无线传感器网络层簇式密钥管理方案的研究

李 琳[①] 王汝传[①②] 姜 波[①] 黄海平[①]
[①](南京邮电大学计算机科学与技术系 南京 210003)
[②](南京大学计算机软件新技术国家重点实验室 南京 210093)

摘 要 密钥管理是无线传感器网络安全机制最关键的技术之一。该文分析比较了各种密钥管理方案，认为组密钥管理更适合于无线传感器网络。并在集中式和分布式两种组密钥管理方案的基础上，提出了新的层簇式密钥管理架构，并解决了这两种方案存在的安全缺陷。而组间通信则采用基于(*t*, *n*)门限方案的密钥分割机制来实现。该新方案能保证无线传感器网络安全需求的同时改善执行效能。

关键词 无线传感器网络，密钥管理，(*t*, *n*)门限方案，层簇式逻辑密钥树

中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2006)12-2394-04

Research of Layer-Cluster Key Management Scheme on Wireless Sensor Networks

Li Lin[①] Wang Ru-chuan[①②] Jiang Bo[①] Huang Hai-ping[①]
[①](*Department of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*)
[②](*State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing* 210093, *China*)

Abstract Key management is one of the most important technologies on the security mechanism of wireless sensor network. Compared with all kinds of key management schemes, group key management is more suitable for wireless sensor network. According to the root-controlling and distributing group key management schemes, this paper proposes a novel layer-cluster key management technique and resolves specific defects of the two schemes. Furthermore, secret sharing mechanism based on (*t*, *n*) threshold cryptography realizes the secure communication among groups. The new proposal can not only meet security demands of wireless sensor network but also improve executing performance.

Key words Wireless sensor networks, Key management, (*t*, *n*) threshold scheme, Layer-cluster logic key tree

1 引言

无线传感器网络(Wireless Sensor Networks, WSNs)是计算机、通信和传感器3种技术相结合的产物。无线传感器网络由许多功能相同或不同的无线传感器节点以Ad hoc自组网络的方式构成，其目的是协作地感知、采集、处理其所覆盖区域中被感知对象的信息，并发布给使用者[1]。无相传感器网络除了具有Ad hoc网络的移动性、断接性、能源受限等共同特性之外，还具有一些明显的特征[2,3]：

(1) 网络规模更为庞大，节点数目更多、密度更大，属于大型动态自组网络；

(2) 网络拓扑结构变化快，网络节点通常缺乏统一的ID标识，易失效；

(3) 网络节点由电池供电，计算能力和通信能力非常有限。

2005-05-16 收到，2005-11-30 改回
国家自然科学基金(60573141，70271050)，江苏省自然科学基金(BK2005146)，江苏省自然科学基金预研项目(BK2004218)，江苏省高技术研究计划(BG2004004，BG2005038)和江苏省计算机信息处理技术重点实验室基金(kjs050001)资助课题

无线传感器网络的这些特点使其在安全性能上面临更大的挑战，而大多数的安全协议和保护机制无法直接应用于无线传感器网络，密钥管理机制亦是如此。目前，应用于Ad hoc网络的一些密钥管理方案，例如局部分布式认证授权方案、完全分布式认证授权方案、自发证书方案、安全Pebble Nets方案等等，均不能有效地适用于无线传感器网络。于是，针对无线传感器网络的特点，研究者们提出了一些新的密钥管理方案。例如基于共享Pair-wise密钥的管理方案和多维空间密钥管理方案，这两种方案基于多项式的预配置，优点是能抵御“节点俘获”、扩展性好，缺点是计算开销较大且不支持相邻节点的身份认证。还有两种基于密钥池的预配置方案——Eschenauer 和 Gligor 提出的基本随机密钥预分配方案[4]以及由Chen, Perrig和Song改进的q-Composite随机密钥预分配方案[5]，它们能有效地支持网络的动态变化且计算负载较小，但仍无法实现相邻节点的身份认证。

由于无线传感器网络往往可能布局在敌方区域，为了防止敌对者恶意地破坏网络(例如仿冒、篡改等)，实现节点间的源端认证是非常必要的。因此，组密钥管理方案比预配置方案更加适用于无线传感器网络[6]。

2　组密钥管理的基本原理

组密钥管理方案是在倒置树的逻辑密钥层次管理方案上的延伸与扩展，其主要目的是为本组的无线传感器节点生成、分发和更新组密钥(group key)。组密钥是所有组成员节点共享的密钥，被用来对组播报文进行加解密、源端认证等操作，以满足私密性、认证性、完整性等需求。

一般而言,无线传感器网络的组密钥管理所要满足的安全需求可分列如下[7,8]:

(1)前向私密性　退出组的成员节点尤其是被敌方控制后被强制退出的恶意节点，无法再利用它所知的密钥解密后来的组报文或生成有效的加密报文；

(2)后向私密性　新加入的传感器节点可以通过更新密钥来参与组通信；

(3)抗同谋破解　被敌方控制的几个恶意节点联合起来无法破解密钥更新后的组密钥；

(4)源端认证性　需要实现组内与组间的认证性，即通信节点是否为合法节点；

(5)鲁棒性与可靠性　当网络中部分节点失效后，组内通信仍能继续进行。

而无线传感器网络的组密钥管理所要满足的性能需求可分列如下[7,8]:

(1)可扩展性　该组密钥管理方案应能适应大规模网络的动态变化；

(2)密钥生成的计算量小、密钥传输所占用的无线带宽小以及时延小等。

目前，组密钥管理方案主要有两种基本形式：一是集中式的组密钥管理，二是分布式的组密钥管理。

2.1　集中式的组密钥管理

如图 1 所示，在网络配置阶段，选择M节点(相对于普通节点而言，具有较好的计算能力和通信能力)作为组控制节点，组成员节点均为叶子节点。加入新节点M_8时，组控制节点为其生成共享密钥k_8，无需更新密钥k_{67}和组密钥K，即能确保后向私密性。

若要删除被敌方控制的恶意节点，例如M_3，则为了保证前向私密性，必须更新密钥k_{345}和组密钥K。组控制节点M先用k_4加密新密钥k_{45}发送给M_4，然后再用k_{45}加密新的组密钥K'发送给M_4。依此类推，从而保证了M_3无法再用先前所知的密钥破坏组内通信。

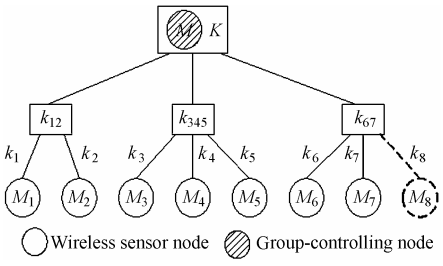

图 1　集中式组密钥管理的拓扑结构

Fig.1 Topologic structure of the root-controlling group key management

该方案的主要缺点在于组控制节点需要保存的密钥数量过多，密钥更新占用带宽较大，当网络规模扩大时，易成为整个网络的瓶颈。

2.2　分布式的组密钥管理

如图 2 所示，分布式组密钥管理无需组控制节点，其组密钥的产生由所有的组成员节点(叶子节点)协商产生。在网络配置阶段，可以约定，每一棵子树最左端的叶子节点为密钥协商的Leader。M_1和M_2将按照某种算法协商出密钥k_{12}，M_3，M_4和M_5协商出密钥k_{345}，M_6和M_7协商出密钥k_{67}。作为Leader，M_1，M_3和M_6再协商出密钥K作为该组的组密钥。

考虑有新节点M_8加入的情况，则由M_1担任Leader的角色，与新节点M_8共同协商出新的组密钥K'。如图 2 所示，M_1将用K加密K'组播报文通知$M_2,\cdots,M_7$。若要删除恶意节点M_1，则M_2将取代M_1作为该子树至该组的新的Leader，它将提供新的密钥k'_{12}，并与M_3、M_6协商出新的组密钥K'。

该方案的主要缺点在于缺乏集中控制机制，没有任何一个成员节点保持完整的密钥拓扑结构，难以确保每个成员节点在网络拓扑发生变化时维持信息的一致性。

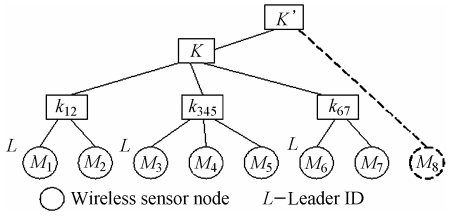

图 2　分布式组密钥管理的拓扑结构

Fig.2 Topologic structure of the distributing group key management

3　层簇式密钥管理方案的设计

3.1　层簇式密钥管理的拓扑结构

针对于组密钥管理的安全需求和性能需求，综合集中式和分布式组密钥管理方案的优点，提出了一种新的适用于无线传感器网络的层簇式密钥管理方案，如图 3 所示。

由图 3 可知，L_0层为最底层，包含了所有的传感器节点，这些节点按照簇生成协议(包括节点类型、通信半径及多跳次数)划分为不同的簇，例如M_1，M_2，M_3，M_4四个节点为一簇，而这些簇就构成了组。每个簇都有一个Leader，可以约定子树的最左叶子节点为Leader。基于L_0层，每个簇的Leader

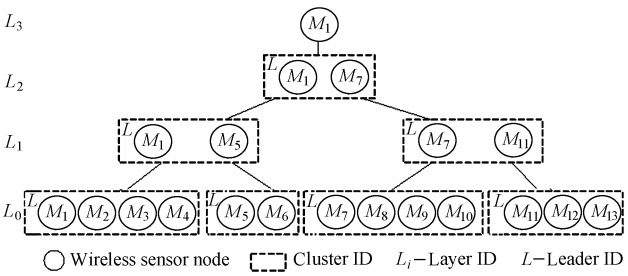

图 3　层簇式密钥管理方案的拓扑结构

Fig.3 Topologic structure of lay-cluster key management

又形成了L_1层，同样执行簇生成协议划分为不同的簇。以此往上类推，直至最高层只剩下一个节点。每一层均存在一个仅由层成员节点共享的层密钥实现层内通信，每一簇也均存在一个仅由簇成员节点共享的簇密钥实现簇内通信，每个簇的Leader都与该簇的其他成员建立了点对点的安全通道。

3.2 密钥生成与密钥更新

(1)簇密钥的生成　每个簇的Leader负责与该簇的成员节点协商产生簇密钥。以图 3 为例，在L_0层，M_1，M_2，M_3，M_4分别提供子密钥 $k_1=g^{s_1}$，$k_2=g^{s_2}$，$k_3=g^{s_3}$ 和 $k_4=g^{s_4}$，其中 g 为 p 阶乘法循环群 Z_p^* 的生成元。M_1 将计算 $ck_1=g^{s_1s_2s_3s_4}$ 作为该簇的簇密钥，同理可得 $ck_2=g^{s_5s_6}$，$ck_3=g^{s_7s_8s_9s_{10}}$ 和 $ck_4=g^{s_{11}s_{12}s_{13}}$。

(2)层密钥的生成　层密钥可由该层所有簇的Leader协商产生，也可以由密钥服务器负责产生，可根据无线传感器网络的组网及配置情况而定。仍以图 3 为例，在L_0层，一种最简单的算法是根据簇密钥 $ck_1,\cdots,ck_4$ 计算层密钥 $L_0K=g^{s_1s_2s_3\cdots s_{12}s_{13}}$。为了进一步增加安全性，在生成层密钥时可采用盲因子。如此一来，密钥服务器或Leader将层密钥广播给层成员节点时，恶意攻击者将难以窃取到真正的层密钥。例如，根据某一单向函数 $h(x)$，M_1节点可随机选择盲因子 $b_1=h(s_1)$，并计算 $ck_1b_1=g^{b_1s_2s_3s_4}$；M_2节点可随机选择盲因子 $b_2=h(s_2)$ 计算 $ck_2b_2=g^{s_1b_2s_3s_4}$；以此类推，$ck_4b_{12}=g^{s_{11}b_{12}s_{13}}$，$ck_4b_{13}=g^{s_{11}s_{12}b_{13}}$，利用插入盲因子后的密钥，各成员节点仍然最终能得到 $L_0K=g^{s_1s_2s_3\cdots s_{12}s_{13}}$。

(3)组密钥的生成　由于所有节点均属于L_0层，因此L_0层的层密钥将作为该组的组密钥。

(4)密钥的更新　当有新的节点加入时，根据簇生成协议和密钥生成协议，新成员节点将提供子密钥，并由该簇的Leader更新簇密钥；层L_i的层密钥更新是由密钥服务器或所有簇的Leader来完成，利用L_{i+1}层的层密钥加密，将新的层密钥组播发送给L_i层所有簇的Leader，然后由这些Leader利用各自在L_i层的簇密钥更新给其它成员节点，这样便能有效保证后向私密性。

当要删除某个恶意节点时，在图3中以删除M_7节点为例，M_7节点所在的最高层为L_2层，为了满足前向私密性的需求，则需要更新L_0—L_2层的层密钥以及M_7节点在各层所在簇的簇密钥。在L_0层，由M_8节点担任M_7节点所在簇的新Leader，重新协商出该簇的簇密钥；同理，M_8节点作为L_1，L_2层新簇的Leader，均需要更新所在簇的簇密钥；更新完簇密钥之后，再由L_2层开始，由上至下更新层密钥。

为了进一步改善密钥更新的性能，密钥服务器或每一层的Leader可事先约定一个密钥更新函数 $K'=f(K,r)$，其中 r 为随机数。当M_7节点被删除时，M_8节点作为新的Leader，随机选择 r'，更新簇密钥 $ck_3'=f(ck_3,r')$；同理，密钥服务器也可根据新的簇密钥来更新层密钥。该方法还能减少带宽占用和网络流量。

(5) 组内节点间的认证　由于该组所有的成员节点共享组密钥(即L_0层的层密钥)，易于实现节点间的认证。更规范的做法是在无线传感器网络的配置阶段为每一个节点提供唯一的ID标识，通过hash函数和共享组密钥进行专门的身份认证。

3.3 基于(t, n)门限方案的组间通信与认证

一个典型的无线传感器网络由传感器节点、接收/发送器(Sink)，Internet或其它任务管理节点构成[1]。由于传感器节点的数目庞多，难以实现一组管理，通常采用多组管理的形式。如图 4 所示，组内通信采用 3.2 节的层簇式组密钥管理机制，而组间可借助于公钥密码体制实现安全链接和认证。

其基本思想为：假设某一区域将无线传感器节点划分为 t 个组，基于传统公钥密码体制，该区域的 Sink 节点生成密钥对{PK，SK }，其中 PK 为公开密钥，SK 为私有密钥。利用密钥分割算法，Sink 节点将为每一组生成子密钥对{ pk_i，sk_i }(i = 1, 2,⋯, t)，其中 pk_i 为第 i 组的公开子密钥，sk_i 为秘密子密钥。

组间的通信与认证过程可描述如下：假设图 4 中的组 1 欲向组 2 发送报文 m，组 1 先用组 2 的公开子密钥 pk_2 加密 m 得 $[m]_{\mathrm{pk}_2}$，再利用自己的子密钥 sk_1 对密文(或其摘要)签名得 $\mathrm{Sig}\left([m]_{\mathrm{pk}_2}\right)_{\mathrm{sk}_1}$；组 2 收到 $\mathrm{Sig}\left([m]_{\mathrm{pk}_2}\right)_{\mathrm{sk}_1}$ 后，先用组 1 的公开子密钥 pk_1 验证签名是否有效，再用其子密钥 sk_2 解密 $[m]_{\mathrm{pk}_2}$ 得到明文 m。

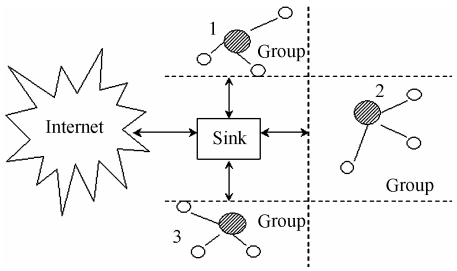

图 4 无线传感器网络的多组管理模式

Fig.4 Multi-groups management mode of wireless sensor networks

以上方案有两个缺陷：(1) 可扩展性差，当该区域新增大量节点并划分为新组时，密钥必须重新分割；(2) 采用传统公钥密码体制，计算复杂度较大。基于(t, n)门限方案的线性插值算法能较好地解决这两个问题，具体过程描述如下：

(1)Sink 节点选择整数 $n(n>2t)$，并选择大素数 p 与 q 且满足等式$(p-1) \bmod q = 0$；

(2)Sink 节点根据 t 值，随机选择一组整数{ a_i, i = 0, 1, 2,⋯, t–1}，并生成线性多项式 $f(x)=\sum_{i=0}^{t-1}a_ix^i \pmod q$，其中 $a_i\in[1,q-1]$；

(3)Sink 节点随机选择整数 c，计算 $\delta=c^{(p-1)/q} \pmod p$>1，生成的 δ 为 GF(p)中阶为 q 的生成元；

(4)Sink 节点广播{p, q, δ }给每一组；

(5)Sink 节点再为每一组选择整数 x_i (i = 0, 1, 2,⋯, n–1)，

生成其各自的子密钥 $f(x_i) \pmod q$ 和公开子密钥 $y_i = \delta^{f(x_i)} \pmod p$。

(6)当对消息 m 进行认证时，源节点可利用自己的子密钥 $f(x_i) \pmod q$以及某一随机整数来产生对消息 m 的签名，而目的节点则可利用其公开子密钥 y_i 对 m 进行合法性认证。

如此一来，即便网络规模由原先的 t 组变为 $3t/2$ 组，也不需要重新进行密钥分割，线性多项式的计算也降低了复杂度。

如果需要进一步降低通信复杂度，可采用基于(t, n)门限方案和对称密码体制的简单 hash 函数密钥链来实现组间认证。Sink 节点生成 $n(n>2t)$单位长度的 hash 密钥链，每一组只需要保存链尾最后一个密钥即可，t 组则共需要消耗 t 长度的密钥。簇与簇之间建立认证关系时，只需要用 t 值和链尾的密钥 K 即可实现认证；一旦 K 泄漏或者过了有效期，则利用 hash 函数计算 K'=hash(t , K)。依此类推，但一般要求网络时钟的同步，且该方案的安全性不及上述方案。

3.4 安全性和有效性分析

(1)如前所述，依据无线传感器网络组密钥管理的安全需求，层簇式的密钥管理方案完全满足前向私密性和后向私密性，密钥更新机制足以抵抗同谋破解的安全隐患，而共享组密钥则易于实现组内节点间的认证；

(2)层簇式的逻辑结构分散了密钥的存储量和计算量，既避免了集中式组密钥管理组控制节点的存储和计算瓶颈问题，又克服了分布式组密钥管理缺乏集中控制的缺陷；

(3)组间的通信与认证依赖于(t, n)门限方案的密钥分割算法，n 值可根据区域容量来设定，增加了灵活性和可扩展性；

(4)密钥分割算法可采用线性插值或 hash 函数链来实现，可根据所需的安全级别和资源情况来进行选择；

(5)簇生成协议保证了分层分组的有效性，使得密钥管理的拓扑结构更加合理与高效，有利于平衡网络的通信流量和传输时延；

(6)层簇式密钥管理方案的节点逻辑结构、密钥更新路径均能较好地适应动态变化的网络环境，具有更强的可扩展性和可靠性。

4　结束语

无线传感器网络以 Ad hoc 方式自组，但其自身的特点和局限决定了其新的安全需求。与应用于 Ad hoc 网络的传统密钥管理方案以及密钥预分配方案相比，组密钥管理方案能较好地解决无线传感器网络的安全问题。本文提出的新的层簇式组密钥管理方案解决了两种基本方案的缺陷，而基于(t, n)门限方案的密钥分割算法则实现了组间的通信和认证，保证安全性的同时改善了执行效能。

由于无线传感器节点计算、存储及通信能力的限制，且为了进一步适应网络拓扑结构的动态变化，节点发现协议和高效的加解密算法仍是下一步研究工作的重点。

参 考 文 献

[1] Akyildiz L F, Weilian S, Sankarasubramaniam Y, Cayirci E. A survey on sensor networks [J]. *IEEE Communications Magazine*, 2002, 40(8): 102–114.

[2] Sourabi K, Gao J, Allawadni V, Pottie G J. Protocols for self-organization of a wireless sensor network [J]. *IEEE Personal Communications*, 2000, 7(5): 16–27.

[3] 李建中, 李金宝, 石胜飞. 传感器网络及其数据管理的问题、概念与进展[J]. 软件学报, 2003, 14(10): 1718–1727.

[4] Eschenauer L, Gligor V D. A key-management scheme for sensor networks [A]. The 9th ACM Conference on Computer and Communication Security (CCS) [C]. Washington DC, USA, Nov. 2002: 41–47.

[5] Chen H, Perrig A, Song D. Random key pre-distribution schemes for sensor networks [A]. IEEE Symposium on Security and Privacy [C]. Berkeley, California, May 2003: 285–289.

[6] 李　晖, 彭志威, 陈克非. 无线传感器网络及其安全问题[J]. 中兴通讯技术, 2004,10(增刊): 30–35.

[7] Tanaka S, Sato F. A key distribution and rekeying framework with totally ordered multicast protocols [A]. In Proceedings of the 15th International Conference on Information Networking [C]. Beppu City, Jun. 2001: 831–838.

[8] 陈　丹, 郑增威, 李际军. 无线传感器网络研究综述[J]. 计算机测量与控制, 2004, 12(8): 701–705.

李　琳：　男，1982 年生，硕士生，研究方向为计算机网络、计算机软件在通信中的应用和信息安全.

王汝传：　男，1943 年生，教授，博士生导师, 主要研究方向为计算机软件、计算机网络和网格、信息安全、移动代理和虚拟现实技术等.

姜　波：　男，1982 年生，硕士生，研究方向为计算机网络、计算机软件在通信中的应用和信息安全.

黄海平：　男，1981 年生，硕士生，助教，研究方向为计算机网络、计算机软件在通信中的应用和信息安全.