基于矩阵空间的分级密钥管理

张彩霞[1,2] 程良伦[1] 王向东[2]
(广东工业大学自动化学院 广州 510006)[1] (佛山科学技术学院自动化系 佛山 528000)[2]

摘 要 为提高无线传感器网络存储资源的利用率,同时增强网络的安全性,提出一种基于矩阵空间的分级密钥预分配管理方案。该方案采用 LU 矩阵子空间对节点逐次进行密钥分配,并在节点对密钥建立后,采用分级矩阵信息删除机制减少部分矩阵信息。实验仿真表明,在保证网络一定连通率的同时,该方案采用的分级矩阵信息删除机制不仅提升了节点的存储效率,而且逐步增强了无线传感器网络的安全性,网络节点最终能实现100%抗捕获攻击能力。

关键词 无线传感器网络,密钥管理,矩阵空间,删除机制
中图法分类号 TP393 **文献标识码** A

Hierarchical Key Management Based on Matrix Space

ZHANG Cai-xia[1,2] CHENG Liang-lun[1] WANG Xiang-dong[2]
(The Faculty of Automation, Guangdong University of Technology, Guangzhou 510006, China)[1]
(Department of Automation, Foshan University, Foshan 528000, China)[2]

Abstract In order to improve the efficiency of the storage resource of wireless sensor networks, enhance security at the same time, this paper proposed a hierarchical key management based on matrix space. This scheme uses sub-space of LU matrix for successive key predistribution and uses removal mechanism to reduce some of the information of matrix of nodes after key establishment. Figures of simulation show that the proposed scheme provides better storage efficiency and better security through the removal mechanism. The security of network can up to 100% in the end.

Keywords Wireless sensor network, Key management, Matrix space, Removal mechanism

无线传感器网络的特殊应用环境通常要求其具有较强的自我安全保护能力,而资源的有限性对无线传感器网络提出了更高的安全要求。近年来,许多研究者对此进行了深入的研究和讨论[1-4],研究主要集中于在实现高安全性的同时如何保证网络的高连通率和低开销。

密钥预分配方案可以在未知无线传感器网络部署知识的前提下实施,具有较强的应用能力。文献[5]通过引入随机图论,首先提出一种可用于无线传感器网络的随机密钥与分配方案,该协议实现简单且存储需求不高,但不能有效地抵抗节点的物理捕获攻击。在此基础上,提出了 q-composite 协议,它在一定程度上提高了节点的抗俘获攻击能力。文献[6]提出单密钥空间密钥预分配方案,以保证网络任意两个节点都能够直接建立配对密钥,在受损节点不超过阈值时,不会泄漏任何机密信息,但其资源开销占有极大。文献[7]对其进行了扩展,但是仍旧不能很好地平衡安全与资源开销的关系。文献[8]在此方面进行了深入的研究,在能源开销与安全性和连通性的平衡方面取得了建设性的成果。但是,如何进一步实现三者的平衡,仍是目前无线传感器网络密钥管理研究的重点和难点。

基于以上考虑,本文提出一种基于矩阵空间的分级密钥预分配管理方案。该方案采用分级密钥 LU 矩阵子空间对节点逐次进行密钥分配,并在节点对密钥建立后,采用分级密钥删除机制逐步删除矩阵信息,在保证网络一定连通率的同时,不仅提升了节点的存储效率,而且不断增强了无线传感器网络的安全性,网络节点最终能实现100%抗捕获攻击能力。

1 LU 矩阵算法及分析

2005年,文献[9]提出了一种基于 LU 矩阵的无线传感器网络密钥预分配方案,该方案首先将对称矩阵分解成相应的上三角矩阵 L 和下三角矩阵 U,而后将 L 矩阵的一行和 U 矩阵的一列信息分配给节点,节点交换 U 矩阵的列信息并与相应的行信息相乘形成节点通信的对密钥。该方案可以保证网络100%的连通性。但是,根据文献[10]分析,由于 U 矩阵几乎是完全公开的,攻击者可以通过获取 U 矩阵信息和部分的 L 矩阵信息来获取网络的任意对密钥,因此网络存在极大的安全隐患。同时,矩阵随着系统规模的扩大而扩大,节点需要耗费大量的传输能量来建立对密钥信息。

2 基于矩阵空间的分级密钥管理

在实际的无线传感器网络中,传感器节点只需要以较高的概率与相邻节点之间保持较高的连通即可,不能直接通信的节点可以通过中间节点进行过渡通信。因此,采取分级密

到稿日期:2011-10-03 返修日期:2011-11-24 本文受国家自然科学基金(60673132),佛山市科技发展专项资金项目(FZ2010030),广东省重大科技专项项目(2009A080207008),佛山市科技发展专项资金项目(FZ2009032),广东省自然科学基金(9152800001000026)资助。
张彩霞(1976—),女,博士生,主要研究方向为信息技术安全、传感器网络化系统,E-mail:zh_caixia@163.com;程良伦(1965—),男,博士,教授,博士生导师,主要研究方向为智能与网络化系统等;王向东(1962—),男,教授,主要研究方向为数学应用。

钥矩阵空间的方法，在牺牲网络部分连通性的基础上，降低了节点间建立密钥时的能量消耗，同时增强了系统的安全性。

2.1 网络模型

假定节点通过飞机等设备随机抛撒在部署区域内，部署后的节点是静止和同构的。这是无线传感器网络一般的应用模型。现实世界中，攻击者常具有很强的节点破坏力，能够捕获节点并获取节点信息，但节点被捕获导致密钥泄漏有一个时间下限[11]，在该时间限制内，节点中的数据是绝对安全的。

2.2 分级密钥矩阵空间预分配

定义 1(α、β密钥矩阵空间) 由 S 个(L_i,U_i)矩阵对元素组成的矩阵空间(L_i 为下三角矩阵，U_i 为上三角矩阵，L_i，U_i 的乘积为对称矩阵)称为 α 密钥矩阵空间；相应地，由 S 个元素组成的矩阵空间称为 β 密钥矩阵空间。

定义 2(分级密钥矩阵空间) 无线传感器网络由于节点能源有限或者易受到物理捕获，因此需要不断地部署新的节点补充到原网络中。第一次部署时所用的密钥矩阵空间称为一级密钥矩阵空间，第二次部署时所用的密钥矩阵空间称为二级密钥矩阵空间，依次类推。在本方案中，由 α_1，β_1 组成一级密钥矩阵空间，由 β_1，α_2 组成二级密钥矩阵空间，依次类推。

步骤 1 在网络部署之前，首先产生一个大的密钥池。

步骤 2 生成 α，β 密钥矩阵空间，随机从该密钥池中选取密钥构造 m_1 个下三角形矩阵 L_i，按照文献[9]的方法取得相应的上三角形矩阵 U_i；随机从 m_1 个(L_i,U_i)矩阵对元素中抽取 S 个元素组成 α_1 密钥矩阵空间，而后从剩下的元素中抽取 S 个元素组成 α_2 密钥矩阵空间，依次类推。同理，随机从密钥池中选取密钥构造 m_2 个(L_i,U_i)矩阵对元素，而后在 m_2 个元素中抽取 S 个元素组成 β_1 密钥矩阵空间，依次类推，组成 β_2，β_3…矩阵空间。

步骤 3 生成分级密钥矩阵空间，从已生成的 α，β 密钥矩阵空间中抽取 α_1，β_1 组成一级密钥矩阵空间，β_1，α_2 组成二级密钥矩阵空间，α_2，β_2 组成三级密钥矩阵空间，依次类推，如图 1 所示。

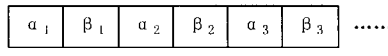

图 1 i 级密钥矩阵空间部署模型

步骤 4 无线传感器网络的网络节点首次被部署之前，系统从一级密钥矩阵空间 α_1，β_1 中随机选取 t 个元素，然后将每个元素的 L_i 的任意一行与 U_i 对应的列信息分配给节点，每个节点存储 t 个行、列信息及相应的矩阵 ID。元素的任意一行列信息只能被分配一次，保证节点间不会生成重复的对密钥信息。

步骤 5 无线传感器网络节点由于能量有限或易受到捕获攻击，在完成所有监测任务的过程中，需要不断地补充节点。则第二次节点部署之前，节点从二级密钥空间选取元素，方法同步骤 4。如果进行 n 次部署，则上述过程重复 n 次。

上述矩阵空间的实现过程如图 2 所示。

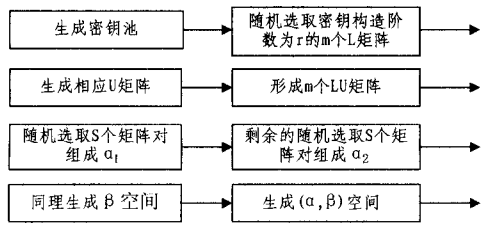

图 2 矩阵空间的实现过程结构图

2.3 密钥的建立及信息删除

预存完密钥矩阵信息的节点被抛撒到部署区域内，节点向周围节点广播自己存储的矩阵的 ID 值，若发现与对方节点具有相同的 ID，则可以直接建立对密钥。节点相互发送 ID 对应的列信息给对方，而后与自己相应的行信息做向量乘法，最终形成两节点通信的公共密钥。

若两邻节点不具备共同的 ID 值，则将中间节点作为中介进行间接密钥建立。即两节点分别广播自己的矩阵 ID 值，同时具有两节点 ID 值的节点即可作为它们的中间过渡节点。

节点在首次部署完成后，随即删除一级密钥矩阵空间的 α 空间信息；第二次部署完成后删除二级密钥矩阵空间的 β 空间信息，以此类推。n 次部署完成后，节点只保留通信密钥，所有矩阵空间的行列信息都被删除，节点不仅可以释放有限的存储空间，而且可以有效地保护节点通信密钥，提高网络的安全性。

3 算法分析与实验仿真

3.1 连通性

根据网络节点的密钥预生成过程可知，两节点之间要建立对密钥，必须拥有同一个 LU 密钥矩阵对的 ID。本文的方案节点在首次部署时，从一级密钥矩阵空间中选取 t 个行列信息，此时网络的连通性为：

$$P_{local1}=1-\frac{(1-\frac{t}{2S})^{4S-2t+1}}{(1-\frac{2t}{2S})^{2S-2t+\frac{1}{2}}} \tag{1}$$

式中，S 表示 α 或 β 中的矩阵的 ID 数，t 为节点选取的矩阵的 ID 数量。

当第二批节点从二级密钥矩阵空间选取信息并部署到网络中时，因为二级密钥矩阵空间与一级密钥矩阵空间共享 β_1 矩阵空间，所以此时的节点不仅相互之间建立通信密钥，而且与一级密钥矩阵空间选取信息的节点也建立通信密钥。此时整个部署节点内部的网络连通率满足：

$$P_{local2}=1-\frac{\sum_{i=0}^{t}C_S^{t-i}C_S^iC_{2S}^{t-i}}{C_{2S}^tC_{2S}^t} \tag{2}$$

第三批节点从三级密钥矩阵空间选取信息并部署到网络中且建立节点间的相互通信密钥时，可以同时与二级密钥矩阵空间中的节点建立通信密钥，此时二、三级密钥矩阵空间选取信息的节点的连通性满足式(2)。图 3 为 P_{local2} 与 E-G 方案两节点共享至少一个矩阵行列式(密钥)的概率随节点矩阵行列式环(密钥环)变化的曲线图(v 为 LU 矩阵的阶数)。

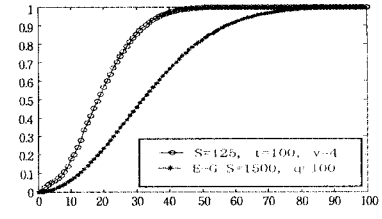

图 3 安全连通性对比

从图 3 仿真分析可以看出，在占有相同节点资源的条件下，本文方案与 E-G 方案相比，提高了网络安全连通概率。这主要是由于本文方案采用了 LU 密钥矩阵空间的方法，节点从密钥矩阵空间选取信息，增加了节点间公共信息的概率。

3.2 安全分析

本文方案在安全性方面，考虑了攻击者在进行节点捕获攻击并获取捕获节点的密钥矩阵信息后，网络中未受损节点之间的安全通信受到的影响程度。

假设在某一时刻，攻击者捕获 x 个节点并成功获取它们的密钥矩阵信息，而后攻击者对网络中未受损的任意两节点的安全通信进行监听。此时，攻击者必须知道两节点间的共享密钥矩阵信息，即共享的密钥矩阵的行列信息。根据 2.2 节可知，这些信息的一部分或者全部可能已经被删除，在这种情况下，攻击者则无法监听未受损节点间的安全通信。现假设受损的节点来自于第 i 级密钥矩阵空间，由于网络节点含有第 $i-2$ 级密钥矩阵空间的信息已全部删除，且第 $i-1$ 级密钥矩阵空间的 α 或 β 子矩阵信息节点也将其删除，因此，节点中仅保留了第 i 级密钥矩阵空间的信息，所以此时仅考虑网络中第 i 级密钥矩阵空间的节点被俘获后的、未受损节点的安全通信，即局部剩余网络受损概率。

受损节点拥有第 i 级密钥矩阵空间中的某个矩阵行列 ID 信息的概率为 $p_R=\frac{t}{2S}$。由于矩阵子空间的元素为矩阵，其阈值为 v（v 表示矩阵的阶数），因此被俘获的行列信息必须超过其阈值时，才有可能进一步泄漏其行列信息。若存在来自于第 i 级密钥矩阵空间的 x 个受损节点，则仅对第 i 级密钥矩阵空间而言，局部剩余网络的任意两个未被捕获节点间的共享密钥为 K 泄漏的概率为：

$$P_{local}=\sum_{i=v+1}^{x}\binom{x}{i}\left(\frac{t}{|2S|}\right)^{i}\left(1-\frac{t}{|2S|}\right)^{x-i}$$

式中，v 为 LU 矩阵的阶数，t 表示每个节点中存储的不同的 LU 矩阵的行列数（即不同矩阵的 ID 数），$|2S|$ 表示 i 级密钥矩阵空间元素的个数，$\frac{t}{|2S|}$ 表示每个节点可能携带某个矩阵对一个行列信息的概率。

图 4 分析了第 i 级密钥矩阵空间节点部署后的局部剩余网络受损概率。从图 4 可以看出，本方案由于采用了 LU 矩阵对，剩余网络被俘具有一定的阈值，该阈值随着矩阵阶数的增加而增加。$v=3$ 时的阈值大约为 80 左右，当 v 增加到 8 时，阈值增加到 210 左右，增加了近 3 倍。增加矩阵的阶数可以提高网络安全性，但同时会增加存储和传输的能量消耗，所以需要根据具体情况来选择合适的值。

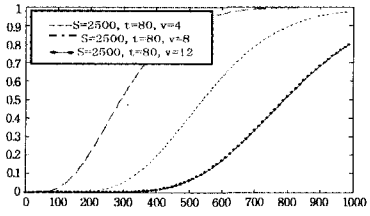

图 4 局部剩余网络被俘概率

对于整个传感器网络而言，除了讨论局部剩余网络受损概率外，还需要了解全局系统的安全性能。根据前文的网络节点部署方案可知，在部署到第 i 级密钥矩阵空间时，网络中节点所存储的前面第 $i-2$ 级密钥矩阵信息已经全部删除，即使节点被俘，其也不会泄漏任何信息。假设网络在整个生命周期一共进行了 i 次部署，需要用第 i 级密钥矩阵空间的信息，则随着网络部署的进行，节点所包含的、未被删除的矩阵空间信息占整个部署周期的比例满足 $y=\frac{2}{i+1}$，即存在局部网络受损的概率（见图 4）。随着部署的进行，网络节点存在的矩阵信息占整个网络的比例越来越小，当完成最后一次部署时，第 i 级密钥矩阵空间的信息也被节点删除，节点此时只拥有与邻居节点的通信密钥。

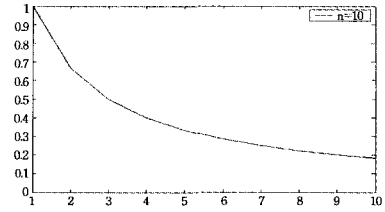

图 5 未删除密钥矩阵空间信息占整个部署矩阵空间的比例

由图 5 可以看出，随着节点部署次数的增加，已部署的节点保存的矩阵空间的信息所占比例越来越小，即已部署节点的安全性逐步增强，完成最后一次部署后网络的安全达到 100%（图中为 10 次部署的状态）。

3.3 存储与能量消耗分析

本文方案的存储消耗与文献[9]的方案相似，其主要消耗集中在计算共享密钥的矩阵行列信息的存储上。文献[9]中，整个网络采用一个大的 LU 矩阵，整个网络节点存储密钥数为 $2n^2$（n 为网络需部署的最大节点数）；本文方案节点存储子矩阵空间逐级删除矩阵空间信息，节点部署时，仅保存与邻节点的通信密钥。

下面比较两种算法在网络节点数量呈线性增长时，整个网络完成部署后存储的密钥数量的增长趋势（见图 6）。

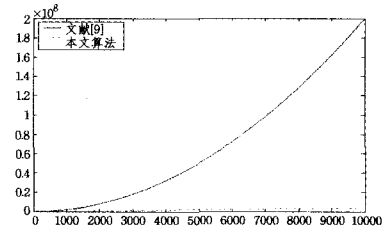

图 6 网络节点数量与总的存储密钥关系

图 6 表明，随着网络规模的逐步增大，文献[9]的整个网络的存储消耗迅速增大；本文算法的删除机制使得节点释放出大量的存储空间，存储效率达到最大化。

本文方案的计算能量主要集中消耗在密钥建立时矩阵行列的相乘，是一次性的，比文献[9]的矩阵阶数小得多，计算消耗相对比较小，对于能量有效的传感器节点是可以接受的。

3.4 整体性能分析

假设网络需要部署 n 个节点，则文献[9]需要形成阶数为 n 的 LU 矩阵；本文参照图 3 的安全连通性分析，在保证网络连通性的同时，每个节点预存储 $t=100$ 个阶数为 $v=4$ 的 LU 子矩阵。本文方案的连通性与 α 或 β 中的元素数及节点选取的元素数量相关。本文方案与文献[9]的性能比较详见表 1。

表 1 本文方案与文献[9]性能比较

	节点之间的通信量	整个网络的存储量	网络的抗俘获攻击力	网络的连通性
文献[9]	n	$2*n^2$	L 容易被还原	100%
本文方案	V=4	100 * n	100%	小于 100%

由表 1 可知，在牺牲部分连通性的情况下，本文节省的通信量与存储消耗随着节点数目的增多而变大，更适合于大规模的无线传感器网络。

结束语 本文着重研究了一种高效的无线传感器网络的

密钥预分配管理方案，其核心思想是针对网络能量有限及节点所处环境的不安全性，提出基于分级矩阵空间的密钥预分配和信息逐步删除机制。仿真结果表明，其较好地满足了在节点资源有限的情况下网络安全性与能量消耗之间的关系，可以较好地应用于大规模的无线传感器网络。

参 考 文 献

[1] Yuan Ting, Ma Jian-qing, Zhong Yi-ping, et al. Key Management Scheme Using Time-Based Deployment for Wireless Sensor Networks[J]. Journal of Software, 2010, 1 (3): 516- 527

[2] Xu Qiao-juan, Zheng Yan-fe, Chen Ke-fe, et al. Random pairwise key pre-distribution scheme based on LU matrix space[J]. Journal of Computer Applications, 2009, 29(7): 1816-1819

[3] Ren Heng, Sun Xing-ming, Ruan Zhi-qiang, et al. An Efficient Scheme Against Node Capture Attacks using Secure Pairwise Key for Sensor Networks[J]. Information Technology Journal, 2011, 10(1): 71-79

[4] 余旺科，马文平，王淑华. 基于部署信息的无线传感器网络密钥预分配[J]. 华中科技大学学报：自然科学版，2010，38(11)：51-54

[5] Eschenauer L, Gligor V D. A Key Management Scheme for Distributed Sensor Networks[C]// 9th ACM Conference on Computer and Communications Security. New York, 2002: 41-47

[6] Blom R. An optimal class of symmetric key generation systems [C]// Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Paris, 1984: 335-338

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

[8] Dai Hang-yang, Xu Hong-bing. Key predistribution approach in wireless sensor networks using LU matrix[J]. IEEE Sensors Journal, 2010, 10(8): 1399-1409

[9] Choi S J, Youn H Y. An Efficient Key Predistribution Scheme for Secure Distributed Sensor Network[C]// 2005 IFIP International Conference on Embedded and Ubiquitous Computing. Nagasak, iSpringe, 2005: 1088-1097

[10] Zhu B, Zheng Y, Chen K, et al. Cryptanalysis of LU decomposition-based key pre-distribution scheme for wireless sensor networks[DB/OL]. http://eprint.iacr.org/2008/411.pdf

[11] Deng J, Hartung C, Han R, et al. A practical study of transitory master key establishment for wireless sensor networks[C]// Proceedings of the 1st IEEE/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks. 2005: 289-299

(上接第 80 页)

表 3 算法间能量消耗以及广播时间比较表

节点数目	能量消耗			广播时间		
	经典	高效算法	提高(%)	经典	高效	提高(%)
100	285.08	265.57	6.85	0.018833	0.017974	4.56
200	560.41	536.47	4.27	0.01962	0.018542	5.49
300	883.14	830.53	5.96	0.018978	0.017807	6.17
400	1237.51	1134.48	8.33	0.020301	0.018589	8.43
500	1561.32	1433.71	8.17	0.019999	0.01846	7.7
600	1929.79	1708.46	11.47	0.020866	0.019222	7.88
700	2275.85	2126.77	6.55	0.020853	0.019529	6.35
800	2671.87	2391.72	10.49	2.10962	1.97193	6.53
900	3040.6	2753.34	9.45	2.14635	1.97706	7.89
1000	3473.21	305.79	12.02	0.022211	0.020182	9.14

结束语 本文首先就多点中继算法与结合覆盖理论的联系进行了论述，然后采用结合覆盖理论提出了一种高效的多点中继算法。通过实验表明，泛洪传播方式下能量节约了6%到12%，传播时间根据节点密度不同，节约了4%到9%。所有的实验结果表明，节点密度越高，本算法执行效率就越高。此外，在真实环境中测试改进后的算法，获取的结果也非常理想。

参 考 文 献

[1] Tseng Y-C, Ni S-Y, Chen Y-S, et al. The broadcast storm problem in a mobile ad hoc network[J]. Wireless Network, 2002, 8 (2/3): 153-167

[2] Qayyum A, Viennot L, Laouiti A. Multipoint relaying: an efficient technique for flooding in mobile wireless networks[R]. Institu National de Recherche en Informatique et en Automatique. 2007

[3] Gonzalez T F. Handbook of approximation algorithms and metaheuristics[M]. London/Boca Raton: Chapman and Hall/CRC Press, 2007

[4] Chavatal V. A greedy heuristic for the set-covering problem [J]. Math operating Research, 1979, 4(3): 233-235

[5] Guturu P, Dantu R. An impatient evolutionary algorithm with probabilistic tabu search for unified solution of some NP-hard problems in graph and set theory via clique finding[J]. IEEE Transaction system Man Cybern B, 2008, 38(3): 645-666

[6] Chiang C C, Dai H K. On the minimum-cost set-covering problem[C]// Proceedings of the 2005 International Conference on Parallel and Distributed Processing Techniques and Applications, PDPTA'05. 2005, 3: 1199-1205

[7] Khan A Y, Rashid S, Iqbal A. Mobility vs predictive MPR selection for mobile ad hoc networks using OLSR[C]// Proceedings—IEEE 2005 International Conference on Emerging Technologies, ICET 2005. 2005: 52-57

[8] Chang Y-K, Ting Y-W, Wu S-C. Power-efficient and path-stable broadcasting scheme for wireless ad hoc networks[C]// Proceedings—21st International Conference on Advanced Information Networking and Applications Workshops/Symposia. AINAW'07. Vol 1, 2007: 707-712

[9] Yawut C, Paillassa B, Dhaou R. Mobility versus density metric for OLSR enhancement[C]// Lecture notes in computer science. Berlin: Springer, vol 4866, 2007: 2-17

[10] Nguyen D, Minet P. Analysis of MPR selection in the OLSR protocol[C]// Ainaw '07: Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops. Washington, DC, USA, IEEE Computer, Soc., Los Alamitos, 2007: 887-892

[11] Liang O, Sekercioglu Y A, Mani N. Gateway multipoint relaysan MPR-based broadcast algorithm for ad hoc networks[C]// 10th IEEE Singapore International Conference on Communication Systems, ICCS 2006. Nov. 2006: 1-6

[12] Johnson D S. Approximation algorithms for combinatorial problems[C]// STOC '73: Proceedings of the 5th Annual ACM Symposium on Theory of Computing. New York, USA, ACM, New York, 2003: 38-49

[13] 彭海英，蔚承英，唐红. 无线自组网分级结构的性能与可扩展性研究[J]. 重庆邮电大学学报：自然科学版，2007，19(2)：172-176