# 移动 Ad hoc 网络安全分簇综述

王衡军 王亚弟 韩继红
(解放军信息工程大学电子技术学院 郑州 450004)

**摘 要** 移动 Ad hoc 网络是由移动节点组成的无线移动通信网络,它具有动态拓扑、无线通信的特点,但又易受到各种安全威胁。规模较大的移动 Ad hoc 网络可以用分簇的方法来减少路由和控制开销,并提高网络的可扩充性。综合分析了以安全为部分或全部目的的移动 Ad hoc 网络分簇方法研究的最新进展。首先分析了移动 Ad hoc 网络的特点、体系结构和面临的安全威胁,然后将较大规模移动 Ad hoc 网络的安全分簇方法分为 3 个重要方面:认证模型、信任度量和不良节点发现。对每个方面的一些典型方案进行了分类论述和综合比较。最后指出了下一步研究中应当着重考虑的问题。

**关键词** 网络,信息安全,移动 Ad hoc 网络,分簇,综述
**中图法分类号** TP393 **文献标识码** A

## Survey of Secure Clustering in Mobile Ad hoc Networks

WANG Heng-jun WANG Ya-di HAN Ji-hong
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004, China)

**Abstract** Mobile ad hoc networks composed of mobile wireless nodes, are particularly vulnerable due to their features of open medium and dynamic changing topology. Clustering is effective in reducing the spending on routing and control and improving the scalability in large mobile ad hoc networks. This paper surveyed the state of the art in secure clustering of mobile ad hoc networks. Firstly, the characters, proposed architectures and security threats of mobile ad hoc networks were analyzed. Secondly, secure clustering schemes were reviewed according to authentication model, evaluation of trust and identification of malicious nodes. We also made a comparison and discussion of their respective merits and faults. Finally, we also presented the challenges which are still worth to further research in this area.

**Keywords** Network, Information security, Mobile ad hoc network, Clustering, Survey

## 1 引言

移动 Ad hoc 网络是由一组带有无线收发装置的移动节点组成的一个无线移动通信网络,它不依赖于预设的网络基础设施而临时组建,网络中移动的节点利用自身的无线收发设备交换信息,当相互之间不在彼此的通信范围内时,可以借助其他节点中继来实现收发设备交换信息。

移动 Ad hoc 网络的体系结构可以分成平面式或分级式。平面式结构中,网络中所有节点的功能和地位相等,不存在瓶颈节点,网络比较健壮,并且覆盖范围一般比较小,相对比较安全。但在用户较多,特别是在移动的情况下,存在处理能力弱、控制开销大、路由经常中断等缺点,因此它主要适用于中小型网络。为了提高网络的可扩展性,中大型移动 Ad hoc 网络通常采用分级结构。最常用的分级结构是分簇网络结构(如图 1 所示):网络被划分成若干个簇;每个簇由一个簇头和多个普通节点组成;簇头形成高一级的虚拟骨干网。分簇结构的最大优点是网络的可扩充性好,路由和控制开销比平面结构小,并且可以减少共享相同信道的节点的数目,从而降低碰撞概率。分簇结构也有缺点:若使维护可靠并能够适应网络拓扑变化,则需要某种分簇算法;节点之间的路由不一定是最优路由;簇首的任务相对较重,它要维护到达其它簇首的路由,还要负责管理和协调簇内的节点,有可能成为网络的瓶颈。

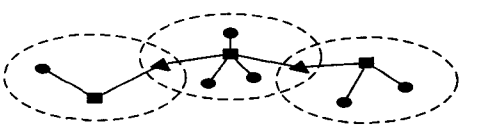

图 1 移动 Ad hoc 网络的分簇结构

不同的分簇算法有不同的优化目标:最小化簇计算和维护开销;最小化簇头数目;最大化簇稳定性;最大化节点生存时间等。目前提出的分簇算法有:基于节点 ID 的分簇算法、最高节点度分簇算法、最低节点移动性分簇算法、考虑簇头负载和簇稳定度的分簇算法、考虑节点能量耗费适用于传感网络的分簇算法、无簇头分簇算法、调节簇尺寸的分簇算法、基于地理位置的分簇算法和基于信道接入的被动分簇算法等。

## 2 移动 Ad hoc 网络安全分簇

移动 Ad hoc 网络面临的安全威胁有:无线通信的广播本

到稿日期:2008-11-05 返修日期:2009-01-21 本文受国防预研项目资助。
王衡军(1973—),男,博士研究生,讲师,主要研究方向为信息系统安全等,E-mail:wanghengjun@163.com;王亚弟(1953—),男,教授,博士生导师,主要研究方向为信息系统安全等;韩继红(1966—),女,博士,教授,主要研究方向为信息系统安全等。

质使其更易受到窃听、假冒、篡改等攻击；移动节点在漫游中可能被俘获，自组网还会面临来自内部节点的攻击；网络拓扑结构、节点数不断变化，节点信任关系也随之变化；网络决策和算法的执行需要多节点协议，这种协作易遭破坏等。

为了更好地解决安全问题，应该在设计网络结构时就考虑安全问题，中大型移动 Ad hoc 网络的簇结构应该与安全方案紧密结合。例如，以分布式 CA 为基础的认证方案，以基于簇结构进行部署是很自然的。同时，由于簇头的重要作用，在簇头的选择上显然应该考虑候选节点的可信任程度。可信度过低的节点，不仅不能担任簇头，而且必须被排除出网络。目前已经出现了一些全部或部分从安全角度考虑的分簇算法。安全分簇算法的特点是在簇的形成与维护的过程中考虑了认证、保密等安全需求，将节点的可信程度等因素纳入网络结构的形成和维护中，其网络结构能较好地适应安全需求。

安全分簇的目的是从网络结构上加强网络的安全性，而认证则是安全活动的首要前提。因此，安全分簇结构一般都要与某种身份认证模型紧密结合，共同形成网络安全的底层基础设施。在运行过程中，因为移动 Ad hoc 网络的特性和敌对环境的威胁，节点的可信任程度会发生变化。因此，簇维护的过程不仅是网络结构的维护过程，也是不良节点的发现与排除过程。所以，安全分簇算法一般还要对节点可信任程度进行度量，并以此度量值作为安全认证、保密通信、不良节点排除等安全行为和簇首选择等网络行为的依据。本文分别从认证模型、节点信任值度量和不良节点的发现 3 个方面综合分析现有移动 Ad hoc 网络的安全分簇方案。

## 3 安全分簇的认证模型

移动 Ad hoc 网络的首要安全问题是节点间的身份认证。身份认证的常用方法是使用公钥密码的 PKI 技术，通过 CA 为每个节点颁发数字证书来实现身份认证和密钥协商。如图 2 所示，安全分簇网络结构中，簇很自然地形成相对独立的簇内安全子区域，而由各簇的簇首 CH 组成的 CH 网络则形成了高一级的安全区域。针对不同级的安全区域，不同的方案给出了不同的安全认证方法。常见的与分簇算法相结合的认证方案有传统的共享口令方案、传统的单 CA 证书方案、基于秘密共享[1]的分布式 CA 证书的方案和自组织证书的方案等。

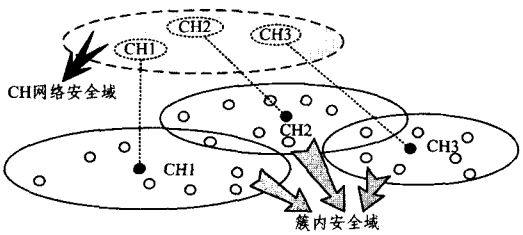


图 2 分簇结构的不同安全区域

文献[2]的基于多级簇的方案使用对称密钥体制。同等级的簇组成一个层，所有的层组成一个等级体系，密钥的产生、分配以及实际的传递沿着体系进行。每一层有一个层密钥，由密钥服务器按需产生，为本层所有成员所知；每个簇有一个簇密钥，由簇首产生，为本簇所有成员所知。簇首与簇内每个节点都有一个共享密钥。簇之间有一个簇共享密钥，用于不同簇之间的节点协商会话密钥。各种级别的密钥和分层体系提供了对选择性通信机制的支持。当有节点加入或离开时，簇必须更新簇密钥。方案具有扩展性、高效性，但安全性较低，存在着单点失效的问题。为了避免单点失效，安全分簇算法大都以基于秘密共享的 CA 证书的方案和自组织证书[3]的方案作为核心安全认证方案。

### 3.1 基于秘密共享的 CA 证书方案

因为 Ad hoc 网络经常处在恶意的环境中，节点容易被攻陷，如果只使用一个权威 CA 来进行证书管理，一旦该节点被攻陷，整个网络将彻底崩溃。而 Ad hoc 网络中多个节点同时被攻陷的可能性则小得多，因此可以使用多个节点一起来实现 CA 的功能，将对一个 CA 的信任分散到对若干个节点的共同信任中。所谓分布式 CA 是利用门限秘密共享的思想将 CA 的私钥进行分割，把分割生成的私钥元（私钥份额）分给某些或全部节点。这些节点称为服务节点，然后由服务节点组成一个虚拟的 CA，共同完成一个完整的 CA 的功能。文献[4]提出使用基于证书的公钥来建立 Ad hoc 网络节点间的信任关系，利用$(k,n)$门限密码，将 CA 的私钥分配给其中 $n$ 个节点，由这 $n$ 个节点中的至少 $k$ 个节点共同完成 CA 的功能，为其他节点签发证书，称之为部分分布式 CA。文献[5]提出了一个类似的方法，不同之处是将 CA 的私钥分配给了所有节点，任意 $k$ 个节点就可以完成 CA 的功能，称之为完全分布式 CA。

文献[6]的方案中，作者认为簇的范围较小，安全较易保障，采用了共享的对称密钥来实现簇内的安全认证与通信。而 CH 网络范围大，为了保证安全而采用了部分分布式 CA。文献[7]在 CBRP 协议的基础上，将簇首的 CA 功能用一个由多个节点组成的委员会（council）来担任。

### 3.2 基于自组织证书方案

自组织证书方案不需要权威的 CA，证书由节点自己发布和维护，类似 PGP，用户通过证书链来实现认证。节点首先发布自己的证书并收集信任节点的证书。当两个节点需要认证时，它们合并各自的证书库，形成认证链路图。如果从图中能发现一条通达的认证链路，则认为认证成功，否则认证失败。认证链也可以通过若干中间可信节点的转接来形成。

文献[8]给出的方案中，任一节点都可以发布证书，簇内节点间的信任依赖于节点之间的监视，簇间节点的信任依赖于证书链。该方案中，为了防止恶意节点发布虚假证书，采用了信任评估技术来确认恶意节点。文献[9]采用了基本类似的方案。文献[10]给出的方案中，CH 网络采用了完全自组织的认证方案，而簇内则采用了传统的单 CA 证书的方式，将 CH 作为 CA 来发布与验证簇内证书。单 CA 容易引起单点失效的问题，因此该方案采用了保护区（dynamic demilitarized zone）的方法，在一定程度上保护了 CA。

### 3.3 两种认证方案的比较

表 1 对以上两种认证方案进行了比较。它们都能防止单点失效，因此是 CH 网络安全认证中常用的方案。通过比较可以看出，秘密共享证书方案虽然付出的代价较大，但是验证快速、简单，适合军事应用。而自组织证书方案虽然无需权威机构参与，但是认证链难以保证安全且形成较慢。

表 1 秘密共享证书方案与自组织证书方案比较

| | 秘密共享证书方案 | 自组织证书方案 |
|---|---|---|

| | | |
|---|---|---|
| 基础结构 | 系统私钥分成若干份由不同节点共享，公钥由所有节点所知 | 各节点的公钥通过交换，形成本地证书数据库 |
| 证书管理 | 由门限个 CA 节点联合颁发 | 节点自己生成，通过信任节点间的传递来分发 |
| 认证方式 | 系统公钥验证 | 合并证书库形成证书链认证 |
| 优势 | 防止单点失效，验证快速、简单，适合战场等紧急场合使用 | 防止单点失效，无需权威机构参与，适合自主性强、安全需求低等场合 |
| 劣势 | 增加节点计算负载和网络流量 | 认证链中节点的可信性难以保证 |

## 4 安全分簇中节点间信任的度量

认证模型对节点的身份给出了明确的回答，非友即敌。由于移动 Ad hoc 网络的特性及其面临的安全威胁，原本可信的节点可能因为被俘等原因而变得不可信，但该节点仍然可能持有有效的证书，因此根据节点在网络运行过程中的各种行为来判定其当时的信任程度就十分必要。目前提出的安全分簇算法大都涉及了有关节点信任的度量问题，所采用的方法大多参考了分布式信任研究的成果。节点间的信任关系的评估一般都采用不确定性和概率论的方法，例如贝斯网、证据理论和模糊集合理论等。

### 4.1 基于权重的信任度量

Guha 等人提出了基于权重的信任传递方法[11]，对不同推荐路径的推荐信任值进行加权平均。评分权重由评分者的可信度/信誉、评分产生的时间、评分和现有得分的距离等因素决定。这种方法克服了简单信誉模型过于粗糙、不能准确描述信任值的弊端，而且算法简单直观，易于理解。然而，这种方法不满足信任合成的结合率，相同的信任证据通过不同方式合成，会产生不同的结果。并且该模型中的推荐权重参数一般由推荐方的信誉、时间等因素决定，主观性非常强，在移动 Ad hoc 网络环境中难以确定。

### 4.2 基于概率的信任度量

Beth 等人首先引入了经验的概念来表述和度量信任关系，并给出了由经验推荐引出的信任度推导和综合计算公式。在 Beth 信任评估模型[12]中，经验被定义为对某个主体完成某项任务的情况记录，对应于任务的成败，经验被分为肯定经验和否定经验。若主体任务成功，则对其肯定经验记数增加；若主体任务失败，则否定经验记数增加。模型中的经验可以由推荐获得，而推荐经验的可信度问题同样是信任问题。直接信任定义为“若 $P$ 对 $Q$ 的所有(包括直接的或由推荐获得的)经验均为肯定经验，则 $P$ 对 $Q$ 存在直接信任关系”。当 $Q$ 被信任时，$Q$ 能成功完成任务的概率被用于评价这种信任关系，而概率的计算则取决于 $P$ 对 $Q$ 的肯定经验记录。Beth 模型考虑了同一个经验推荐者出现在不同推荐路径上的情况。相同的经验信息经不同的路径被多次传递，产生不同的推导结果，该公式采用取推导值平均的方法得到一个唯一值。Beth 模型对直接信任的定义比较严格，仅采用肯定经验对信任关系进行度量。另外，其信任度综合计算采用简单的算术平均，无法很好地消除恶意推荐所带来的影响[13]。文献[8,9]采用了与 Beth 方法类似的信任度量方法。

文献[14,15]将实体间的信任关系分为直接信任值和信任强度，提出了较为完善的基于推荐信任向量和 Beta 分布的信任评价模型。其中，直接信任值基于 Beta 分布求得：

$$T=\frac{g+1}{g+b+2}$$

其中，$g,b$ 分别表示成功经验数与失败经验数。文中还基于权重最大化算法提出了多路信任合成的方法。当有 $N$ 条推荐路径时，$i$ 对 $j$ 的推荐信任值为：

$$T_{ij}=\frac{\sum T_{il}^{c}T_{lj}}{\sum T_{il}},(l\in\{1,2,\cdots,N\})$$

其中，$T_{il}$ 表示 $i$ 对第 $l$ 条推荐路径的信任值。最后，由直接信任值和推荐信任值得出对实体的整体信任值。但该模型没有考虑信任随时间衰减的特性，由概率值直接表示信任也不够准确。

信任论中熵的有关概念也被用于信任度量[16]。基于概率的信任度量方法是被采用最多的信任评估方法。

### 4.3 基于主观逻辑的信任度量

Jøsang 等人引入了证据空间(evidence space)和观念空间(opinion space)的概念来描述和度量信任关系，并提供了一套主观逻辑(subjective logic)算子用于信任度的推导和综合计算[17,18]。证据空间由一系列主体产生的可观察到的事件组成。主体产生的事件被简单地划分为肯定事件(positive event)和否定事件(negative event)。Jøsang 基于 Beta 分布函数描述二值事件(binary event)后验概率的思想，给出了一个由观察到的肯定事件数和否定事件数决定的概率确定性密度函数，并以此来计算主体产生某个事件的概率的可信度。Jøsang 信任度评估模型提供的主观逻辑算子主要有合并(conjunction)、合意(consensus)和推荐(recommendation)。其中合并用于不同信任内容的信任度综合计算，合意根据参与运算的观念(信任度)之间的关系分为独立观念间的合意、依赖观念间的合意和部分依赖观念间的合意 3 类。所谓观念依赖是指观念是否部分或全部由观察相同的事件所形成。合意主要用于对多个相同信任内容的信任度综合计算。推荐主要用于信任度的推导计算。与 Beth 模型相比，Jøsang 模型对信任的定义较宽松，同时使用了证据空间中的肯定事件和否定事件对信任关系进行度量。模型没有明确区分直接信任和推荐信任，但提供了推荐算子用于信任度的推导。另外，其信任度使用三元组来表示，而不是 Beth 模型中的单一数值。该模型同样无法有效地消除恶意推荐带来的影响[13]。

### 4.4 基于路径独立的信任度量

Reiter 和 Stubblebine 在文献[19]的实体认证中引入路径独立的概念。在分布系统中，$A$ 从它的最信任点 $C$，到终端实体 $B$ 的信任路径通常是不固定的。由于通过中间可信节点转发会削弱信任关系的可信度，为了提高信任的正确性，必须对信任路径进行优化。选择最短路径是一种优化策略，它使信任路径上的转发节点数目最少，从而降低了风险。考虑到信任路径搜索的计算速度以及对路径的安全性要求，给出了认证路径长度，路径长度受限制的优化路径可由广度优先法、深度优先法、Dijkstra 法等搜索得到。

若一些路径除了起点和目标节点外相互没有公共节点，则认为它们是相互独立的。此时，这些信任链相互没有依赖，多路径就是指的这种独立路径。若用图论描述，则图 $G(V,E)$ 代表公钥和网络的证书，其中 $V$ 表示节点的集合，$E$ 表示边的集合。相对于请求节点的最信任点为 $C$，目标节点为 $B$，路径长度限制为 $d$。寻找路径长度受限的全部独立路径是 NP 完全问题，在寻找独立路径时，采用启发式近似算法，定义一个路径的评价函数 $\varphi$，采用优化算法在 $\varphi$ 最小的情况下

找出一条路径 $P$，然后从图中消除该路径上的中间节点及边，再重复寻找路径，显然这样得出的路径是彼此独立的。选择评价函数 $\varphi$，主要为了便于找出尽量多的独立路径。例如评价函数可以取为路径的长度，也就是路径上中间节点的数目；评价函数也可取为路径上各中间节点的连接度的和。

## 5 不良节点发现

通过观察一跳邻居节点的行为能够发现不良节点。文献[20]提出了一种名为 watchdog 的方法来实现不良节点的发现。watchdog 运行于每个节点上，负责监视邻居节点的行为，并根据一定的策略作出对邻居节点的判定。通过本地监视技术来发现和排除不良节点的思想在很多研究[21,22]中都得到了普遍的应用。文献[10]采用了分层监视的方法，全网节点按信任值划分为 5 个等级，最高等级的节点经选举担任 CA 和簇首，高等级的节点监视低等级的节点的行为。

而远程不良节点则需要通过信任值的度量来确定。当信任值过低时，就认为节点是不可信的。当采用自组织证书认证方案时，还可以在证书链形成过程中发现恶意节点[8]。当请求节点需要远程节点的证书时，它可以向多个中间节点要求推荐该远程节点的证书，通过对比来自不同节点推荐的该远程节点的证书，可以发现其中的恶意节点。

**结束语** 由于移动 Ad hoc 网络的特性和面临的威胁，传统的安全解决方案无法应用。从网络结构就考虑安全是解决移动 Ad hoc 网络安全的根本之举。本文从应用于大规模移动 Ad hoc 网络的安全分簇方案的认证模型、信任度量与不良节点发现 3 个重要环节介绍了相关研究成果。

整体来说，移动 Ad hoc 网络安全研究仍然处于理论探索阶段，其安全分簇的进一步研究应考虑以下方面：分布式 CA 给网络造成的资源消耗过大、效率较低。集中式 CA 存在单点失效问题，自组织证书又缺乏权威性，易受攻击，因此与分簇相结合的认证研究应结合多种方案或发展新的快速轻量的认证方法；簇结构的不平衡性和节点安全运算对资源的消耗促使安全分簇朝向均衡和自适应的方向发展；发展适合特殊应用场合的安全分簇方案十分必要，如单兵战术应用、军用飞机、舰队、紧急救援等。

## 参 考 文 献


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

[2] Li J H, Levy R, Yu M, et al. A scalable key management and clustering scheme for ad hoc networks[C]// Hong Kong, China. Association for Computing Machinery. New York, NY 10036-5701, United States, 2006

[3] Capkun S, Buttyan L, Hubaux J P. Self-organized public-key management for mobile ad hoc networks[J]. IEEE Transactions on Mobile Computing, 2003, 2(1): 52-64

[4] Lidong Z, Haas Z J. Securing ad hoc networks[J]. IEEE Network Magazine, 1999, 13(6): 24-30

[5] Kong J, Zerfos P, Luo H, et al. Providing Robust and Ubiquitous Security Support for Mobile Ad hoc Networks[M]. Riverside, California, USA, 2001

[6] Bechler M, Hof H, Kraft D, et al. A cluster-based security architecture for Ad hoc networks[C]// Hongkong, China. Institute of Electrical and Electronics Engineers Inc. Piscataway, NJ 08855-1331, United States, 2004

[7] Shah V, Deng H, Agrawal D P. Parallel Cluster Formation for Secured Communication in Wireless Ad hoc Networks[C]// Networks, 2004(ICON 2004). Proceedings of 12th IEEE International Conference. 2004(2): 475-479

[8] Ngai E C H, Lyu M R. An authentication service based on trust and clustering in wireless ad hoc networks: Description and security evaluation[C]// Taichung, Taiwan. Institute of Electrical and Electronics Engineers Computer Society. Piscataway, NJ 08855-1331, United States, 2006

[9] Ngai E C, Lyu M R. Trust-and clustering-based authentication services in mobile ad hoc networks[C]// Hachioji, Japan. Institute of Electrical and Electronics Engineers Inc. Piscataway, United States, 2004

[10] Rachedi A, Benslimane A. Trust and mobility - based clustering algorithm for secure mobile Ad hoc networks[C]// Papeete, French Polynesia. Institute of Electrical and Electronics Engineers Computer Society. Piscataway, NJ 08855-1331, United States, 2006

[11] Guha R, Kumar R, Prabhakar - Raghavan A T. Propagation of Trust and Distrust[C]// New York, NY, USA. Association for Computing Machinery. 2004

[12] Beth T, Borcherding M K B. Valuation of trust in open networks [M]. Springer-Verlag, 1994

[13] 张仕斌，何大可，盛志伟. 信任管理模型的研究与进展[J]. 计算机应用研究，2006，23(7)

[14] 刘玉龙，曹元大. 分布网络环境主观信任模型研究[J]. 北京理工大学学报，2005，25(6)：504-508

[15] 刘玉龙，曹元大，李剑. 一种新型推荐信任模型[J]. 计算机工程与应用，2004，40(29)：47-49

[16] Sun Y, Yu W, Han Z, et al. Trust modeling and evaluation in Ad hoc networks[C]// St. Louis, MO, United States: Institute of Electrical and Electronics Engineers Inc. New York, NY 10016-5997, United States, 2005

[17] Jøsang A K S J. A Metric for Trusted Systems[M]. Austrian Computer Society, 1998: 541-549

[18] Jøsang A. The right type of trust for distributed systems[M]. Lake Arrowhead, California, United States: ACM, 1996

[19] Stubblebine R M K G S. Resilient authentication using path independence[J]. Computers, IEEE Transactions on, 1998, 47(12): 1351-1362

[20] Marti S, Giuli T J, Lai K, et al. Mitigating routing misbehavior in mobile ad hoc networks[M]. Boston, Massachusetts, United States, 2000

[21] Yang H, Shu J, Meng X, et al. SCAN-self-organized network-layer security in mobile Ad hoc networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 261-273

[22] Michiardi P R M. Core: A collaborative reputation mechanism to enforce node coperation in mobile Ad hoc hetworks[C]// Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security. 2002, 228: 107-121