无线传感器网络门限密钥共享模型

柳亚男* 王 箭 杜 贺
(南京航空航天大学计算机科学与技术学院 南京 210016)

摘 要：针对现有传感器网络密钥管理方案存在的网络连通度低、抗俘获性差、节点能耗高等问题，该文提出一种基于(q,l)门限秘密共享的密钥共享模型，采用“虚拟簇头共享密钥，物理簇头重构密钥”的方式完成簇头与簇成员的密钥协商。该模型实现了簇成员能耗最低、抗俘获性最优的目标，同时门限参数 l 和 q 能够调节簇头的抗俘获性、容错性和高效性。理论分析与实验证明，与传统的概率型方案相比，该模型有效地提高了节点抗俘获性和网络连通度，并降低了节点能耗。

关键词：无线传感器网络；门限；密钥共享；密钥协商；簇
中图分类号：TP309; TP393 **文献标识码**： A **文章编号**：1009-5896(2011)08-1913-06
DOI: 10.3724/SP.J.1146.2010.01155

Threshold Key Sharing Model in Wireless Sensor Networks

Liu Ya-nan Wang Jian Du He
(*College of Computer Science and Technology*, *Nanjing University of Aeronautics and Astronautics*, *Nanjing* 210016, *China*)

Abstract: Most traditional probabilistic key management schemes of wireless sensor networks have disadvantages of low connectivity, poor resiliency against node capture, and high energy-consumption. A key sharing model is proposed based on (q,l)-threshold secret sharing. In this model, a key is divided into shadows to be shared by "virtual cluster heads" and re-constructed by the "physical cluster head". For tiny cluster member nodes, this model is optimized in improving their resilience against node capture attacks and saving the energy consumption. At the same time, the cluster head nodes' properties of security, tolerance and efficiency can be adjusted by controlling the parameters of q and l. Both theoretic analysis and the experimental results prove that, this model improves effectively the resilience against nodes capture attack and the network connectivity, and decreases the nodes' overheads.

Key words: Wireless sensor networks; Threshold; Key sharing; Pairwise key establishment; Clusters

1 引言

无线传感器网络(WSNs)通常部署在敌对环境中，易受到各种恶意攻击，如物理俘获节点，投放伪装节点，搭线窃听等[1]。因此必须对节点间通信进行加密和认证以保证安全性，而密钥管理是保密通信与消息验证的前提和关键。由于传感器节点的存储、计算与通信资源受限，所以传统的基于公钥或可信中心的密钥管理方案并不适用[2]。因此，必须对 WSNs 密钥管理开展针对性研究，其中如何平衡高安全和低能耗两个需求是技术难点。

针对平坦式网络，2002 年 Eschenauer 等人[3]首次提出“概率型”方案——随机密钥预分配方案；2003 年后文献[4–7]在 E-G 方案基础上提出了 Q-composite 等一系列概率型方案。该类方案中节点的通信量和计算量非常小，但密钥存储量大，网络连通性和安全性差。2005 年以后，文献[8–11]提出“计算型方案”，利用多项式、对称函数等数学结构建立密钥对。计算型方案在少量增加通信量和计算量的前提下，提高了节点抗俘获性。

针对层次型网络，2003 年 Jolly 等人[12]为 3 层传感器网络提出低能耗的密钥管理协议(LEKM)，其中节点的存储、通信和计算开销较小，然而簇头抗俘获性差。2007 年 Du 等人[13]提出非对称的随机密钥预分配方案(AP)，将 E-G 思想分别应用于簇间和簇内密钥协商中。2009 年 Boujelben 等人[14]结合 AP 方案和 Blom[15]对称矩阵密钥协商方案，提出非对称的矩阵预分配方案，使邻居节点通过寻找共享矩阵来建立密钥对。根本上说，AP 和 Boujelben 方案仍是概率型方案，因此安全性差、连通度低、存储开销大等问题仍然存在。

2010-10-26 收到，2011-05-05 改回
国家 863 计划项目(2009AA044601)资助课题
*通信作者：柳亚男 lynne_liu@yahoo.cn

为解决现有方案存在的问题，本文基于门限秘密共享，提出了传感器网络(q,l)门限密钥共享模型。模型采用“虚拟簇头共享密钥，物理簇头重构密钥”的方式完成簇头与簇成员的密钥协商。该模型充分发挥簇头的资源优势，由簇头承载大部分的计算、存储和通信开销，以实现簇成员能耗最低和抗俘获性最优的目标。此外，门限参数l和q起到了调节簇头安全性、容错性和高效性的作用。通过调节l和q可分别实现簇头存储最优、通信最优、抗俘获性最优等目标。与传统的概率型方案相比，该密钥共享模型有效地提高了节点抗俘获性和网络连通度，降低了节点能耗，并具备一定的容错性。

2 网络结构模型

层次型传感器网络以簇为单位分布，一个簇中有一个簇头和多个簇成员(图 1)。其中簇头是特殊的无线通信设备，在存储、计算、通信和能源等方面具备更高的能力；簇成员是能力较低的普通传感器，为降低其能耗，规定簇内成员只能与其簇头进行通信[12]。

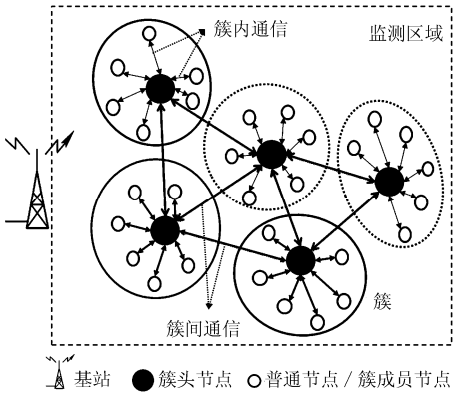

图 1 层次型传感器网络结构

层次型网络中，簇头与簇成员的资源配置存在很大差异，因此簇间与簇内最好采用不同的密钥管理方案(混合式方案[16])。首先，由于簇头能够承载较高的计算和通信开销，因此簇间层可采用公钥方案[17,18]，这样既提高节点抗俘获性又降低存储量。其次，由于簇头与簇成员资源不平衡，将平坦式网络的传统方案直接应用于簇内层时效率低且安全性差。例如，文献[13]的 AP 方案将概率型方案 E-G[3]分别应用于簇内和簇间层，因此很难实现网络全连通，而且簇头与簇成员的密钥存储量都很大。

与 AP 方案不同，本文提出的传感器网络(q,l)密钥共享模型不是对传统密钥管理方案的简单改进，而是针对簇内通信提出的新的密钥协商方案。该模型充分发挥簇头节点资源丰富的优势，以实现普通节点能耗最低、抗俘获能力最优等目标。

3 传感器网络(q,l)门限密钥共享模型

3.1 秘密共享

(q,l)秘密共享中，共享秘密S (secret)被一个可信的分发者(dealer)拆分成l个不同的秘密分片(shadows)，然后分片被分发给不同的合法使用者(holders)。集合其中任意q个分片交由秘密恢复者(combiner)即可轻易将S恢复；但是任何少于q个分片的组合均不能恢复S，也不能从中获得S的任何信息[19]。秘密共享为敏感信息的存储和使用提供了安全保护手段。一个秘密共享方案通常分为“秘密拆分”和“秘密重构”两个阶段。

秘密共享开辟了密钥管理的新思路，并广泛用于组密钥管理中[20]，但尚未应用到传感器网络中。(q,l)密钥共享模型是将秘密共享应用于传感器网络密钥管理的探索性研究，试图解决簇成员与簇头的密钥协商问题，并实现降低节点能耗、提高抗俘获性等目标。

3.2 定义

定义 1 网络的簇结构形成之后，普通节点s加入到由簇头节点CH_i控制的簇内，此时称CH_i为s的物理簇头(PCH)，同时称s为CH_i的簇成员。假设所有节点的物理位置是固定的，则每个普通节点有且仅有一个物理簇头。

定义 2 在密钥预分配阶段，为普通节点s指定并关联l个簇头节点并使之与s共享秘密信息，这些簇头节点称为s的虚拟簇头(VCH)。网络部署完成后，s的某个虚拟簇头可能成为它的物理簇头。虚拟簇头的个数l $(1 \le l \le n)$可根据需要进行调整。

3.3 密钥预分配 —— 密钥拆分

节点投放前，密钥预分配包括以下 4 步：

(1)生成全局密钥池P。

(2)为普通节点s分配密钥k_s。密钥从P中随机选出，且同一密钥只能分配一次。

(3)为s随机指定l个不同的虚拟簇头：$\{\mathrm{VCH}_1, \mathrm{VCH}_2, \cdots, \mathrm{VCH}_l\}_s$，将虚拟簇头 id 存入$s$。

(4)选择秘密共享方案，根据其“秘密拆分”原则将k_s拆分成l个“分片”$\mathrm{SD}(s)$并分别存入$\{\mathrm{VCH}_1, \mathrm{VCH}_2, \cdots, \mathrm{VCH}_l\}_s$中。

3.4 密钥对的建立 —— 密钥重构

节点投放后，网络被划分为若干个簇。簇间层安全向导建立后(簇间层的密钥管理不在本文中讨论)，各簇头发起建立簇内密钥对的会话。簇内密钥对建立过程如图 2 描述：

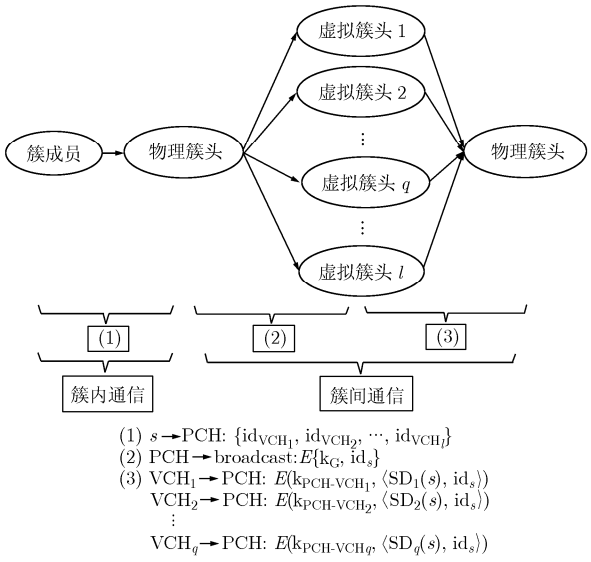

图 2 普通节点 s 与其物理簇头 PCH 建立密钥对 $k_{s\text{-PCH}}$ 的过程

(1) s 将其虚拟簇头的 id 发送给物理簇头 PCH; (2)PCH 在簇间层广播 “分片请求消息”; (3) s 的虚拟簇头将 k_s 的分片发送给 PCH。PCH 只要获得 q 个分片即可重构出密钥 k_s。节点 s 与其物理簇头将 k_s 作为它们的密钥对 $\mathrm{k}_{s\text{-PCH}}$。其中，(1)是簇内通信，(2), (3)是簇间通信，k_G 表示全体簇头节点共享的组密钥，$\mathrm{k}_{\mathrm{PCH\text{-}VCH}i}$ ($i=1,\cdots,q$)表示 PCH 与 VCH_i 的共享密钥对。

4　安全性和性能分析

4.1 (q, l)密钥共享通用模型

4.1.1 安全性分析　敌对区域中，敌方通过物理俘获节点以获取秘密信息是主要的攻击手段之一。根据被俘节点泄露出的信息，能够直接得到或间接计算出未俘节点密钥的概率(F)表示节点的抗俘获性。F 越小说明节点抗俘获性越强。节点抗俘获性是衡量密钥管理方案安全性的重要指标。

$$F=\frac{\text{未捕获节点中被泄露的密钥数}}{\text{未捕获节点的密钥总数}} \tag{1}$$

分别讨论(q, l)密钥共享模型中普通节点和簇头节点的抗俘获性。普通节点只存储一个密钥，且任意一对邻居节点的密钥对都是独一无二的，因此普通节点能够完全抵抗物理俘获攻击。簇头是保证网络正常运行的重要节点，其中存储了大量的密钥分片信息，通过读取被俘簇头的内存，敌方有可能计算出未俘节点的密钥。当网络中有 x 个簇头节点被俘获后，敌方能够计算出任一密钥 k_s 的概率 $p(x)$ 为

$$p(x)=\begin{cases}0, & 0\le x<q\\ 1-\sum\limits_{i=0}^{q-1}\dfrac{C_l^iC_{n-l}^{x-i}}{C_n^x}, & q\le x<n\end{cases} \tag{2}$$

(q, l)密钥共享模型中，任一密钥 k_s 被拆分成 l 个分片，当敌方集齐 q 个分片便有可能计算出 k_s。因此当 $x<q$ 时，从信息论角度看 k_s 是确定安全的；但是当 $x\ge q$ 时，密钥 k_s 存在被恢复的可能，然而 k_s 的拥有者 —— 节点 s 可能并未被俘。用 $F(x)$ 表示簇头的抗俘获性，其中 m 表示普通节点总数，n 表示簇头节点总数。

$$F(x)=p(x)\cdot\frac{m}{m-\dfrac{mx}{n}}=p(x)\cdot\frac{n}{n-x} \tag{3}$$

仿真模拟(q, l)密钥共享模型的密钥预分配、密钥对建立和物理俘获簇头等过程，实验结果如图 3(a)–3(d)所示：对于确定的 q 和 l，$F(x)$ 随着 x 的增加而增加；对于确定的 x，$[l-q]$ 越大 $F(x)$ 越小，网络越安全；当 $l=q$ 时，(q, l)门限密钥共享模型退化为无门限的(l, l)模型，此时 l 越大，簇头抗俘获性越好。通过适当调整 q 和 l 的取值，网络可以满足任何安全需求。

4.1.2 节点能耗分析

存储开销：普通节点只需存储一个密钥，其存储开销是固定且最低的。簇头节点需要存储 $[ml/n]$ 个密钥分片，其存储开销相对普通节点更高。对于理想的秘密共享来说，分片的大小与共享秘密本身大小相同。

通信开销：建立密钥对的过程中，普通节点只需发送一次消息，通信量非常低；簇头发送一次广播消息，接收$(1+q)$个消息，通信量对于资源丰富的簇头来说是较低且可接受的。

计算开销：普通节点的计算开销是 0。簇头节点在进行密钥重构时的计算量取决于选择的秘密共享方案。如选择 Shamir 方案[19]，簇头的计算量是一次 Lagrange 插值计算。

4.1.3 网络性能分析

安全连通度：定义为通信双方能够建立密钥对的概率。与概率型方案[13,15]不同，(q, l)密钥共享模型实现了簇内全连通，即任一成员节点都能与其物理簇头成功建立密钥对。

网络容错性：密钥被拆分为 l 个分片，物理簇头只要收集到其中 q 个即可重构密钥。因此，允许少量簇头节点因损坏或其它原因导致的分片发送失败。而且$(l-q)$值越大，网络容错性越强，但抗簇头俘获性会越差。l 和 q 是调节网络容错性和安全性的重要参数。

4.2 (1, l)计算最优模型

当 $q=1$ 时密钥分片退化成密钥本身，物理簇头只需向虚拟簇头直接获取密钥而无需计算，因此(1, l)模型是计算最优的。然而该模型要求簇头必须安装硬件保护装置，否则平均一个被俘簇头将直接泄露 $[ml/n]$ 个密钥。

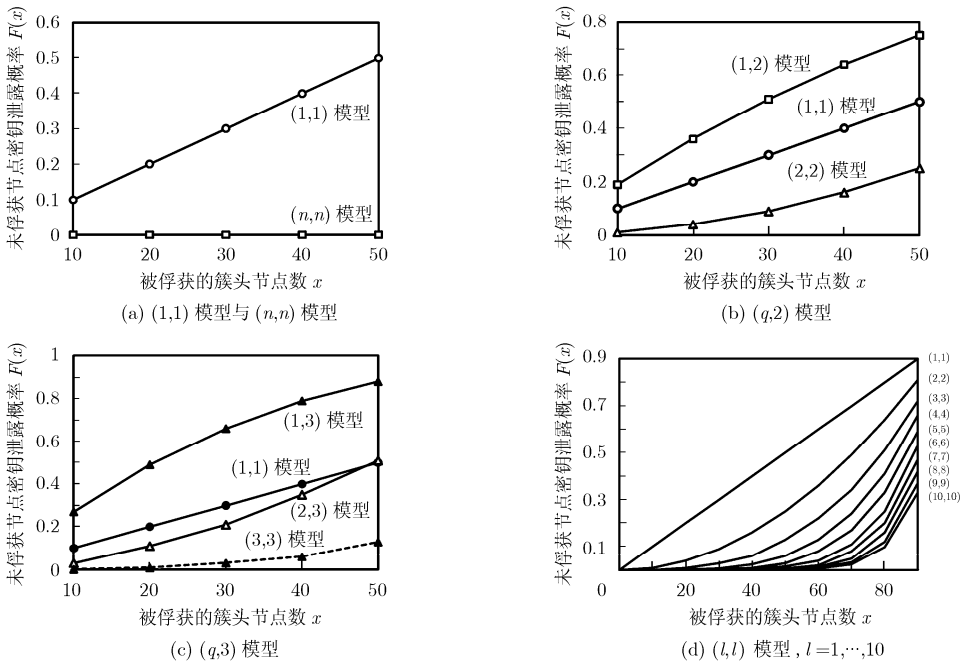

图 3 (q,l)通用模型簇头抗俘获攻击的能力 (注：仿真实验中簇头节点数为 $n=100$)

4.3 (1,1)存储最优模型

当$l=1$时密钥分片退化成密钥本身并存储于唯一的虚拟簇头中。(1,1)模型类似于 Jolly 等人[12]提出的 LEKM 方案，每个簇头仅存储$[m/n]$个密钥(分片)，因此是存储最优的。同$(1,l)$模型一样，簇头节点必须安装硬件保护装置。

4.4 (q,n)通信最优模型

分片交换过程中，物理簇头与虚拟簇头间的距离是影响节点通信量的重要因素。当$l=n$时普通节点的虚拟簇头是全体簇头，因此其物理簇头只需和离自己最近的$(q-1)$个簇头节点交换分片信息，这极大地降低了网络的通信开销。容易推断$(1,n)$是计算和通信最优模型。

4.5 (n,n)抗俘获最优模型

当参数$q=l=n$，表明密钥的存储和重构都需要全体簇头的共同参与。(n,n)模型是节点抗俘获性最优的，它能够给网络提供最坚固的安全保障，但它对簇头节点的存储、计算和通信要求比较高，适用于安全需求高而硬件配置较高的网络。

4.6 与概率型密钥管理方案比较

AP 方案[13]是典型的概率型密钥管理方案，虽然节点的计算和通信量较低，但存储负载、网络连通度和节点抗俘获性三者间的矛盾难以调和。文献[14]方案引入对称矩阵以提高节点抗俘获能力，但同时增加了存储开销，且连通度低的问题也未解决。

图 4，图 5 分别描述了 AP 方案中普通节点、簇头节点的密钥存储量与网络连通度的矛盾关系。文献[14]方案中节点存储的矩阵个数与连通度关系与 AP 相同，但相同的连通度下，文献[14]方案的节点存储量是AP的λ倍(λ是Blom矩阵的安全参数[15])。而(q,l)密钥共享模型中网络连通度始终为 1，且与节点的存储量、网络规模都无关。

图 6 比较了不同方案中普通节点的抗俘获性 $f(x_s)$ (x_s 是被俘获的普通节点数量)。实验结果表明，AP 方案和文献[14]方案中节点存储量越大，其抗俘获性越差。而(q,l)模型对物理俘获普通节点的攻击具有完全抵抗能力。图 7 比较了不同方案簇头节点的抗俘获性。假设簇头节点未安装硬件保护装置，从图中可看出选择的(3,3)模型比 AP 方案，文献[14]方案有明显优势。

(q,l)密钥共享模型中，簇成员节点的计算和通信量与 AP 方案相同，且簇头和簇成员的抗俘获性比 AP 和文献[14]方案有显著提高；簇头的计算和通信开销比 AP 有少量增加，但由于簇头配置较高且资源丰富，因此能够承担相对高的计算和通信负载。表 1 给出了几种不同方案的综合比较结果。

5 结束语

基于门限秘密共享，本文为层次型传感器网络提出了一种(q,l)门限密钥共享模型，有效地解决了簇成员与簇头密钥协商的问题。通过少量增加簇头节点开销，实现了簇成员节点能耗最低、抗俘获能力最优的目标。理论分析与实验数据证明，与传统

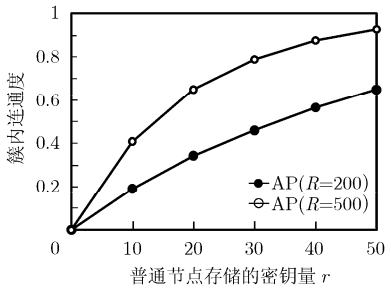

图4 AP方案的簇内连通度

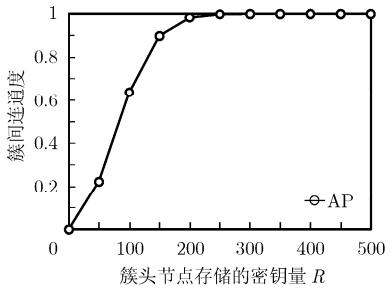

图5 AP方案的簇间连通度

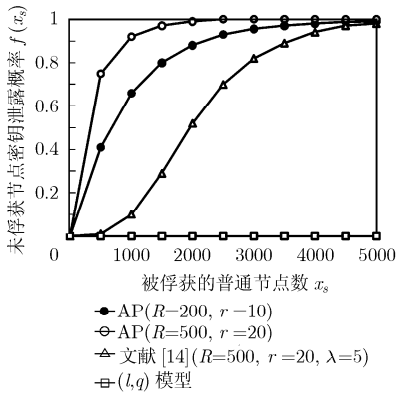

图6 普通节点抗俘获能力

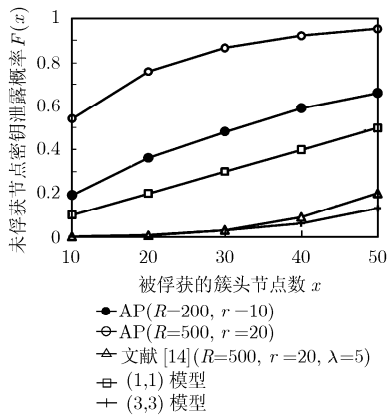

图7 簇头节点抗俘获能力

注：仿真网络中共部署普通节点 $m = 10,000$ 个，簇头节点 $n = 100$ 个。AP 方案密钥池与文献[14]方案矩阵池大小均为 10,000。

表 1 (q, l) 密钥共享模型与 AP 方案、文献[14]方案的综合比较

方案名称	存储开销		连通度		节点抗俘获能力	
	普通节点	簇头节点	簇内	簇间	$f(x_s = 1000)$	$F(x = 30)$
(1,1)密钥共享模型	1 密钥	100 分片	1	1	0	0.32
(3,3)密钥共享模型	1 密钥	300 分片	1	1	0	0.01
AP 方案($R = 200$, $r = 10$)	10 密钥	200 密钥	0.2	0.97	0.66	0.36
AP 方案($R = 500$, $r = 20$)	20 密钥	500 密钥	0.65	1	0.92	0.76
文献[14]方案 ($R = 500$, $r = 20$, $\lambda = 5$)	100 矩阵元素	2500 矩阵元素	0.65	1	0.1	0.03

注：密钥、分片与矩阵元素大小相同，R 和 r 分别为簇头和簇成员节点存储的密钥/矩阵个数。

的概率型方案相比，(q , l)密钥共享模型在保证网络全连通的前提下显著提高了节点的抗俘获能力。此外，门限参数 l 和 q 起到了调节传感器网络安全性、容错性和节点能耗的作用。

混合型方案是层次型传感器网络密钥管理研究的发展方向[16,21]。目前适用于簇间密钥协商的方案有很多，但专门针对簇内层提出的方案非常少。本模型的提出填补了这一研究空白，为混合型密钥管理的进一步发展提出了新思路。

参 考 文 献

[1] Chen X, Makki K, Yen K, *et al*.. Sensor network security: a survey [J]. *IEEE Communications Surveys & Tutorials*, 2009, 11(2): 52–73.

[2] Perrig A, Stankovic J, and Wagner D. Security in wireless sensor networks [J]. *Communications of the ACM*, 2004, 47(6): 53–57.

[3] Eschenauer L and Gligor V D. A key management scheme for distributed sensor networks [C]. The 9th ACM Conference on Computer and Communication Proceedings, Washington, DC, USA, Nov. 17–21, 2002: 41–47.

[4] Chan H W, Perrig A, and Song D. Random key predistribution schemes for sensor networks [C]. 2003 IEEE Symposium on Security and Privacy Proceedings, Berkeley,

CA, May 11–14, 2003: 197–213.

[5] Du W L, Deng J, Han Y S, *et al*.. A key management scheme for wireless sensor networks using deployment knowledge [C]. The 23th Annual Joint Conference of the IEEE Computer and Communications Proceedings, Hong Kong, China, Mar. 7–11, 2004: 586–597.

[6] Levi A, Tasç S E, Lee Y J, *et al*.. Simple, extensible and flexible random key predistribution schemes for wireless sensor networks using reusable key pools [J]. *Journal of Intelligent Manufacturing*, 2009, 21(5): 635–645.

[7] Jaworski J, Ren M, and Rybarczyk K. Random key predistribution for wireless sensor networks using deployment knowledge [J]. *Computing*, 2009, 85(1–2): 57–76.

[8] Liu D G, Ning P, and Li R F. Establishing pairwise keys in distributed sensor networks [J]. *ACM Transactions on Information and System Security*, 2005, 8(1): 41–77.

[9] Wang J, Xia Z Y, Harn L, *et al*.. Storage-optimal key sharing with authentication in sensor networks [C]. Parallel and Distributed Processing and Applications Proceedings, Nanjing, China, Nov. 2–5, 2005: 466–474.

[10] Kim J M, Han Y J, and Park S H, *et al*.. N-dimensional grid-based key predistribution in wireless sensor networks [C]. 2007 International Conference on Computational Science and Its Applications Proceedings, Kuala Lumpur, Malaysia, Aug. 26–29, 2007: 1107–1120.

[11] Wen M, Zheng Y F, Ye W J, *et al*.. A key management protocol with robust continuity for sensor networks [J]. *Computer Standards & Interfaces*, 2009, 31(4): 642–647.

[12] Jolly G, Kusçu M C, Kokate P, *et al*.. Low-energy key management protocol for wireless sensor networks [C]. The 8th IEEE International Symposium on Computers and Communications Proceedings, Kemer-Antalya, Turkey, June. 30–July 3, 2003: 335–340.

[13] Du X J, Xiao Y, Guizani M, *et al*.. An effective key management scheme for heterogeneous sensor networks [J]. *Ad Hoc Networks*, 2007, 5(1): 24–34.

[14] Boujelben M, Cheikhrouhou O, Abid M, *et al*.. Establishing pairwise keys in heterogeneous two-tiered wireless sensor networks [C]. The 3rd International Conference on Sensor Technologies and Applications Proceedings, Athens, Greece, June 18–23, 2009: 442–448.

[15] Blom R. An optimal class of symmetric key generation system [C]. A Workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques, EUROCRYPT 84 Proceedings, Paris, France, Apr. 9–11, 1984: 335–338.

[16] Landstra T, Jagannathan S, and Zawodniok M. Energy-efficient hybrid key management protocol for wireless sensor networks [J]. *International Journal of Network Security*, 2009, 9(2): 121–134.

[17] Watro R, Kong D, Cuti S, *et al*.. Tinypk: securing sensor networks with public key technology [C]. The 2nd ACM Workshop on Security of Ad hoc and Sensor Networks Proceedings, Washington DC, USA, Oct. 25–29, 2004: 59–64.

[18] Hu W, Corke P, Shih W, *et al*.. Secfleck: a public key technology platform for wireless sensor networks [C]. The 6th European Conference on Wireless Sensor Networks Proceedings, Cork, Ireland, Feb. 11–13, 2009: 296–311.

[19] Shamir A. How to share a secret [J]. *Communications of the ACM*, 1979, 22(11): 612–613.

[20] Harn L and Lin C L. Authenticated group key transfer protocol based on secret sharing [J]. *IEEE Transactions on Computers*, 2010, 59(6): 842–846.

[21] Zhang J Q and Varadharajan V. Wireless sensor network key management survey and taxonomy [J]. *Journal of Network and Computer Applications*, 2010, 33(2): 63–75.

柳亚男： 女，1984 年生，博士生，研究方向为传感器网络密钥管理.

王 箭： 男，1968 年生，教授，博士生导师，研究方向为信息安全(包括应用密码学、安全系统分析与设计等).

杜 贺： 男，1984 年生，博士生，研究方向为数字签名.