algorithms[J]. *Acta Eleclronics Sinica*, 2007, 35(1): 180–184.

[9] Lee J C, Leung V C M, Wong K H, Cao J N, and Chan H C B. Key management issues in wireless sensor networks: Current proposals and future developments[J]. *IEEE Wireless Communications*, 2007, 14(5): 76–84.

[10] Xiao Y, Rayi V K, Sun B, Du X J, Hu F, and Galloway M. A survey of key management schemes in wireless sensor networks[J]. *Computer Communications*, 2007, 30(11-12): 2314–2341.

[11] Estrin D. Wireless sensor networks tutorial part IV: sensor networkprotocols. http://nesl.ee.ucla.edu/tutorials/mobicom02/slides/Mobicom-Tutorial-4-DE.pdf. 2007.9.

章 睿： 女，1981 年生，博士生，研究方向为信息安全.

刘吉强： 男，1973年生，副教授，博士后，主要研究方向为信息安全.

赵 佳： 女，1980年生，讲师，博士，主要研究方向为信息安全.