基于 HuffMHT 的自组织网络实体认证协议

周贤伟 郭继文
(北京科技大学信息工程学院 北京 100083)

摘 要：针对自组织网络节点能量消耗和存储有限的特点，该文提出一种适合于自组织网络的基于 HuffMHT 的实体认证方案。该方案利用 HuffMHT 的思想可获得有效的安全策略；并使用对称密钥算法和公钥加密算法相结合，有效地降低了认证时延，提高了网络生命期和安全性。此外，在自组织网络设定簇头和建立 HuffMHT 时，该文给出了功耗最小算法和引入 Christofides 算法，缩短节点之间发射信号的距离，有效地降低节点能耗，提高了网络生命期。

关键词：自组织网络；网络安全；实体认证；Huffman-Merkle 散列树
中图分类号：TP393.04 **文献标识码**： A **文章编号**：1009-5896(2010)04-0852-05
DOI: 10.3724/SP.J.1146.2009.00169

HuffMHT-Based Entity Authentication Scheme for Ad hoc Networks

Zhou Xian-wei Guo Ji-wen
(*School of Information Engineering*, *University Science and Technology of Beijing*, *Beijing* 100083, *China*)

Abstract: Ad hoc Networks is characteristic of limited energy and memory. A novel entity authentication scheme based on HuffMHT for Ad hoc Networks is proposed to solve such problems. This method using the concept of HuffMHT can obtain an effective safe strategy. At the same time, symmetrical key algorithm and public key algorithm are just combined to reduce the authentication delay effectively and increase the network lifetime and enhances the security of the networks. Moreover, when clustering head and HuffMHT is built up in the Ad hoc Networks, Power-consumption-least algorithm are designed and Christofides algorithm are used in this paper, respectively, distance which notes effectively transmit signal together are reduced, the power which notes consume is debased, the network lifetime is increased.

Key words: Ad hoc network; Network security; Entity authentication; Huffman Merkle Hush Tree (HuffMHT)

1 引言

移动自组织网络是有许多无线移动节点构成的不依赖于任何固定基础设施的没有严格的控制中心的临时性自治系统。由于它具有组网快速、高抗毁性和无固定基础设施的特点，逐渐成为无线网络研究的重点之一。然而，从网络结构的特点看，移动自组织网络面临着严重的安全威胁：容易受到窃听、假冒等攻击；网络中的节点可能会来自其它节点的自私攻击；网络拓扑结构也随之节点的加入而随之变化；算法和协议的执行需要多个节点的协作，这样给敌手提供了更多的机会。随着自组织网络越来越多应用到多个领域，其网络的安全性显得尤为重要。自组织网络结构的动态变化，即网络的自组织性，使得更容易放置恶意节点、敌手对其假冒攻击等[1]，因此对新加入网络的节点必须执行身份认证以保证网络的安全性。

目前研究者已提出了一些的基于自组织网络的实体认证方案：基于信任管理的认证机制[2−4]和基于公钥证书的认证机制[5,6]。基于信任机制的认证方案主要依据节点自己的经验来判断并维护网络的安全运行。由于节点的计算能力有限，基于公钥证书的认证机制不适合在低端设备进行认证。因此现有的认证方案并不能很好地满足特殊情况下的自组织网络。文献[7]给出了基于 Merkle 散列树的实体认证协议，其计算过程要执行一个完全的二叉树。然而实际的有效计算只与叶子节点有关系。

根据自组织网络网络动态变化，以及采用数字签名能量消耗较大和对称密钥安全性低的缺点，本文提出一种基于 HuffMHT[8](Huffman Merkle Hush Tree)的自组织网络的实体认证方案。该方案利用 HuffMHT 的结构特征可获得有效的安全性，并使用对称密钥算法和公钥加密算法相结合，有效地降低了认证时延[9]，提高了网络生命期[10]。另外，在自组织网络设定簇头和建立 HuffMHT 时，文中设计了功耗最小算法和引入 Christofides 算法[11]，缩短了节点之间发射信号的距离，提高网络生命周期。

2009-02-13 收到，2009-11-22 改回
国家自然科学基金(60773074)和国家 863 计划项目(2007AA01Z213)资助课题
通信作者：郭继文 guojiwen@yeah.net

2　网络结构

自组织是无严格中心的分布式网络，节点与节点之间的关系都是平等的，两个节点之间的通信大多是通过多跳的方式到达。通常网络内的节点依据区域、地理环境以及节点的位置分为多个逻辑簇[12,13]，各簇依据能量[14]选出一个节点为簇头。针对自组织网络的特点，通过构造移动的网络管理中心使得节点之间的通信以树状结构完成。簇头与网络管理中心通信，而各簇内成员与该簇的簇头进行信息交换。然而在一些实际情况中，例如把自组织网络应用于军事领域，每个单兵作为自组织网络中的一个节点，他们通信设备的性能应该是一致的。本文将根据节点之间的距离在每个簇中选择簇头，即功耗最小算法。假设簇内所有节点具有相同的能量初始值且簇内成员之间的信息通信都是一跳可达的，如图 1 所示。

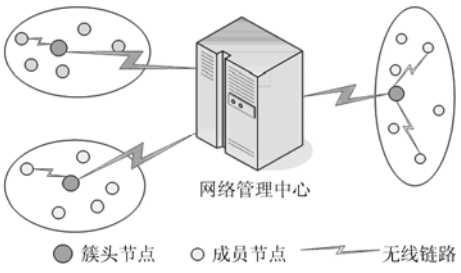

图 1 自组织网络集中式结构

设自组织网络中簇的个数为 n。每个簇 C_i 都有唯一的标识符 N_i；用 ID_i 表示簇 C_i 的簇头，其中 $i=1,2,\cdots,n$。用 K_{Ni} 和 $(\mathrm{PR}_{Ni},\mathrm{PU}_{Ni})$ 分别表示簇 C_i 的会话密钥和公钥对，这些密钥是在簇形成后由簇头产生。会话密钥与 HuffMHT 的更新频率一致并通过安全信道将其发送给本簇的每个成员。用 $(\mathrm{PU}_i,\mathrm{PR}_i)$ 表示网络管理中心的公钥对，每次认证完成都进行更新，其中 $i=1,2,\cdots,n$。规定簇 C_i 只知道它对应的一个公钥 PU_i，即簇与簇之间的通信必须由网络管理中心转发。V 表示网络管理中心维护的认证数据集，即 $V=\{(N_i,\ \mathrm{PR}_i,\ \mathrm{PU}_{Ni},\ s_j),\ i=1,2,\cdots,n\}$，其中 s_j 是簇 C_i 的认证密钥。网络管理中心是一种移动的管理平台，它将分布在地面上的节点进行逻辑分簇并管理和维护分簇后的网络状态。

3　认证协议设计

假设当前整个网络体系是安全的且所有成员是可信任的。在执行的认证过程中，网络管理中心起着很重要的作用，因此设网络管理中心是绝对安全的。

3.1 网络分簇

在执行节点认证过程之前，首先网络管理中心采用分簇算法对网络进行分簇，且簇内节点的个数为 $|C_i|$。然后依据节点之间的距离在每个簇中选择本簇的簇头，即功耗最小算法，该算法的时间复杂度为 $O(|C_i|^2)$。假设网络在分簇在过程中是安全的并且簇头的选择也由网络管理中心利用功耗最小算法来确定。功耗最小算法的具体步骤如表 1。

表 1

名称	目标与步骤
功耗最小算法	输入：所有节点之间的距离 输出：找到该簇的簇头，使得簇头给本簇其它成员广播消息时需要的功耗最小 第 1 步：用 d_{jk} 表示簇 C_i 中第 j 个节点与第 k 个节点之间的距离，其中 $j,k=1,2,\cdots,C_i$； 第 2 步：计算 $\min\limits_{j}\max\limits_{k}\{d_{jk}^2\}$，其中 $j,k=1,2,\cdots,C_i$； 第 3 步：返回 j。

由于簇头节点能量消耗很大，所以选择一个簇头来完成多次认证过程是不现实的。那么可以多次执行功耗最小算法获得多个次最优簇头来轮换使用。若某个簇内的簇头失效，则可以从若干个备用簇头中选者并继续进行节点的重新认证过程。

当各簇产生簇头之后，先由簇头产生公钥对 $(\mathrm{PR}_{Ni},\mathrm{PU}_{Ni})$ 以及该簇的唯一标识符 N_i，然后通过安全信道将 PU_{Ni} 和 N_i 发送到网络管理中心，最后网络管理中心有了合法簇的唯一标识符，从而能有效地防止整个簇或恶意节点的冒充攻击。

3.2 HuffMUT构建

首先选取簇内的 m 个节点作为叶子节点，使得这些节点要均匀地分布在该区域内，则由 m 个认证节点和簇头构成一个完全图的顶点集，而每条边上的权值用各节点之间距离的平方来表示。那么这样的加权完全图满足三角不等式。运用 Christofides 算法可以得到该图的一个近似最小哈密顿圈，算法的近似比为 $1/2$，时间复杂度为 $O(m+1)^2$。接着从簇头开始依照哈密顿圈的顺序给这些节点分配相应的序号，记为 $A_0,A_1,A_2,\cdots,A_m$。认证节点 A_j 先利用伪随机生产器生成一个伪随机序列 s_j，通过散列计算 $m_j=h(s_j)\ (j=1,2,\cdots,m)$ 得到 m 个叶子密钥。最后发送给 A_{j+1}，由 A_{j+1} 计算 $m_{1-(j+1)}=h(m_{1-j}\mid m_{j+1})\ (j=1,2,\cdots,m-1)$，其中 $m_{1-1}=m_1$。

3.3 密钥分配

密钥分配在实体认证过程中占有重要地位，它能有效防止恶意节点的入侵攻击等。网络管理中心

从本簇的所有叶子节点中随机选取一个作为认证节点，不妨令 A_j 为当前这个簇的认证节点并对其它任何节点保密(包括它的认证密钥)。认证节点 A_j 和该簇簇头通过协商产生一共享密钥 K_{Si} 且只有该簇簇头和 A_j 知道，簇头 ID_i 利用 K_{Si} 加密 m_{1-m} 并发送给认证节点。此时 ID_i 给网络管理中心发送一个请求包 $E_{\mathrm{PR}_{Ni}}(\mathrm{Request}\,||\,N_i\,||\,\mathrm{Time}_i)$，当网络管理中心收到请求包后，通过 PU_{Ni} 解密并验证请求包的时间戳 Time_i 是否过期，其中 N_i 用来鉴定信息源。

网络管理中心首先产生一个公钥对 $(\mathrm{PR}_i, \mathrm{PU}_i)$，并向簇头 ID_i 发送响应信息包 $E_{\mathrm{PU}_{Ni}}(\mathrm{PU}_i\,||\,\mathrm{Request}\,||\,N_i\,||\,\mathrm{Time}_i)$。当接收信息包后，簇头用 PR_{Ni} 解密就得到网络管理中心分配给它的 PU_i。进一步通过共享密钥 K_{Si} 加密 PU_i 发送信息包 $E_{K_{Si}}(\mathrm{PU}_i\,||\,\mathrm{Time})$ 发给认证节点 A_j。当认证节点收到簇头发来的信息后，通过 K_{Si} 解密得到网络管理中心分配给本簇的 PU_i。然后用 PU_i 加密 s_j，将信息包 $E_{\mathrm{PU}_i}(s_j\,||\,N_i||\mathrm{Time}_i)$ 发送给网络管理中心。网络管理中心通过解密得到 C_i 的认证密钥 s_j。最后簇头产生一个会话密钥 K_{Ni} 并通过安全信道发送给本簇的每个成员，这样簇内成员之间就建立了一信任关系，其中 K_{Ni} 用于簇内节点之间进行相互转发信息。

3.4 认证开始

首先待认证节点 T 通过安全信道向网络管理中心发出请求包 $(\mathrm{Localization}_T, K_T)$，其中 K_T 是 T 的对称密钥，$\mathrm{Localization}_T$ 是 T 的位置信息。网络管理中心根据 $\mathrm{Localization}_T$ 得到相应的认证数据集 $(N_i^{'}, \mathrm{PR}_i, \mathrm{PU}_{Ni}, s_j^{'})$，并发送信息包 $E_{K_T}(N_i^{'}\,||\,\mathrm{PR}_i\,||\,\mathrm{PU}_i\,||\,s_j^{'})$ 给 T，其中 $N_i^{'}$ 和 $s_j^{'}$ 分别为簇 C_i 的唯一标识符和认证密钥。

T 产生一认证请求包，并向簇头 ID_i 发送信息包 $E_{\mathrm{PU}_{Ni}}(E_{\mathrm{PR}_i}(\mathrm{Request}\,||\,N_i^{'}\,||\,\mathrm{Time}_i))$。当 ID_i 收到认证请求包后，先用 PR_{Ni} 和 PU_i 进行解密，然后再验证时间戳是否过期以及标识符是否为 N_i。若通过验证，则 ID_i 先给 T 返回一信息包 $E_{\mathrm{PU}_i}(\mathrm{Response}\,||\,N_i\,||\,\mathrm{Time}_i)$，并向 A_j 发信息包 $E_{K_{Si}}(\mathrm{MAC}_{K_{Si}}(m_{1-m})\,||\,m_{1-m}\,||\,\mathrm{Time}_i)$；否则拒绝认证。

当 T 收到数据包后，先通过 PR_i 解密并验证时间戳是否过期，若消息合法则将消息包 $E_{s_j^{'}}(\mathrm{Request}\,||\,\mathrm{Time}_i)$ 发送给 A_j。A_j 先用 s_j 进行解密，然后验证时间戳是否过期。若通过验证则 A_j 向 ID_i 发送消息包 $E_{K_{Si}}(\mathrm{True}\,||\,\mathrm{Time}_i)$，再由 ID_i 向所有认证节点发布信息包 $E_{K_{Ni}}(\mathrm{PU}_i\,||\,\mathrm{Start\_Message}\,||\,\mathrm{Time}_i)$；否则拒绝认证。

3.5 认证完成

除 A_j 外的所有叶子节点向 T 发送信息包 $E_{\mathrm{PU}_i}(m_k\,||\,\mathrm{Time}_i)$ $(k=1,2,\cdots,j-1,j+1,\cdots,m)$。$T$ 通过解密就得到了 $m-1$ 个叶子密钥 m_k。依据 HuffMHT 的结构和 $s_j^{'}$，计算得到根密钥 $m_{1-m}^{'}$，并向 A_j 返回信息包 $E_{s_j^{'}}(\mathrm{MAC}_{K_{s_j^{'}}}(m_{1-m}^{'})\,||\,m_{1-m}^{'}\,||\,\mathrm{Time}_i)$。

当 A_j 收到信息包后，先解密然后验证时间戳是否过期以及根密钥 $m_{1-m}^{'}$ 是否与簇头发来的根密钥 m_{1-m} 一致。若验证通过，则簇头向所有成员发送确认信息包；否则重新密钥分配，并通知网络管理中心该簇可能存在安全隐患。

4 性能与安全分析

当簇头与网络管理中心通信时，由于网络管理中心可以得到能量补充，该协议采用安全性较高的公钥加密数据；当簇内节点之间的通信时，该方案主要采用对称密钥加密数据。因此该认证机制采用了公钥加密和对称密钥相结合的策略，既能保证认证过程的安全性又能延长网络的生命期。

4.1 协议性能

从认证协议中可以看出，基于 HuffMHT 的实体认证协议需要计算根密钥运算量非常小。假设构建的认证树是 $k+1$ 层且根节点为第 1 层。基于 HuffMHT 的计算量是 k；而基于 Merkle 散列树[7]的计算量是 $2^{k+1}-1$。从而基于 HuffMHT 的认证协议在能量效率上比 Merkle 散列树要好。如果网络的规模较大，那么基于 HuffMHT 的实体认证协议将显示出更好的优越性。

电波在理想的、均匀的、各向同性的介质中传播，且仅考虑由电波的扩散而引起的传播损耗，则称这样的空间为自由空间[15]。设无线电波波源是以 O 点为中心均匀地向外辐射。辐射功率为 P,辐射场的半径为 R，距离中心 O 点处的能量密度为 S，可以得到：$S=P/4\pi R^2$ [15]。若保证以 O 点为中心、以 R 为半径的辐射场区域内一定的接受功率密度阈值，每增加 1 倍距离，则天线的发射功率就需提高 4 倍。因此，节点之间的信息传输距离将对整个网络的能耗产生很大影响。

由于簇内所有节点具有相同的能量初始值，簇头既要与网络管理中心通信又要向簇内成员节点广播消息，从而距离成为选者簇头的主要依据之一。下面验证功耗最小算法的正确性和可行性。

定理 1 功耗最小算法是正确的。

证明 用反证法。设第 j 个节点为该簇簇头。如果算法是不正确的，不妨设第 $j^*(\neq j)$ 个节点对其它所有节点广播消息的功耗更小。那么它们分别存在节点 k 和 k^* 使得 $d_{jk}^2 < d_{j^*k^*}^2$，但这与功耗最小算法矛盾。 证毕

显然，功耗最小算法是多项式时间算法且解不唯一，则它是可行的。从而，该文将功耗最小算法和 Christofides 算法分别用于设定簇头及建立 HuffMHT，降低了节点之间的信息传输距离，减少了节点能耗，提高了网络生命期。

4.2 协议安全性

从协议中可以看出，所有发送和接受的信息包都是加密的，攻击者通过中间攻击的方式来截获、偷听或任意修改消息是不可能的。另外，信息包在发送时都增加了时间戳，这可以有效防止重放攻击；每个消息包都用加密或消息认证码的方式来保证数据的安全性和完整性，因此恶意节点通过攻击网络的链路来破坏网络健壮性是不容易的。该方案采用了公钥加密和对称密钥相结合的认证方式，从而它能更好地防止其它攻击：

(1)Sybil 攻击　整个网络的每个簇都有唯一的身份标识符，只有合法身份的用户才能正确解密数据并继续执行认证协议。它可以防止恶意节点假冒其它节点来获取有效信息。

(2)剥夺“睡眠”攻击　待认证节点发送的认证请求中包含某簇簇头的唯一标识符，只有信息包中的标识符与簇头中的标识符一致时，簇头才通知成员节点进行认证过程。它能有效防止恶意节点不断向某个簇发生认证请求包而耗尽该簇内所有节点的能量。

假设簇内每个节点受到攻击的概率是相同的。如果恶意节点在公钥认证过程中攻击簇头，那么攻击的成功率是$1/|C_i|$。由于认证密钥只有认证节点知道，则随后攻击认证节点 A_j 的成功率是$1/(|C_i|-1)$。因此，仅攻击两个节点来破坏网络的成功率是$2/(|C_i|\times(|C_i|-1))$。若恶意节点能有效区分所有节点是那个簇的，那么通过攻击簇内半数的节点来破坏网络的成功率约为$[(\lfloor|C_i|/2\rfloor\times(\lfloor|C_i|/2\rfloor-1)]/[(\lfloor|C_i|/2\rfloor+1)\times(\lfloor|C_i|/2\rfloor+2)]$；否则通过攻击簇内半数节点来破坏网络的成功率约为$[(\lfloor|C_i|/2\rfloor\times(\lfloor|C_i|/2\rfloor-1)]/[(\lfloor|C_i|/2\rfloor+1)\times(\lfloor|C_i|/2\rfloor+2)\times n^{\lfloor|C_i/2|\rfloor}]$。

定理 2　设网络内节点数为 $a\,(a\geq 2)$ 且分为 n 个簇，每个簇的节点个数至多相差 1，恶意节点无法区分任何一个节点是属于哪个簇。当网络内的节点个数趋于无穷时，恶意节点通过攻击$\lfloor a/2n\rfloor$个节点来破坏网络成功率的极限值为 0。

证明　略

假设网络中分别有 60，100 和 200 个节点，这些节点均匀地分布在一个方形区域内。通过仿真恶意节点攻击半数的簇内节点来验证认证机制的安全性。下面用 MATLAB 仿真得到了恶意节点破坏网络的成功率与簇内节点数和网络规模的关系：

从图 2 中可以得出：当网络中有 60 个节点且分为 20 个簇时，恶意节点攻击网络的成功率约为 0.1%；若网络中有 100 个节点，那么攻击网络的最大成功率约为 0.05%。恶意节点攻击网络的成功率与网络内节点的数目是成反向关系，节点数越多攻击的成功率就越低。当网络中每个簇的节点数约为 3，此时网络安全性最差，从而网络的安全性与分簇的情况有关系。随着网络节点数目的增加，恶意节点攻击网络的成功率是以一个数量级下降，而由分簇引起安全性波动的范围仅在同一数量级上变化。因此网络内的节点数量对网络的安全性比网络分簇影响大。从上述对安全性的仿真结果可以看出，该认证方案是安全的。

5　结束语

由于自组织网络的拓扑结构不断变化和网络的自组织性使得敌手更容易入侵，所以研究网络的安全性是非常有必要的，尤其是认证机制。该文运用 HuffMHT 的思想，结合对称密钥和公钥加密算法，同时设计了功耗最小算法和引入了 Christofides 算法，提出一种基于 HuffMHT 的自组织网络实体认证方案。该协议可防御 Sybil 攻击、剥夺“睡眠”攻击等。但是该方案在密钥分发与更新时都依赖于网络管理中心是绝对安全的，以及簇头节点在认证过

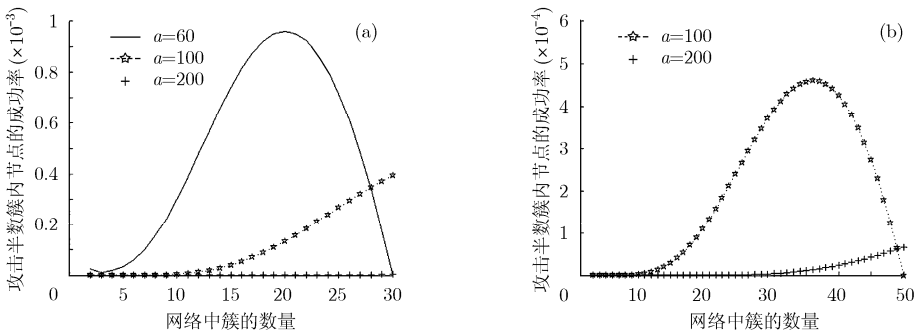

图 2 攻击多个节点的成功率

程中的安全性显得尤为重要，这使得它们成为了恶意节点攻击的目标。此外，由于哈密顿圈是 NP-hard 问题，本文通过 Christofides 算法只求出了一个近似解，仅给出最小能量消耗的一个上界。因此该认证方案还需要在安全性的依托和能量消耗的控制方面做进一步的完善。

参 考 文 献

[1] Karlof C and Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures [C]. IEEE International Workshop on sensor Network Protocols and Applications, California Univ., Berkeley, CA, USA, 2003: 113–127.

[2] Rebahi Y, Mujica-V V E, and Sisalem D. A reputation-based trust mechanism for ad hoc networks [C]. Proc. 10th IEEE Symposium on Computers and Communications, Fraunhofer Fokus, Germany, 2005: 37–42.

[3] Sun Y L, Han Z, and Yu W, *et al*.. Attacks on trust evaluation in distributed networks [C]. IEEE Conference on Information Sciences and Systems, CLSS 2006-Proceedings, Rhode Island Univ., Kingston, RI, 2007: 1461–1466.

[4] Tuptuk N and Lupu E. Risk based authorisation for mobile ad hoc networks [J]. Lecture Notes in Computer Science, Springer-verlag, 2007, 4543: 188–191.

[5] Rabadi N M and Mahmud S M. Privacy protection among drivers in vehicle-to-vehicle communication networks [C]. 4th Annual IEEE Consumer Communications and Networking Conference, CCNC2007, Las Vegas, NV, USA, 2007: 281–286.

[6] Papapanaqiotou K, Marias G F, and Georqiadis P *et al*.. Performance evaluation of a distributed OCSP protocol over MANETs [C]. 3rd IEEE Consumer Communications and Networking Conference, Piscataway, NJ, USA, 2006, 1: 1–5.

[7] Wang L N, Shi D J, and Qin B P, *et al*.. Clustering-based merkel hash tree entity authentication scheme [J]. *Chinese Journal of Sensors and Actuators*, 2007, 20(6): 1338–1343.

[8] Munoz J L, Forne J, and Esparza O, *et al*.. Efficient certificate revocation system implementation: huffman merkle hash tree (HuffMHT) [J]. Springer-Verlag Berlin Heidelberg, LNCS, 2005, 3592: 119–127.

[9] Aboudagga N, Refaei M T, and Eltoweissy M. Authentication protocols for ad hoc networks: taxonomy and research issues [C]. International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems, Montreal, Quebec, Canada, 2005: 96–104.

[10] Hu W, Chou C T, and Jha S, *et al*.. Deploying long-lived and cost-effective hybrid sensor networks [J]. *Ad hoc Networks*, 2006, 4(6): 749–767.

[11] Korte B and Vygen J. Combinatorial Optimization Theory and Algorithms (Fourth Edition) [M]. Springer-Verlag Berlin Heidelberg, 2008: 527–529.

[12] Skold M, Yeongyoon C, and Nilsson J. An analysis of mobile radio Ad hoc networks using cluster architectures [C]. 57th IEEE Vehicular Technology Conference, Swedish Defence Res. Agency, Linkoping, Sweden, 2003, 1: 181–185.

[13] Chiasserini C F, Chlamtac I, and Monti P, *et al*.. An energy-efficient method for nodes assignment in cluster-based ad hoc networks [J]. *Wireless Networks*, 2004, 10(3): 223–231.

[14] Heinzelman W B, Chandrakasan A P, and Balakrishnan H. An application-specific protocol architecture for wireless microsensor networks [J]. *IEEE Transactions on Wireless Communications*, 2002, 1(4): 660–670.

[15] 叶银法, 陆健贤, 罗丽等. WCDMA 系统工程手册[M]. 机械工业出版社, 2006: 470–471.

Ye Y F, Lu J X, and Luo L, *et al*.. Handbook of WCMA System Engineering [M]. China Machine Press, 2006: 470–471.

周贤伟： 男，1963 年生，教授，博士生导师，研究领域为移动通信、下一代网络、电波传播和信息安全.

郭继文： 男，1982 年生，博士生，研究领域为密码学与信息安全.