一种轻量级的无线传感器网络密钥建立协议

刘 伟 罗 嵘 杨华中
(清华大学电子工程系 北京 100084)

摘 要：该文提出了一种适用于无线传感器网络的轻量级密钥建立协议。该协议以预置的瞬时初始密钥为基础，通过优化密钥建立过程中的信息交互，能够获得更好的可扩展性和更低的能量开销。对该协议的完成时间和网络的连通概率的理论分析表明，该协议是可行的。从仿真结果可以看出，该协议在典型的网络规模下可以获得超过 97% 的连通概率。与同类协议相比，可以在保证足够的连通概率的情况下以更短的时间完成密钥建立。当网络密度为单跳 30 个节点时，建立时间小于 5.2 s。此外，该协议的能量开销只有同类协议的 25%，因此更适合应用于资源受限的无线传感器节点。

关键词：无线传感器网络；初始密钥；密钥建立；完全连通概率；协议开销
中图分类号：TP393 **文献标识码**： A **文章编号**：1009-5896(2010)04-0869-06
DOI: 10.3724/SP.J.1146.2009.00349

A Lightweight Key Establishment Protocol for Wireless Sensor Networks

Liu Wei Luo Rong Yang Hua-zhong
(*Department of Electronic Engineering*, *Tsinghua University*, *Beijing* 100084, *China*)

Abstract: In this paper, a lightweight key establishment protocol for wireless sensor networks is proposed. By optimizing information exchanges in the process of key establishment, this temporal initial key based protocol is able to achieve better extensibility and lower energy consumption. Theoretical analysis of finish time and totally connected probability verifies that this protocol is feasible. The simulation results show that, the connected probability is larger than 97% for typical network density. Compared with similar protocols, this protocol needs much less time to finish with enough connected probability. The finish time is less than 5.2s at the network density of 30 nodes per hop. Moreover, energy consumption is only 25% of those of similar protocols, which makes this protocol more suitable for resource constrained sensor nodes.

Key words: Wireless sensor network; Initial key; Key establishment; Totally connected probability; Protocol overhead

1 引言

无线传感器网络通常需要部署在开放甚至不友好的环境内，比如野外和战场。同时，它所监测的信息往往具有敏感性和隐私性。因此，必要的安全机制对于无线传感器网络的正常运行非常重要。由于传感器节点的能力非常有限，在这种网络中提供安全保障比传统网络要困难得多，所采用的安全机制要消耗尽可能少的计算、通信和存储资源。现有的安全机制通常采用复杂度较小的对称密码系统来提供安全服务。对称密码系统在通信双方使用相同的密钥进行操作，这就需要合理的机制来建立这些密钥。由于传统的不对称密码系统复杂度过高，无法在传感器节点上有效实现，从而导致很多以其为基础的密钥建立协议，比如 TLS 和 Kerberos，无法直接应用于无线传感器网络[1]。

无线传感器网络中最简单和最安全的密钥管理机制分别为全局共享密钥机制和预置独立对密钥机制[1]。全局共享密钥机制在整个网络内使用同一共享密钥，即网络中所有节点使用相同的密钥进行加密和认证[2,3]。这种机制不需要额外的计算和通信开销来产生密钥，只需要存储一个或少量几个密钥。然而，这种机制存在极大的安全隐患，只要一个节点被捕获就会影响整个网络的安全性。预置独立对密钥机制是给各个节点对预置独立的密钥，即网络中任意两个节点对使用的密钥都在部署前预置。这种机制的安全性很高，捕获一个节点不会使其余节点之间的通信安全性受到影响。它的缺点是存储开销非常大，不适合存储资源非常有限的传感器节点。

2009-03-19 收到，2009-08-13 改回
国家 863 计划项目(2006AA01Z224)资助课题
通信作者：罗嵘 luorong@tsinghua.edu.cn

目前可行的无线传感器网络密钥管理机制可以分为 4 类：基站辅助管理机制、随机密钥预分配机制、瞬时共享密钥机制和明文密钥交换机制，下面对这 4 种机制的相关研究工作分别进行介绍。文献[4]提出利用可信任基站辅助节点对建立链路密钥，这种机制只对小规模的网络有效，很难扩展到大规模的网络。同时，这种机制无法将被捕获节点限制在局部区域内，被捕获节点可以与网络中任意节点建立安全连接。

文献[5]最早提出了随机密钥预分配的概念。在这种机制下，节点预先装载一定数目的密钥，这些密钥从密钥池中随机选取。节点部署后，按照相互之间拥有相同密钥的概率建立安全连接。为了保证一定的连通概率，节点需要预装足够数目的密钥，这对于存储受限的节点而言是很大的负担。同时，相邻节点需要发送大量的数据才能确定是否拥有相同密钥，从而导致很大的通信开销。文献[6–14]在此基础上做了更详细的分析，对这一机制进行了扩展。在对随机密钥预分配深入研究的基础上，文献[15–18]提出了结合网络拓扑进行密钥管理的机制，但其本质上仍然属于随机密钥预分配机制。

文献[19]最早提出了基于瞬时共享密钥的密钥管理协议 LEAP，通过预置相同的初始密钥，相邻节点在部署后通过必要的信息交互建立链路密钥。这一协议与本文提出的协议属于一类，但本文提出的协议在建立链路密钥的过程中需要更少的信息交互，因此具有更好的可扩展性和更低的能量开销。文献[20]最早提出了一种明文密钥交换机制，这一机制基于入侵者在特定时间只会出现在特定地点的观察，通过随机产生并明文发送链路密钥，来建立相邻节点间的安全连接。这一机制不需要预置任何初始密钥，并且其密钥建立过程是完全分布式的。然而，由于不要求节点认证，恶意节点可以随意加入网络。文献[21]将文献[20]的思想引入 LEAP 协议，通过引入随机性来降低 LEAP 协议中初始密钥被捕获对整个网络的影响。

综上所述，现有协议在算法复杂度、可扩展性和安全性等方面存在着一定的缺陷，无法在低成本节点组成的大规模网络中有效实现。为此，本文结合全局共享密钥机制和预置独立对密钥机制各自的优缺点，提出了一种轻量级的密钥建立协议，在不引入过多开销的前提下，达到了接近预置独立对密钥机制的安全性。本文剩余内容的结构如下：第 2 节介绍了本协议所需的数学基础以及对应用场景的假设；在第 3 节描述协议具体内容的基础上，第 4 节对协议的完成时间和网络的连通概率进行了分析和仿真；最后一节给出了本文的结论。

2 数学模型和应用假设

2.1 单向散列函数

在本协议的实现过程中，需要利用同一个原始密钥产生节点对之间的链路密钥，同时要保证链路密钥的泄露不会影响原始密钥的保密性。也就是说，即使有很多链路密钥被捕获，也不可能根据这些链路密钥反向推导出原始密钥。这可以通过单向散列函数来实现。单向散列函数作用于任意长度的消息 M，生成固定长度 m 的散列值 h：

$$h = H(M) \tag{1}$$

2.2 对无线传感器网络应用场景的假设

在实际的无线传感器网络应用中，网络在刚刚部署的瞬间就有节点被捕获并导致密钥信息泄漏的可能性非常小。一般来说，根据现有的技术手段，从被捕获节点的存储设备中提取密钥至少需要几十秒的时间[21]。也就是说，节点被捕获导致密钥信息泄漏有一个时间下限 $T_{\min}$，在这个时间限制之内，可以认为节点中的数据是绝对安全的。本文提出的密钥建立协议就基于这一假设，在时间限制 $T_{\min}$ 内完成链路密钥的建立，然后清除原始的密钥信息，以提供接近于预置独立对密钥机制的安全性。

无线传感器网络的通信模式很少会有端到端的任意通信。常见的通信模式基本上只有两种，即相邻节点之间的通信以及节点与基站之间的通信，因此建立链路密钥和节点基站对密钥就可以满足绝大部分应用需求。本文提出的协议正是用于这一目的。同时，链路密钥可以作为建立其它类型密钥的基础[19]。

在预置相同初始密钥的情况下，如果两个相邻节点需要建立安全连接，完全可以根据初始密钥按照约定的机制生成链路密钥，只要保证这一机制具有对称性和单向性即可，没有必要进行过多的计算和通信。因此，本文提出的协议可在引入少量计算和通信开销的情况下，建立节点间的链路密钥。

3 轻量级的密钥建立协议

3.1 网络拓扑结构

本文在单跳网络结构下描述和分析密钥建立协议，即所有节点都在相互的通信范围内。这里假设节点间的连接是对称的，即如果 i 能够接收到来自 j 的消息，那么 j 也能够接收到来自 i 的消息。在通常的传感器网络应用场景下，这一假设是合理的[22]。

3.2 密钥建立协议

本文提出的密钥建立协议分为 3 个阶段：预置初始信息阶段、链路密钥建立阶段和初始密钥清除

阶段，其中链路密钥建立阶段又分为邻居节点发现阶段和链路密钥生成阶段。下面分别对其进行详细介绍。

3.2.1 预置初始信息阶段　在网络部署之前，可信任节点产生一个初始密钥 K_0，并为每一个节点随机产生一个地址 i，然后计算节点 i 与基站的密钥：

$$K_i = H(K_0, i, K_0) \tag{2}$$

可信任节点将初始密钥对(K_0, K_i)装载到节点 i 中，其中 K_0用于本协议中链路密钥的建立，K_i作为节点 i 的唯一身份标识，可用于与基站的通信。这里有一个隐含的假设，即可信任节点被捕获导致初始密钥 K_0泄漏的机率很小。在大多数应用中，这一假设是合理的，因为可信任节点通常是功能更强、保护更多的基站节点或服务器。

3.2.2 链路密钥建立阶段　所有节点预置初始信息后，可以通过随机撒播或人工安装等方式进行部署。这里不要求预先了解网络的拓扑信息，因为该协议的运行不依赖于邻居节点的身份。网络部署后，所有节点启动，进入链路密钥建立阶段。

(1)邻居节点发现　每个节点 i 随机产生并记录一个随机数 nonce_i，作为链路密钥建立过程中所需的特征随机数。在链路密钥建立过程中使用随机数是为了引入空间差异性。随后，每个节点在退避时间窗内随机选择一个退避时间，准备对外广播自己的身份消息。在退避时间内，节点将监听信道。当退避时间结束时，如果节点 i 发现没有其它节点使用信道，那么节点 i 将对外广播自己的身份消息 $i||\text{nonce}_i$。如果在退避时间内节点 i 发现有邻居节点开始广播身份消息，那么它将停止监听信道，开始接收该身份消息。接收完成后，节点 i 根据收到的地址和随机数计算与发送节点的链路密钥。假设一次退避过程中没有碰撞发生，那么所有邻居节点都能收到最早结束退避时间的节点的身份消息广播。重复这一过程，直到密钥建立过程的时间限制 $T_{\min}$ 结束。这一过程可以用图 1 来加以说明。

图 1 假设节点 i 最早结束退避时间，其身份消息的发送时间为 T_T，此时所有邻居节点处于接收状态，接收时间为 T_R=T_T。接收到身份消息后，邻居节点计算与 i 的链路密钥，计算时间为 T_C。如果身份消息的发送时间大于链路密钥的计算时间，那么链路密钥的计算可以被推迟并嵌入到下一次身份消息广播的过程中。在身份消息长度和单向散列函数确定的情况下，T_T和 T_C的取值是固定的，因此即使两个节点有可能同时最早结束退避时间而造成碰撞，其它节点仍能够通过监听信道来后退 T_T+T_C(或 T_T)的时间，从而能够进入下一次退避过程。

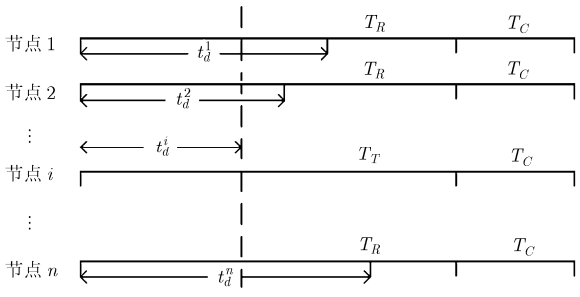

图 1 一次链路密钥建立过程示意图

(2)链路密钥生成　假设节点 j 接收到节点 i 的身份广播，这时它可以计算与节点 i 的链路密钥：

$$K_{j,i} = H(K_0, f(j,i), K_0) \tag{3}$$

为了保证 i和 j在仅知道对方身份的情况下产生相同的链路密钥，$f(i, j)$应满足以下条件：

$$f(i,j) = f(j,i), \quad \forall i, j \tag{4}$$

这样，节点 i 接收到节点 j 的身份广播，就可以生成

$$K_{i,j} = H(K_0, f(i,j), K_0) = K_{j,i} \tag{5}$$

因此，只要节点 i和节点 j在相互的通信范围内，并且二者的身份广播都没有出现碰撞，就可以产生相同的链路密钥。这一过程只需要知道双方的身份消息，并不需要进行额外的数据交互。为了保证不同的邻居节点对不会生成相同的链路密钥，同时考虑到传感器节点的计算能力有限，本文使用以下函数：

$$f(i,j) = \begin{cases} i \,||\, \text{nonce}_i \,||\, j \,||\, \text{nonce}_j, & i > j \\ j \,||\, \text{nonce}_j \,||\, i \,||\, \text{nonce}_i, & j > i \end{cases} \tag{6}$$

3.2.3 初始密钥清除阶段　当时间限制 $T_{\min}$ 到期后，不论网络中是否还有节点未完成身份广播，算法都应该结束，从而避免初始密钥 K_0 被捕获。这时节点清除初始密钥 K_0，进入正常的应用数据通信阶段。

4　理论分析与仿真

4.1 协议完成时间分析

假设第 1 次退避开始后，节点 i 最早结束退避时间，其余节点接收到 i 的身份广播后计算与 i 的链路密钥，然后进入下一次广播尝试。因此，第 1 次链路密钥建立过程所需的时间为

$$t_1 = t_d^i + T_T + T_C \tag{7}$$

如果身份广播时间 T_T大于链路密钥计算时间 T_C，那么 T_C可以延迟并嵌入到下次身份广播过程中，此时有

$$t_1 = t_d^i + T_T \tag{8}$$

为了后面表示方便，将 t_d^i 记为 t_d^n，表示从退避时间

窗中选择 n 次得到的最小值。依次进行下去，直到最后一个节点广播完自己的地址，因此算法完成的总时间为

$$t=\sum_{k=1}^{n}(t_d^k+T_T+T_C)\text{ 或 }t=\sum_{k=1}^{n}(t_d^k+T_T) \tag{9}$$

此处假设每次退避后，不会出现两个或两个以上节点同时最早结束退避时间造成身份消息碰撞的情况。从下一小节的推导中可以看到，当退避时间窗的长度足够大时，两个或两个以上节点同时最早结束退避时间造成身份消息碰撞的概率非常小，因此这种假设是合理的。如果确实出现了两个或两个以上节点同时最早结束退避时间造成身份消息碰撞的情况，那么在一次退避后会有多个身份消息被发送，即多个节点在同一个退避周期内完成身份消息广播，从而使总的退避次数小于节点个数 n。在这种情况下，算法完成的总时间要小于上述公式中的 t。给定时间限制 $T_{\min}$，如果式(9)给出的时间 t 小于 $T_{\min}$，那么发生碰撞情况下的完成时间也必然小于 $T_{\min}$。

为了在给定的时间限制 $T_{\min}$ 内完成算法，必须满足

$$t=\sum_{k=1}^{n}(t_d^k+T_T+T_C)<T_{\min}\text{或}t=\sum_{k=1}^{n}(t_d^k+T_T)<T_{\min} \tag{10}$$

为了使算法在给定时间限制内有可能完成，必须保证

$$T_{\min}-n(T_T+T_C)>0\text{ 或 }T_{\min}-nT_T>0 \tag{11}$$

即

$$n<\frac{T_{\min}}{T_T+T_C}\text{ 或 }n<\frac{T_{\min}}{T_T} \tag{12}$$

另一方面，如果节点个数 n_0 能满足：

$$n_0T_D=T_{\min}-n_0(T_T+T_C)\text{ 或 }n_0T_D=T_{\min}-n_0T_T \tag{13}$$

那么对于任意的 $n<n_0$，密钥建立过程在时间限制 $T_{\min}$ 内完成的概率均为 1。也就是说，n_0 决定了算法支持节点个数的最小值，因此

$$n>\frac{T_{\min}}{(m-1)T_{\text{uint}}+T_T+T_C}\text{或}n>\frac{T_{\min}}{(m-1)T_{\text{uint}}+T_T} \tag{14}$$

4.2 完全连通概率分析

完全连通是指所有的节点对之间都建立了双向的链路密钥。如果节点 j 成功接收到节点 i 的身份消息，但节点 i 并未成功接收到节点 j 的身份消息，那么只有节点 j 计算了它与 i 的密钥，节点 i 并未计算它与 j 的密钥，即使这两个密钥值相同。在这种情况下，看起来建立了 i 到 j 的单向连接，但由于节点 i 并没有计算与节点 j 的密钥，因此它们之间并不能进行任何安全通信。即使节点 j 使用生成的密钥加密或验证了发往 i 的数据分组，节点 i 也不能对这些分组做任何有效的处理。

为了实现完全连通，必须保证每次退避周期都不能出现碰撞，即每次退避周期都不能出现两个或两个以上节点同时最早结束退避时间的情况，因此完全连通概率可以表示为

$$P=P(k)P(k-1)\cdots P(2)P(1) \tag{15}$$

这里 $P(k)$是在剩余 k 个节点未广播身份消息的情况下，退避周期内不出现碰撞的概率，即不出现两个或两个以上节点同时最早结束退避时间的情况。不出现碰撞的情况有很多种，一种是 k 个节点选择了不同的退避时间，这时必然不会发生碰撞；另一种是即使有两个或两个以上节点选择了相同的退避时间，但最小的那个退避时间值没有重复，这样也不会发生碰撞(这是因为有相同退避时间值的节点在监听阶段都会发现信道忙，因此都不会发送，自然就不会产生碰撞)。这个问题可以抽象为一个数学问题：有 0~(m–1)共 m 个整数，从中选出 k 个，最小值不重复的概率是多少，因此有

$$\begin{aligned}P(k)&=\frac{k\left[(m-1)^{k-1}+(m-2)^{k-1}+\cdots+2^{k-1}+1^{k-1}\right]}{m^k}\\&=k\sum_{i=1}^{m-1}(m-i)^{k-1}\Big/m^k\end{aligned} \tag{16}$$

4.3 仿真结果

根据式(15)，可以确定在不同的退避时间窗长度 m 下，完全连通概率 P 与节点个数 n 的关系，如图 2 所示。

从图 2 可以看出，完全连通概率取决于退避时间窗的大小。当网络节点密度较小时，较小的退避时间窗就能保证足够的完全连通概率。当退避时间窗足够大时，对于典型的网络密度(单跳范围内 20–30 个节点)，完全连通的概率超过 97%。因此，退避时间窗长度的选取需要根据实际应用中可能出现的最大网络密度来确定。

为了与同类协议 LEAP[19]和 OTMK[21]具有可比性，这里以 Mica2 节点为目标平台，使用 Avrora 仿真器对协议完成时间做实际分析。对于下面的实验仿真，仿真结果都是对同一实验执行 10^5 次统计得到的。为了获得足够的完全连通概率，选择退避时间窗的长度为 8192 个时隙。

密钥建立完成时间与网络密度的关系如图 3 所示。从图 3 可以看出，当网络密度小于每跳 30 节点时，协议的实际完成时间小于 5.2 s。为了更直观地与 LEAP 和 OTMK 进行比较，将它们的完成时间列于表 1。从表 1 可以看出，即使在网络密度更高的情况下，本协议的完成时间也远小于 LEAP 和

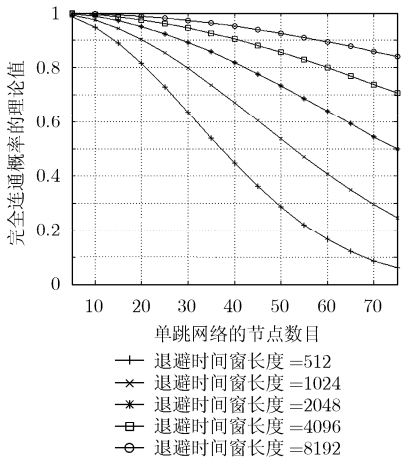

图 2 不同节点个数下的完全连通概率

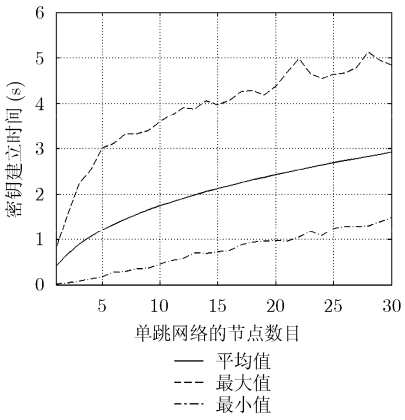

图 3 实际完成时间与网络密度的关系

表 1 与同类协议完成时间的比较

协议名称	节点密度	完成时间
LEAP+	20	170 s
基本 OTMK	10	100 s
简化 OTMK	10	20 s

OTMK 的完成时间。在同样的网络密度下，本协议的优势会更加明显。由于在整个执行阶段处理器和收发机都处于工作状态，因此完成时间的优势直接转化为能量开销的优势。与最简单的简化 OTMK 相比，本协议能够节省的能量也接近 75%。

5 结论

结合全局共享密钥机制和预置独立对密钥机制各自的优缺点，本文提出了一种轻量级的密钥建立协议，在不引入过多开销的前提下，达到了接近预置独立对密钥机制的安全性。通过对该协议完成时间和网络连通概率的分析和仿真，可以看到通过合理选择协议参数，该协议对不同的网络规模有良好的可扩展性，同时在典型的网络规模下可以获得超过 97%的完全连通概率。与同类协议相比，该协议可以在保证足够的完全连通概率的情况下以更短的时间完成。在网络密度为单跳 30 个节点时，完成时间小于 5.2 s。同时，该协议的能量开销只有同类协议的 25%，因此更适合应用于资源受限的无线传感器节点。

参 考 文 献

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

[2] Karlof C, Sastry N, and Wagner D, *et al*.. Tinysec: a link layer security architecture for wireless sensor networks[C]. The 2nd ACM Conf. Embedded Networked Sensor Systems, Baltimore, Maryland, USA, Nov. 3–5, 2004: 162–175.

[3] Basagni S, Herrin K, and Rosti E, *et al*.. Secure pebblenets[C]. The 2nd ACM Int'l Symp. Mobile Ad hoc Networking and Computing, Long Beach, CA, USA, Oct. 04–05, 2001: 156–163.

[4] Perrig A, Szewczyk R, and Wen V, *et al*.. SPINS: Security protocols for sensor networks[C]. The 7th Int'l Conf. Mobile Computing and Networking, Rome, Italy, Jul. 16-21, 2001: 189–199.

[5] Eschenauer L and Gligor V. A key-management scheme for distributed sensor networks[C]. The 9th ACM Conf. Computer and Communications Security, Washington, DC, USA, Nov. 17–21, 2002: 41–47.

[6] Chan H, Perrig A, and Song D. Random key predistribution schemes for sensor networks[C]. The IEEE Symp. Security and Privacy, Oakland, California, USA, May. 11–14, 2003: 197–213.

[7] Zhu S, Xu S, and Setia S, *et al*.. Establishing pair-wise keys for secure communication in Ad Hoc networks: a probabilistic approach[C]. The 11th IEEE Int'l Conf. Network Protocols, Atlanta, Georgia, USA, Nov. 4–7, 2003: 326–335.

[8] Du W, Deng J, and Han Y, *et al*.. A pairwise key predistribution scheme for wireless sensor networks[J]. *ACM Transactions on Information and System Security*, 2005, 8(2): 228–258.

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

[10] Huang D, Mehta M, and Liefvoort A V D, *et al*.. Modeling pairwise key establishment for random key predistribution in large-scale sensor networks[J]. *IEEE/ACM Transactions on Networking*, 2007, 15(5): 1204–1215.

[11] Law Y W, Yen L H, and Pietro R D, *et al*.. Secure

k-connectivity properties of wireless sensor networks[C]. The 4th IEEE Int'l Conf. Mobile Ad-hoc and Sensor Systems, Pisa, Italy, Oct. 8–11, 2007: 1–6.

[12] Wu J and Stinson D R. Minimum node degree and k-connectivity for key predistribution schemes and distributed sensor networks[C]. The 1st ACM Conf. Wireless Network Security, Alexandria, Virginia, USA, Mar. 31–Apr. 2, 2008: 119–124.

[13] Camtepe S A and Yener B. Combinatorial design of key distribution mechanisms for wireless sensor networks[J]. *IEEE/ACM Transactions on Networking*, 2007, 15(2): 346–358.

[14] Delgosha F, Ayday E, and Fekri F. MKPS: a multivariate polynomial scheme for symmetric key-establishment in distributed sensor networks[C]. The ACM Int'l Wireless Communications and Mobile Computing Conference, Honolulu, Hawaii, USA, Aug. 12–16, 2007: 236–241.

[15] Liu D and Ning P. Location-based pairwise key establishment for static sensor networks[C]. The 1st ACM Workshop on Security of Ad hoc and Sensor Networks, Fairfax, VA, USA, Oct. 31–31, 2003: 72–82.

[16] Du W, Deng J, and Han Y, *et al*.. A key management scheme for wireless sensor networks using deployment knowledge[C]. The 23rd IEEE Conf. Computer Communications, Hong Kong, Mar. 7–11, 2004: 586–597.

[17] Liu D, Ning P, and Du W. Group-based key predistribution for wireless sensor networks [J]. *ACM Transactions on Sensor Networks*, 2008, 4(2): 1–30.

[18] Canh N T, Truc P T H, and Hai T H, *et al*.. Enhanced group-based key management scheme for wireless sensor networks using deployment knowledge[C]. The 6th Annual IEEE Consumer Communications and Networking Conference, Las Vegas, Nevada, USA, Jan. 10–13, 2009: 1–5.

[19] Zhu S, Setia S, and Jajodia S. LEAP+: efficient security mechanisms for large-scale distributed sensor networks [J]. *ACM Transactions on Sensor Networks*, 2006, 2(4): 500–528.

[20] Anderson R, Chan H, and Perrig A. Key infection: smart trust for smart dust[C]. The 12th IEEE Int'l Conf. Network Protocols, Berlin, Germany, Oct. 5–8, 2004: 206–215.

[21] Deng J, Hartung C, and Han R, *et al*.. A practical study of transitory master key establishment for wireless sensor networks[C]. The 1st IEEE/CreateNet Int'l Conf. Security and Privacy for Emerging Areas in Communication Networks, Athens, Greece, Sep. 5–9, 2005: 289–299.

[22] Woo A and Culler D E. A transmission control scheme for media access in sensor networks[C]. The 7th Int'l Conf. Mobile Computing and Networking, Rome, Italy, Jul. 16–21, 2001: 221–235.

刘 伟： 男，1981 年生，博士生，研究方向为无线传感器网络的低功耗设计技术、无线传感器网络的安全机制和无线传感器网络的数据融合等.

罗 嵘： 女，1970 年生，副教授，研究方向为 VLSI 设计技术、嵌入式系统设计、电子设计自动化等.

杨华中： 男，1967 年生，教授，研究方向为微系统芯片的新结构、面向通信和媒体处理的芯片设计、传感器节点的片上集成和模拟及混合信号系统设计等.