一种基于单向函数的适用于传感器网络的密钥预分配方案*

王袁希儿[1,2]，武传坤[1]
(1. 中国科学院 软件研究所 信息安全国家重点实验室，北京 100084；2. 中国科学院 研究生院，北京 100039)

摘　要：网络的密钥管理方案作为所有上层安全、应用的基础，对网络的安全性能、服务性能起着至关重要的作用。简要介绍了无线传感器网络中密钥管理问题上近年来的研究成果，在此基础上提出了一种基于单向函数的密钥预分配方案，并对其安全性和连通性进行了详细的分析。

关键词：无线传感器网络；密钥管理；密钥预分配
中图分类号：TP301.6　　**文献标志码**：A　　**文章编号**：1001-3695(2008)07-2148-04

One way function-based key predistribution scheme for sensor networks

WANG Yuan-xi-er[1,2], WU Chuan-kun[1]
(1. *State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing* 100084, *China*; 2. *Graduate School, Chinese Academy of Sciences, Beijing* 100039, *China*)

Abstract: Key management, the foundation of upper level security service and application service, has been carefully studied nowadays. This paper introduced the research status of key management for WSN, proposed a new key pre-distribution scheme based on one-way functions, and analyzed its connectivity and security features in detail.

Key words: wireless sensor networks; key management; key pre-distribution scheme

无线传感器网络(WSN)是由大量传感器节点通过无线通信方式形成的多跳自组织网络，通过汇聚节点与外部网络连接，用于采集信息、协同处理数据，将采集到的信息即时传递给用户。传感器网络在军事、国家安全、反恐防灾等安全敏感领域的应用使得其安全问题日益受到重视。传感器节点物理上暴露，容易被敌手俘获(compromise)、携带能源有限、计算能力低且存储空间小，这都为其安全的实现提出了挑战。

本文回顾介绍了近年来国内外在密钥管理方面的研究成果，分析了各种密钥管理方案的特点，并在此基础上提出了一种基于单向函数的密钥预分配方案。方案中节点通过多个单向函数建立两种不同的通信密钥，在保证安全性能的同时，进一步节省节点的密钥存储空间，以支持更大规模的网络。

1　相关研究

密钥管理机制主要有自增强机制、可信任服务器分配机制和预分配密钥机制。其中，自增强机制基于公钥密码体制，不适用于低功耗的无线传感器网络。可信任服务器分配机制需要可靠的第三方进行密钥分配，如 SPINS[1] 中提出利用基站为每对通信节点分配通信密钥，这样过于依赖基站的密钥管理机制，不适用于大规模、自组织、缺少固定基础设施的无线传感器网络。普遍认为密钥预分配机制是最适合无线传感器网络的密钥管理机制，它使用预置在节点中的密钥信息，在网络布置后动态地建立网络安全通信链路。以下介绍近年来最重要的几种密钥预分配方案。为了行文方便，首先约定文中使用的符号如下：

P　密钥池　　n　传感器节点总数
$f()$　单向函数　　k　传感器节点拥有单向函数总数
ID　节点在网络中的惟一标志
m　单向函数总数 $m = |P|$
V　节点的通信节点空间
k_m　传感器节点的主密钥
$E_k(m)$　用密钥 k 对消息 m 进行加密
SD　网络安全性能指标
R　随机数

Laurent Eschenauer 和 Virgil Gligor 首先提出基于随机图理论的随机密钥预分配方案[2]。在网络部署前生成一个密钥池，每个节点从密钥池中随机选择 x 个密钥构成密钥环(key ring)。网络布置后，邻居节点通过广播密钥的标志 ID，发现共享密钥并以此进行安全通信。该方案中密钥池越大网络安全性越高，但是相应地却会引起网络连通性降低，难以兼顾良好的安全性和连通性。此外，密钥由多个节点共享，缺乏认证性，单个节点的暴露会导致其他未被俘获的节点之间的通信密钥暴露，对网络安全产生较大影响。

Chan 等人对以上方案提出了 q-复合和多路增强[3] 等改进，以提高网络安全性能。q-复合方案中要求共享 q 个以上密钥的节点才能建立安全通信链路。链路的通信密钥由两个节点间所有共享密钥一起生成，如 $K = k_1 \oplus \cdots \oplus k_s$。其中 $k_1 \cdots k_s$ 为节点间的共享密钥，且 $s \geq q$。该方案中，为了保证一定的连

收稿日期：2007-06-02；修回日期：2007-09-04　　基金项目：国家“863”计划资助项目(2006AA01Z423)

作者简介：王袁希儿(1983-)，女，四川成都人，硕士，主要研究方向为无线传感器网络安全(wangyuanxier@is.iscas.ac.cn)；武传坤(1964-)，男，研究员，博导，主要研究方向为密码学、信息安全.

通性, 随着 q 的增大, 要求密钥池减小, 这样在俘获节点数量较少的情况下, 方案体现出极好的安全特性; 但是当敌手俘获节点数量较大时, 网络安全性能反而不如基本方案。多路增强机制中, 如果两个节点 s、t 之间拥有共享密钥 k_{st}, 且存在 j 条独立路径, 分别途经节点 $v_1, v_2, \cdots, v_j$, 则通信密钥 $k = k_{st} \oplus r_1 \oplus \cdots \oplus r_j$。其中: r_i 为中间节点 v_i 生成的随机数, $i = 1, 2, \cdots, j$。这样敌手需要俘获多于 j 个节点才能获得该链路的通信密钥。多路增强机制有效地提高了网络安全性能, 但是增加了额外的通信开销。此外, 他们还提出使用随机分配的密钥对(pairwise key)作为通信密钥, 以增强网络安全性能; 记为 RPK 方案。方案中节点随机选择 k 个节点作为通信对象, 基站为其分配网络惟一的通信密钥对, 即每个密钥对仅为两个节点共享。这样的方案有完美的抗节点俘获性能, 但是由于连通性差, 极大地限制了网络的规模。

Blom 和 Blundo 分别提出基于对称矩阵[4]和对称多项式[5]的密钥预分配方案。节点利用网络布置前载入的矩阵或多项式信息, 计算并建立通信密钥对。在俘获节点数量少于 λ 时(λ 为矩阵的阶数或多项式的次数), 网络拥有完美的抗节点俘获安全性能, 但当被俘获节点数突破门限时, 敌手可以恢复出用于密钥建立的多项式或原始矩阵, 则整个网络所有密钥暴露。该类方案有很好的抗节点俘获门限性质, 便于新节点的加入, 可扩展性好, 但是计算量非常大, 增加了网络的能量开销。

UAO 方案[6]使用单向函数建立通信密钥, 在低计算开销的情况下, 保证了完美的安全性能, 与基本密钥对随机预分配方案相比, 增大了可支持网络规模。方案为每个节点 SN_i 分配惟一标志 ID_i 和单向函数 f_i。SN_i 随机选择 r 个节点: $SN_{v1}, SN_{v2}, \cdots, SN_{vr}$。每个被选中的节点 SN_{vj} 使用自己的单向函数 f_j, 为节点 SN_i 计算密钥 $k_j = f_j(ID_i)$。节点 SN_i 存储所有密钥及对应节点标志 $\langle k_j, ID_j \rangle$。这样在网络布置后, 假设节点 SN_i 和 SN_j 节点为邻居节点, 节点 SN_i 存储有密钥信息 $\langle k_j, ID_j \rangle$, 则节点 SN_j 用自己的单向函数 f_j 生成密钥 $k_j = f_j(ID_i)$, 并以此密钥作为双方的通信密钥。与随机密钥对分配方案相比, 该方案保持了完美的节点抗俘获性能, 且一定程度上节省了存储空间, 可以支持更大的网络规模。

2　基于单向函数的密钥分配方案

本文的密钥预分配方案提出了利用多个单向函数来建立通信密钥, 与 UAO 方案相比, 本方案更进一步提高了网络的连通性, 降低密钥所需的存储空间, 从而扩大了支持网络规模。方案在密钥预置阶段为节点随机地分配多个单向函数, 节点利用这些单向函数建立两种不同的通信密钥。其中没有共享单向函数的节点以一定概率建立一种高安全性能的通信密钥, 称为安全密钥; 有共享单向函数的节点通过这些共享单向函数进行普通密钥的建立, 称为普通密钥, 其安全性较安全密钥稍差, 主要目的就是为了提升网络连通性。

2.1　初始化及密钥预置阶段

在初始化阶段, 系统首先生成 m 个单向函数 $f_1, f_2, \cdots, f_m$ 构成密钥池 P; 然后为网络中每个节点 SN_i 分配惟一标志 ID_i、节点主密钥 k_{mi}, 并随机地从 P 中选出 k 个单向函数 $f_{i1}, f_{i2}, \cdots, f_{ik}$ 分配给节点。单向函数分配完毕后, 为节点建立通信节点空间 $V_i = \{SN_{i1}, SN_{i2}, \cdots, SN_{is}\}$。其中 SN_{ij} 为与节点 SN_i 没有共享单向函数的节点, $j \in [1, s]$。

在密钥预置阶段, 节点 SN_i 在其通信节点空间 V_i 中随机选择 rk 个通信对象, 并将其随机、平均地分配给自己的 k 个单向函数 $f_{i1}, f_{i2}, \ldots, f_{ik}$, 即每个单向函数 f_s 拥有 r 个互不重叠的通信对象节点 SN_{s1}、$SN_{s2} \cdots SN_{sr}$。其中节点 SN_{sj} 对应的标志为 ID_{sj}, $s = i_1$、i_2、$\cdots$、i_k。节点 SN_i 为自己的每一个单向函数 f_s 的每一个通信对象 $SN_{sj}(j = 1, 2, \cdots, r)$ 生成随机数 R_{sj}, 并计算密钥 $k_{sj} = f_s(ID_{sj} \quad R_{sj})$。最后向节点 SN_{sj} 中加载密钥信息 $\langle k_{sj}, E_{kmi}(s, R_{sj}), ID_i \rangle$。值得注意的是, 节点 SN_i 并不需要存储该密钥信息, 而是在密钥发现阶段动态地生成。

2.2　密钥发现阶段

在密钥发现阶段, 节点利用预置阶段存储的密钥信息和单向函数依据是否拥有共享单向函数建立两类不同的通信密钥: 安全密钥和普通密钥。没有共享单向函数的节点通过预置阶段存储的密钥信息建立安全密钥; 而拥有共享单向函数的节点之间通过使用共享单向函数建立普通密钥。

首先节点 SN_i 广播如下信息: $ID_i, f_{i1}(ID_i), f_{i2}(ID_i), \cdots, f_{ik}(ID_i)$。

收到该广播信息的节点, 先查找自己存储的密钥信息中是否有相关的密钥是由节点 SN_i 生成的, 若有则进行安全密钥的建立, 具体过程如模式一中介绍。否则节点检查是否与广播发送者有共享单向函数, 如果有则利用共享的单向函数建立普通密钥, 具体过程如模式二中介绍; 对于两种情况都不满足的节点, 则可通过中间接点以及多路增强等技术建立间接密钥, 其过程与随机密钥分配方案等文献中所述完全一致, 在此就不再赘述。

模式一(安全密钥的建立): 假设节点 SN_i 和 SN_j 没有共享单向函数, 并且节点 SN_j 存储有相关密钥信息 $\langle k_j, E_{kmi}(s, R_j), ID_i \rangle$。节点 SN_j 在收到广播信息后, 首先检查自己存储的密钥信息, 发现相关密钥信息 $\langle k_j, E_{kmi}(s, R_j), ID_i \rangle$; 然后向节点 SN_i 发送安全密钥建立请求, 并将 $E_{kmi}(s, R_j)$ 作为密钥建立材料一同发送给节点 SN_i。节点 SN_i 收到请求和密钥建立材料后, 用自己的主密钥 k_{mi} 解密密钥建立材料信息, 得到用于生成密钥的单向函数的标志 s 以及相应的随机数 R_j; 然后节点 SN_i 本地生成通信密钥 $k_j = f_s(ID_j \oplus R_j)$。通过简单的挑战响应进行认证后, 节点 SN_i 和 SN_j 就可利用 k_j 作为双方的通信密钥。对于节点 SN_i 和 SN_j 都分别存储有对方产生的密钥信息的情况, 即节点 SN_i 存储有密钥 k_i, 节点 SN_j 存储有密钥 k_j, 则可以使用 k_i k_j 作为通信密钥。

模式二(普通密钥的建立): 假设节点 SN_i 和 SN_j 有共享单向函数 $f_{s1}, f_{s2}, \cdots, f_{sq}$。节点 SN_j 收到广播信息后, 同样首先检查自己存储的密钥信息中是否有相关的密钥。查找完毕后没有发现相关密钥信息存储, 则计算 $f_{j1}(ID_i), \cdots, f_{jk}(ID_i)$; 其中 $f_{j1}, \cdots, f_{jk}$ 是节点 SN_j 的 k 个单向函数; 然后节点 SN_j 比较自己的计算结果与收到的广播信息 $f_{i1}(ID_i), f_{i2}(ID_i), \cdots, f_{ik}(ID_i)$ 中是否有相同的结果, 若有则证明有共享的单向函数。假设节点 SN_j 发现有 $f_{j1}(ID_i) = f_{s1}(ID_i) = f_{i1}(ID_i)$, $f_{j2}(ID_i) = f_{s2}(ID_i) =$

$f_{i2}(ID_i), \cdots, f_{jq}(ID_i) = f_{sq}(ID_i) = f_{iq}(ID_i)$，则双方使用 $k = f_{s1}(ID_i \quad ID_j) \oplus \cdots \oplus f_{sq}(ID_i \quad ID_j)$ 作为通信密钥。为了保证这种共享单向函数发现方法的正确性，方案要求单向函数具有抗碰撞性，如可以使用 hash 函数作为单向函数。

2.3 节点加入和撤销

为延长网络生命期，无线传感器网络中常常会有新节点加入，以替代被撤销、损坏的节点继续工作。新节点的加入过程与网络密钥建立阶段相同，新节点通过广播自己的信息，同已有节点建立通信。为了保持新节点加入后网络的连通度，要求新节点多次进行广播，避免由于节点休眠、移动等因素造成的邻居节点没有建立安全通信链路的情况。

节点撤销通常发生在节点暴露、能量耗尽或节点损坏的情况下。当节点暴露时，网络应该将节点使用的所有通信密钥全部删除。此外，由于单向函数的暴露会影响由此生成的普通密钥安全，完全由已暴露的单向函数生成的普通密钥也应该删除撤销。对于未暴露节点使用的由已暴露的单向函数生成的安全密钥和部分由这些已暴露单向函数生成的普通密钥，仍可以继续使用。例如，假设节点 SN_1、SN_2、SN_3、SN_4 为网络中未暴露的节点，$f_1, f_2, \cdots, f_b$ 为网络中已经暴露的全部单向函数，k_a 是由 f_1 生成的节点 SN_1 与 SN_2 之间的安全密钥，k_b 是由 f_1、f_2 生成的节点 SN_3 与 SN_4 之间的普通密钥，k_c 是由 f_b、f_{b+1} 生成的普通密钥。根据已暴露的单向函数 f_1、f_2 和节点 SN_3、SN_4 的标志敌手可以破解密钥 k_b，因此对于完全由已暴露的单向函数生成的普通密钥应该撤销。对于安全密钥 k_a，虽然敌手已知用于生成该密钥的单向函数 f_1，但是由于密钥生成材料信息是通过节点的主密钥加密传输的，敌手无法通过窃听得知密钥到底是由哪个单向函数生成的，密钥生成时使用的是哪个随机数，从而无法破解该安全密钥，可以继续使用。对于部分由已暴露单向函数生成的普通密钥 k_c，由于敌手不能通过分析得到 f_{b+1}，该密钥仍然安全，可以继续使用。

具体撤销的步骤可以采取以下方法：当发现某个节点被俘获时，基站广播该节点的标志，以及该节点的所有单向函数的标志。节点在本地保存一个已撤销节点和单向函数列表。当收到来自于基站的广播消息时，首先更新撤销列表；然后删除与该被撤销节点之间的通信密钥；最后根据更新后的撤销列表将完全由已撤销的单向函数生成的普通密钥删除。

2.4 单向函数的生成和存储

为了保证多个单向函数的存储不占用节点过多的存储空间，可采用以下方法生成和存储：

a) 生成单向函数族 $f(r, x)$。

b) 对 $i \in [1, m]$ 计算 $f_i(x) \in P$。其中 $f_i(x) = f(R_i, x)$，R_i 是随机数，它惟一确定一个单向函数。

这样节点只需存储 $f(r, x)$ 和 k 个随机数，即相当于存储了 k 个单向函数。只要 r 的取值范围足够大，敌手就无法确定密钥池 P 以及各个节点使用的单向函数。这样本方案中单向函数的存储并不过多地占用节点的存储空间。此外如前文已经提到本方案中选用的单向函数要具备抗碰撞性，才能保证协议的正常运行。

3 性能分析

3.1 连通性分析

由随机图理论[7]可知，为了让网络连通概率达到 P_c 网络节点间的连通概率 p 应该满足式(1)：

$$p = d/(n-1) = \ln(n) - \ln(\ln(p_c))/n' \tag{1}$$

其中：n 表示节点的邻居数；d 表示节点的度，即一个节点与其邻居节点建立的安全链路数。本方案基于随机图理论，假设网络节点均匀密集分布，用 q 表示节点间无共享单向函数的概率，则通信节点空间 V 的大小期望为 $E(|V|) = q \times (n-1)$。考虑到网络中任意两个没有共享单向函数的节点，它们之间没有安全密钥的概率为

$$[1 - (r \times k)/q(n-1)]^2 \tag{2}$$

那么网络中任意两个节点间存在通信密钥的概率应该是节点间有安全密钥或普通密钥的概率和，可表示为

$$p = q \times \{1 - [1 - (r \times k)/q(n-1)]^2\} + (1-q) = 1 - q[1 - (r \times k)/q(n-1)]^2 \tag{3}$$

其中：$q = [(m-k)!]^2/(m-2k)!\ m!$。

在本方案中，节点仅需要存储由通信对方生成的安全密钥，普通密钥以及自己生成的安全密钥都可以在需要时临时生成，因此节点用于密钥存储的空间大小 s 的期望为 $E(s) = r \times k$，具体表示为

$$s = p(n-1) \quad 1 - \sqrt{n \times n' - \{\ln(n) - \ln[-\ln(p_C)]\}(n-1)/n \times n'q} \tag{4}$$

从文献[3,6]可得 UAO 方案和随机密钥对分配方案中节点存储空间的占用情况为

$$s_{UAO} = (n-1) \quad 1 - \sqrt{1 - (n-1)\{ln(n) - \ln[-ln(p_C)]\}/n \times n'} \tag{5}$$

$$s_{RPK} = (n-1)^2\{\ln(n) - \ln[-\ln(p_C)]\}/n \times n' \tag{6}$$

利用以上结论，选取参数 $P_c = 0.99$，$n' = 30$ 进行仿真。从图 1 中可以看到，随着参数 k 的增大，本方案比 UAO 方案进一步节省了存储空间，从而提高了对大规模网络的支持程度。当 $k = 30$ 时，为使网络达到相同的连通度，本方案所需要的存储空间约为 UAO 方案的 3/5，与随机密钥对分配方案相比本方案在连同性能上的优势更加明显，约为 RPK 方案所需存储空间的 1/3 弱。存储空间需求变化图如图 1、2 所示。

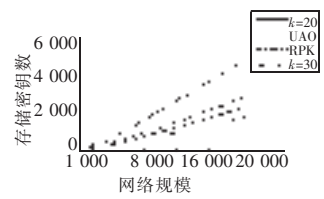

图 1 存储空间需求变化图
参数：m=5 000，P_c=0.99，n'=30

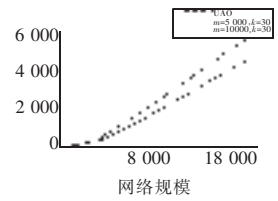

图 2 存储空间需求变化图
参数：m=5 000，P_c=0.99，n'=30

由式(2)可以分析出密钥存储量主要是随 q 减小而减小，而 q 值主要取决于参数 m 和 k 的大小，随着单向函数总数 m 的减少，节点选取单向函数个数 k 的增多，网络连通性将有显著的提高。从图 1、2 的仿真中可以得到的结论验证了对理论公式分析的正确性。

3.2 安全性分析

本文使用节点暴露后对剩余网络中通信链路的影响程度来表征网络的安全性能。具体使用攻击后敌手可以对剩余网

络　行窃听的链路数和网络总链路数的比值来表示网络的安全程度, 记为 SD。文中分别用符号 SD_s和 SD_n来表示安全密钥和普通密钥的安全性能。

对于安全密钥, 如前文中已述, 由函数的单向性和密钥生成时实用的随机数 R 的随机性可知, 敌手不能通过已俘获节点的密钥和单向函数来有效地推断出未俘获节点之间的安全密钥。假设节点 SN_i与 SN_j存在安全密钥 $k_i = f_s(\mathrm{ID}_j \oplus R)$, 且节点 SN_i与节点 SN_p都有单向函数 f_s。当节点 SN_p暴露时, 虽然敌手获得单向函数 f_s, 但并不知道该密钥就是由 f_s生成, 且敌手无法获得随机数 R, 从而不能以超过随机猜测的优势计算出密钥 k_i。而没有单向函数 f_s的节点暴露, 更不会影响到该密钥的安全性。因此该类密钥的安全指标 $SD_s = 0$, 即节点的暴露不影响未被俘获的节点之间的安全密钥。

本方案中普通密钥的安全性质与 $q = 1$ 的 q-composite 方案相同, 用 y 表示敌手俘获的节点个数, 则由文献[3] 该类密钥的安全指标可表示为

$$SD_n = \sum_{i=1}^{k} \left(1 - (1 - k/m)^y\right)^i p(i)/p$$

$$p(i) = \left[\binom{m}{i}\binom{m-i}{2(k-i)}\binom{2(k-i)}{k-i}\right] / \binom{m}{k}^2 \qquad (7)$$

综上, 方案的总体安全指标表示为

$$SD = q \times SD_S + (1 - q)\, SD_n = (1 - q)\, SD_n \qquad (8)$$

选取参数 $n = 10\ 000$, $n' = 30$, $P_c = 0.99$ 对以上结论仿真如图 3 所示。

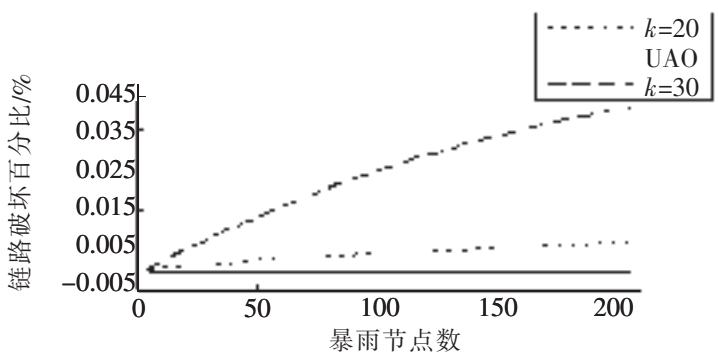

图 3　网络安全性能仿真

参数: n=10 000, m=5 000, P_c=0.99, n'=30

从图 3 中可以看到, UAO 方案在抗节点俘获方面有完美的安全性。本方案选择 $m = 5\ 000$, $k = 20$ 和 $m = 5\ 000$, $k = 30$ 分别进行仿真。可以看到, 当 $k = 20$ 时, 链路的安全性能只有微弱的损失; 当节点俘获数量在$(200/10\ 000) = 2\%$ 时, 链路的破坏仅仅在 0.5% 左右; 当 k 增加到 30 时, 链路的破坏有所增加; 当网络中 2% 的节点被敌手俘获后网络中有近 4% 的链路遭到破坏。而文献[8] 中指出随机密钥分配协议在 0.1% 的节点俘获情况下有高达 18.13% 的链路遭到破坏, 对比之下不难看出本方案的安全性能虽然不是完美的, 但是足以满足一般网络的安全性能要求。

4　结束语

本文提出了一种基于单向函数的密钥预分配方案, 使用多个单向函数建立安全密钥和普通密钥。通过这两种密钥的建立, 兼顾了良好的网络安全性和连通性。与密钥随机分配方案相比, 本方案有出色的安全性能, 抗节点俘获能力强; 随机密钥对分配方案(RPK) 和 UAO 方案相比, 本方案大大节省了用于密钥存储的空间, 进一步提高了网络的连通特性, 以支持更大规模的无线传感器网络。

参考文献:

[1] SCHENAUER L, GLIGOR V D. A key-management scheme for distributed sensor networks[C]//Proc of the 9th ACM Conference on Computer and Communication Security. Washington DC: [s. n.], 2002: 41-47.

[2] CHAN Hao-wen, PERRIG A, SONG D. Random key predistribution schemes for sensor networks[C]//Proc of IEEE Symposium on Security and Privacy. Berkeley: [s. n.], 2003: 197-213.

[3] BLOM R. An optimal class of symmetric key generation systems [C]//Proc of EUROCRYPT'84. Paris: Springer-Verlag, 1985: 335-338.

[4] BLUNDO C, SANTIS A D, HERZBERG A, *et al*. Perfectly-secure key distribution for dynamic conferences[C]//Proc of the 12th Annual Intl Cryptology Conf. Santa Barbara, California: Springer-Verlag, 1993: 471-486.

[5] WU Y S, SHIEH S P. Adaptive random key distribution schemes for wireless sensor networks[C]//Proc of Int'l Workshop on Advanced Developments in Software and Systems Security. 2003: 91-105.

[6] SPENCER J. The strange logic of random graphs[M]. [S. l.]: Springer-Verlag, 2000.

[7] PERRIG A, SZEWCZYK R, WEN V, *et al*. SPINS: security protocols for sensor networks[C]//Proc of the 7th Annual ACM International Conference on Mobile Computing and Networks MobiCom. Rome: [s. n.], 2001: 189-199.

[8] 李志军, 秦志光, 王佳昊. 无线传感器网络密钥分配协议研究[J]. 计算机科学, 2006, 33(2): 87-91.

(上接第 2147 页)

4　结束语

本文将多重秘密共享和代理签名技术结合在一起, 提出了一种存在特权集的门限代理群签名方案。该方案除了满足一般代理签名体制的基本性质之外, 还具有特权集与门限特性、签名的不可伪造性、验证的匿名性与身份的可追查性等良好特性, 具有重要的实际应用价值。

参考文献:

[1] AMBO M, USUDA K, OKAMOTO E. Proxy signature for delegating signing operation[C]//Proc of the 3th ACM Conference on Computer and Communications Security. 1996: 48-57.

[2] SUN H M. An efficient nonrepudiable threshold proxy signature scheme with known signers[J]. Computer Communications, 1999, 22(8): 717-722.

[3] LI Z C, ZHANG J M, LUO Jun, *et al*. Group-oriented (t, n) threshold digital signature schemes with traceable signers[C]//Proc of Lecture Notes in Computer Science2040. London: Springer-Verlag, 2001: 57-69.

[4] TSAI C S, TZENG S F, HWANG M S. Improved nonrepudiable threshold proxy signature scheme with known signers[J]. Informatica, 2003, 14(3): 393-402.

[5] XUE Qing-shui, CAO Zhen-fu. Security analysis and improvement of some threshold proxy signature schemes[J]. Journal of Communication and Computer, 2005, 2(1): 17-25.

[6] 陈伟东, 冯登国. 一类存在特权集的门限群签名方案[J]. 软件学报, 2005, 16(7): 1289-1295.

[7] 冯登国, 裴定一. 密码学导引[M]. 北京: 科学出版社, 1999.