基于分簇的 Ad hoc 网络分布式认证方案

周南润　　万　辉
(南昌大学电子信息工程系　南昌　330031)

摘　要：认证是保证 Ad hoc 网络通信安全的重要技术。该文针对分布式认证方案分别运用在平面 Ad hoc 网络和分簇结构中的优缺点进行了比较研究，提出了一种区域认证方案，该方案采用分簇结构，将 Ad hoc 网络分割为相互独立的认证区域，既减少了网络开销，又增强了认证服务效率，且安全性和可扩展性较好，适用于大规模 Ad hoc 网络。

关键词：Ad hoc 网络；信息安全；分簇；认证
中图分类号：TP393.08　　**文献标识码**：A　　**文章编号**：1009-5896(2009)09-2247-05

Distributed Authentication Scheme for Cluster-Based Ad hoc Networks

Zhou Nan-run　　Wan Hui
(*Dept. of Electronics Information Engineering*, *Nanchang University*, *Nanchang* 330031, *China*)

Abstract: Authentication is critical to secure communication in Ad hoc networks. This paper discusses the shortcomings of distributed authentication schemes in Ad hoc networks with flat structure and the advantages of adopting clustering structure. A zone authentication scheme is proposed to enhance the efficiency of authentication services with less communication cost. The scheme adopts the clustering structure and divides the networks into independent authentication areas, and fits well in the large Ad hoc networks with better scalability and security.

Key words: Ad hoc network; Information security; Clustering; Authentication

1　引言

Ad hoc 网络是由若干无线节点相互协作进行网络互联的一种多跳自组织临时性自治的新型无线网络。Ad hoc 网络广泛地应用于军事、抢险救灾、移动会议等场合，并成为学术界研究的热点。Ad hoc 网络具有不依赖于基础设施、拓扑动态变化、多跳通信、资源受限等特点，相对于一般的依靠基础设施的无线网络，更容易受到窃听、假冒、拒绝服务等攻击[1]，因此安全性问题是 Ad hoc 网络亟待解决的问题。

现有的依靠基础设施的网络广泛采用PKI (Public Key Infrastructure)技术通过认证中心(CA)提供信息安全服务。Ad hoc网络是无中心的对等网络，难以直接通过CA提供信息安全服务。1999年Zhou和Hass将Shamir门限秘密共享引入到Ad hoc网络中，采用分布式的认证结构为网络中的节点提供信息安全服务[2]，增强了认证服务的可用性，却面临着认证服务效率不高、容错性差、计算负载大等缺点。2001年Kong等[3]改进了Zhou等人的方案，将分布式认证转化为本地认证，降低了网络负载，增强了认证服务效率，但每个节点都共享签名密钥并参与子密钥更新[4]，增加了签名密钥暴露的可能性且系统开销大，管理和维护的费用高。葛蒙等针对分布式认证方案提出了一种密钥管理方案，在保证网络安全性和鲁棒性的前提下，通过增加签名子密钥的冗余度来提高认证服务的可用性[5]。王化群等提出了一种适用于Ad hoc网络的密钥管理方案，保证了系统签名密钥和节点子密钥的安全[6]。熊焰等人提出了多跳步加密签名函数签名的分布式认证方案，提高了基于门限签名的分布式认证方案的安全性[7]。文献[8]提出了一种基于RSA门限签名算法的Ad hoc网络分布式认证方案，通过动态地增加签名门限值增强了Ad hoc网络的安全性。

分布式认证运用在平面式的Ad hoc网络结构中时，随着网络规模的增大，路径获取、数据传输等通信开销迅速增大，极可能耗尽有限的网络资源，以致节点无法获取认证服务。而采用分簇的层次网络结构能够减少路由维护的代价，增大网络的吞吐量，增强链路的稳定性和服务的可扩展性[9, 10]。Dong等将分布式认证方案运用在分簇的Ad hoc网络中，

2008-10-06 收到，2009-04-09 改回
国家自然科学基金(10647133)，江西省自然科学基金(2007GQS1906)，江西省教育厅科技项目(赣教技字[2007]22)，江西省教育科学“十一五”规划项目重点课题(07ZD017)和南昌大学引进人才科研启动费资助课题

有效地增强了认证服务的可用性，改善了网络规模增大时认证服务可用性差的问题[11, 12]，但由簇头承担认证服务加重了簇头的负担，而且由于节点移动的随机性，提供认证服务的节点在网络中的分布不均匀，边缘地区难以获取服务。

本文通过采用区域认证的管理机制, 在分簇的Ad Hoc网络中配置分布式认证服务，以进一步提高服务的可用性和安全性，并合理地分配资源，同时提高服务的可扩展性。

2 基于分簇的Ad hoc网络分布式认证服务

2.1 网络模型

首先作如下假设：

(1)网络中的每个节点都拥有唯一的、公开的身份ID。ID字段由节点优先级PID和节点标识NID组成，PID字段反映节点的性能和安全性，NID字段表示节点的身份信息。每一节点拥有一份关于其身份ID的初始证书，用于验证彼此身份。

(2)网络中存在足够多的性能好、安全性高的节点。性能越好、安全性越高的节点其PID值越低，并且节点具有检测恶意节点的机制。

网络初始化时，所有节点按照最小 ID 分簇算法[10]组成 Ad hoc 网络，节点周期性地向其邻居节点广播 Hello 包(包括身份 ID、初始证书等)，每个节点验证对方身份，并将本节点 ID 值与收到的 Hello 包比较，如果优先级最高(PID 值和 NID 值最小)，则成为簇头节点，其它节点以成员身份加入各簇。采用最小 ID 分簇算法，性能好、安全性高的节点更可能成为簇头，这有利于增强网络的性能，同时分簇结构可以明显地减少路由开销，增强认证服务的效率和鲁棒性。

2.2 认证服务系统模型

2.2.1 签名密钥的生成 簇头协商参数 p， q， g，门限值 k 和节点优先级阈值 $\mathrm{PID}_{\mathrm{th}}$ 并公开，其中 p，q 是两个安全的大素数，$q \mid p-1$； g 为 Z_p^* 上 q 阶子群 G_q 的生成元。所有 PID 值小于阈值的簇头节点可以参与签名密钥的生成，不失一般性假设参与节点的集合为 $B=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$，其中 $n \geq 2k-1$。B 中的节点按照分布式秘密共享生成算法[13]生成签名密钥SK 的子密钥，步骤如下：

第 1 步 $\mathrm{ID}_i(i=1,2,\cdots,n)$ 随机选择一个整数 $s_i \in Z_q$，计算并向其它节点广播 $y_i = g^{s_i} \bmod p$ 和签名。

第 2 步 ID_i 随机地在 $Z_q[x]$ 中构造一个 $k-1$ 次多项式 $f_i(x) = s_i + \sum_{j=1}^{k-1} a_{i,j}x^j$ 。

第 3 步 ID_i 计算 $f_i(\mathrm{ID}_j) \bmod q$ ($j=1,2,\cdots,n$)，ID_i 保存 $f_i(\mathrm{ID}_i) \bmod q$ 并将其余的 $n-1$ 个结果秘密地发送给对应的 $n-1$ 节点，同时广播 $(g^{a_{i,1}}, g^{a_{i,2}}, \cdots, g^{a_{i,k-1}}) \bmod p$ 和签名。

第 4 步 ID_i 收到 $f_j(\mathrm{ID}_i) \bmod q$ ($j=1,2,\cdots,n;\ j \neq i$)后，检验式(1)是否成立。

$$g^{f_j(\mathrm{ID}_i) \bmod q} \equiv y_j \prod_{m=0}^{k-1} (g^{a_{j,m}})^{\mathrm{ID}_i^m} \bmod p,\ j=1,2,\cdots,n;\ j \neq i \tag{1}$$

如果式(1)成立，ID_i 接受 $f_j(\mathrm{ID}_i) \bmod q$；否则广播对 ID_j 的控诉和证据，参与节点验证此消息，并将 ID_j 当作恶意节点从 B 中排除 ID_j，排除后的新节点集合为 B'。

第 5 步 $\mathrm{ID}_i \in B'$ 计算 $\mathrm{sk}_i = \sum_{j \in B'} f_j(\mathrm{ID}_i) \bmod q$，所有节点计算 $\mathrm{PK} = \prod_{j \in B'} y_j \bmod p$，其中 sk_i 为签名密钥SK 的子密钥，PK 为 SK 对应的公钥。

经过上述步骤，B' 中的所有簇头共享签名密钥 SK，B' 中的任意 k 个簇头通过拉格朗日插值法可以恢复 SK：

$$\mathrm{SK} = \sum_{i=1}^{k} \mathrm{sk}_i l(\mathrm{ID}_i) = \sum_{i=1}^{k} \mathrm{sk}_i \prod_{j=1, j \neq i}^{k} \frac{\mathrm{ID}_j}{\mathrm{ID}_j - \mathrm{ID}_i} \tag{2}$$

网络中的所有节点知道SK 对应的公钥PK，用于验证 SK 的签名。由于簇头是虚拟骨干网的构成节点，能够更快地协作生成签名密钥。

2.2.2 区域认证方案 Dong等人的方案[11]由网络中的簇头构成一个虚拟CA，采用门限签名算法给节点提供认证服务，大大增加了簇头的负担。本文提出的区域认证方案由其它可信节点承担认证服务(称这些节点为DCA)，以减少簇头的开销。簇头以分布式的方式将签名密钥的子密钥分发给各DCA节点，DCA节点的数量关系到服务可用性的高低，增加DCA节点的数量在增强服务可用性的同时，也会降低安全性，一方面增加了签名密钥暴露的可能性，这可以通过周期性的子密钥更新予以抵抗；另一方面攻击者Malice虽然不能短时间攻破 k 个DCA节点，但具有较强的伪装和欺骗能力，可通过伪装成善意的节点请求认证服务。假设网络中的DCA节点总数为 N，Malice成功欺骗一个节点的概率为 α，则成功获得一份证书的概率为

$$P_1 = \sum_{i=k}^{N} C_N^i \alpha^i (1-a)^{N-i} \tag{3}$$

当 N 较大或者门限值 k 较小时，Malice有较大的成功概率；如果Malice已经获得 l ($l<k$) 个子密钥，其成功概率更大。为了抵抗Malice的攻击，本文提出区域认证方案，将Ad hoc网络分割成多个独立的认证区域，联合同区域的 k 个DCA能够提供合法的认

证服务，而不同区域的k个DCA无法提供合法服务。区域认证方案包括区域建立、DCA初始化、认证3个阶段。

(1)区域建立：簇头查看其邻接路由表，若某簇头优先级是邻接簇头中最高的，则此簇头成为该区域的管理中心(MC)，MC向邻接簇广播认证区域建立消息(包括身份ID，区域标识A，初始证书和签名等)，邻接簇头验证此消息并加入区域A。MC选举$k+\beta$个PID<$\mathrm{PID}_{\mathrm{th}}$的节点成为DCA节点，其中参数$\beta$为一小整数，用于防止个别DCA节点退出网络，或恶意发放错误的部分证书，使得节点无法获取合法证书。

(2)DCA初始化：区域A内的簇头验证并初始化每个DCA节点，若簇头少于l ($l>k$)个，则邀请该区域邻接簇头参与。假设区域A内簇头的集合为$H=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_l\}$，对应的签名密钥的子密钥分别为$\mathrm{sk}_1,\mathrm{sk}_2,\cdots,\mathrm{sk}_l$，公开值为$\mathrm{Ver}_{\mathrm{sk}_i}=g^{\mathrm{sk}_i} \bmod p$，$i=1,2,\cdots,l$，DCA节点集合为$M=\{\mathrm{ID}_{m_1},\mathrm{ID}_{m_2},\cdots,\mathrm{ID}_{m_{k+\beta}}\}$，设$M$中的某个节点为$\mathrm{ID}_m$，则初始化过程如下：

第1步　$\mathrm{ID}_i\in H$ $(i=1,2,\cdots,l)$计算$P_{\mathrm{ID}_i}(\mathrm{ID}_m)$，并生成$l-1$个随机数$d_{ij}$ $(j=1,2,\cdots,l;j\neq i)$，将相应的d_{ij}秘密地发送给ID_j $(j=1,2,\cdots,l;j\neq i)$，广播$(g^{P_{\mathrm{ID}_i}(\mathrm{ID}_m)},\ g^{d_{i1}},g^{d_{i2}},\cdots g^{d_{il}}) \bmod p$和签名。$P_{\mathrm{ID}_i}(\mathrm{ID}_m)$可表示为

$$P_{\mathrm{ID}_i}(\mathrm{ID}_m)=\mathrm{sk}_i l_{\mathrm{ID}_i}(\mathrm{ID}_m) \bmod q \tag{4}$$

其中$l_{\mathrm{ID}_i}(\mathrm{ID}_m)=\prod_{t=1,t\neq i}^{l}\frac{\mathrm{ID}_m-\mathrm{ID}_t}{\mathrm{ID}_i-\mathrm{ID}_t}$。

第2步　ID_j ($j=1,2,\cdots,l$)收到$l-1$个d_{ij}后，计算$P'_{\mathrm{ID}_j}(\mathrm{ID}_m)$。

$$P'_{\mathrm{ID}_j}(\mathrm{ID}_m)=\left(P_{\mathrm{ID}_j}(\mathrm{ID}_m)+\sum_{i=1,i\neq j}^{l}\mathrm{sign}(\mathrm{ID}_j-\mathrm{ID}_i)\cdot(d_{ij}+d_{ji})\right) \bmod q \tag{5}$$

并将结果秘密地发送给ID_m，其中sign(•)为符号函数。

第3步　ID_m计算$\mathrm{sk}'_m=\sum_{j=1}^{l}P'_{\mathrm{ID}_j}(\mathrm{ID}_m) \bmod q$，检验式(6)是否成立。

$$g^{\mathrm{sk}'_m}\equiv\prod_{i=1}^{l}(\mathrm{Ver}_{\mathrm{sk}_i})^{l_{\mathrm{ID}_i}(\mathrm{ID}_m)} \bmod p \tag{6}$$

如果式(6)成立，ID_m接受sk'_m，即ID_m的子密钥$\mathrm{sk}_m=\mathrm{sk}'_m$；否则检验式(7)是否成立，

$$g^{P'_{\mathrm{ID}_j}(\mathrm{ID}_m)}\equiv(\mathrm{Ver}_{\mathrm{sk}_j})^{l_{\mathrm{ID}_j}(\mathrm{ID}_m)}\cdot\prod_{i=1,i\neq j}^{l}(g^{d_{ij}+d_{ji}})^{\mathrm{sign}(\mathrm{ID}_j-\mathrm{ID}_i)} \bmod p \tag{7}$$

如果式(7)成立，ID_m接受$P'_{\mathrm{ID}_j}(\mathrm{ID}_m)$；否则，$\mathrm{ID}_m$广播对$\mathrm{ID}_j$的控诉和证据。设排除$\mathrm{ID}_j$后的新集合为$H'$，$H'$中每个节点公开$\mathrm{ID}_j$发给它们的随机数，则$\mathrm{ID}_m$的子密钥$\mathrm{sk}_m=\sum_{\mathrm{ID}_i\in H'}(P'_{\mathrm{ID}_i}(\mathrm{ID}_m)-\mathrm{sign}(\mathrm{ID}_i-\mathrm{ID}_j)(d_{ji}+d_{ij})) \bmod q$。

第4步　H'中的节点重复第1步-第3步为其余DCA节点分发子密钥。生成一份子密钥需要一轮随机数交互，事先计算$k+\beta$份子密钥所需的随机数，可以一次性完成随机数交互。

第5步　区域A内所有DAC节点收到子密钥后，MC随机地在$Z_q[x]$中构造一个秘密值为0的$k-1$次共享多项式$f'(x)=0+\sum_{j=1}^{k-1}a_{i,j}x^j$；计算秘密因子$s'_{m_i}=f'(\mathrm{ID}_{m_i}) \bmod q$，$i=1,2,\cdots,k+\beta$，并将相应的$s'_{m_i}$秘密地发送给$\mathrm{ID}_{m_i}$，公开$\left(g^{s'_{m_1}},g^{s'_{m_2}},\cdots,g^{s'_{m_{k+\beta}}}\right)\cdot \bmod p$和签名。

第6步　ID_{m_i}收到秘密因子s'_{m_i}后，计算$g^{s'_{m_i}}\cdot \bmod p$并与相应的公开值比较，并检验式(8)是否成立，

$$\prod_{i=1}^{k+\beta}\left(g^{s'_{m_i}}\right)^{\prod_{r=1,r\neq i}^{k+\beta}\frac{\mathrm{ID}_{m_r}}{\mathrm{ID}_{m_r}-\mathrm{ID}_{m_i}}} \bmod p=1 \tag{8}$$

如果式(8)成立，计算签名子密钥$\mathrm{sk}'_{m_i}=\mathrm{sk}_{m_i}+s'_{m_i}$；否则广播一条对MC的控诉和证据，重新选举区域A的管理中心。

区域内的每个DCA节点ID_{m_i}拥有秘密值sk_{m_i}和sk'_{m_i}，sk_{m_i}为SK的子密钥，sk'_{m_i}为伪子密钥，用于签名部分证书。由于不同区域的MC随机选择不同的多项式$f'(x)$，不同区域的DCA节点无法通过拉格朗日插值多项式恢复SK，因而不同区域的DCA节点签名的部分证书无法组合生成SK的合法证书。DCA节点参与秘密共享更新时，删除伪子密钥并恢复SK的真子密钥参与更新，完成后MC按照步骤第5步和第6步发放新的秘密因子。若区域内有新的DCA节点加入，MC发送新的秘密因子给区域内的DCA节点，DCA节点使用秘密因子生成新的伪子密钥。

(3)认证：当区域内的节点请求认证服务时，区域内所有DCA节点验证节点身份，采用门限签名算法对认证信息(包括节点的身份ID、公钥等)签名得到部分证书，将部分证书发送给请求节点，请求节点验证部分证书并组合k个正确的部分证书得到完整证书。由于不同区域DCA节点签名的部分证书无法组合生成SK的合法证书，区域间认证服务具

有相互独立性，能够将网络中认证服务的开销平衡到各区域，同时某个区域认证服务不可用不影响其它区域，增强了服务的鲁棒性。

3 区域认证方案的维护

Ad hoc 网络中的节点在不停地漫游，需要维护以下几种角色的节点：(1)簇头：簇头退出簇头角色时，在簇内广播退出消息，并成为备份 DCA 节点，用于保证当区域内的某个 DCA 节点不能提供服务时快速承担其角色。簇内节点重新选举新簇头，若新簇头没有子密钥，则向邻接簇头请求发放子密钥。若簇头离开网络，广播退出消息并自动删除秘密值；(2)DCA 节点：本区域 DCA 节点漫游到其它区域时，成为其它区域的备份 DCA 节点，管理中心选举该区域优先级最高的备份 DCA 节点成为新的 DCA 节点，并重新发放新的秘密因子。DCA 节点退出网络时，发送退出消息并自动删除秘密值；(3)管理中心：管理中心退出时(正常退出或意外退出)，在区域内重新选举 ID 最优者担任。

若某认证区域内节点较少，管理中心可以撤销此区域，以减少维护的开销，区域内的各簇自由决定加入邻接区域，区域内 DCA 节点则成为其它区域的备份 DCA 节点。区域内节点过多造成 DCA 节点负担过大时，管理中心可以将此区域分割成两个邻接认证区域。

子密钥更新是保证签名密钥安全的重要机制。网络中所有节点同时参与子密钥更新会造成网络负载过大，更新过程难以进行，应采用波浪式的递推过程完成子密钥更新。当到达更新时刻，管理中心启动更新，并邀请域内簇头参与。簇头是虚拟骨干网的构成节点，能比普通节点更快地完成子密钥的更新。接着区域内簇头依次为邻接区域簇头和本区域 DCA 节点更新子密钥，这样更新过程波浪式地在网络中推进，只会增加局部网络负载，可以避免因所有节点参与造成更新过程难以完成。其次，多个管理中心可能在同一时刻启动多个更新过程，应采用冲突避免机制。当到达更新时刻，管理中心先侦听是否有其它区域管理中心广播更新消息，如果有，则不广播；否则，退避一小段时间后再广播更新消息并同时进行侦听，如果收到其它区域管理中心的更新消息，则比较其 ID 值，优先级低的管理中心撤销其消息，由高优先级管理中心启动更新过程。

4 仿真分析

在 NS-2 下对方案进行仿真分析，参数如下：MAC 层采用 MAC 802.11 协议；节点数为 150，请求认证服务节点数为 10 个，移动模型采用 Random Waypoint，最大移动速度 5 m/s，停留时间 10 s；仿真场景大小 1500 m×1000 m，网络中最多随机存在着 30 个固定比特率源，数据包发送率每秒 100 个；请求门限值 $k+\beta$ 分别等于 5，7，10 (其中 $\beta=2$)，若一次请求有不少于门限值 k 个 DCA 节点返回数据包，则认证成功；路由协议分别采用 DSR (平面型 Ad hoc 网络路由协议)和 CBRP (分簇 Ad hoc 网络路由协议)两种路由协议。

图 1 为认证平均成功率，分布式认证方案运用在 DSR 路由协议的网络中认证成功率在 $k+\beta$ 值较大时较低，其原因主要是采用平面型网络结构链路的性能较差，容易因路由丢失而丢包，并且多个 DCA 节点同时向请求节点发送数据包，造成链路拥塞而丢包。Dong 等人的方案和本文的方案(ZAS)采用分簇的网络结构，认证成功率比采用 DSR 路由协议的平面型网络结构高，其原因是采用分簇的网络结构有效地改善了通信链路的性能，保证了认证数据包的可靠传输。由于本文采用的区域认证方案请求服务节点与区域内 DCA 节点通信的跳数较少，认证数据包传输可靠性较高，认证成功率比 Dong 等人的方案高。

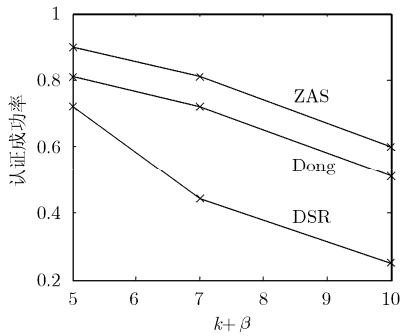

图 1 认证成功率

图 2 为 10 次成功认证的数据包处理总开销(其中数据包处理开销为源节点、中间节点和目的节点数据包处理开销的总和)，$k+\beta$ 值增大时，数据包的处理开销也随之增大，采用 DSR 路由协议的平面型网络结构因通信路由跳数多处理开销较大，随 $k+\beta$ 值增大数据包处理开销增加也较明显。Dong 等人的方案和本文的方案采用分簇的网络结构，通信路由跳数较少，降低了数据包处理所需的开销。本文的方案请求认证节点与 DCA 节点在同一区域，通信的跳数较 Dong 等人的方案少，因而数据包开销也较少。

在安全性方面，由于离散对数问题的难解性，攻击者无法从节点发布的公开值中获取秘密信息，在 DCA 节点初始化过程中，一旦有恶意节点发放错误的秘密值，其它节点可以通过计算验证值检测

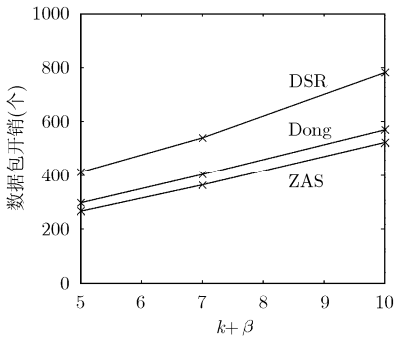

图 2 认证数据包处理开销

发现。其次本文提出的方案签名密钥由网络优先级较高的节点共享，节点安全性高，减少了密钥暴露的可能性，对于具有较强的伪装和欺骗能力的 Malice 的攻击，Malice 在区域 A 内成功获得一份合法证书的概率为

$$P_2 = \sum_{i=k}^{k+\beta} C_{k+\beta}^{i} \alpha^{i} (1-a)^{k+\beta-i} \tag{9}$$

与式(3)相比，因为 $N > k+\beta$，则 $P_2 < P_1$；可见区域认证方案可以有效地减小 Malice 成功的概率。区域间认证服务还具有相互独立性，某个区域认证服务不可用不影响其它区域，增强了服务的鲁棒性的同时，又能将网络中认证服务的开销平衡到各认证区域。另外同一区域内节点相距较小，节点间信任值的估计更为准确[14]，节点获取的证书可信度也较高，而且一旦有节点被俘获或为恶意节点，被发现的概率也较大(例如通过视距观察或节点直接碰面)，通过广播控诉报文可以迅速地将恶意节点在网络中隔离。同时区域认证方案采用基于门限签名的分布式签名算法，具有密钥的分布式管理和安全性高等优点，能有效地增强 Ad hoc 网络的安全性。

5　结论

本文提出的区域认证方案采用了分布式的证书服务，适合于 Ad hoc 网络无中心、自组织的特点，能有效地将证书服务的开销平衡到网络中各区域，既提高了证书服务的效率，又具有较好的安全性和可扩展性，分簇网络结构的应用也减少了网络中的通信开销，增强了网络的可扩展性和鲁棒性。仿真结果表明区域认证方案通信开销小，可用性较好，适合于大规模 Ad hoc 网络。

参 考 文 献

[1] Ramanathan R and Redi J. A brief overview of mobile Ad hoc networks: challenges and directions [J]. *IEEE Communications Magazine*, 2002, 40(5): 20–22.

[2] Zhou Li-dong and Haas Z J. Securing Ad hoc networks [J]. *IEEE Networks Special Issue on Network Security*, 1999, 13 (6): 24–30.

[3] Kong J J, Zerfos P, and Luo H Y, *et al*.. Providing robust and ubiquitous security support for mobile Ad hoc networks [C]. IEEE 9th International Conference on Network Protocols, Riverside, California, USA, 2001: 251–260.

[4] Herzberg A, Jakobsson M, and Jarecki S, *et al*.. Proactive public-key and signature schemes [C]. Proc of the 4th Annual Conference on Computer Communications Security, Zurich, Switzerland, 1997: 100–110.

[5] 葛蒙, 赵曦滨, 林国恩. 适用于移动自组织网的鲁棒性密钥管理[J]. 清华大学学报(自然科学版), 2008, 48(7): 1194–1197.
Ge Meng, Zhao Xi-bin, and Lam Kwok-yan. Robust key management for mobile Ad hoc networks [J]. *Journal of Tsinghua University* (*Science and Technology*), 2008, 48(7): 1194–1197.

[6] 王化群, 张力军, 赵君喜. Ad hoc网络中基于环Zn上椭圆曲线和RSA的密钥管理[J]. 通信学报, 2006, 27(3): 1–6.
Wang Hua-qun, Zhang Li-jun, and Zhao Jun-xi. Key management based on elliptic curves over the ring Zn and RSA in Ad hoc networks [J]. *Journal on Communications*, 2006, 27(3): 1–6.

[7] 熊焰, 苗付友, 张伟超, 等. 移动自组网中基于多跳步加密签名函数签名的分布式认证[J]. 电子学报, 2003, 31(2): 161–165.
Xiong Yan, Miao Fu-you, Zhang Wei-chao, *et al*.. Secure distributed authentication based on multi-hop signing with encrypted signature functions in mobile Ad hoc networks [J]. *Acta Electronica Sinica*, 2003, 31(2): 161–165.

[8] Pietro R D, Mancini L V, and Zanin G. Efficient and adaptive threshold signatures for Ad hoc networks [J]. *Electronic Notes in Theoretical Computer Science*, 2007, 171(1): 93–105.

[9] 安辉耀, 卢锡城, 彭伟. 移动自组网中一种基于簇的多路径路由算法[J]. 软件学报, 2007, 18(4): 987–995.
An Hui-yao, Lu Xi-cheng, and Peng Wei. A cluster-based multipath routing algorithm in mobile Ad hoc networks [J]. *Journal of Software*, 2007, 18(4): 987–995.

[10] Gerla M and Tsai J T C. Multicluster, mobile, multimedia radio network [J]. *ACM/Baltzer Journal of Wireless Networks*, 1995, 1(3): 225–265.

[11] Dong Y, and Sui Ai-fen, *et al*.. Providing distributed certificate authority service in cluster-based mobile Ad hoc networks [J]. *Computer Communications*, 2007, 30(11/12): 2442–2452.

[12] Bechler M, Hof H J, and Kraft D, *et al*.. A cluster-based security architecture for Ad hoc networks [C]. Proc of the 23rd IEEE INFOCOM'04, Hong Kong, China, 2004, 4: 2393–2403.

[13] Pedersen T. A threshold cryptosystem without a trusted party[C]. Proceeding of Crypto' 91, Brighton, UK, 1991: 522–526.

[14] Spiewak D and Fusenig V, *et al*.. The importance of location on trust in mobile networks [J]. *WSEAS Transactions on Communications*, 2008, 7(5): 349–360.

周南润：　男，1976 年生，副教授、博士，研究方向为信息安全和量子通信.

万　辉：　男，1985 年生，硕士生，研究方向为无线通信安全.