doi:10.3969/j.issn.1000-436x.2012.12.012

机会网络中基于社会属性的按需密钥管理方案

陈曦[1,2]，李光松[3]，田有亮[1]，马建峰[1]

(1. 西安电子科技大学 计算机网络与信息安全教育部重点实验室，陕西 西安 710071；
2. 中国电子科技集团公司第二十研究所，陕西 西安 710068；3. 解放军信息工程大学 信息工程学院，河南 郑州 450002;)

摘 要：针对机会网络的间歇性连通、快速移动、自组织管理等特征，提出了基于社会属性的按需密钥管理方案。首先利用基于身份的门限签名方案，实现了节点社会属性的自认证。随后结合机会网络的路由特性，节点之间根据社会属性匹配度有选择地颁发身份证书，并建立可度量的信任网。算法在优化证书图的同时，避免了恶意节点可能导致的无效证书链路的生成。实验仿真表明，该方案可提供较高的证书链重构成功率与节点认证可达率，并有效地降低了密钥管理所需的网络开销。

关键词：机会网络；密钥管理；身份密码学；门限密码学；社会属性；证书图

中图分类号：TP393 **文献标识码：**A **文章编号：**1000-436X(2012)12-0093-07

On-demand key management based on social attribute for opportunistic networks

CHEN Xi[1,2], LI Guang-song[3], TIAN You-liang[1], MA Jian-feng[1]

(1. Key Laboratory of Computer Networks and Informatio urity (Ministry of Education), Xidian University, Xi'an 710071, China;
2. The Twentieth Research Institute of China Electronics Technology Group Corporation, Xi'an 710068, China;
3. Department of Information Research, PLA Information Engineering University, Zhengzhou 450002, China)

Abstract: An on-demand key management scheme was proposed based on social attributes, which could conform to the characteristics of intermittent connectivity, high mobility and self-organized management in opportunistic networks. By utilizing the identity-based threshold signature scheme, the authentication of nodes' social attributes was realized. Due to the specialty of the opportunistic routing protocols, nodes selectiv ly issued the identity certificates for each other to establish the Web of trust based on the matching of social attributes. Consequently, the performance of certificate graph was efficiently optimized comparing to the traditional met . Meanwhile, thanks to checking the social attribute evidences, the invalid certificate chains caused by malicious nodes were avoid to be built. Simulation result shows that, the scheme can provide high success ratio for reconstruction of certificate chains and high user reachability through low network costs in opportunistic networks.

Key words: opportunistic networks; key management; identity-based cryptography; threshold cryptography; social attribute; certificate graph

收稿日期：2011-08-30；**修回日期：**2012-02-08

基金项目：长江学者和创新团队发展计划基金资助项目(IRT1078)；**国家自然基金委员会——广东联合基金重点基金资助项目**(U1135002)；**国家科技部重大专项基金资助项目**(2011ZX03005-002)；**中央高校基本科研业务费基金资助项目**(JY10000903001)

Foundation Items: The Program for Changjiang Scholars and Innovative Research Team in University(IRT1078); The Key Program of NSFC-Guangdong Union Foundation (U1135002); The Major National S&T Program (2011ZX03005-002); The Fundamental Research Funds for the Central Universities (JY10000903001)

1 引言

随着智能手机、平板电脑等个人通信设备的普及与多样化，机会网络[1~3]受到国内外学术界越来越多的关注[4,5]。机会网络是移动自组织网(MANET)、容迟网络(DTN)和社会网络(SocialNet)等概念相结合的产物。在机会网络中，移动设备利用携带者日常活动所带来的相遇性机会进行自组织通信，并以“存储—携带—转发”的模式[6]实现消息传输与共享。与传统的 MANET 不同，机会网络并未假设节点之间存在完整的端到端路径，节点仅利用本地信息计算并选择下一跳路由，不需要获取整个网络的拓扑信息。因此，机会网络在面对恶劣环境时有着更好的可用性及适应性。与此同时，机会网络高度的自组织性、间断性与移动性对网络中节点与数据的安全保障带来极大的挑战。作为实现各种安全协议与框架的基础，密钥管理方案的设计在机会网络中显得尤为重要。

目前，还没专门针对机会网络而设计的密钥管理方案，而传统的 DTN 与 MANET 等无线网络中的密钥管理方案均无法适应机会网络。一方面，机会网络中节点身份完全平等，不存在可信第三方或认证中心对网络中节点的注册、注销及节点间的通信进行管理及保护。因此，DTN 中基于身份密码学[7, 8]使用 PKG(private key generator)对网络中节点提供安全认证的密钥管理方案无法应用于机会网络；另一方面，机会网络中的节点长期处于断路状态，其无法在有效时间内与网络中的多个节点建立连接，所以 MANET 中基于门限密码学[9, 10]的密钥管理方案也无法适用。相对于前 2 种方案，基于证书链的密钥管理方案[11, 12]更符合机会网络的自组织特性：用户自行生成公私钥对，并为可信的节点签署证书，从而建立本地证书库实现认证。然而该方案在网络规模较大时，证书数据库的生成、维护的开销都会显著增加，难以适应机会网络中节点设备低功耗的特性。而且此类方案并未给出节点间信任关系的评估方法，从而无法度量所建立证书链的可信度。因此，当网络中存在恶意节点时，会导致证书图出现大量的无效路径。

与 MANET 和 DTN 不同，机会网络兼具社会网络概念。研究表明，人们的日常行为存在规律性与周期性[13]，并可归纳为一系列的节点社会属性。如图 1 所示，机会网络路由正是通过计算移动节点携带者之间的社会属性匹配度来预测下一次可能的相遇性机会，从而选择合适的下一跳，直至将消息最终转发至目的节点[14, 15]。因此，针对机会网络的路由特性以及目前传统 DTN 与 MANET 密钥管理方案中存在的问题，本文提出了一种基于社会属性的机会网络按需密钥管理架构。本方案分为两部分：1) 通过基于身份的门限签名方案，实现节点社会属性信息的分布式认证；2) 根据节点间社会属性匹配度的不同，使用自组织密钥管理方案有选择地进行节点身份证书的签发与收集，保证证书链与路由路径建立的一致性。本方案避免了相遇概率较小的节点之间进行无用的证书颁发与交换，从而优化了节点本地证书数据库，降低了密钥管理所需的节点计算量与网络通信负载。此外，利用节点间社会属性匹配度，实现了信任可度量的证书链路，避免了潜在恶意节点可能引起的证书图路径失效问题。

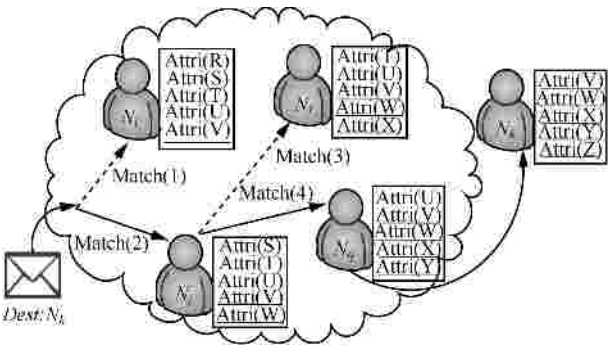

图 1 基于社会属性的机会网络路由

2 相关背景研究

目前，DTN 与 MANET 等无线网络中的密钥管理方案主要可分为三类：基于身份密码学的密钥管理方案、基于门限密码学的分布式密钥管理方案和基于证书链的自组织密钥管理方案。

2.1 基于身份密码学的密钥管理

在间歇性连通的网络环境中(如 DTN)，由于节点之间以及节点与认证服务器之间无法建立实时连接，源节点无法有效地获取并验证目的节点的公钥信息，因此传统的 PKI(public key infrastructure)架构无法正常的工作。而在身份密码学架构中，身份证和 E-mail 等可认证的身份信息被直接用作用户的公钥，而私钥由 PKG 生成，从而避免传统 PKI 中公钥证书的获取及维护。Seth[16]第一个提出了基于 IBC(identity-based encryption)的 DTN 密钥管理架构：每一个子域拥有一个域 PKG，每一个域 PKG

继承其父 PKG 的部分公钥信息。用户可问询与其最近的域 PKG 或根 PKG 获取自身的私钥，从而实现交互认证。Asokan[17]从网络负载、网络连接需求度等多方面对传统 PKI 与 IBC 架构进行了详细比较，证明 IBC 更加适合间歇性连通的网络环境，并能够有效地保证端到端的机密性。然而不同于 DTN，在机会网络中节点之间通过完全自组织的方式进行创建、加入和离开网络，并进行消息的传输与共享，不存在特定的网关或 CA (certificate authority)充当可信的 PKG。此外，机会网络中节点移动频繁，基于 PKG 的认证方式无法实现节点在不同子网内的漫游切换。

2.2　分布式的密钥管理

针对 MANET 分布式的网络架构，Zhou[18]提出了基于门限密码学的密钥管理方案。在(n,t)方案中，通过门限算法将系统的私钥分配给 n 个网络服务节点，从而实现单 CA 安全服务能力的分布式部署。当网络中新加入节点需要获得 CA 签名时，网络中任意 t 个服务节点可以协作为其生成相应的证书。Kong[19]在 Zhou 的方案的基础上进行了改进，提出了全分布的密钥管理方案：网络中每一个节点都持有部分系统私钥信息，新加入节点只需联系本地的 t 个邻居节点即可重构完整的身份证书。但此类方案暗含了一个假设：网络中大多数节点之间存在至少一条完整的通信路径，节点可在有效时间内与 t 个不同的节点建立连接并获取相应的部分签名。而在机会网络中，节点间只能通过相遇性机会建立短暂的连接，更多的时间处于断路状态。因此分布式的密钥管理方案不能满足机会网络这样高度间歇性连通的环境。

2.3　自组织的密钥管理

Hubaux[11]首先提出了自组织密钥管理方案，随后 Capkun[12]对该方案进行了详细的论证与性能仿真。类似于 PGP(pretty good privacy)，网络中节点自行生成并发布证书，通过证书链的建立实现节点间的认证。与 PGP 不同，该方案并未假设网络中存在证书目录服务器，而是由每个节点维护本地证书数据库。当节点间需进行认证时，它们首先合并对方的证书数据库，并在新生成的证书图中寻找相应的证书链路从而进行认证。Yi[20]提出了 2 种基于虚拟 CA 和证书链的复合密钥管理方案：1) 通过自组织证书链的建立来提高虚拟 CA 的覆盖范围；2) 使用经过虚拟 CA 认证的可信节点作为证书链的初始节点，从而提高证书链路的安全性。然而此类密钥管理方案在大规模的网络环境下，节点所需建立的证书链数量将呈指数增加，证书数据库的维护与查询代价很高、扩展性较差。此外，Capkun 与 Yi 的方案[12, 20]都未提及节点间的信任关系如何判定与度量。因此，若网络中存在恶意节点非法颁发证书，则可导致证书图中出现大量的无效证书链路，造成证书数据库无法正常工作。而在机会网络这样一个开放式的环境中，随时存在恶意节点加入的可能。因此，此类方案同样无法适应机会网络。

3　基于社会属性的按需密钥管理方案

本密钥管理方案分为 2 个阶段：1) 节点社会属性分布式自认证阶段，通过基于身份的门限签名方案，拥有相同属性的节点共同为自身的社会属性生成属性私钥，并分配给每一个成员，新加入的拥有该属性特征的节点通过相遇性机会获取部分签名服务，并逐步构建自身属性的签名证书；2) 基于社会属性的信任网生成及维护阶段，节点间以社会属性匹配度作为信任关系的判定标准，为可信的相遇节点颁发身份证书，并构建本地身份证书库。以下给出本方案的具体算法以及在机会网络中详细的实施方案。

3.1　社会属性分布式自认证

社会属性自认证阶段基于身份门限签名方案[21]，共由 4 个算法组成：系统公钥初始化、社会属性秘密分配、社会属性部分签名生成、社会属性完整签名生成与验证。以下分别对其进行详细的表述。

算法 1　系统公钥初始化。

设G_1和G_2为 2 个阶为大素数q的循环群，其中G_1为加群，且生成元P，G_2为乘法群。双线性映射$\hat{e}$满足$\hat{e}:G_1\times G_1\to G_2$。定义抗碰撞散列函数$H_1:\{0,1\}^*\to G_1$，$H_2:\{0,1\}^*\times G_2\to Z_q^*$。假设网络中节点在出厂时已执行以上操作，共享系统参数$sys=\{G_1,G_2,q,P,\hat{e},H_1,H_2\}$。

设网络在初始化阶段共有 n 个节点。每一个节点u_i随机选择$x_i\in Z_q^*$。同时创建$t-1$阶多项式函数$f_i(x)=a_{i,0}+a_{i,1}x+\cdots+a_{i,t-1}x^{t-1}$，其中$a_{i,k}\in Z_q^*$，且$a_{i,0}=x_i$。$u_i$计算$b_{i,k}=a_{i,k}P\ (k=0,1,2,\cdots,t-1)$，并将私钥子份额$sk_{i,j}=f_i(j)\ (j=1,2,\cdots,n)$发送给$u_j$。

节点 u_j 计算等式 $sk_{i,j}P=\sum_{k=0}^{t-1}j^k b_{i,k}$ 是否成立，从而确定私钥子份额的有效性。如果无效，u_j 广播诉讼 $suit_i$。当 $suit_i$ 的数量达到门限 T_{suit_i} 时，则 u_i 为不合格节点，系统重新进行初始化。经过以上操作，每个节点 u_j 可计算其系统私钥份额 $sk_j=\sum_{i=1}^{n}sk_{i,j}$。显然可见，系统的私钥为 $SK=\sum_{i=1}^{n}x_i=\sum_{i=1}^{n}f_i(0)$。节点 u_i 遇到节点 u_j 时，向其问询部分公钥 $Pub_j=sk_jP$。当 u_i 拥有 t 份公钥份额后，便可重构系统公钥 $Pub_{sys}=\sum_{j=1}^{t}Pub_j$。从而 u_i 可得到完整的系统参数 $SYS_i=\{G_1,G_2,q,P,\hat{e},H_1,H_2,Pub_{sys},sk_i\}$。

算法 2 社会属性秘密分配。

设网络中 n_A 个节点 u_{A_i} 拥有社会属性 A，它们可共同生成一个秘密 s_A，任意 $t_A(t_A\le n_A)$ 个节点可恢复这个秘密。首先，n_A 个节点共同执行以下操作：设 G 是由椭圆曲线上的点所构成的阶为素数 q 的群，定义一个拟多项式函数 $F:N\cup\{0\}\to G$，从 G^* 随机选择 $C_i,D_{i1},D_{i2},\cdots,D_{it_A-1},Q_1,Q_2$；从 Z_q^* 随机选择 $c_i,d_{i1},d_{i2},\cdots,d_{it_A-1},r$；其中 $Q_1=xP$，$Q_2=yP$。则对于任意的 $S\in G$，$x\in 1,\cdots,n_A$，定义函数

$$F_i(x)=C_i+xD_{i1}+\ldots+x^{t_A-1}D_{it_A-1} \tag{1}$$

$$f_i(x)=c_i+xd_{i1}+\ldots+x^{t_A-1}d_{it_A-1} \tag{2}$$

$$Com(S,r)=\hat{e}(S,P)\hat{e}(Q_1,Q_2)^r \tag{3}$$

节点 u_{A_i} 计算 $s_{A\_ij}=F_i(j)\in G$ 与 $r_{ij}=f_i(j)\in Z_q$ $(j=1,\cdots,n_A)$，并向 u_{A_j} $(j=1,\cdots,n_A)$ 发送 (s_{A_ij},r_{ij})。u_{A_i} 广播 $h_{i0}=Com(C_i,c_{i0})$ 和 $h_{ik}=Com(D_{ik},d_{ik})$ $(k=1,\cdots,t_A-1)$。节点 u_{A_j} 通过式(4)检测 (s_{A_ij},c_{ij}) 有效性

$$Com(s_{A\_ij},c_{ij})=\prod_{k=0}^{t_A-1}h_{ik}^{j^k}\quad(i=1,\cdots,n_A) \tag{4}$$

若有效性检测失败，u_{A_j} 将广播针对相关节点 u_{A_i} 的诉讼 Acc_i。当 Acc_i 的数量达到门限 T_{Acc_i} 时，则 u_i 为恶意节点，对其进行隔离处理。剩余的合格节点 u_{A_i} 广播 $j_{i0}=\hat{e}(C_i,P)$ 和 $j_{ik}=\hat{e}(D_{ik},P)$ $(k=1,\cdots,t_A-1)$。节点 u_{A_j} 通过式(5)检测广播信息的有效性

$$\hat{e}(s_{A\_ij},P)=\prod_{k=0}^{t_A-1}j_{ik}^{j^k} \tag{5}$$

若有效性检测失败，u_{A_j} 将广播相关节点 u_{A_i} 的诉讼，并对恶意节点进一步排除。网络中节点计算所分享的属性秘密 $s_{A\_j}=\sum s_{A\_ij}\in G$，并计算 $j_k=\prod j_{ik}$ $(k=1,\cdots,t_A-1)$，且设 $d=j_0$。

算法 3 社会属性部分签名生成。

节点 u_{A_j} 计算自身的社会属性 A 的私钥份额 $A_{priv\_j}=sk_jQ_{ID_A}$，其中 $Q_{ID_A}=H_1(ID_A)$，ID_A 为属性 A 的属性名。节点 u_{A_j} 通过以下方法向节点 u_{A_i} 提供部分签名服务：u_{A_j} 计算 $a_i=H_2(Q_{ID_i},d)$ 和 $b_j=a_iA_{priv\_j}+s_{A\_j}$，其中 $Q_{ID_i}=H_1(ID_i)$，ID_i 为 u_{A_i} 的公开身份信息。则节点 u_{A_j} 为节点 u_{A_i} 生成的部分签名为 $s_{A\_ji}=Sig_j(A,u_{A\_j})=(b_j,a_i)$。

算法 4 社会属性完整签名生成与验证。

通过计算 $b=\sum_{j=1}^{t_A}l_jb_j$，节点 u_{A_i} 可重构自身社会属性 A 的完整签名 $s_{A\_i}=(b,a_i)$，其中 $l_j(x)$ 为拉格朗日系数。

验证节点 u_{A_i} 的社会属性 A 的完整签名 $s_{A\_i}=(b,a_i)$ 的有效性，可先计算

$$w=\hat{e}(b,P)\hat{e}\left(Q_{ID_A},-Pub_{sys}\right)^{a_i} \tag{6}$$

若等式 $H_2(Q_{ID_i},w)=a_i$ 成立，则签名“有效”；反之，则“无效”。

通过算法 1~算法 4，节点可实现自身属性的分布式认证：网络中每个移动节点维护一份社会属性列表 *AttriTable*，用于存放自身属性的属性名 *AttriName* 以及对应的属性认证证书 *AttriCert*。在网络预热期，移动节点通过算法 1 共同为系统生成公私钥对，并持有系统参数 *SYS*。随后，拥有相同社会属性 A 的节点集合 u_{A_j}，通过算法 2 以分布式的方法为属性 A 生成一个秘密信息 s_A，并各自持有部分秘密信息 s_{A_j}。当同样拥有社会属性 A 的节点 u_{A_i} 新加入网络，u_{A_i} 通过与初始节点的相遇机会，使用算法 3 收集相关的属性签名 s_{A_ji}。当新加入节点收集到大于或等于 t_A 个签名时，其可重构属性 A 的完整签名 s_{A_i}，随后该节点将相关证书存于 *AttriTable*，用于向其他节点证明自己拥有社会属性 A 的真实性。

3.2 基于社会属性的信任网生成

1) 证书颁发：在机会网络中，移动节点自行生成身份公私钥对 *PK/SK*。当节点 u 与节点 v 出现相

遇性机会，并进入对方的安全通信区域内，u 首先向 v 问询其 $AttriName$ 列表，并计算自身与 v 之间的社会属性匹配度 $Match(u,v)$。若 $Match(u,v)$小于门限 $Thres_{attri}$，则放弃与节点 v 的通信；若大于门限 $Thres_{attri}$，则 u 进一步向 v 问询其属性证书列表 $AttriCert$，并通过算法 4 验证每一个属性证书的有效性。若属性证书认证失败，则记录该节点为恶意节点；若认证成功，则节点 u 向节点 v 颁发身份证书 $Cert_{u\_v}$，并根据匹配度 $Match(u,v)$计算证书有效期 T_{u_v} 以及证书可信度 $Relia_{u\_v}$

$$T_{u\_v} = T_{\max} \times Match(u,v) \tag{7}$$

$$Relia_{u\_v} = Relia_{\max} \times Match(u,v) \tag{8}$$

其中，$T_{\max}$ 为最大证书有效期，$Relia_{\max}$ 为证书最大可信度。身份证书 $Cert_{u\_v}$ 的结构为

$$Cert_{u\_v} = Sig_u(ID_u, ID_v, k_v, T_{u\_v}, Relia_{u\_v})$$

证书 $Cert_{u\_v}$ 代表节点 u 相信节点 v 的所宣称的公钥 k_v 与其身份 ID_v 的绑定(ID_v,k_v)的真实性。

2) 证书的收集与合并：在网络预热期，节点 u 与相遇的每一个合法节点进行证书的互换与合并，收集尽可能多的证书信息，以便有效地建立证书链捷径，扩大本地证书库 G_u 的认证范围。当网络进入正常运转期后，节点本地证书数据库趋于饱和，只有当相遇节点与自身的属性匹配度 $Match(u,v)$大于门限 Th_{attri} 时，才进行身份证书图的互换与合并，从而避免大量无用证书的导入所造成的网络传输负载与本地证书数据库查询认证的计算负载。

3) 证书数据库更新：当目标节点的证书过期时，颁发者需等待下一次相遇性机会，并重新计算自身与目标节点之间的属性匹配度 $Match(u,v)$。根据 $Match(u,v)$，设定新的有效期 T_{u_v} 及可信度 $Relia_{u\_v}$。此外，节点 u 对自身身份证书数据库 G_u 中每一条证书边 E 维护一个计数器 $Counter_E$。若证书边 E 在更新周期内参与节点认证的次数小于门限 Th_{join}，则对其进行删除以提高数据库运行效率。

4) 证书吊销：若网络中移动节点的私钥出现泄露、节点被侵占或节点与自身公钥的绑定关系出现变化时，需主动对节点的公钥进行吊销。证书吊销可通过证书颁发者进行吊销，也可通过证书拥有者自行进行吊销。对于移动节点公私钥对的周期性变更以及证书过期所引起的证书吊销，可通过节点间相遇性机会将吊销信息 $Revoke_{\text{request}}$ 逐步在网络中进行传播。而对于私钥泄露与节点被侵占所引起的证书吊销，网络中节点必须对该类 $Revoke_{\text{request}}$ 进行无偿、及时的转发，以便尽早通知证书的其他使用者，防止恶意节点利用已泄密节点的私钥为同谋节点颁发证书。

5) 证书冲突：若网络中节点 u 的本地证书库 G_u 中存在多条可达节点 v 的证书链 $chain(u\_v)$，而通过不同的证书链进行验证，获取到的节点 v 的公钥证书不同，即证书信息出现冲突时，节点 u 需分别计算多条证书链的可信度，选择可信度最高的证书链所验证的公钥证书作为 v 的有效公钥，并对其余证书链中节点的公钥信息提前进行证书更新，从而去除本地证书库中存在的无效、错误证书。这里，证书链 $chain(u_v)$的可信度定义为

$$Relia_{chain(u\_v)} = \prod_{i \in chain(u\_v)} Relia_{u\_i} \tag{9}$$

其中，i 为证书图中 $chain(u_v)$所经过的顶点。

4　性能仿真

本节使用 ONE 仿真器[22]对方案进行了模拟仿真。实验场景方面，选取了芬兰首都赫尔辛基的部分实体街道地图，大小为 3 800m×3 000m。选用 Working Day Movement[23]作为节点移动模型，并参用文献[23]的相关场景设置，以便真实地模拟用户日常活动中的行为模式。设网络中移动节点数量为 200，其中 160 个初始节点，剩余 40 个节点为新加入节点，需要与 t 个初始化节点进行通信，以便获取系统公钥参数。每 15 个节点共享相同的社会属性，其中 10 个节点共同为该属性产生密钥，剩余 5 个节点需收集 t_A 份的部分属性证书，从而重构自身社会属性证书。节点的步行速度为 0.8~1.6m/s，车辆的行驶速度为 8~12m/s。移动节点之间只可通过蓝牙接口进行通信，通信半径为 10m，数据传输速率为 150~250KB/s。社会属性证书自生成阶段预热期为 1h；对于节点信任网生成阶段，设系统证书图为 $G(V,E)$，节点 u 的本地证书子图为 G_u，alg 为本地证书库生成算法，$size$ 为本地证书库大小。定义证书链重构成功率 $Succ$[12]为

$$Succ(G,alg,size) = \frac{\left|\left\{(K_u,K_v) \in V \times V : K_u \to_{G_u \cup G_v} K_v\right\}\right|}{\left|\left\{(K_u,K_v) \in V \times V : K_u \to_{G} K_v\right\}\right|} \tag{10}$$

如式(9)所示，证书链重构成功率 $Succ$ 代表相遇节点合并证书子图后，能够成功重构系统证书图中所存在的认证链路的概率。

图 2 比较了本文所提出的按需密钥管理与经典的自组织密钥管理两种方案的证书链重构成功率 *Succ*。其中门限 t=15，t_A=4，$size \in [10,70]$，*alg*=*Maximum Degree*[12]。此外，通过 Certificate Graph 模型[24]构造人工系统证书图，系统运行时间为 3h。如图 2 所示，由于按需密钥管理方案只为消息路由有可能经过的节点生成证书链路，因此只需维护较小的本地证书图。在节点存储受限的情况下，可提供较高的证书链重构成功率。而自组织密钥管理方案，由于周期性向邻居节点收集证书，存储了大量低利用率证书。在本地证书库大小受限时，证书链重构成功率很低。此外，由于人工证书图有着更为显著的小世界特性[25]，同方案下人工证书图较随机图有着更高的证书链重构成功率。

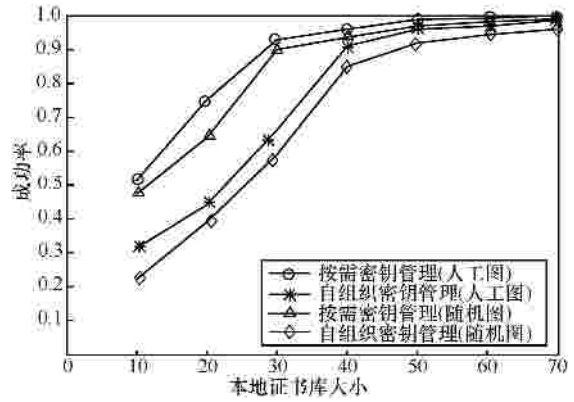

图 2 证书链重构成功率

图 3 给出了移动节点本地证书库中，门限 t_A 的变化对于节点平均认证可达率 *UR* 的影响。节点认证可达率 UR_u 定义为：与节点 u 社会属性匹配度大于或等于 50%的节点中，u 可以在本地证书库中查询到相应认证链路的概率。设 $SIMI_u$ 代表网络中与节点 u 社会属性匹配度大于或等于 50%的节点集合，则

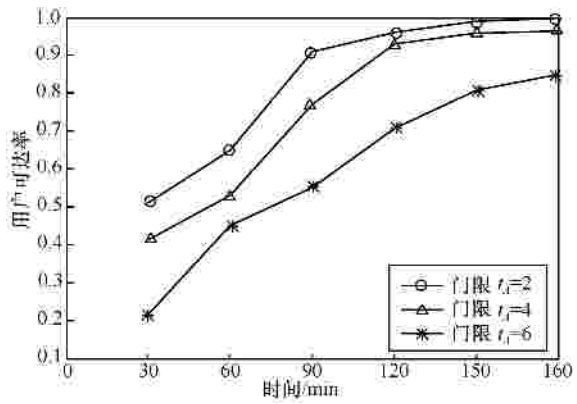

图 3 节点平均认证可达率

$$UR_u = \left|\left\{K_u \to_{G_u} K_v, v \in SIMI_u\right\}\right| / \left|SIMI_u\right| \quad (11)$$

$$UR = \sum UR_u / |u| \quad (12)$$

如图 3 所示，在门限 $t_A \le 4$ 时，网络中节点维持了较高的平均认证可达率。但是当 t_A 为 6 时，节点平均认证可达率 *UR* 有较大幅度的下降。因此，选择合适的门限对本方案十分重要。

表 1 对比了按需密钥管理方案与自组织密钥管理方案在节点本地证书图平均最短路径长度以及节点最大通信负载[12]等方面的差异。在按需密钥管理方案中，由于移动节点只与自身有着较大社会属性匹配度的节点颁发并交换证书，避免了相关度较低的节点之间建立长证书链路，证书链的平均最短路径长度较低，节点本地证书图呈现更高的聚合性。另一方面，虽然属性证书的自认证增加了部分通信开销，但由于降低了需颁发及交换证书的候选节点数量，本地证书库所需维护的证书数量大幅减少。因此，方案所需的总体通信负载降幅明显。

表 1 性能比较

方案	平均最短路径	最大通信负载
按需密钥管理	5.81	25
自组织密钥管理	6.23	36

5 结束语

本文提出的基于社会属性的按需密钥管理方案实现了机会网络中完全分布式的自组织密钥分发与维护。本方案首先基于身份与门限密码学，完成了网络中节点社会属性的自认证。随后，节点通过可验证的社会属性信息计算自身与其他节点的社会属性匹配度，并以此作为信任网建立的基线，生成本地认证证书库。相对于传统的自组织密钥管理，本方案去除了节点间不必要的证书颁发与证书图合并，并避免了潜在恶意节点可能引发的证书链失效问题。消息路由路径与节点信任链路径建立方式的一致性保证了节点本地证书数据库运行的高效与消息传输的安全。实验仿真表明，在门限选择合适的情况下，本方案生成的证书图聚合度高、平均最短路径小，只需较低的计算与通信负载便可实现高效的节点间交互认证。

本方案在初始化阶段，仍然需要较长的预热期。如何利用节点的社会属性信息，构建可在短时间内产生小世界现象的机会网络证书图，是下一步需要研究的工作。

参考文献：

[1] PELUSI L, PASSARELLA A, CONTI M. Opportunistic networking: data forwarding in disconnected mobile ad hoc networks[J]. IEEE Communications Magazine, 2006, 44(11): 134-141.

[2] CONTI M, GIORDANO S, MAY M, *et al*. From opportunistic networks to opportunistic computing[J]. Communications Magazine, IEEE, 2010, 48:126-139.

[3] CONTI M, KUMAR M. Opportunities in opportunistic computing[J]. Computer, 2010, 43(1): 42-50.

[4] SCOTT J, HUI P, CROWCROFT J, *et al*. Haggle: A networking architecture designed around mobile users[A]. Proc of the Third Annual IFIP Conference on Wireless On-Demand Network Systems and Services (WONS)[C]. 2006.

[5] HUI P, CHAINTREAU A, SCOTT J, *et al*. Pocket switched networks and human mobility in conference environments[A]. Proc of ACM SIGCOMM Workshop on Delay-Tolerant Networking[C]. 2005. 244-251.

[6] ZHANG Z. Routing in intermittently connected mobile ad hoc networks and delay tolerant networks: overview and challe ges [J]. IEEE Communications Surveys & Tutorials, 2006, 8(1): 24-37.

[7] SHAMIR A. Identity-based cryptosystems and signature schemes[A]. Proc of the CRYPTO 84 on Advances in Cryptology[C]. New York. Springer-Verlag, 1984. 47-53.

[8] BONEH D, FRANKLIN M K. Identity-based encryption from the Weil pairing[A]. Proc of the 21st Annual International Cryptology Conference on Advances in Cryptology[C]. London: Springer-Verlag, 2001. 213-229.

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

[10] FELDMAN P. A practical scheme for non-interactive verifiable secret sharing[A]. Proc of the 28th Annual Symposium on Foundations of Computer Science[C]. 1987. 427-438.

[11] HUBAUX J P, BUTTYAN L, CAPKUN S. The quest for security in mobile ad hoc networks[A]. Proc of the 2nd ACM International Symposium on Mobile Ad Hoc Networking & Computing[C]. New York, USA, 2001. 146-155.

[12] 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.

[13] NGUYEN H A, GIORDANO S, PUIATTI A. Probabilistic routing protocol for intermittently connected mobile ad hoc network (PROPICMAN)[A]. Proc of the IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks(WoWMoM)[C]. 2007. 1-6.

[14] BOLDRINI C, CONTI M, JACOPINI J, *et al*. HiBOp: a history based routing protocol for opportunistic networks[C]. Proc of the IEEE International Symposium on World of Wireless Mobile and ultimedia Networks(WoWMoM)[C]. 2007. 1-12.

[15] VERMA A, SRIVASTAVA A. Integrated routing protocol for opportunistic networks[J]. International Journal of Advanced Computer Science and Applications, 2011, 2(3): 85-92.

[16] SETH A, KESHAV S. Practical security for disconnected nodes[A]. Proc of the First Workshop on Secure Network Protocols (NPSec)[C]. 2005. 31-36.

[17] ASOKAN N, KOSTIAINEN K, GINZBOORG P, *et al*. applicability of identity-based cryptography for disruption-tolerant networking[A]. Proc of the 1st International MobiSys Workshop on Mobile Opportunistic Networking[C]. New York, 2007. 52-56.

[18] ZHOU L, HAAS Z. Securing ad hoc networks[J]. IEEE Networks, 1999, 13(6):24-30.

[19] KONG J, ZERFOS P, LUO H, *et al*. Providing robust and ubiquitous security support for mobile ad-hoc networks[A]. Proc of the 9th International Conference on Network Protocols[C]. 2001. 251-260.

[20] YI S, KRAVETS R. Composite key management for ad hoc networks[A]. Proc of the 1th International Conference on Mobile and Ubiquitous Systems: Networking and Services[C]. Urbana, USA, 2004. 52-61.

[21] BAEK J, ZHENG Y. Identity-based threshold signature scheme from the bilinear pairings[A]. Proc of the International Conference on Information Technology: Coding and Computing (ITCC'04)[C]. 2004. 1-124.

[22] KERÄNEN A, OTT J, KÄRKKÄINEN T. The ONE simulator for DTN protocol evaluation[A]. Proc of the 2nd International Conference on Simulation Tools and Techniques[C]. 2009. 2834-2838.

[23] EKMAN F, KERÄNEN A, KARVO J, *et al*. Working Day movement model[A]. Proc of the 1st ACM SIGMOBILE Workshop on Mobility models[C]. New York, 2008.

[24] HUBAUX J P, BUTTYAN L, CAPKUN S. Small worlds in security systems: an analysis of the PGP certificate graph[A]. Proc of the ACM New Security Paradigms Workshop[C]. New York, USA, 2002. 28-35.

[25] MILGRAM S. The small world problem[J]. Psychology Today, 1967, 2(1): 60-67.

作者简介：

陈曦（1984-），男，浙江绍兴人，西安电子科技大学博士生，主要研究方向为机会网络、安全协议设计、可信计算等。

李光松（1977-），男，山东德州人，解放军信息工程大学讲师，主要研究方向为无线网络安全、密码算法设计与分析等。

田有亮（1982-），男，贵州盘县人，西安电子科技大学博士生，主要研究方向为博弈论、安全协议分析及分布式密码体制等。

马建峰（1963-），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为信息安全、容忍入侵与无线网络安全等。