分类号：_____ 密级：_____

U D C：_____ 编号：_____

工程硕士学位论文

（在职人员）

移动 Ad Hoc 网络中信任模型的研究

硕士研究生 ：花向东

指导教师 ：李健利 副教授

企业导师 ：刘美茹 教 授

学位级别 ：工程硕士

工程领域 ：计算机技术

所在单位 ：哈尔滨铁道职业技术学院

论文提交日期：2008 年 3 月

论文答辩日期：2008 年 6 月

学位授予单位：哈尔滨工程大学

摘　要

移动 Ad Hoc 网络是一种新型的无线网络，它不需要现有网络基础设施的支持，可以在任何时间、任何地点，快速构建起一个通信支撑环境。但由于其自身的开放媒质、动态拓扑、分布式协作和受限能力等特点，移动 Ad Hoc 网络极其容易受到攻击。所以安全问题是移动 Ad Hoc 网络中的基本问题，也是当前该领域的研究热点之一。而信任关系的建立是所有安全策略实施的基础，所以本文重点研究移动 Ad Hoc 网络中的信任模型。

本文讨论了移动 Ad Hoc 网络的基本概念、特点、安全需求及安全威胁。通过对现有的移动 Ad Hoc 网络中的信任模型的深入研究，发现现有的信任模型存在很多仅依靠传统安全策略无法解决的问题，如身份信任关系的建立、撤销等缺乏决策标准；行为信任模型中普遍缺少身份信任的保障等。

为了解决这些问题，本文提出了一种基于 PKI 的分级移动 Ad Hoc 网络信任模型，本模型与已有模型相比，具有如下特点：

（1）将身份信任和行为评估机制有机的结合起来：身份信任关系的建立增强了行为信任评估过程的安全性和可信性；反之，行为信任评估为实现节点的身份信任关系更新、撤销，进一步增强认证过程的安全性、可靠性，提供了决策依据。

（2）把 PKI 体系中 CA 服务功能分为数字证书生成和数字证书维护两部分。节点离线地获得证书进入网络，既减轻了 Ad Hoc 网络的负担，也提高了 CA 的安全性；数字证书的更新、撤销工作在 Ad Hoc 网络中来完成。

针对多频分级结构的 Ad Hoc 网络，模型采取集中式和分布式相结合的混合模式，在簇头节点间采用门限密码的思想，分布式存储系统的证书更新主密钥，提高了系统的安全性。簇头负责簇内的安全和路由，对簇内节点的安全性实施有效的控制，提高了安全服务的可用性、可控性。

（3）改进信任度维护算法，用“撤销系数”调整网络的安全性和可靠性，用“恢复系数”降低了恶意节点的影响，有效地控制了信任评估中的不确定因素。

最后，对改进后的信任模型的安全性进行了分析和评估。

关键词：移动 Ad Hoc 网络；信任模型；身份认证；密钥管理；信任度

Abstract

Mobile Ad Hoc networks (MANET) are new paradigm of wireless networks, which can be quickly put up to provide mobile communication without any underlying infrastructure anytime and anywhere. However, wireless MANET is particularly vulnerable due to its fundamental characteristics, such as open medium, dynamic topology, distributed cooperation, and constrained capability. Security is essential for MANET, and it is also one of the hot areas in MANET research nowadays. Because that the establishment of trust relation is the basis to implement all the security policies, this dissertation focus on the trust model for Mobile Ad Hoc networks.

The foundational conception, features, security requirements and security threats of MANET are introduced. Thorough research of the trust models for Mobile Ad Hoc Networks. Finding that there are many problems that can not be solved through traditional security policies: such as the establishment and revocation of identity trust relationship lack of decision standard; In behavior trust model it is not ensure of identity trust at large.

In order to solve these problems, A trust model based on PKI of hierarchy MANET is introduced. It has characteristic as follows:

(1)This dissertation integrates identity trust and the trust evaluation mechanism: the establishment of identity trust relationship, it boosts security and creditability of the trust evaluation mechanism; contrarily, creditability of the trust evaluation mechanism provide decision-making gist for updating and revocation of identity trust relationship, and for boosting up security and dependability of authentication process more.

(2)CA function of PKI system is disparted two parts, nodes digital certificate making and maintenance. Nodes enter into network gaining digital certificate non-line. It not only mitigate burden of MANET, but advance security of CA; updating and revocation of digital certificate are completed in Ad Hoc network.

Contraposing various frequencies hiberarchy of MANET, the trust model takes mix mode of integrating muster mode and distributing mode, The model introduce share a secret in cluster-headers, certificate updating system secret key

are distributed storage, enhancing the security of system; Cluster-headers is responsible to the security and routing, actualizing effective control to security of cluster member, enhancing the usability of the security service.

(3) Thesis improves arithmetic of evaluation and maintenance for digital certificates trust identity, the security and reliability of MANET can be adjusted by revocation coefficient, the effect of hostility node can be debased by comeback coefficient, these can be control the incertitude complication of the trust evaluation mechanism availably.

Finally, this dissertation analyzes and evaluates the security of the improved trust model.

Keywords: Mobile Ad Hoc networks; Trust model; Identity authentication; Key management; Trust degree

哈尔滨工程大学

学位论文原创性声明

本人郑重声明：本论文的所有工作，是在导师的指导下，由作者本人独立完成的。有关观点、方法、数据和文献等的引用已在文中指出，并与参考文献相对应。除文中已经注明引用的内容外，本论文不包含任何其它个人或集体已经公开发表的作品成果。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律结果由本人承担。

作者(签字)：花向东

日 期：2008 年 6 月 19 日

第1章 绪论

1.1 课题研究目的和意义

近几年来，无线网络在支持移动性方面的发展非常迅速，它为人们的生活带来了诸多的便利。现阶段常见的移动网络是以蜂窝网络或者无线局域网等形式出现的，它需要一些基础设施予以支撑，如机站、接入点等等。移动 Ad Hoc 网络的出现打破了这一制约，它是无线局域网的一种特殊模式。这是一种自组织的无线多跳网，整个网络中没有固定的基础设施，也没有固定的路由器，所有节点都是可移动的，并且能以任意的方式动态地保持与其它节点之间的联系。在这种环境下，由于移动终端的无线覆盖范围的有限性，两个不在彼此无线传输范围内的移动节点无法直接进行通信，需要中间节点的转发。这时，中间节点不仅是一个移动主机，它还充当了一个路由器的角色，它要寻找和维持到其它节点的路由并转发消息分组。

随着人们的通信需求的不断增加，以及移动通信终端设备的不断发展，通信服务质量成了一个亟待解决的问题。如何实现“无论何时、无论何地”的即时通信也就成了现今学者研究的热点。

移动 Ad Hoc 网络，由于其无需固定基础设施支持、能够快速简单组网，且能够自组织、自修复，正在成为下一带无线网络的有力竞争者。目前，无线移动 Ad Hoc 网络已经从军事化向民用化发展，在不久的将来它的应用范围可以覆盖工业、商业、医疗、家庭、办公环境、军事等各种场合。

但是，由于移动 Ad Hoc 网络的自组织、自管理，采用无线信道通信，网络拓扑结构动态变化等特性，使得 Ad Hoc 网络中移动节点较固定节点而言更易受到各种网络攻击，例如，攻击者更容易通过无线链路来窃听、假冒、篡改和重放网络上传输的信息；动态的拓扑结构，使得攻击者更容易干扰节点之间交换的路由刷新信息；路由算法需要多个节点之间合作，有些不可信节点可能拒绝合作，终止路由转发，引起网络通讯中断等。所以 Ad Hoc 网络的安全问题尤为突出，传统的解决方案已经不再合适，必须研究新的安全解决方案来实现移动 Ad Hoc

网络中的安全通信。

目前对移动 Ad Hoc 网络的安全研究主要集中在：信任模型、密钥管理、安全路由、入侵检测、可用性等几个方面。而信任关系的建立是安全通信的前提，所有安全策略实施的基础，所以本文重点研究信任模型的建立。

1.2 信任模型的研究现状

目前文献中提出的移动 Ad Hoc 网络信任模型，大致分为两类：一类主要完成网络节点间的身份认证，证书管理；另一类则主要完成节点间的行为信任，以实现网络中的安全路由。

1.2.1 基于身份认证的信任模型研究现状

移动 Ad Hoc 网络安全研究领域，对实现 Ad Hoc 网络中节点的身份信任多采用分布式认证方法。

基于 Shamir 提出的(k，n)门限秘密共享技术[1]，Zhou 和 Haas 最早提出了 Ad Hoc 网络中的部分分布式认证方案[2]。此方案将 Ad Hoc 网络节点分为三类：客户端、服务器和组合节点。客户端是一般的网络节点，服务器和组合节点都是证书授权机构 CA(Certification Authority)的一部分。服务器负责产生部分证书，并存储所有节点的证书。组合节点负责组合部分证书产生有效的证书。在网络初始化阶段，一个特殊的服务器节点产生证书签名私钥的 n 个分量，并分发给 n 个服务器节点。组合节点只有组合任意 k 个部分证书才能为客户端产生有效的证书。

此方案适用于有计划的、长期的 Ad Hoc 网络。从功能方面来看，此方案要求存在管理机构，以创建网络并给等待加入网络的节点颁发有效证书；缺乏证书回收机制，而且基于网络中的一个节点子集愿意并且能够作为服务器节点的假设；证书的生成依赖于一个组合节点，一旦组合节点被攻破，整个网络将失去安全保障；网络中只有 n 个固定的服务器节点拥有私钥分量，在网络拓扑结构变化时，必须考虑网络分割问题，确保每个客户端都能获得至少 k 个证书服务器的服务。

完全分布式认证[3][4]与部分分布式认证不同的是，方案将一个 RSA 证书签名密钥分量分发给网络中所有节点。有新节点要求加入时，拥有私钥分量的 k 个节点可以合作为新节点生成新的私钥共享分量。此方案设计了证书回收的方法：假设所有节点能够监测一跳范围内邻居的行为。如果节点 A 发现一个邻居节点 B 有

恶意行为，则将其证书加入到自己的证书撤销列表(CRL)中，并在网络中发布对B的指控。任何一个收到指控信息的节点首先从自己的CRL中查看是否存在A的证书，如果存在，就忽略这个指控；如果不存在，则将B定义为怀疑节点；当收到关于B的k个指控时，就将B的证书加入到自己的CRL中。

此方案也是适用于有计划的、长期的Ad Hoc网络。由于将私钥分量分配给网络中的所有节点，所以不再需要专门的服务器节点，但同样需要管理机构的参与，以完成网络的初始化过程。该方案提出了基于恶意行为的证书撤销机制，但并没有明确定义恶意行为。将私钥分量分配给网络中的所有节点，增强了系统的可用性，但也将共享秘密更多的暴露给攻占者，增加了系统的危险性。

考虑到Ad Hoc网络带宽有限，移动终端计算能力低等特点，有人提出了一种基于IBE (Identity-based Encryption，基于身份的加密)和秘密共享的分布式密钥管理和认证方案[6]。方案由分布式密钥产生和基于标识的认证两部分组成。分布式密钥产生部分负责产生网络主公/私钥对(Q_M，SK_M)和每个节点的公/私钥对。主私钥由所有节点协作产生，并以(k，n)门限方式共享，主公钥则由公式$Q_M = \sum_{i=1}^{n} S_i P$计算得到，其中$S_i$为每个节点拥有的主私钥分量，P为IBE加密模型中使用的公共参数，主公钥对网络中所有节点公开。每个节点的私钥也由k个节点合作产生。认证部分完成节点间的身份认证和通信保密性。一旦认证成功，通信双方可以交换会话密钥，以用于进一步的通信。

该方案与RSA等公钥方法相比具有更小的计算和通信开销。但主私钥完全由网络节点分布式产生，缺乏信任基础，存在很大的安全隐患，例如，无法抵御中间人攻击和冒充攻击。每个节点的公钥可以从节点的身份标识直接获得，省去了证书的产生、分发和存储的开销，然而，这也意味着节点的私钥无法进行更新。由网络中k个节点为节点产生私钥增加了通信开销，也引入了新的安全隐患。另外，该方案也没有考虑秘密分量验证、秘密分量更新等安全因素。

自颁发证书管理模型[7]的基本思想是由用户自己产生私钥和证书，不需要任何CA的参与。该方案适用于自发的Ad Hoc网络。网络中节点没有优先级关系。并且不需要初始化阶段和管理中心，因此可用于无状态网络。由于它不基于公钥加密，因此不需要节点有很强的计算能力。

该方案中建议的证书选择算法基于短途搜寻算法。该算法是基于著名的小世

界理论，并且该算法仅仅保证获得一条证书链的可能性。

每个用户存储有限数量的证书。这些证书被分为三类：

(1)用户发行给别人的证书。

(2)别人发行给用户的证书。

(3)其它证书。

显然，每个用户很容易知道并存储出自己发行的证书。例如：A 发行证书给 B，然后本地存储该证书。然后通知 B， A 给它发行了一张证书，B 于是存储该证书。通过这种方式，很容易获得前两个证书库的证书。第三类证书通过一定的算法来选择。

虽然自颁发证书管理的理论基础很好，但还存在很多不合理因素：假定信任是可以传递的；通信双方的证书链只是概率的存在，尤其是在网络最初建立阶段，存在图中两个节点不可达的情况；为了保证任意通信双方都能够建立信任关系，每个节点保存的证书数量会随着网络中节点数目的增加而急剧增多，这给网络节点的存储能力和检索能力提出了很高的要求：由于没有可信方的参与，没有明确的信任保证，且信任度会随着证书链的延长迅速降低；恶意用户可以通过伪造大量的证书来破坏网络的安全。

另外，针对高度自发性的、规模较小的移动 Ad Hoc 网络，有人提出基于口令验证的身份认证方法，解决的是类似网络会议这样的情况。人们要在一个房间(或者在较小的区域)内召开移动 Ad Hoc 网络会议，他们之间很熟悉并相互信任。用户希望在会议期间建立安全的无线网络，除了与会成员之外的其他人不能获得会议中的任何信息。基于口令验证的密钥交换是一种面向群组的方法，它不进行单个节点的验证，也没有处理节点的加入和离开的问题。

1.2.2 基于行为评估的信任模型研究现状

行为信任评估本质上就是通过收集和处理实体行为的证据信息，获得经验，并以此为依据作出信任决策。因此，一般行为信任模型多以行为信任评估的方法为依据进行分类。由于信任的不确定性特征，行为信任评估一般都采用不确定性推理和概率论的方法。

有研究者提出了基于权重的信任传递方法[9]，对不同推荐路径的推荐信任值进行加权平均。评分的权重由评分者的可信度/信誉、评分的产生时间、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，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。

概率论非常符合信任模型中证据收集过程的需求。Beth 等人[9]首先将信任分为直接信任和推荐信任，利用概率统计的方法计算信任值，并提出了信任的合成方法。Yao Wang 等人用贝叶斯网络来解决信誉问题，通过计算二元评分(正或负)的条件概率值来评估信誉，但并没有考虑信任的主观性和随时间衰减等特性[10]。贝叶斯网络以概率论中的贝叶斯定理为计算基础，是不确定性推理的常用方法之一，为计算信誉值提供了准确的理论基础。由于其计算时的先验概率、充分性量度、必要性量度等值多由专家经验给出，有些文献中称之为主观贝叶斯方法。然而，这种方法过份依赖专家经验，主观性较强，在移动 Ad Hoc 网络环境中很难实现。另外，当网络节点数目增多时，需要计算的条件概率数量会迅速增加，很难收敛而得到信誉值。因此，贝叶斯网络的方法很难应用于移动 Ad Hoc 网络环境中的信任建模。

刘玉龙等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[11]。

该信任评价模型由直接信任值和推荐信任值得出对实体的整体信任值。但该模型并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。

还有研究者以信息论为理论基础评估信任[12]，利用熵表示信任的不确定性。该模型同样以贝叶斯公式为理论基础计算实体间的直接信任值，并且考虑了信任随时间衰减的因素。但该模型没有考虑多于两路的推荐信任合成的问题，不满足信任合成的结合率，无法处理同时来自多方的信任推荐，也没有明确区分直接信任与间接信任。

基于概率的不确定性推理方法不能处理“无知(ignorance)”的情况，而证据理论对无知的处理则非常深刻的反映了信任不确定性的本质特征。但是，此类模型并没有克服证据理论合成的固有缺陷，当证据冲突时会产生极不合理的结果。

George 等人[13]提出的模型中，把信任评估问题看作是带权重的有向图 G(V，E)(信任图)上的最短路径问题，分别利用基于路径的半环和基于距离的半环传递与合成信任。在基于路径的半环中，向量(t，c) (trust value， confidence value)表

示信任，其中 confidence value 代表信任评估的质量。

在基于距离的半环中则用(c/t，c)表示信任。该模型的信任只基于直觉上的需求，缺乏理论基础，而且信任的产生只基于本地观察也不够完整。

鉴于 Ad Hoc 网络的特殊性和重要性，自 20 世纪 90 年代后期开始，国内的一些大学和研究所开始关注 Ad Hoc 网络技术，并对它进行了一些研究。比如:解放军理工大学、清华大学、西安电子科技大学、北方交通大学等。目前国内对 Ad Hoc 网络进行研究的现状是比较零散、缺乏统一的规划和协调，没有相应的官方或民间组织来协调大家的研究工作。由于 Ad Hoc 网络技术在民用领域尚无广泛的应用，国家对 Ad Hoc 网络技术的关注和支持力度有限。

1.2.3 现有模型存在的主要问题

现有的两类信任模型都是希望通过建立节点间的信任关系解决移动 Ad Hoc 网络中的安全问题，但它们都只关注身份信任或行为信任的一个方面，而忽略了另一方面，不够完善。主要问题表现在：

(1)目前 Ad Hoc 网络中的身份信任模型要么缺乏信任基础，要么基于全局时间同步的假设，很难实现。另外，一些证书撤销方法只简单的利用指控计数，缺少信任依据和评估标准。

(2)在行为信任的建模方法中，所提方案或存在明显的缺陷，或不适用于 Ad Hoc 网络环境。同时，行为信任评估模型中普遍没有身份信任和通信保密性的保障，很难实现安全、准确的信任评估。

(3)现有的模型主要针对有计划性、长期的Ad Hoc网络，即出于将Ad Hoc网络建成主干网络的考虑。作为一种特殊的通信网络技术，Ad Hoc网络确实具有很多独有的特点，这使得它在很多特殊场合的应用具有独特的优势。但必须认识到，Ad Hoc网络并不是一种广域网络的解决方案，因此不可能像GSM、CDMA 等那样成为主流的移动通信技术。由于整个网络具有移动性和无中心性，它也不可能像因特网那样成为覆盖全球的网络系统。

1.3 论文研究的主要内容和组织结构

由于 Ad Hoc 网络本身在安全方面的弱点以及应用环境的多样性，使得处理和解决它的安全问题非常困难。所以，当前的着眼点应是借鉴有线网络领域内取

得的经验，针对具体的 Ad Hoc 网络中某些致命和特殊的安全威胁进行深入细致的研究，设计一些行之有效的安全措施和机制，以解决实际网络环境中不断遇到的安全攻击和隐患。

本文主要针对 Ad Hoc 网络应用于军事、抢险救灾等领域，该类 Ad Hoc 网络中的节点和网络协议虽然是以分布式和 P2P(Peer-to-Peer)的形式运行，但逻辑上有一个统一的管理和控制机构，相应的也有统一的安全规定或纪律。这种类型的 Ad Hoc 网络安全环境的特定和基础条件为：一般会有公共的服务节点和基础安全保障(如物理上的保障)；节点间具有安全协作责任，普通节点间的差异性不大；可能会有大规模的协同攻击，安全风险很大[14]。

这种Ad Hoc网络比较适合采用多频分级的体系结构。多频分级的体系结构是指将网络划分为簇(cluster) ，每个簇由一个簇头(cluster - header) 和多个簇成员(cluster member) 组成，这些簇头形成高一级的网络。用不同的频率实现不同级的通信，低级节点的通信范围较小，而高级节点要覆盖较大的范围[15]。如图1.1就是一个双频的两级网络。

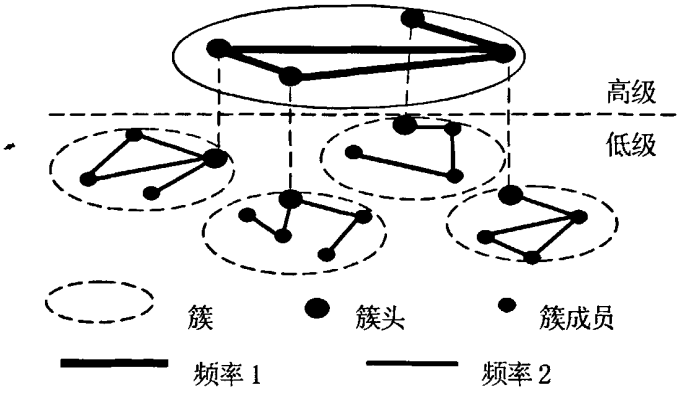

图1. 1 双频分级结构Ad Hoc网络

本文研究的Ad Hoc网络采用以上体系结构，网络中的信任模型采用一种中心式与分布式相结合的混合模式。为了获得安全服务的有效性，簇内管理采用的是中心式的模式，由簇头节点管理。簇头节点是具有良好性能的设备，并且是相对独立的，它们之间采用分布式管理，以减小单点失效带来的危害。

本文认为身份信任与行为信任是互相联系、互为补充的，可以将两种模型有

机的整合在一起，以更好的实现移动 Ad Hoc 网络环境中的通信安全。

身份信任关系的建立是一切后续安全机制实施的前提。没有彼此间身份的信任，一切安全措施都是没有保障的。然而，在移动 Ad Hoc 网络的分布式环境中，有些安全问题仅依赖身份信任是无法解决的。例如利用指控方式实现证书撤销时，在没有信任保障的情况下，很难防止网络节点的恶意指控行为发生。因此，本文的信任模型将有机地结合身份信任与行为信任评估机制，在基于 PKI 的身份信任模型中引入行为信任评估机制，以节点行为信任度值描述节点的行为，更好的实现网络节点间的身份信任，从而更好的实现移动 Ad Hoc 网络环境中的通信安全；同时，行为信任还可以解决身份信任无法解决的路由安全问题。

本文具体的章节安排如下：

第 1 章 简要介绍本课题研究的目的和意义；分析现有信任模型的优缺点和所存在的问题；最后，给出本文的主要工作和组织结构。

第2章 介绍移动Ad Hoc网络的背景知识、应用、特点及其脆弱性；深入分析Ad Hoc网络的安全需求和安全威胁。

第 3 章 深入研究移动 Ad Hoc 网络的安全策略和关键技术。

第 4 章 在前面研究、分析的基础上，改进基于 PKI 的移动 Ad Hoc 网络身份信任模型，引入行为信任评估机制，更好的实现网络中信任关系的建立、更新、撤销等服务；给出信任度维护算法。

第 5 章 对改进的信任模型的安全性进行分析与评估。

最后总结本文的研究工作，并对今后的工作进行展望。

第2章 移动Ad Hoc网络面临的安全问题

Ad Hoc 网络是一种由移动节点组成的临时性自治系统。作为一种无线移动网络，Ad Hoc 网络和传统的移动网络有着许多不同，其中一个主要的区别就是Ad Hoc 网络不依赖于任何固定的网络设施，而是通过移动节点间的相互协作来进行网络互联。目前 Ad Hoc 网络主要应用于军方和对安全敏感的环境中，以及在一些需要紧急组网的情况下。同时移动 Ad Hoc 网络也正逐步应用于商业环境中，比如传感器网络、虚拟教室和家庭网络。由于这种网络具有一些特殊的特点，使得 Ad Hoc 网络的安全问题尤为突出。

2.1 移动Ad Hoc网络简介

Ad Hoc一词来源于拉丁语，是“特别地，专门地为某一即将发生的特定目标、事件或局势而不为其他的”的意思。它强调的是多跳、自组织、无中心的概念，所以国内一般把Ad Hoc网络译为“自组网”，或者“多跳网络”等等。Ad Hoc网络起源于20世纪70年代的美国军事领域，它是在美国国防部DARPA(Defense Advanced Research Project Agency)资助研究的“战场环境中的无线分组数据网(PRNET）”项目中产生的一种新型的网络。DARPA当时所提出的网络是一种服务于军方的无线分组网络，实现基于该种网络的数据通信。后来，DARPA 又于1983年和1994 年分别资助进行了抗毁可适应性网络（SURAN：Survivable Adaptive Network）和全球移动信息系统（GloMo，GlobalInformation Systems）两个项目的研究，以便能够建立某些特殊环境或紧急情况下的无线通信网络。Ad hoc网络就是吸取了PRNET、SURAN 以及GloMo等项目的组网思想，从而产生的一种新型的网络。

目前所提到Ad hoc网络继承和发扬了DARPA所资助的无线分组数据网的思想，特别是PRNET。PRNET强调的是在一个广阔的区域实现多跳的无线通信，基于这种多跳的无线信道特点，PRNET面临着诸如媒质接入、寻址、路由、网络初始化和控制等难题。但PRNET所倡导的系统自组织（self-organizing）特性使得PRNET网络系统组建灵活，网络的抗破坏性强。

简而言之，移动 Ad Hoc 网络是一组无线移动节点的集合，这些移动节点可以在没有任何网络基础设施和集中化管理的情况下进行通信。网络中不需要任何类似于基站或者移动交换中心这样的集中化控制设施。移动 Ad Hoc 网络为用户提供了不受限制的移动性和连通性，整体网络具有移动性；在相同的网络规模下，节点的发射功率较低；支持多种网络无线通信技术和随时随地的数据传输。正是由于移动 Ad Hoc 网络不需要任何的固定基础设施，所以要组建这种网络是非常灵活和方便的。图 2.1 是移动 Ad Hoc 网络的一个例子。

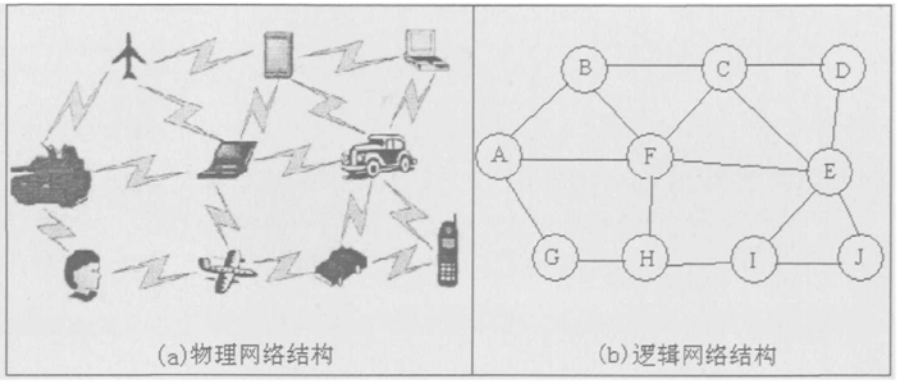

图 2.1 移动 Ad Hoc 网络的结构示意图

由于移动 Ad Hoc 网络的特殊性，它的应用领域[15-18]与普通的通信网络有着显著的区别。它适合被用于无法或不便预先铺设固定网络基础设施的场合、需快速自动组网的场合等。针对 Ad Hoc 网络的研究是因军事通信应用而发起的。因此军事应用仍然是移动 Ad Hoc 网络的主要应用领域。同时在民用和商用领域，移动 Ad Hoc 网络也有着非常广阔的应用前景，它可支持移动商务、移动会议、移动办公、个域网络、自然或人为灾难营救过程中的信息交换以及临时交互式通信等。可以预测，移动 Ad Hoc 网络在未来的移动通信领域将扮演非常重要的角色。

(1) 军事通信。军事应用是移动 Ad Hoc 网络技术的主要应用领域。因其特有的无需架设网络基础设施、可快速展开、抗毁性强等特点，它是数字化战场通信的首选技术。Ad Hoc 网络技术已经成为美军战术互联网(Tactical Internet)的核心技术，美军的近期数字电台(NTDR，Near-Term Digital Radio)和无线互联网控制器等主要通信装备都使用了 Ad Hoc 网络技术。据报道，在美国对伊拉克战争中，移动 Ad Hoc 网络得到了有效的应用。

(2)紧急和临时场合。因发生了地震、水灾等自然灾害或其它各种原因而导致固定的通信网络基础设施被破坏或无法正常工作时，快速恢复通信是非常重要的。借助于移动 Ad Hoc 网络技术，可快速建立临时网络，从而为灾难营救赢得时间，以减少其带来的危害。类似的，当处于边远或偏僻野外地区时，同样无法依赖固定或预设的网络设施进行通信，Ad Hoc 网络技术的独立组网能力和自组织特性，是在这些场合进行通信的最佳选择。

(3)传感器网络。传感器网络是 Ad Hoc 网络技术的另一大应用领域。对于很多应用场合来说传感器网络只能使用无线通信技术，而考虑到体积和节能等因素，传感器的发射功率不可能太大。使用 Ad Hoc 网络实现多跳通信是一种非常实用的解决方法。分散在各处的传感器组成 Ad Hoc 网络，可以实现传感器之间和与控制中心之间的通信。这在爆炸残留物检测等领域有广阔的应用前景。

(4)移动会议。目前，越来越多的人携带笔记本电脑、个人数字助理(PDA)等各种便携式设备参加各种会议。如果与会者不用借助路由器、交换机或基站等网络设施，就能将各种移动终端快速地组建成临时的无线移动 Ad Hoc 网络，从而完成提问、交流、资料分发等各种任务，无疑将具有重要的现实意义。当在室外某个环境时，同样可以借助移动 Ad Hoc 网络来协同完成某项任务。

(5)移动商务。移动商务[19, 20]利用各种移动设备，通过无线网络收发信息，从而完成各种交易。它不是当前有线网络中电子商务的简单模仿，由于移动商务的概念与商务运作无所不在的特点有着天然的耦合性，其必将在未来的时间里取代传统的电子商务，以提供无线信息服务、无线网络接入服务、语音提示服务、基于位置信息的服务和数字化内容服务。通过提供更加丰富的个性化服务，从而制造一个全新价值的网络经济。

(6)个域网络。个域网络(PAN，Personal Area Network)是移动 Ad Hoc 网络技术的另一应用领域。其不仅可用于实现 PDA、手机、掌上电脑、手提电脑等个人电子通信设备之间的通信(如蓝牙技术中的超网[21])，还可用于个域网之间的多跳通信，用以建立更大范围的网络互联。

(7)与移动通信系统的结合。Ad Hoc 网络还可以与蜂窝移动通信系统相结合，利用移动节点的多跳转发能力扩大蜂窝移动通信系统的网络覆盖范围，均衡相邻小区的业务，提高小区边缘的数据速率等[22, 23]。

在实际应用中，移动 Ad Hoc 网络除了可以单独组网实现局部通信外，还可

以作为末端子网通过网关或接入点接入其它的固定或移动通信网络，与 Ad Hoc 网络以外的主机进行通信。因此，Ad Hoc 网络也可以作为各种通信网络的无线接入手段之一。

2.2 移动Ad Hoc网络的特点及其脆弱性

但由于 Ad Hoc 网络具有开放媒质、动态拓扑、缺乏中心授权、分布式合作、受限的网络能力等基本特点，使其特别容易受到攻击。

较之有线网络和传统的无线网络，移动 Ad Hoc 网络具有其自身的一些特点，而这些特点决定了移动 Ad Hoc 网络特别容易受到攻击。下面分析移动 Ad Hoc 网络的主要特点以及由此引起的网络脆弱性[15-18]。

(1) 在移动 Ad Hoc 网络中，所有的信息都通过带宽受限的无线链路传输。这一点使得 Ad Hoc 网络的物理安全难以保证，没有充分物理保护的节点易于被捕获、损害和破坏。攻击者可能会窃听无线链路，从而试图获得秘密信息，这违反了保密性原则；攻击者也可能主动干扰无线信道，对传输中的数据进行删除、修改、重放等操作，甚至插入错误的信息或者伪装成一个合法节点，这违反了服务可用性、数据真实性和完整性、不可否认性等原则。

(2) 移动 Ad Hoc 网络的拓扑结构是动态变化的。移动中的主机可以独立漫游，随时加入或者离开网络。节点同它们的邻居之间的关系是暂时的而不是长久的，其信任关系不断变化。在大多数情况下，人们难以清晰地描绘网络中的成员关系；尤其在大规模的网络中，假设能在大多数节点之间建立一种信任关系是不现实的。所以，在这种拓扑结构动态变化的网络中，不能简单应用一些静态的安全解决方案。在移动 Ad Hoc 网络的大部分路由协议中，节点之间交换关于网络拓扑结构的信息，然后在源节点和目的节点之间建立一条路由。那么攻击者就可以伪造一个合法的路由变化信息，从而给出不正确的更新。比如说一个恶意节点可以用错误的路由信息拥塞网络，发起拒绝服务攻击。

(3) 移动 Ad Hoc 网络中没有中心支持基础设施。所以，基于公钥密码学和证书授权的认证难以在该网络中实现。同时，在 Ad Hoc 网络中不能建立一个防御线，也难以区分可信任的节点和不可信任的节点。也不可能假设所有的节点都有一个安全联盟。

(4)在移动 Ad Hoc 网络中，控制不是集中的，它依赖于所有节点的合作参与。网络中的任何节点都不可能单独支持网络的某个特定功能。这时，恶意节点就可以通过拒绝合作来中止合作算法，从而使网络不能正常运行。一些集中化的入侵检测机制也不能使用。

(5)移动 Ad Hoc 网络能力受限。这一点包括两个方面：一是移动节点的处理能力和计算能力有限，这使得一些移动节点无法或者难以进行复杂的公钥密码运算；二是移动节点大部分都是由电池供电的，这样，一些攻击者可以通过强迫一个节点重放分组或进行一个复杂运算等手段，耗尽节点的电能，从而发起一种特殊类型的拒绝服务攻击。

从上述讨论中，可以清楚地看到：移动 Ad Hoc 网络由于具有开放媒质、动态拓扑、缺乏集中化管理、资源受限等特点，其本身是不安全的，要达到其安全性是极其困难的。下面分析移动 Ad Hoc 网络可能存在的一些安全威胁和安全目标。

2.3 移动Ad Hoc网络的安全威胁及安全目标

由于无线 Ad hoc 网络具有如前所述的不同于传统网络的特点，必然会带来一些新的安全威胁。虽然传统的安全机制，例如认证协议、数字签名和加密，在实现 Ad hoc 网络的安全目标时依然具有重要的作用。但由于这些新威胁的来源不同，表现的攻击行为以及对网络通信的影响也不一样，因此，应根据不同的安全威胁提出不同的安全策略，以满足不同的安全需求。

对于网络的攻击一般可分为主动攻击和被动攻击两种[24]，分别来自于不同的攻击者。在无线 Ad hoc 网络中，攻击者主要是以下三种类型的节点之一：恶意节点(malicious nodes)、妥协节点(compromised nodes)、自私节点(selfishnessnodes)，有时也将这些节点统称为行为不端的节点(misbehaving nodes)。

恶意节点包括网络内部的和外部的节点，一般通过主动攻击(如:更改路由信息、伪造数据包、假扮合法节点等)来实现干扰路由协议的正常功能、散布假消息、妨碍信息的获取等目的；妥协节点通常是指拥有合法用户身份的网络内部节点，它们掌握着一些诸如群组密钥一类的共享秘密，通过主动攻击来危害整个网络的通信；自私节点也是指网络的内部节点，它们是无线 Ad hoc 网络特有的一类攻击

者，通过不参与网络的基本操作(例如，不转发数据包)而严重地降低网络性能，甚至可能导致网络被分割。

无线 Ad hoc 网络受到的安全威胁主要包括两个方面：外部威胁和内部威胁[25]。外部威胁一般是由恶意节点发起的被动窃听，或者主动攻击(例如，拒绝服务攻击、假冒合法节点的欺骗攻击等)。它一般通过标准安全机制如防火墙、加密认证机制来防范。内部威胁通常来自于妥协节点或者自私节点的攻击。它对网络的危害要比外部威胁大。一般要结合其他的安全技术如数字签名、认证和入侵检测等进行防范。

根据无线Ad hoc网络的特点，安全威胁所针对的对象主要是路由和共享秘密。针对路由的威胁，首先是因为网络没有固定的拓扑结构，节点进行通信往往要重新发现路由、修改路由。这个过程很可能被恶意节点利用，通过包截取、包撤销、包重发、包篡改、包伪造等途径实现攻击，导致网络路由不能及时更新或者产生错误的路由信息而使网络不能正常通信。其次是由于资源的有限性，带来自私节点对路由的威胁。例如黑洞攻击(blackhole attacks)就是因自私节点不执行包转发等基本网络操作，导致某些节点始终不可达，同时源站也没有收到任何告知发送失败的返回消息，这时自私节点就像一个黑洞。另外，还有合谋的恶意节点给路由带来的威胁，如蠕虫洞攻击(wormhole attack)。两个合谋的意节点通过私自的网络连接创建一个蠕虫洞，利用其将数据包或路由信息包在转发过程中故意绕过某个节点，使得某个节点始终不可达。这种攻击可能造成多于两跳的路由无法被发现。

针对共享秘密的威胁，主要是因为传输媒介的共享性，致使信道上的任何消息都可能被窃听，使虚假的消息也可以被随意插入。所以攻击者可能利用密码分析等方法来获取共享秘密，如得到私钥或者共享密钥等，从而破坏消息的保密性、完整性。

针对上面所指出的安全威胁，移动Ad hoc网络的安全需求主要包括[24,26]：认证性、保密性、完整性、可用性和抗抵赖性。

(1) 认证性：使每个节点能够确认与其通信的节点身份。如果没有认证，攻击者很容易冒充某一节点，从而得以获取重要的资源和信息，并干扰其他节点。

(2)保密性：保密性是保证特定的信息不会泄露给未经授权的用户。像有关军事战略或战术上的敏感信息在网络上传输，必须机密、可靠。否则这些信息被敌

方破获，后果将不堪设想。路由信息在有些情况下也必须保密，因为这些信息可能被敌方用来识别和确定目标在战场上的位置。

(3)完整性：完整性保证信息在发送过程中不会被中断。如果没有完整性，在网络中的恶意攻击或无线信道干扰都可能使信息发送中断。

(4) 可用性：可用性就是指网络服务对用户而言必须是可用的， 也就是确保网络节点在受到各种网络攻击时仍然能够提供相应的服务。这里的网络攻击主要是指拒绝服务攻击。在Ad Hoc 网络中拒绝服务可以发生在任何一层上：在物理层和媒体接入层，攻击者可以通过无线干扰来扰乱物理通信信道；在网络层，攻击者可以攻击路由协议；在高层，攻击者可以攻击各种高层服务。针对Ad Hoc 网络还有一种叫做"剥夺睡眠"的特殊的攻击，这种攻击使得移动节点的电池很快耗尽，从而达到拒绝服务的目的。

(5)抗抵赖性：抗抵赖性可以确保一个节点不能否认它已经发出的信息，它对检查和孤立被占领节点具有特别重要的意义。当节点A接收到来自被占领节点B的错误信息时，抗抵赖性保证节点A能够利用该信息告知其他节点，B已被占领。

以上列出了移动 Ad Hoc 网络应该达到的一些基本的、必须的安全需求。这些安全需求需要通过一些密码技术来实现，比如说可以利用证书和数字签名、用户认证、端--端加密、生物特征、用户识别码、口令、入侵检测、接入控制、审计追踪、病毒扫描、防火墙等标准安全技术。

2.4 本章小结

在本章中，首先介绍了移动 Ad Hoc 网络背景及其应用前景，分析了该网络的特点并指出该网络特别容易受到攻击，已有的一些针对有线网络和传统的无线网络的安全解决方案不能直接应用在移动 Ad Hoc 网络中。接着，分析了移动 Ad Hoc 网络的可能存在的一些安全威胁和一些安全需求。可以看出，要保护移动 Ad Hoc 网络的安全需要很大的努力。在设计一个 Ad Hoc 网络安全解决方案时，应该根据不同的应用场合，要考虑满足尽可能多的网络安全需求，并且将网络的安全风险降至最低。

第3章 建立信任模型的关键技术研究

和其它网络一样，移动 Ad Hoc 网络也要提供可靠性、权威性、完整性、不可抵赖性、可用性等安全服务。获得这些安全服务的方法就是采用适易的安全机制。安全机制的目标是建立一个安全的移动 Ad Hoc 网络，而信任关系是所有安全策略实施的基础。针对不同的移动 Ad Hoc 网络环境，需要有不同的安全策略。随着移动 Ad Hoc 网络技术的发展，越来越多的移动 Ad Hoc 网络应用被开发出来。因此，针对不同的网络应用，已经提出了许多关于移动 Ad Hoc 络的安全解决方案。对这些安全策略进行深入分析和研究，是提出改进的信任模型的基础。

3.1 PKI技术的研究

公开密钥基础设施(PKI，Public Key Infrastructure)是信息安全基础设施的一个重要组成部分，是一种基于公开密钥理论与技术建立起来的安全体系，是为网络用户、设备提供信息安全服务的具有普适性的信息安全基础设施，是一组建立在公开密钥算法基础上的用来创建、管理、存储、分发和吊销公钥的硬件、软件、人员、策略和过程的集合。该体系在统一的安全认证标准和规范基础上提供在线身份认证，核心是要解决信息网络空间中的信任问题，确定信息网络空间中各主体的安全利益。

3.1.1 PKI 技术

PKI 是为适应网络开放环境应运而生的一种技术，是一套比较完善的网络安全解决方案。作为一种技术体系，PKI 可以作为支持真实性、完整性、保密性和不可否认性的技术基础。PKI利用公钥技术，采用证书管理公钥，通过 CA 把用户的公钥和用户的其他标识信息捆绑在一起，实现密钥和证书的自动管理，为用户建立起一个安全、可信的网络运行环境，使用户可以在多种应用环境下方便地使用加密和数字签名技术，从技术上解决网上身份认证、信息保密性、完整性和抗否认性等安全问题。

在实际应用中，PKI 体系可被划分为客户端部分和服务端部分。

客户端是证书的用户或者是已经被颁发证书的主题，是 PKI 体系的使用者，主要是对 PKI 体系中公钥算法的应用；服务端则是 PKI 体系的管理者，主要运行 PKI 体系中公钥管理的各种管理服务：认证中心 CA 负责发行和撤销证书。注册中心 RA 负责建立证书主题标识，实现主题和它的证书间的映射。注册功能也可以由 CA 完成，因此 RA 是一个可选组件。

PKI 包含如图 3.1 的组件：

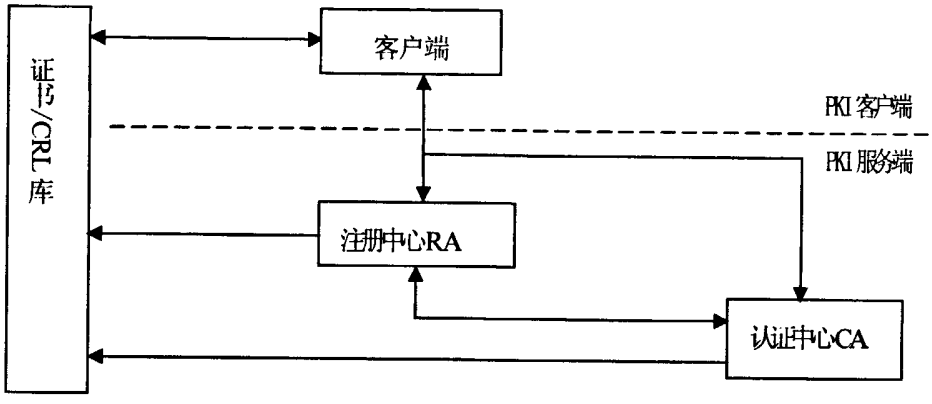

图 3.1 PKI 的主要组件

PKI 应该提供的基本服务是：注册，初始化，证书，密钥更新，证书撤销及证书和撤销通知分发。PKI 也提供其它服务。包括：密钥恢复，密钥产生，交叉认证，安全时间戳和不可否认性等。

(1)注册

注册服务建立实体和公钥映射。需要提供的信息包括：对 RA 的公钥和用于证书的信息。例如：姓名，e-mail 地址，组织等。RA 也需要端实体证明它拥有相应的私钥，例如：产生数字签名。RA 需要验证来自端实体的信息。这要求端实体出示身份标识，如身份证。最后，当 RA 已经验证了端实体的标识，它联系 CA 请求产生证书。

(2)初始化

在端实体能够使用 PKI 服务之前，它的证书信息必须被初始化。其中最重要的一项是要包含 CA 的公钥，用来验证任何 CA 颁发的证书。其它的信息包括证书库的地址和其它用户会与之联系的 PKI 组件的地址。初始化也包括端实体公/

私钥对的产生。

(3)证书颁发

一旦收到来自 RA 的请求，CA 产生并签署证书。该过程包括：填充 RA 提供的信息和添加额外需要的信息。CA 最后用自己的私钥 skCA 对证书进行数字签名。

(4)密钥更新

密钥对仅仅在有限时间内有效。密钥更新服务提供传送一个新的密钥对并发行相应证书的功能。

(5)证书撤销

CA 负责维护它发行的证书的状态。例如，某个证书由于私钥被暴露而变成无效证书，CA 需要撤销该证书。如果证书中包含的信息变得无效，也需要撤销证书。

(6)撤销通知的颁发

证书被发行后，需要使得该证书对拥有者和希望使用它的用户都是可用的。CA 产生证书后，它有很多种方式分发。例如：通过公共可访问服务器或者直接提供给证书拥有者。在证书被撤销的情况下，PKI 必须提供机制通知证书的使用者。通常的方法是 CA 发行一个证书撤销列表 CRL，列出所有已经被撤销的证书。证书使用者通过 CRL 检查证书是否仍然有效。由于 CRL 是定期发行的，因此在证书被控制和被撤销之间可能存在一定的延迟。解决该问题可以通过提供在线 CRL 允许用户实时查询证书状态。

3.1.2 PKI 技术应用于 Ad Hoc 网络中的研究

虽然 PKI 技术在 Internet 中得到了飞速发展，并取得了良好的应用效果。但 Internet 是一种较为宽松的网络，并未对 PKI 体系的应用形成限制，而 Ad Hoc 网络是一种受限性非常强的网络，因此，需要调整 PKI 体系来达到 Ad Hoc 网络的要求。

PKI 体系的核心是 CA 服务，但 CA 体系是 PKI 体系的服务端部分，因此需要结合 Ad Hoc 网络对 PKI 体系的要求，对 CA 体系进行技术上的改进，使其适合 Ad Hoc 网络应用，保障 Ad Hoc 网络安全。但其思想体系，即管理方式，则无需太多的变动[57]。

Ad Hoc 网络节点在初始化进入网络之前可以和 CA 取得联系，一旦进入网络后，由于网络的动态性，很难再按照预期的目标同 CA 发生联系以获取 CA 服务。CA 服务包括：数字证书申请与颁发、数字证书更新、数字证书撤销和数字证书验证。因为数字证书申请与颁发需要对节点进行审核，是一个离线操作，可以放在节点初始化工作过程中完成。若数字证书的更新、撤销工作能在 Ad Hoc 网络中来完成，则网络节点经过初始化进入网络后，将无需再与 CA 发生联系。

这样就把 CA 的工作分为：数字证书生成和数字证书维护两部分。数字证书生成就是数字证书申请与颁发，属于网络节点的初始化阶段，因此可以脱离 Ad Hoc 网络单独来运行；数字证书维护就是对数字证书的更新、撤销或者信任度进行维护管理，属于后期维护阶段，因此需要在 Ad Hoc 网络内运行。

本文中阐述的离线的可信任机构完全独立于 Ad Hoc 网络体系，负责网络节点的初始化工作，审核节点的真实性，并为节点生成数字证书。对于数字证书的维护工作则由维护算法在 Ad Hoc 网络运行阶段中实现。

3.2 基于信任分散的安全策略的研究

在 Ad Hoc 网络中所有的节点都容易受到攻击，也容易被俘获。如果在 Ad Hoc 网络中采用一个 CA 来管理整个网络节点的公开密钥，若该 CA 节点被俘获，则整个网络就会崩溃。所以此时的安全策略就是：将这种对一个 CA 的信任分散到对若干个节点的共同信任，即信任分散。

门限加密方案通过秘密共享解决了信任分散问题。秘密共享允许秘密在一组用户中共享，然而任何单个用户从秘密分量中无法推导出系统秘密。只有足够数量秘密分量联合方能够重构系统秘密。n 个分量持有者中有 k 个分量就可以重构系统秘密的机制称为(k，n)门限机制。并且秘密共享方案被不断的改进以获得更高的安全性。下面分析秘密共享方案及其扩展。

3.2.1（k，n）门限秘密共享方案分析

(k，n)门限秘密共享方案[11]基于拉格朗日插值多项式。该方案的基本思想是将秘密 S 分成 n 份(每份称为秘密分量或影子)，每个用户掌握其中的一份。任意大于或等于 k 个用户合作方可以恢复秘密 S，而任意小于 k 个用户合作则无法得到关于 S 的任何信息。具体算法是：

(1)设 GF(P)是一个有限域，S 是一个秘密，令 $S=a_0$，可信中心随机选取 $a_1,a_2,\cdots a_{k-1}\in GF(P)$，构造一个 GF(P)上的 k-1 次多项式，如式（3-1）：

$$f(x)\equiv a_0+a_1x+a_2x^2+\cdots+a_{k-1}x^{k-1}(\mathrm{mod}\,p) \tag{3-1}$$

(2)可信中心在 GF(P)内选择n(n<p)个非零的、互不相同的元素 x_1，x_2 …，x_n，其相应的函数值为 $f(x_i)$，$0\leq$ 。

(3)将 $(x_i,f(x_i))$ 分配给 n 个秘密共享者。

(4)恢复秘密时，只需n个秘密共享者中的 k 个提供他们的参数 $(x_i,f(x_i))$，得到 k 个 k 元线性方程组，即可解出 S，如式（3-2）：

$$S=f(0)\equiv\sum_{i=1}^{k}f(x_i)l_i(0)(\mathrm{mod}\,p) \tag{3-2}$$

式中：$l_i(x)=\prod_{\substack{i=1\\ i\neq j}}^{k}\frac{x-x_j}{x_i-x_j}$。

这类(k，n)门限体制具有以下特点：

(1)在分享秘密的成员总数 n 不超过 p 的条件下可以增加新成员，即计算新的秘密份额不会改变已有的秘密份额。

(2)通过选用常数项不变的另一个 k-1 次的新多项式，可以将某个成员的秘密份额作废，除非他可以找到 k-1 个成员的秘密份额构成该新多项式。

(3)可以根据成员重要性不同分给不同个数的秘密份额，实现分级方案。

(4) 秘密的恢复算法，其计算复杂度仅为 $O(t^3)$。

3.2.2 可验证的秘密共享方案分析

门限秘密共享方案存在一个很大的安全隐患：只有重构出私钥以后，才能通过公钥验证签名的正确性，而无法对私钥分量进行验证。只要存在一个虚假或错误的密钥分量，就不能重构出正确的私钥。一旦生成的私钥错误，就必须重新收集私钥分量进行计算。这使得 Byzantine 攻击非常有效，即通过不断提供不同的假私钥分量破坏认证私钥的生成。

为了改进缺少验证机制的缺陷，出现了可验证秘密共享方案(VSS，Verifiable Secret Sharing)[28]该方案的秘密共享方法是(k，n)门限秘密共享方法，安全性基于计算离散对数难题。

设p、q为素数，且q | (p-1)，g为Z_P中阶为q的元素。与门限秘密共享方案类似，系统先为每个成员产生秘密共享分量$S_i=f(x_i)$，多项式为$f(x)=\sum_{j=0}^{k-1}a_j x^j$。秘密分配者广播所有的$\delta_j = g^{a_j} \bmod p$。每个秘密共享者可以通过公式(3-3)，验证秘密分量的正确性。

$$g^{s_i} = \prod_{j=0}^{k-1} \delta_j^{v_i^j} \tag{3-3}$$

3.2.3 加密函数签名方案分析

门限秘密共享方案还有一个安全隐患存在于系统私钥重组阶段。如果密钥重组节点被攻破，则攻击者就可以获得私钥重组所需的k个分量，或者直接获得系统私钥。为了克服这个缺陷，熊焰等人提出了基于多跳步加密签名函数的分布式认证方案[29]。该方案同样基于(k，n)门限秘密共享的方法，但利用RSA算法构造签名函数以防止私钥泄露。首先计算$m=h^d \bmod n$，其中h是随机数，n为RSA算法中的参数而非(k，n)门限秘密共享中的n；d为RSA算法中的私钥，e为RSA算法中的公钥。则生成的加密的签名函数为式（3-4）：

$$f_{signed}(u) = m^{(u)} \bmod n \tag{3-4}$$

对于一个被签名信息x，只需计算式（3-5）：

$$z = f_{signed}(x) = m^x \bmod n = (h^d)^x \bmod n = (h^x)^d \bmod n \tag{3-5}$$

检验签名正确性，先计算：$y=h^x \bmod n$，再用公钥e验证等式$y=z^e \bmod n$是否成立即可。

设网络中拥有私钥分量的节点为(v_1，v_2，…，v_n)，需要信息认证的节点C将需要被签名的信息发送给节点v_1。v_i首先构造加密的签名函数，如式（3-6）：

$$f_{signed}(u) = (h^{S_i})^u \bmod n \tag{3-6}$$

式中：S_i——为v_i所拥有的私钥分量

利用签名函数为C的信息进行签名，然后发送给节点v_2。v_2执行同一过程，然后将v_1、v_2签名后的信息发送给下一节点。直到v_k执行完同一过程，即对C的信息签名完毕，由v_k将签名后的信息发回给C。

该方案为防范循环移动攻击，还加入了私钥分量刷新过程；并利用协同一致算法[30]来发现并清除网络中具有 Byzantine 行为的恶意节点。

基于多跳步加密签名函数的分布式认证方案能够保护私钥分量和认证私钥不外泄，有效抵御假冒攻击。

3.2.4 主密钥分量更新方案分析

门限秘密共享方案另一个安全隐患就是容易受到移动攻击者(Mobile Adversaries)[31]攻击，即在一个足够长的时间内，攻击者可以攻击 k 个秘密分量持有者，获得 k 个秘密分量，重构秘密。为了抵御这种攻击，又有研究者提出了主动秘密更新(Proactive Secret Update)方案。其大致思路是在不改变秘密的前提下，对秘密分量进行周期性的更新。不同时间窗口内的秘密分量不能合并重构出秘密。

目前，基于同步网络环境下的主动秘密更新方案是研究比较多、比较重要的一种方案[32]，大致可以分为以下三部分：

1．初始化：过程与基本门限秘密共享方案相同，先将秘密分量 $S_i=f(v_i)$ 分配给 n 个用户，其中秘密为 $S=f(0)$。在时间窗 t 内，秘密分量记作 $S_i^{(t)}$，t=0，1，…，相应的多项式记作 $f^{(t)}(u)$；

2．秘密分量更新：通过增加一个常数项为零的随机多项式 $\delta(u)$ 更新 $f^{(t)}(u)=(f^{(t-1)}(u)+\delta(u))\bmod p$，其中 $\delta(u)$ 满足 $S=S+0=f^{(t-1)}(0)+\delta(0)$，则更新后的秘密分量为 $S_i^{(t)}=f^{(t)}(v_i)$；

3．秘密分量恢复：该方案要求主动秘密更新系统必须能够识别系统中丢失或损坏的分量，并在必要时恢复正确的秘密分量。

该协议假设网络能安全地传送信息。另外，为了证明新分量的正确性，协议中需要增加分量验证机制。

3.3 信任的基本理论

日常生活的每个方面都直接或隐含的包含着信任的因素。信任是人类的一种主观意识，其各种表现形式很容易识别出来，但要严格的定义和理解信任却非常困难[33]。Marsh 指出对信任的研究主要来自社会学、(社会)心理学和哲学三个领域[34,35]。

这里引用 X.509 的 2000 年版对信任的定义为(X.509,3.3.54)："一般说来，

如果一个实体假定另一个实体会严格地像它期望的那样行动，那么就称它信任那个实体。”其中的实体是指在网络或分布式环境中具有独立决策和行动能力的终端、服务器或智能代理等[36]。由此定义可见，信任包含了一种关系以及对该关系的期望。而期望是一个主观概念，对这种期望可以使用信任度（即信任水平）的概念。

3.3.1 信任与安全的关系

信任与安全是两个联系非常紧密的概念。在计算机网络中，传统安全机制的目的是抵御外部攻击，保护系统和数据不受恶意和未授权方的破坏。其安全目标概括为认证性、保密性、完整性、抗否认性、可用性。但在新型的开放式、分布式网络和在线电子商务环境中，还存在来自资源(信息)提供者和内部恶意成员的破坏[32]，例如，Ad Hoc 网络内部节点的“自私”行为，被攻破节点提供错误路由信息的行为等。传统的安全机制无法抵御这些新型的安全威胁，信任机制则是解决这些安全问题的有效手段。

本文将基于证书或标识的对实体身份的信任称为身份信任，将基于实体行为和信誉的对实体能力、可靠性等属性的信任称为行为信任。身份信任确保行为信任评估的安全性、准确性，是后续安全机制实施的基础；行为信任为身份信任关系的安全建立、更新及撤销提供保障。可见，信任中也融入了传统安全的因素，二者互为补充、不可分割[37]。

3.3.2 信任的相关术语

由于信任含义的复杂性、多面性，使得这个研究领域的术语也缺乏一致性[28]。为了叙述清晰、准确，现对本文涉及到的与信任相关的术语介绍如下：

(1)信誉：被全局所了解并接受的一个实体的性质或名望称为信誉[32]。信誉基于团体的推荐或评估，而信任则是个体的、主观的现象。信任通过综合个体直接经验和推荐或信誉获得。在信任的产生过程中，个体直接经验显然要比推荐或信誉重要，但在缺少个体直接经验的情况下，信任通常要基于信誉获得。

(2)信任值(信任度)：表示实体之间信任等级的数值称为信任值。

(3)信任推荐：实体 M 明确的将自己对客体 B 的信任值传递给主体 A 的过程称为信任推荐。信任推荐基于信任的条件传递性和主体 A 对实体 M 的信任。

(4)直接信任：主体 A 通过与客体 B 的直接交互经验获得的对 B 的信任值。

(5)间接信任：主体 A 通过其他实体对客体 B 的信任推荐获得的对 B 的信任值。

(6)信任模型：通过形式化的方法描述信任，并通过特定算法计算实体间信任值的模型。信任模型通常由信任表述、信任度量和信任度评估等元素构成。

(7)信任锚：信任模型中，当可以确定一个身份或者有一个足够可信的身份签发这个证明其签发的身份时，才能做出信任那个身份的决定。这个可信的实体称为信任锚[36]。

在一个网络环境中实体间建立安全通信的实质是通信双方之间信任关系的确立，如何建立这些信任关系将依赖于不同的网络应用环境和安全策略，需要采用不同的信任模型来实现。信任模型为信任关系的建立和管理提供了一种框架，它描述了如何建立这些信任关系，以及寻找和遍历信任路径的规则。

3.4 本章小结

本章首先分析了传统网络中 PKI 的体系结构及其应该提供的基本服务，指出 Ad Hoc 网络是一种受限性非常强的网络，因此，需要调整传统网络中的 PKI 体系来达到 Ad Hoc 网络的要求。通过深入分析，提出了在 Ad Hoc 网络中布设 PKI 服务体系应注意的问题，并着重研究了在 Ad Hoc 网络中 PKI 技术的改进；然后深入研究了(k，n)门限秘密共享技术及其扩展方案；最后由于信任概念的不统一，介绍了本文应用到的信任概念。

第4章 基于PKI的分级移动Ad Hoc网络信任模型

经过分析和研究，本文设计了针对多频分级结构的移动 Ad Hoc 网络信任模型。模型参照部分分布式模型的体系结构，继承了秘密共享的信任分散方式，采取集中式和分布式相混合的安全机制。其中身份信任关系的建立、更新、撤消参照 PKI 的证书管理机制，引入行为评估机制为证书更新、 撤销、主私钥分量更新和路由选择等做决策的依据。

4.1 模型概述

4.1.1 模型的设计思路

第 1 章研究了很多已有安全解决方案，有基于密钥交换的，有基于 PGP 的，有基于信任分散的。可以看出基于信任分散的秘密共享建立身份信任是其中比较好的一种方案。然而，现有的分布式方案都存在这样或那样的问题，主要包括：有些算法为了追求安全性，设计过于复杂，已经很难在 Ad Hoc 网络环境下实现；有些算法的实现需要基于过多的假设，而这些假设在现实环境中是不可能成立的；还有一些算法只关注信任关系建立的某些方面，而忽略了其他因素(例如，没有信任更新、撤销机制)，不够完善。另外，节点因自私原因而不运行服务和节点服务的安全问题仍无法解决。

由于 Ad Hoc 网络的组建通常有着特殊的应用目的，如：军事战场、抗灾救险等，因此其网络安全管理应是集中可控的，以克服网络底层节点自由加入的混杂性。另外从网络运行和管理角度而言，也希望网络安全是集中可控的，这样便于对网络管理，且在必要时能实现对网络的全局控制。对全局可控的信任模型的一个具体实现是CA体系，它已在传统的Internet网络安全中取得了良好应用效果，且已成为一个维护网络安全的标准。对 Ad Hoc 网络来说，采用 CA 体系作为其网络安全的信任基础还具有下列优点：

(1)CA 体系是对全局可控信任模型一种很好的实现，其思想体系已相对比较完善和成熟，可以直接引入 Ad Hoc 网络中。因为信任模型和其实现更确切地来

说是一个管理上的问题，而非技术上的问题。因此若采用一个新体系就会存在一个逐渐适应的发展过程，这期间很可能会有很多方面考虑不够周全，从而出现管理上的安全漏洞。

(2) CA 体系已在 Internet 中得到了广泛应用，形成了一系列的标准。若 Ad Hoc 网络能沿用 CA 体系，则在其与 Internet 网络互连时，网络安全方面的管理标准能很好的兼容，不会存在互连上的障碍。

为进一步提高网络的可控性，网络采用多频分级结构。基于分簇的结构将网上节点划分成一些相对独立的自治域，既提高了安全服务的可用性和可扩充性，也适合对某些紧急情况快速做出反应，具有很好的可控性，适合于大规模的 Ad Hoc 网络。首先，分级结构有较好的可扩展性。其次分级结构通过路由信息局部化提高了系统的吞吐量。分级结构使路由信息局部化，簇内节点无须知道其他簇的拓扑结构，一个簇的拓扑变化不会被其它簇感知，这减小了路由控制报文的开销。再次，分级结构中节点的定位要比平面结构简单得多。在平面结构中，若想知道一个节点的位置，需要在全网中执行查询操作。而在分级结构中，簇头知道自己簇成员的位置，只要查询簇头就可以得到节点的位置信息。还有，分级结构可通过移动性管理来实现序列寻址。按照节点与簇的关系为节点分配逻辑序列地址，由簇头充当类似于 HLR 和 VLR 功能的位置管理服务器，就可以简单地实现节点定位和寻址。再有，分级结构是无中心和有中心模式的混合体，可以采用两种模式的技术优势。分级后网络被分成了相对独立的簇，每个簇都有控制中心。基于有中心的 TDMA、CDMA、轮询等技术都可以在分级的网络中使用。基于有中心控制的路由、移动性管理、网络管理技术也可以移植到 Ad Hoc 网络中来[15]。

本文在总结前人工作的基础上，为Ad Hoc网络选择了多频分级的体系结构，应用PKI/CA体系，使网络信任具有很好的全局可控性。并在已有的分布式模型的基础上，改进了身份信任关系建立、更新、撤消算法，给出了CA系统在信任模型下的实现方案；在身份信任模型中引入行为评估机制，给出了数字证书信任度维护算法，为更好实现身份信任的更新、撤消及安全路由等操作提供有力的依据。

4.1.2 模型假定及结构

本模型建立在以下基本假定之上：

(1) 存在一个离线的可信任管理机构；

(2) 每个节点具有唯一的非 0 的 ID 号，如 MAC 地址；

(3) 网上的节点性能是不同的，存在性能优良并且物理安全性高的节点；

(4) 网络中节点数目是可变的，不断有新的节点离开或加入网络；

(5) 每个节点都具有某种监视机制，可以监视网络的异常情况，尤其是其一跳邻居节点的行为。

本文将信任分为身份信任与行为信任，信任模型也依据此原则构造，分为身份信任证书管理模块和行为评估证据收集模块两个主要部分，总体结构如图 4.1 所示。这是本文讨论的重点。

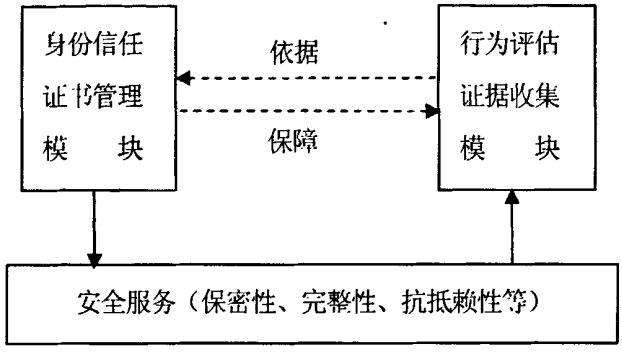

图 4.1 模型总体结构

其中，身份信任是安全服务的基础，而安全服务为行为信任评估和保密通信提供安全保障。同时，信任关系的更新、撤销等操作都是建立在行为信任评估基础上的。

4.1.3 模型提供的服务

信任模型的身份信任证书管理和行为评估证据收集两个模块提供的主要服务包括：网络证书服务、CA 维护及行为信任评估，如图 4.2。

网络证书服务负责网络节点间身份信任关系的建立、更新及撤销，具体操作可表示为证书认证、更新和撤销。CA 维护主要包括：网络初始化阶段簇头节点的主私钥分量的分发；网络运行阶段簇头节点的主私钥分量的周期性更新。行为信任评估提供的服务则主要是：以直接观察和其它节点的信任推荐为依据，对所有节点的路由转发行为进行信任评估，计算节点的信任度值，得到的信任值作为证书撤销、主私钥分量更新和路由选择等决策的依据。

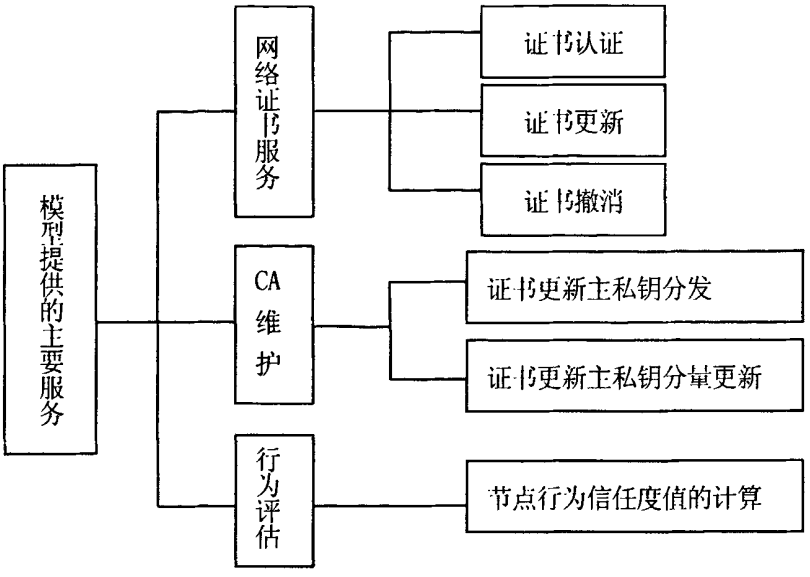

图 4.2 模型提供的主要服务

4.1.4 模型中信任信息的存储方法

本模型中，每个节点需要存储本地信息库，如表4.1。

表4.1 节点本地信息库

节点 ID	公/私钥对	网络公钥	证书更新主私钥分量	证书更新主私钥分量版本号
IDv_i	pk_i/sk_i	PK	S_i	$sm_i(t)$

节点本地信息库的各表项说明

(1) 节点 ID：网络节点在网络中的唯一标识，用于确定网络节点的身份。节点进入网络之前，由离线的管理中心分配；

(2) 公/私钥对：节点当前证书使用的密钥对；

(3) 网络公钥：管理中心公布的、所有节点都知道的网络主公钥，用于验证证书的私钥签名；

(4) 证书更新主私钥分量、证书更新主私钥分量版本号：簇头节点自己掌握的网络主私钥分量及与之对应的主私钥分量版本号，普通节点这两项为空。

簇头节点还需要维护并定期向网络发布节点证书状态信息库和CRL库。节点证书状态信息库如表4.2，为节约网络资源，表内只包括网络内所有有效簇头节点和本簇内节点；证书撤销列表（CRL）库则包括网络内所有被撤消的节点证书和撤消时间。

表 4.2 节点证书状态信息库

节点证书	$Certv_1$		$Certv_2$		…	$Certv_n$	
信任度	$Wv_1(t)$		$Wv_2(t)$		…	$Wv_n(t)$	
被指控的节点证书	$Certv_j$	…	$Certv_m$	…	…	$Certv_k$	…
指控时间	t_j	…	t_m	…	…	t_k	…

节点证书状态信息库的各表项说明

(1) 节点证书：由离线管理中心签发的身份与公钥绑定的签名数字证书，它包含的主要内容如下：

$Certv_i$ =（身份IDv_i，公钥pk_i，有效期T，私钥签名sig_{SK}）

(2) 信任度：记录了从T开始的一个单位时段上该节点的信任度值的大小W(t)，由4.3节中的信任度维护算法计算得到；

(3)被指控的节点证书：依次记录所有被i指控过的节点j的证书信息，包括i对自己的指控（此时，i对其它节点的指控无效）。为计算各节点T时刻的信用值大小时提供指控关系值$R_{ij}(T)$；

(4)指控时间：记录节点i对节点j发起指控的时间信息，如果该时间段i对j发起过多次指控，则只记录第一次发起指控的时间信息。

4.1.5 模型工作机制

信任模型的主要工作可以概括为提供网络证书管理、CA 维护及行为信任评估三项服务。网络整个生存周期则可以划分为初始化和正常运行两个阶段。

在 Ad Hoc 网络中建立安全的通信环境，首先要实现通信节点间的身份信任，即进行身份认证，认证的过程也是节点间初始信任关系建立的过程。在 Ad Hoc 网络初始化阶段，每个网络节点需要离线的向可信的管理中心申请获得身份与公钥绑定的签名证书。可信的管理中心随机产生证书签发公/私钥对和证书更新公/私钥对，用两个主私钥对证书签名。证书签发主私钥由离线的管理中心保管，只

用于对证书的签名；将证书更新主私钥由(k, n)门限共享机制分解，分发给网络中选定的所有簇头节点，由网络中的簇头分布式保管，用于网络运行阶段由簇头节点合作进行证书更新。然后公开两个主公钥及证书更新主私钥验证参数，退出网络。节点获得证书后才能成功的进入网络，根据需要加入自己选择的簇。网络初始化阶段完成后，Ad Hoc 网络就可以进入正常运行阶段了。

在 Ad Hoc 网络正常运行阶段，信任模型的主要工作有：簇头节点合作为每个节点更新公钥证书；撤销非法节点的证书，即解除与非法节点的信任关系；周期性的更新每个簇头节点掌握的证书更新主私钥分量；评估节点的行为等。

网络节点利用身份与公钥绑定的签名证书进入网络与其他节点建立身份信任关系。为避免公钥加密计算复杂、开销大。因此，网络节点间每次会话，通过协商一个会话密钥，利用对称密码算法进行保密通信。这样就实现了节点间通信的保密性，从根本上防止了外部攻击者的窃听、冒充和篡改等恶意行为，另外也为信任评估等提供了基本的安全保障。

为了保证身份认证的安全性、有效性，节点的签名证书一般都具有一定的有效期，网络节点不信任其他节点过期的签名证书。因此，节点的签名证书需要进行更新。本模型中，簇头节点的通信范围大，普通节点的通信范围小。因此，节点证书更新采取由所在簇的簇头代理的方式，这也是为什么要生成两组公/私钥对的原因。考虑到 Ad Hoc 网络中节点可以任意离开和加入网络等特性，由簇头节点定期发布证书状态信息库和 CRL 库，这样则可以不用考虑 Ad Hoc 网络中全局时钟不同步的问题。簇头节点只以节点的证书是否被撤销和其行为信任值为依据，决策是否响应网络节点的证书更新请求。这意味着不可信的网络节点无法获得新的合法证书，也无法再与其他网络节点建立身份信任关系，实际上已经被排除出网络了；而可信节点即使由于特殊原因暂时离开网络，再次回到网络后，仍可获得簇头节点的证书更新服务。同时，请求证书更新的网络节点也会对簇头节点的证书更新服务进行信任评估。不愿提供证书服务的簇头节点的信任值会不断降低，以致最终被剥夺证书签名权力，甚至排除出网络。不同节点提出证书更新请求的时间会不相同，因此它们进行证书更新的时间也各不相同。证书更新时间上的分散也减轻了网络负载，避免了网络拥塞问题。

网络节点的证书在有效期内可能会由于各种原因而失效，例如节点被破坏，或是节点的私钥被攻击者获得等。因此，网络证书服务必须提供证书撤销机制。

本文采用由簇头节点定期发布 CRL 库实现节点证书撤销。网络节点发现节点 v 的非法行为后，就向 v 所在簇的簇头发送一个对 v 的证书的撤消指控。簇头节点收集有关信息，依据信任度维护算法，计算 v 的信任度。当 v 的信任度为 0 时，簇头将其证书加入 CRL 表，并向全网广播。

可见，一个网络节点有两种可能被排除出网络：一是节点的签名证书到期后，由于无法得到门限个簇头节点的信任而不能获得有效的更新证书而被排除出网络；二是由于其受到网络中一定数量节点的指控信任度变为 0 而被排除出网络。

信任模型 CA 维护方面的工作主要是定期更新簇头节点的证书更新主私钥分量。在主私钥分量更新方面，模型采取改进文献[32]中的方案，即在该方案中加入分量验证机制。不可信的簇头节点，不会得到更新分量，实际上已经被排出了网络；而可信的簇头节点，既使遭到传输错误，也可以由先完成密钥分量更新的 k 个簇头节点处获得新的证书更新主私钥分量。

上述的网络证书服务及 CA 维护都是以行为信任评估机制为保障的。同时，行为信任评估机制还可以解决来自 Ad Hoc 网络内部的路由安全问题。网络节点能够评估簇头节点的证书服务行为和所有节点路由转发行为的可信程度。网络节点以行为信任值为决策依据，动态的进行路由选择和证书服务选择。

节点的行为用信任度值来描述，用撤消系数和恢复系数有效地控制恶意节点对网络的影响，提高网络安全服务的可用性。

模型中的身份信任关系的建立和信息保密传输增强了信任评估过程的安全性和可信性。行为信任评估不仅能实现安全路由和提高网络性能，而且可以进一步增强认证过程的安全性、可靠性。下面，详细描述在 Ad Hoc 网络中实现身份可信和行为可信的具体方法。

4.2 基于证书的身份信任方案

本模型中身份信任关系的建立、更新与撤消算法，参考了已有文献[29-32]中的相关算法，综合了其中的优点。

本模型以一个离线的可信管理中心为信任锚，网络中所有的信任关系就是在这个信任锚的基础上进行分散、扩展的。整个网络拥有共同的网络主公/私钥对(PK,SK)。主私钥 SK 由簇头节点以(k,n)门限方式共享，任意小于 k 个节点不能恢

复主私钥的任何信息。每个节点自己产生一个用户公/私钥对(pk_i,sk_i)，用于节点间的认证和安全的交换会话密钥。节点离线的获得身份与公钥绑定的签名证书后，才能够成功的加入网络，而证书的更新等则由网络中的簇头节点合作完成。具体算法描述如下：

4.2.1 初始化

假设 Ad Hoc 网络初始化是在安全、可控的环境下进行的，离线的可信管理机构在要加入网络的所有节点中，分布式地为网络配置 n 个性能优良的节点，这些节点有相当强的计算、存储能力和功率，物理安全性较好。由这些节点充当簇头节点，建立一个两级的网络。例如在战地环境中，存在通信车、装甲车、士兵用通信终端等多类移动节点，性能优良的节点如通信车、装甲车这样的设备可以充当簇头节点。可见，假设是合理且容易实现的。网上节点可以按位置或业务分为 n 个簇，分别归属于这些簇头节点。簇头与簇头之间通信使用一个频率，簇头与簇内节点通信使用另外一个频率。本文还假定簇头节点有较大的功率，互相都在对方的无线覆盖范围之内，可以直接通信。

本文不采用完全分布式认证方案中由所有网络节点合作产生共享秘密分量的方法。主要是因为：由节点自己产生主私钥共享分量缺少信任锚，且增加了不可控环节，降低了可信度；再有由节点自己产生主私钥共享分量，节点需要和网络中所有节点进行交互，这在 Ad Hoc 网络这种动态环境中实现是非常困难的，甚至是无法实现的。另外，这也增加了节点的计算任务与多方交互环节，引入了更多的不安全因素。

假设初始化阶段网络内簇头节点集合为 B=（CH_1，CH_2，…，CH_n）。GF(p)是一有限群，且 p>n。H(u)为单向函数，$S_k(u)$是以 k 为密钥的签名函数(下文若无特别说明，H(u)即指单向函数，$S_k(u)$指以 k 为密钥的签名函数)。则初始化的步骤如下：

(1)可信的管理中心产生证书签发公/私钥对(E,D)和证书更新公/私钥对(PK，SK)，为每个节点 u_i 产生一个全局唯一的身份 IDu_i，每个节点 u_i 生成安全获得数字证书所需的临时公/私钥对 e_i/d_i，广播：(IDu_i， e_i，$S_{di}(H(IDu_i, e_i))$)，并向可信的管理中心发出证书申请并由临时私钥签名：$S_{di}(IDu_i, pk_i)$。

(2)可信的管理中心为每个网络节点产生身份与公钥的绑定证书 $Certu_i$。然

后，可信的管理中心将绑定证书加密发送给节点 u_i。绑定证书用节点的临时公钥加密传输，保证了证书内容不被篡改。节点可以通过网络主公钥 PK 验证证书。

(3) 可信的管理中心随机选取一组数 $a_1, a_2, \cdots, a_{k-1} \in GF(P)$，得到 GF(p)上的 k-1 阶多项式即式（4-1）：

$$f(x) \equiv a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} (\mathrm{mod}\, p) \tag{4-1}$$

(4) 可信的管理中心为每个簇头节点 CH_i 计算证书更新主私钥 SK（=f(0)）的共享分量 $S_i = f(CH_i)$，并利用 CH_i 的临时公钥 e_{CHi} 加密发送给 CH_i。这保证了其他簇头节点无法获得 CH_i 的证书更新主私钥分量。

(5) 任何 k 个节点都可以通过如下公式（4-2）合作恢复出证书更新主私钥：

$$SK = f(0) \equiv \sum_{i=1}^{k} f(CH_i) l_i(0) (\mathrm{mod}\, p) \tag{4-2}$$

其中：$l_i(x) = \prod_{\substack{i=1 \\ i \neq j}}^{k} \frac{x - CH_j}{CH_i - CH_j}$

(6) 为了实现对主密钥分量的验证机制，管理中心还需公布验证参数：设 q 为使 $P \mid (q-1)$成立的素数，g 为 Z_p 中阶为 P 的元素。可信的管理中心计算 $\beta = \{g^{SK} \bmod q, g^{a_1} \bmod q, \cdots, g^{a_{k-1}} \bmod q\}$，并向所有簇头节点公布 g 和 β。

(7) 收到证书更新主密钥分量的簇头节点通过 g 和 β 验证分量 S_i 的正确性，即验证式（4-3）是否成立：

$$g^{S_i} = g^{SK + a_1 CH_i + \cdots + a_{k-1} CH_i^{k-1}} \equiv g^{SK} \cdot (g^{a_1})^{CH_i} \cdots (g^{a_{k-1}})^{CH_i^{k-1}} \bmod q \tag{4-3}$$

如果等式不成立，则证明密钥分量是不正确的，簇头节点拒绝接收，继续发出主私钥分量申请。

(8) 簇头节点周期性地广播簇令信息，包括簇头节点证书，节点证书状态信息库和 CRL 库及对这些信息的签名。

Ad Hoc 网络初始化完成后，管理中心退出网络，以保证 Ad Hoc 网络的无中心特性和安全性。

普通节点通过离线的管理中心获得身份与公钥的绑定证书，携带合法证书加入网络。按这种离线方式获得认证，满足了军事应用等强安全性的需求；同时，

也减少了簇头节点合作为新节点签发证书的计算和通信负担。在网络运行的任何阶段都不重现证书更新主私钥 SK，这有效防止了恶意节点或泄密节点获得 SK。同时，节点身份 ID 由管理中心分配，并由网络主私钥签名，保证了网络中 ID 的唯一性，也有效防止了攻击者冒充节点身份以及节点否认身份。

4.2.2 身份证书认证

节点间通过认证数字证书建立身份信任。一个新节点 V 要加入网络时，它首先收集簇头发布的簇信令信息。当节点 V 收到了簇头 CH 的簇信令信息或簇 CH 成员节点的信息时，首先验证消息的正确性。如果验证正确 V 需要加入簇 CH，V 首先向簇头 CH 发送一个申请加入消息；由于 V 和簇头 CH 可能不能直接通信，需要其它节点的转发，所以，申请加入消息要由簇头公钥进行加密。簇头 CH 验证 V 的证书，决定是否允许 V 的加入。若同意，则 V 加入簇 CH，并把 V 的证书加入到节点证书状态信息库。

网络中一个节点从一个簇漫游到另一个簇时，新的簇头可以把该节点当作新加入的节点处理。但此时簇头是否同意该节点加入，还要查询此节点以前的信任度值。

节点 v 加入簇后，证书由簇头保存。与其它节点通信时，其它的节点查询节点 v 的证书状态，从而决定是否与其通信。若查询不到节点 v 的证书状态信息，则 v 不会被信任。

身份信任关系建立之后，要实现安全的通信，还需要对通信信息进行加密。Ad Hoc 网络带宽有限，且节点计算能力不强，因此，应尽量避免使用计算量较大的公钥加密算法。网络节点间的会话时间与证书有效期相比是很短暂的，节点间每次通信都交换证书，势必给网络带来很大的通信负担。因此本文采用公钥认证，对称密码体制进行保密通信的方案，即网络节点间通过公钥证书建立身份信任关系，然后通过协商会话密钥进行保密通信。节点间的保密通信采取每次会话协商一次会话密钥的方式。证书存储于簇头节点可以减少节点间的证书交换次数，以此降低节点间的通信量。

节点 A 要与节点 B 通信，查询簇头的节点证书状态信息库，若 B 在本簇内，则获取 B 的证书。若不在本簇内，则由簇头向其它簇头进行查询。节点 A 获得 B 的证书后，向 B 发送请求会话消息，用 B 的公钥加密。节点 B 若同意与 A 通信，

则生成通话密钥，发回给 A，双方就可以进行保密通信了。若 B 不同意与 A 通话，则忽略 A 的消息。

会话密钥协商过程如图 4.3。

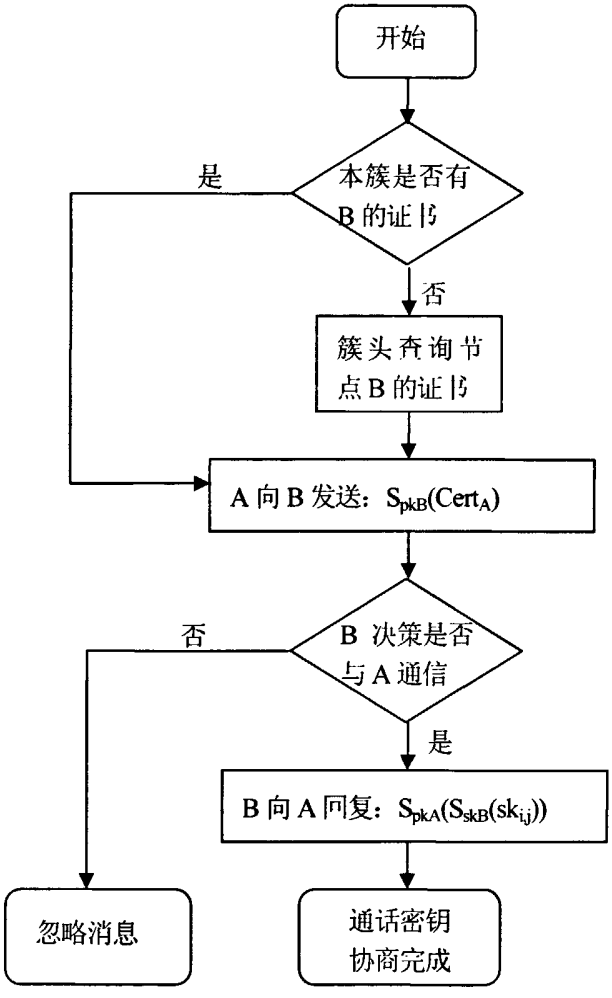

图 4.3 通话密钥协商过程

4.2.3 身份证书更新

网络节点在整个网络生存期内都使用一个证书，即节点公/私钥对始终不改变，是不安全的。节点使用同一证书时间越长，被攻击者或恶意节点攻破的机率越大。因此，信任模型中必须具备节点证书更新的机制。

本模型采用按需进行证书更新策略实现网络节点证书的更新，即网络节点根

据自己的判断，密钥是否安全，决定是否提出证书更新请求。不同节点的提出证书更新的请求时间会不相同，证书更新时间的分散也避免了网络拥塞问题。

节点 v 判断自己的密钥不再安全，就生成新的公/私钥对，并向所在簇的簇头节点发出证书更新请求。此时，簇头节点已经具有了对节点 v 的信任评估值。簇头节点检索自己的节点证书状态信息库，并以此为依据，决定是否为节点 v 签发新的证书。簇头节点如果认同请求，就计算自己的部分签名 Sig_iM，并向网络中其它簇头节点申请部分签名分量，簇头收集到足够多的签名分量（至少 k 个）后，将这些分量发回给节点 v，节点 v 获得了 k 个(k 为((k,n)门限秘密共享方案中的门限值)证书签名分量，则可以成功实现证书更新；如果无法获得 k 个证书签名分量，就无法获得新的签名证书，实质上，v 已经被排除出网络了。

本文采用分布式可验证签名方案实现网络节点的证书更新，具体步骤如下：

(1) 申请证书更新的网络节点 v 向自己所在簇的簇头节点 CH_i 发送证书更新请求，请求的内容为：Spk_{CHi}（S_{skv}(IDv，$pk_{v\text{-}new}$)，H(IDv，$pk_{v\text{-}new}$)）。新证书的内容用 sk_v 签名是对 v 的身份认证，单向函数保证了新证书的完整性。所有内容用 pk_{CHi} 加密，一是对簇头的身份认证，二是防止其它恶意节点破坏新证书的内容。

(2) 收到请求消息的簇头节点 CH_j 同意为其更新，就利用自己掌握的证书更新主私钥分量对证书签名，产生签名证书分量 $Cert_{ij}=S_{SjIj(0)}$(IDv，$pk_{v\text{-}new}$)，然后将 S_{CHi}($cert_{ij}$, H($Cert_{ij}$，g^{Sj})) 及验证参数 g 和 β 发送给 CH_i。

(3) CH_i 收到 CH_j 发送的($Cert_{ij}$ H($Cert_{ij}$，g^{Sj})) 后，需要验证 $Cert_{ij}$ 的正确性。利用验证参数 g 和 β 计算：

$$g^{s_j} = g^{SK+a_1CH_j+\cdots+a_{k-1}CH_j^{k-1}} \equiv g^{SK}\cdot(g^{a_1})^{CH_j}\cdots(g^{a_{k-1}})^{CH_j^{k-1}} \pmod q$$

CH_i 由 CH_j 提供的 $Cert_{ij}$ 和自己求得 g^{Sj} 即可得到 H($Cert_{ij}$，g^{Sj})，如果与 CH_j 发送的 H($Cert_{ij}$，g^{Sj})相等，则接受 $Cert_{ij}$，否则丢弃。

(4) 收集到 k 个经过验证的签名证书分量后，组装新证书：

$$Cert_{v\text{-}new}=\prod_{j=1}^{k} cert_{ij} = (ID_v, pk_{v-new})^{\sum_{j=1}^{k} S_j I_j(0)} = (ID_v, pk_{v-new})^{SK}$$

加密发回给节点 v。并更新节点证书状态信息库。

节点最后获得新的网络证书，但无法得到关于 SK 的任何消息。

4.2.4 身份证书撤消

现有的 Ad Hoc 网络信任模型多采用分布式存储 CRL 列表的方式，即由每个网络节点自己维护一个 CRL 列表。然而这种方式占用了网络节点大量的存储资源。本模型由簇头负责创建并维护一张即时更新的证书撤销列表(CRL)。用户在验证证书时，通过查询 CRL 来确定证书是否有效。

节点证书的撤销操作分为无条件撤销和有条件撤销两种[57]。无条件撤销是节点对自己的证书发出指控操作。这种操作一旦发生，节点证书直接被撤销，不再有效。有条件撤销是由其他节点联合对该节点做出指控，直到该节点的信任度值为0，节点证书同样会被撤销。

无条件撤销是一种自撤销，其可信性较高，通常是由于密钥泄密而声明自己数字证书不可信的一种情况。一旦这种撤销操作发生，其数字证书的可信度一定要变为0，表明数字证书已不可信。簇头则直接将其证书加入CRL列表。

有条件撤销是一种互撤销，存在一定的随意性，所以这种撤销操作的可信性需要打一定折扣，不能使单一的撤销操作起决定作用，而需多数节点共同联合作用。假定每个节点都具有某种监视机制，如安装了入侵检测机制，可以监视其一跳邻居节点。

本模型的有条件撤消采用行为信任评估机制来实现节点证书撤销，簇头节点通过计算节点的信任度值，当某节点的信任度为 0 时，簇头节点就将该节点加入到自己的 CRL 库中，则该节点在整个网络中都不再被信任。

当簇头节点 CH 不再被信任时，其簇内的节点可以重新加入别的簇（如新节点加入），并及时进行证书更新。

基于信任评估进行身份信任关系撤销，可以有效防止不良节点的恶意指控。

4.2.5 簇头节点的证书更新主私钥分量更新

为了防止移动攻击者通过攻破k个(k为(k，n)门限秘密共享方案中的门限值)或更多个簇头节点而获得证书更新主私钥，模型需要具有主私钥分量更新机制。大致思路是在不改变主私钥的前提下，周期性的更新每个簇头节点掌握的证书更新主私钥分量。

Ad Hoc 网络中没有系统时钟，每个节点可能认为的系统时间是不同的，本文规定，最先到达更新时间的簇头节点发起更新，如果有簇头节点判断到时间要进

行分量更新了，就发起更新过程，将更新消息广播出去，其它簇头节点只要收到更新消息，不管自己的本地时钟是否到时间，都开始进行分量更新过程。

随着时间的推移，网络节点的时钟漂移差距可能会达到一个非常大的不同，这样会严重影响了分量更新的效率。为了使网络中所有簇头节点的时钟漂移差距不至于过大，让每次某个簇头节点发起分量更新结束后，在全网进行一次时钟同步。为了公平起见，这一时钟同步不是只以发起更新的簇头节点的时钟为准。而是由该簇头节点向其他簇头节点广播时钟同步消息。获得消息的其它簇头节点向发起更新簇头节点返回自己的本地时钟，发起更新簇头节点收到 k 个本地时钟后，取平均值来获得本次时间同步的参考时间 t，然后考虑一定的消息延迟△t,并在网络中广播同步时间 t+△t。网络中簇头节点收到同步时间消息后，都同步自己的本地时钟。

为了避免由于异步网络不定的消息延迟，至使有些簇头节点的主私钥分量不能及时更新，引入分量的版本号概念。由于分量是具有版本号的，这样旧版本的分量不能参与新版本的密钥分量重组。那么它要能正常参与网络运行，就要主动联系发起更新簇头节点而完成自己的分量更新。记网络初始化完成后，簇头节点掌握的主私钥分量版本号为 0，以后每经过一个时间周期，所有簇头节点掌握的主私钥分量进行一次更新，版本号也累加 1。

网络生存时间按周期刷新时间 T 分为多个时段，经过时间 T，各个簇头节点持有的系统私钥分量将做周期性的更新，更新依赖于某些门限密码体制的秘密分量的同形特性。

同形特性[92]是指如果(S_1， S_2，…，S_n)是私钥 SK 的共享分量，(S'_1， S'_2，…，S'_n)是私钥 SK 的共享分量，则($S_1+S'_1$， $S_2+S'_2$，…，$S_n+S'_n$)是 SK+SK′的共享分量。例如 Shamir 的多项式插值秘密共享方案满足此同形特性。令 SK′=0，则($S_1+S'_1$， $S_2+S'_2$，…，$S_n+S'_n$)是 SK 的一个新的共享分量。

证书更新主私钥分量的周期性更新过程：

(1) 设(S_1, S_2, …, S_n)为证书更新主私钥分量，分别被簇头节点 CH_1，CH_2，…，CH_n 所持有。簇头节点 CH_i, i=1, 2, …, n 随机产生一个 Zp 上的 k-1 次多项式：

$$\varphi_i(x) = b_{i1}x + b_{i2}x^2 + \cdots + b_{i,k-1}x^{k-1} \qquad (4\text{-}4)$$

计算$S_{ij} = \phi_i(CH_j)$得到(S_{i1}，S_{i2}，…，S_{in})，S_{ij}($1 \leqslant j \leqslant n$)称为子密分量。由式（4-4）可知$\varphi(0)=0$。将每一个子密分量 S_{ij} 用簇头 CH_j 的公钥加密后传给 CH_j;

同时广播（$g^{b_{i1}}$，$g^{b_{i2}}$，…，$g^{b_{in}}$）和 g。

(2) 每一个 CH_j 收到(S_{1j}，S_{2j}，…，S_{nj})后，验证：

$$g^{S_{ij}} \equiv \prod_{t=1}^{k-1}(g^{b_{it}})^{CH_i^t} \tag{4-5}$$

如果等式（4-5）成立则接受，否则拒绝。

(3) CH_j 计算新的私钥分量 $S'_j = S_j + \sum_{i=1}^{n} S_{ij}$ 。

从而完成每个簇头节点所持有的系统私钥分量的刷新。这样周期性地刷新密钥，更新后的密钥和更新前的密钥不能合作恢复出系统私钥，攻击者只有在系统刷新密钥的周期间隔内收集到 k 个系统密钥分量才能恢复出系统私钥，合理的周期刷新时间 T 能避免攻击者获得 k 个当前时间的有效系统私钥分量。

上述过程可能会遭到子密分量的传输错误，然而只要有 k 个簇头节点达成一致，就可完成系统主密钥分量的更新。其它簇头节点就可以由先完成密钥分量更新的簇头节点获得新的系统私钥分量。

4.2.6 新簇头节点证书更新主私钥分量的生成

随着新节点的加入，网络规模不断扩大，离线的管理中心可以根据网络的规模和对网络状态的评估，适当增加簇头节点的个数。在新成员入网时，可以从中选择一些节点作为簇头节点，发给它私钥的同时，也给它一个系统私钥分量，并发放一个用系统私钥签名的宣布此节点为簇头节点的票据，票据格式如下：{ID，管理中心，服务器节点，签名}，由此节点在网上传播该票据，任何节点都可以用系统公钥验证此消息的正确性，从而信任此节点为簇头节点。根据网络规模和状态调整服务节点的数量，既确保了系统的安全性，也提高了服务的可用性。

当簇头节点的安全受到威胁时，本方案采取下述方式产生新的簇头：该簇内节点 CH_{new} 在网络中存活一段时间后，网络中的簇头节点就对 CH_{new} 建立了一定的信任(也可以理解为 CH_{new} 在网络中的信誉，可能是信任，也可能是不信任)。此时 CH_{new} 就可以申请获得网络的证书更新主私钥分量，从而升级为簇头节点了。但是，如果 CH_{new} 没有成功升级为簇头节点，它不能无限制的连续提出申请。在一个时间段内，簇头节点只处理 CH_{new} 的第一次申请，而对它后续的申请不予响应。这也是有效防止恶意节点 DoS 攻击的一种策略。下面，具体介绍 CH_{new} 申请升级为簇头节点的过程。

(1) CH_{new} 向网络中自己信任的簇头节点发送升级申请。

(2) 收到请求的簇头节点如果信任 CH_{new} ，就为其计算共享子分量，加密传送给 CH_{new} 。

(3) CH_{new} 收集够 k 个正确的共享子分量，就对收集到的共享子分量求和即得 CH_{new} 掌握的主私钥共享分量，此时 CH_{new} 成功升级为簇头节点。

(4) 所有簇头节点更新自己的簇头节点证书库。

CH_{new} 升级为新的簇头节点，原簇头节点消毁它所持有的证书更新主私钥分量。这在一定程度上防止了簇头节点的单点威胁。

4.3 基于信任度的行为信任方案

在改进的信任模型中，身份信任关系的建立、更新和撤销以及网络的安全路由都以行为信任评估为依据。信任评估的准确性、合理性将直接影响到信任模型的安全与效率。文献[38]提出了只需部分节点合作的证书撤销算法。该算法考虑的因素太少，可靠性不够。本文在有关文献研究的基础上，提出了一种更适合于 Ad Hoc 网络的分布式证书撤销算法，只需要网络中部分节点的合作，通过引入撤消系数和恢复系数进一步提高了算法的可靠性和合理性；并通过对节点证书状态表的更新维护，不仅方便了对信任度值的计算，而且还提供了网络当前有效节点的证书状态信息和信任度值信息。下面详细介绍本文改进的信任度维护算法。

4.3.1 信任度的有关概念

定义 4.1 设 $0 \le W_i(T) \le 1$，$i \ge 1$、$T \ge 0$，且 i、T 为整数，这里 i 为数字证书的编号，T 为时间，称 $W_i(T)$ 为“信任度”，它描述了数字证书 i 在时刻 T 的信任度值。

T=0 表示 Ad Hoc 网络的初始时刻，根据模型的假定有 $W_i(0)=1$，表示在 Ad Hoc 网络的初始时刻，所有节点的数字证书都是完全可信的。节点证书的有效性由 $W_i(T)$的值决定。$W_i(T)$的值越大该节点的可信度越高，当 $W_i(T)=1$ 时该节点证书完全可信；当 $W_i(T)=0$ 时此证书完全不可信，将其撤销。这两个状态与传统 CA 体系数字证书的两个状态是一致的，因此信任度是对传统 CA 体系二元信任状态的一种扩展。

定义 4.2 设 $R_{ij}(T)$是取值为 0 或 1 的二元变量，i、j 为数字证书的编号，T 为时间，这里称 $R_{ij}(T)$为时刻 T 节点 i 对节点 j 的“撤销关系”。当 $R_{ij}(T)=1$ 时，表

示在时刻 T 节点 i 对节点 j 发出了撤销操作；当 $R_{ij}(T)=0$ 时，表示在时刻 T 节点 i 对节点 j 没有发出撤销操作。

在 Ad Hoc 网络中，证书撤销操作以消息的形式在网络中广播，各个簇头节点通过收集网络消息，来计算证书的信任度。证书撤销操作的消息格式为：($Cert_i \rightarrow Cert_j$, T，E，S)。其中，$Cert_i \rightarrow Cert_j$ 表示 i 对 j 发出指控；T 为指控时间；E 表示撤销原因；S 为 i 利用自己的私钥对指控信息 $Cert_i \rightarrow Cert_j$ 以及 T 的签名；

在 Ad Hoc 网络运行的某一时刻，网络节点之间的撤销关系可用一个有向图来表示，如图 4.4 所示。图中箭头的发出节点表示该时刻发出撤销操作的节点；箭头的终止点表示该时刻被撤销的节点。

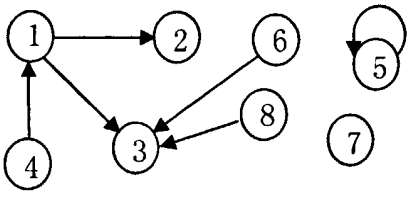

图 4.4 Ad Hoc 网络节点撤销关系

本文在对算法的分析中补充如下假设：(1) 网络中共有n 个节点，i =1, 2, …, n 为节点号。其数字证书为$Cert_i$；(2) T =1, 2, 3, …为一系列离散的证书撤销时间点。假定节点之间的指控操作是周期性发生的，也即节点只有在特定的时间点上才能发出指控操作 (T=0为网络开始运行的时刻)；(3) 节点i在T−1～T时段发现节点j异常，则i在T时刻发出指控操作；(4) 节点i对节点j在同一个时段发起过多次指控，那么网络中簇头节点在接收到这些指控时，只记录第一次接收到的指控，其他被丢弃。

4.3.2 信任度维护算法

在 Ad Hoc 网络中，证书的有效性不能由某单一节点或单方面的因素决定，应由累积多个节点多方面因素的联合作用决定，其综合作用的结果最终表现在节点信用值 $W_i(T)$的变化上。因此，一个节点证书的撤销与否应该由多个节点对其行为的指控操作以及节点当前时刻的信任值决定，以提高证书强制撤销机制的可靠性。

为了减少单一节点的撤销作用力，增加多个节点的联合撤销作用力，引入“撤

销系数α”(0<α<1)，则每个节点只能以自身信任度值α倍的撤销力度，即α $W_i(T)$，去对其它异常节点的数字证书发出撤销操作。撤销系数α的确定与网络安全的稳定性和数字证书撤销效率有关，应根据网络实际应用情况来决定。假设系统可以容忍 K 个恶意节点，α必须小于 1/K，否则在网络开始运行时，K 个恶意节点联合便可撤销任意其他节点的证书。详细讨论留在后面的安全性分析。

在 T 时刻，当节点 j 证书被强制撤销时，应为曾经被 j 指控过的节点 i 平反，即需要抵消节点 j 对节点 i 的撤消作用，引入“恢复系数 β”，可令 $\beta=\alpha$，补偿节点 i 的损失。恢复系数 β 的引入，可有效地降低恶意节点对信任度值的影响，减少行为评估中的不确定因素。

因此，一个节点信任度随时间变化的迭代更新关系如式(4-6)所示。

$$W_i(T)=W_i(T-1)-\alpha\sum_{j=1,j\neq i}^{n}W_j(T-1)R_{ji}(T-1)+\beta\sum_{l=1,l\neq i}^{n}W_l(T-1)R_{li}(T-1)k_l(T) \qquad (4-6)$$

其中，当节点 l 的证书被撤消时，$k_l(T)=1$；证书有效时，$k_l(T)=0$。

式(4-6)即为节点信任度维护算法，说明节点在 T 时刻的信用值大小与节点在 T-1 时刻的信用值大小有关。一个节点信任度值的大小，不仅与其他节点对其监控作用有关，而且跟自身的行为也有密切联系。

根据定义 4.1，T 时刻 Ad Hoc 网络节点的信任度可表示成向量形式，如式(4-7)，称之为“信任度向量”。

$$W(T)=[W_1(T),W_2(T),\cdots,W_n(T)] \qquad (4-7)$$

由式 (4-6)，节点信任度 W(T)可能会出现结果为负值的情况。按照定义 4.1 中的要求有 $0\le W_i(T)\le 1$。所以这里引入一个“校正函数”f(x)，其表达式如式(4-8)所示。

$$f(x)=\begin{cases}x & x\ge 0\\ 0 & x\le 0\end{cases} \qquad (4-8)$$

所以，对信任度向量 W(T)进行校正的过程如式(4-9)所示。

$$W(T)=f(W(T))=[f(W_1(T)),f(W_2(T)),\cdots,f(W_n(T))] \qquad (4-9)$$

至此就完成了 Ad Hoc 网络信任度向量 W(T)的一次更新。

下面介绍节点证书撤消机制的实现过程：它包括无条件撤销算法和有条件撤销算法两个过程，且随着 Ad Hoc 网络的运行时间 T 的变化，信任度向量 W(T)会按上述算法过程不断地迭代更新。

(1)无条件撤销

这种证书撤销方式比较简单，只需节点对自身证书发出指控操作后签发给网络中的簇头节点即可，簇头节点自行验证和计算。用该方式撤消证书后，只要考虑恢复系数。具体步骤如下：

①T时刻，网络中任意节点i向簇头节点广播指控信息：($Cert_i \rightarrow Cert_i$,T，E，S)。

②簇头节点在接收到该信息后，验证 pki(S)=Certi→ Certi ‖T 是否成立，其中，pki(S)为接收消息的簇头用发送节点的公钥对接受到的信息 S 进行解密。

③如果成立，则在自己维护的证书状态表中将证书状态信息置为 0，从表中提取节点 i 的指控记录，依次计算曾被节点 i 指控过的所有节点的新信用值为：

$W_j(T)=W_j(T-1)+\beta W_i(T-1)R_{ij}(T-1)$

④将各节点的新信任度值存储到节点证书状态信息表中，并删除表内的所有与节点 i 有关的指控记录和受控记录。

⑤如果不成立，则丢弃该指控信息。

(2)有条件撤销

这种撤销方式需要网络中部分节点的合作才能完成。具体步骤如下：

①T时刻，网络中任意节点i 向其他节点广播对节点j的指控信息：($Cert_i \rightarrow Cert_j$，T，E，S)，$i \neq j$。

②簇头节点接收到指控信息后， 验证 $pki(S)=Cert_i \rightarrow Cert_j \| T$ 是否成立。若成立则接收，否则丢弃。

③簇头节点首先按不同节点发出的指控信息进行分类，分别存储到节点证书状态信息表中的相应位置。然后计算在T时刻所有节点的新信任度值为：

$$W_i(T)=W_i(T-1)-\alpha\sum_{j=1,j\neq i}^{n}W_j(T-1)R_{ji}(T-1)$$

④对 $W_i(T)$使用校正函数进行校正后，如果发现有节点 i 的信任度值变为 0，先在自己维护的节点证书状态信息表中将证书状态信息置为 0，再从表中提取节点 i 的指控记录，可得：

$W_j(T)=W_j(T-1)+\beta W_i(T-1)R_{ij}(T-1)'$

再次使用校正函数对$W_j(T)$进行校正，将各节点的新信用值存储到节点证书状态信息表中，并删除表内的所有与节点i有关的指控记录和受控记录。

信任度维护算法由簇头节点维护，大大降低了对普通节点性能的要求。节点只需通过查询簇头的节点证书状态信息表，就可得到网络节点的当前信任度。根

据信任度可选择信任度较高的节点来使用，或者根据网络业务的重要性不同来选择可接受的信任度阈值。

Ad Hoc 网络中，各个节点的信任度不同。信任度高的节点在 Ad Hoc 网络中会被优先使用，因此属于网络中的重要节点，具有较高的使用频率，可以优先享受网络资源和其它节点的服务。在这种激励下，每个节点都努力为网络服务，以提高其它节点对自己的信任。不愿与其它节点合作的节点也得不到其它节点的信任，最终将被排除出网络。

4.4 本章小结

首先，本章概述了改进后的信任模型的体系结构、功能以及主要工作机制；然后，详细描述了以信任度评估为辅助手段，实现网络节点间身份信任关系的建立、更新及撤销的方法。

第5章 信任模型安全性分析

上一章，详细描述了本文提出的 Ad Hoc 网络信任模型中网络节点身份信任关系建立、更新、撤销的方法，并给出了信任度评估的方法。下面，分别对信任模型中身份信任和信任度维护算法的安全性进行分析。

5.1 身份信任算法的安全性分析

在改进的信任模型中，所有网络节点都是以一个离线的可信管理中心作为信任锚建立信任关系的，这增强了网络的可控性，即增强了整个网络的可信程度。由于网络节点的签名证书是以离线方式生成的，因此签名证书的安全性就基于签名算法的安全性。例如，如果采用 RSA 或 ECC 算法进行证书签名，那么证书的安全性就取决于 RSA 或 ECC 密码体制的安全性。另外，离线颁发节点身份与公钥绑定的签名证书，一方面可以抵御网络中的中间人攻击，另一方面也实现了抗否认性。

在签名算法安全的前提下，攻击者要成功的进入网络只有一种方法。即攻击者攻破离线的管理中心，获得网络两个主私钥。然而，攻破离线管理中心的代价要远远大于其进入网络的收益，且离线管理中心的安全性不属于 Ad Hoc 网络安全范畴；攻击者既使攻破网络中 k 个以上的簇头节点(k 为(k，n)门限秘密共享中的门限值)，由 k 个证书更新主私钥分量组合得到证书更新主私钥 SK，也不能签发证书。并且，(k，n)门限秘密共享方案已经证明是安全的[11]。另外，在信任模型中引入了证书更新主私钥分量更新机制，不同版本的证书更新主私钥分量不能合并重构出秘密。因此，攻击者要获得 SK，必须在一个证书更新主私钥分量更新周期内攻破 k 个以上的簇头节点，这进一步增强了网络证书更新主私钥的安全性。

在网络节点间身份认证及保密通信阶段，通信发起方使用通信接收方的公钥加密传输自己的身份证书，保证了证书消息的保密性，有效防止了利用虚假证书消息造成的 DoS 攻击。证书消息中的单向函数保证了证书内容的完整性。通信双方成功获得彼此的身份证书后，通过对方的公钥进行会话密钥协商，并且在网络运行的任何阶段都不向外透露自己的私钥。因此，协商会话密钥的安全性基于公

钥密码算法的安全性。

在网络节点证书更新阶段，节点证书更新申请消息的整个内容由簇头节点的公钥加密，防止了恶意节点对消息内容的窃听、篡改；节点新的公钥通过节点的私钥签名，既实现了对节点身份的认证，也防止了恶意节点的假冒攻击；单向函数则保证了消息的完整性。另外，簇头节点以信任度值为依据决策是否为网络节点更新证书，提高了证书更新的可信程度，进一步提高了证书更新的安全性。

改进的信任模型在证书撤销中引入了信任度评估机制，有效防止了对节点的恶意指控攻击。

改进的信任模型采用集中与分布相结合的混合模式，在每个簇中，簇头负责管理簇内的安全，当簇头发现节点有严重恶意行为（如假冒、篡改、黑洞攻击等）时，很容易实现对恶意节点的撤消；当簇头受到安全威胁时，可以通过簇头选举机制将簇头职责转让给另外一个簇内节点，从而在一定程度上减轻了簇头的单点威胁。新簇头节点获取证书更新主私钥分量的机制，保证了簇头的安全性和可用性。簇头节点持有的证书更新主私钥分量周期性更新机制有效地提高了系统的安全性。

考虑最坏的情况，假设攻击者掌握了网络的两个主私钥，成功进入了网络。由于每个网络节点自己生成并保存公/私钥对，并且在网络运行的任何阶段都不向外暴露私钥，因此攻击者破解节点私钥加密信息的难度在于公钥密码算法的安全性。在公钥密码算法安全的前提下，攻击者无法获得网络节点间由私钥加密传输的任何信息，也无法与其他节点进行通信。这意味着攻击者无法获得网络节点的信任，最终会被撤销证书，排除出网络。

通过以上分析可见，身份信任算法可以保证 Ad Hoc 网络中节点的身份可信及通信保密性。

5.2 信任度算法的安全性分析

网络中最易遭到攻击者攻击和破坏的对象是普通节点。对普通节点的攻击有两种结果。一种是毁坏节点私钥，使得节点无法使用数字证书完成信任性验证工作；另一种是获得节点私钥，并利用节点私钥行使其在 Ad Hoc 网络中的权利。对于毁坏节点私钥的攻击方式，只会使网络中单个节点受到损失，无法继续正常工

作，但并不影响网络整体的信任度维护，网络从整体上讲仍是安全的，没有遭到破坏。

对于获得节点私钥的攻击方式则比较危险。如果节点能在攻击者获得其私钥之前对自己的证书发出无条件撤销，并向网络广播自己的撤销消息，则网络整体的信任度也不会遭受损失。危险的是节点在攻击者获得其私钥之后才对自己的证书发出无条件撤销，或者根本就无力对自己的证书发出无条件撤销，只能靠网络检测机制来发现。在这段时间中，攻击者就可利用获得的私钥对 Ad Hoc 网络信任度维护体系进行干扰和破坏，使网络无法继续工作。这样，节点的安全问题最终归结到信任度的安全上。

根据上章中数字证书信任度维护算法可知，每个节点对其它节点的撤销作用力与节点自身当前信任度有关。因此攻击者会尽量获取当前信任度较高的节点私钥，以便对网络信任度形成更大的干扰；同时由于每个节点对其它节点的撤销系数为$\alpha(0<\alpha<1)$，即只有α倍的权利去表决一个节点的不可信，因此 Ad Hoc 网络中只有一个恶意节点时，其对网络信任度的扰乱并不起决定性作用，且其行为很容易被发现而被簇头节点撤销。因此攻击者要想使 Ad Hoc 网络中的节点证书失效，即让其信任度$W_i(T)=0$，特别是要让网络中当前信任度为 1 的节点证书失效，攻击者就需要$1/\alpha$个信任度为 1 的恶意节点进入 Ad Hoc 网络去合谋这件事情，如果恶意节点的信任度低于 1，则需要更多的恶意节点参与。但是攻击者获取的节点私钥数量越多，其恶意行为被发现的可能性就越大。所以要想对 Ad Hoc 网络信任度体系形成干扰，攻击者至少需要 $1/\alpha$个恶意节点，这就需要攻击者去获取更多的网络节点私钥。

攻击者获得节点私钥并能对网络的信任体系进行干扰是一个概率事件，这个事件与节点的配置有关。为了便于对信任度安全性进行分析和度量，这里假设 Ad Hoc 网络每个普通节点的配置都相同，攻击者获得任一普通节点私钥并能对网络信任体系进行干扰的事件概率为$p(0<p<1)$。

攻击者获取节点私钥数量的概率事件可以用一个几何概率来描述。由于攻击者获得任一节点私钥并能对网络信任度进行干扰的事件概率为 p，则其成功获得 n 个节点私钥而未被发现的概率为式（5-1）：

$$P(n)=P^n(1-P) \tag{5-1}$$

式(5-1)表明攻击者获得 n 个节点私钥而未被发现的概率为 P(n)，且随着 n 的增大，P 在减小。

由于攻击者至少需要 1/α个恶意节点才能对 Ad Hoc 网络信任度形成影响性的干扰，而根据式(5-1)，攻击者获得 1/α个节点私钥的概率为式（5-2）：

$$P(1/\alpha)=p^{1/\alpha}(1-p) \qquad (5\text{-}2)$$

式(5-2)中的 p(1/α)随着 1/α的增大 P 在减小。因此在给定α的情况下，攻击者想成功干扰 Ad Hoc 网络信任度使其网络节点证书失效的可能性最大为 p(1/α)，也就是说本模型中数字证书信任度维护算法的可靠性至少为 p(1/α)。因此可以根据实际网络可靠度的要求来调节α的取值。假设实际系统要求能够容忍 N 个恶意节点的联合撤销操作，则α应取 1/N 。α反应了网络的可靠性，其与网络的安全性是直接相关的。

α的取值越小，数字证书信任度维护算法的可靠性越高，系统能够容忍恶意节点联合撤销的数量会越大。但这对正常节点对恶意节点的撤销带来困难性，需要更多的节点去参与。通常在 Ad Hoc 网络中，对网络中恶意节点的检测都是由邻居节点承担的，因此要保证平均每个节点周围不少于 1/α个邻居节点，以便恶意节点的信任度能迅速变为 0，被迅速隔离出 Ad Hoc 网络。

信任度维护算法中，还引入了恢复系数 β，有效地控制了恶意节点对信任度的影响，提高了网络的安全性。

5.3 本章小结

本章从身份信任算法的安全性和信任度评估算法的有效性两个方面对改进的 Ad Hoc 网络信任模型进行了分析。分析结果表明，改进的信任模型能够很好的实现 Ad Hoc 网络中的认证性、保密性、数据完整性、节点的抗抵赖性及系统的可用性。另外，信任度评估机制对提高网络的安全性和可用性，特别是路由安全性起到积极的作用。

结　论

移动 Ad Hoc 网络作为一种特殊的移动计算机网络和移动互联网的实现形式，在保障信息的安全性、身份的合法性、行为的抗抵赖性和服务的可用性等安全目标方面与传统有线网络是一致的。因此建立适合于移动 Ad Hoc 网络的 PKI/CA 系统以提供安全通信环境是其未来应用必须要解决的问题。

本文从研究 Ad Hoc 网络的结构特点入手，详细分析了 Ad Hoc 网络当前面临的挑战以及现有信任模型的优缺点。针对多频分级结构的 Ad Hoc 网络的特点，提出一种集中式和分布式相结合的混合式信任模型。面向簇结构的移动 Ad Hoc 网络，可以使该方案具有可扩充性，良好的可控性，提高了安全服务的可用性。在簇头节点间采用门限密码的思想，分布式存储系统的主密钥提高了系统主密钥的安全性，簇头持有的系统私钥分量的定期更新机制更有效地增加了系统的安全性；本文借助 PKI/CA 安全体系的思想建立身份信任关系，节点离线地获得网络证书进入网络；簇头负责簇内的安全和路由，对簇内节点的安全性实施有效的控制；引入行为信任度值的概念，动态的决策节点证书的更新与撤销，增强了信任评估方法的可用性与可控性。通过对撤销系数和恢复系数的调节来调整网络的安全性和可靠性，减少了行为信任评估中的恶意节点对信任度的影响。

总之，本文本着兼顾安全性与实用性的原则，对 Ad Hoc 网络信任模型进行了研究与改进。由于作者的能力和时间有限，本文的研究工作尚有很多不成熟和不完善的地方，主要表现在：

(1) 虽然分级结构的 Ad Hoc 网络具有良好的可扩展性，大大降低了对普通节点的性能要求，可以有效地利用有限的带宽等；但簇头的安全性如何保证是个需要进一步深入研究的问题；

(2) 需要离线的可信中心的介入，这在一定程度上影响了信任模型的灵活性和适应性；

(3) 模型中的许多参数还需要进一步量化，例如门限秘密共享的门限值、节点证书更新周期的时间长度、撤销系数 α 值等。

当然，要靠一已之力设计出绝对完善的 Ad Hoc 网络安全方案是不可能的。

另外，仅依赖信任模型也是无法完全实现 Ad Hoc 网络安全的，信任模型本身还需要入侵检测等安全机制辅助才能够正常工作。可见，要建设安全、高效、健壮的 Ad Hoc 网络，还需要广大科研工作者进入更加广泛和深入的研究。

参考文献

[1] A. Shamir. How to Share a Secret . Communication of ACM， 1979，22（11），612-613 页

[2] Lidong Zhou， Zygmunt J. Haas. Securing Ad Hoc Networks . IEEE Networks Special Issue on Network Security，1999,13(6),24-29

[3] H Luo， S Lu. Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks. Technical Report 200030， UCLA Computer Science Department 2000

[4] H Luo，et al. Self-securing Ad Hoc Networks . IEEE Symposium on Computers and Communications 2002. Italy. 2002. (7)

[5] 崔国华，金豪.基于 IBE 和秘密共享的分布式密钥管理和认证.信息安全与通信保密.2005，(2)，53 页

[6] Jean-Pierre Hubaux， Levente Buttyán， Srđan Čapkun. The Quest for Security in Mobile Ad Hoc Networks . Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing(MobiHoc)， 2001

[7] Srđan Čapkun， Levente Buttyán，Jean-Pierre Hubaux. Self-Organized Public-Key Management for Mobile Ad Hoc Networks. IEEE Transactions on Mobile Computing. 2003.2(l)

[8] Guha R，Kumar R，Raghavan P. Propagation of trust and distrust . WWW2004，New York， USA. 2004，17-22 页

[9] Beth T， Borcherding， M Klein B. Valuation of trust in open networks. Proceedings of the European Symposium on Research in Security (ESORICS)，Brighton：Springer-Verglag.1999.59-63 页

[10] Wang Y， Vassileva J. Bayesian network-based trust model. Proceedings of the IEEE/WIC International Conference on Web Intelligence. 2003

[11] 刘玉龙，曹元大.分布式环境主观信任模型研究.北京理工大学学报.2005.25(6). 504-508 页

[12] Yan Sun, Wei Yu, Zhu Han, and K. J. Ray Liu. Trust Modeling and Evaluation in Ad Hoc Networks . accepted, IEEE Globecom 2005

[13] George Theodorakopoulos, John S. Baras Trust Evaluation in Ad Hoc Networks. ISR Technical Report MS 2004-2, MSc Thesis, 2004.(5)

[14] 李承，汪为农.浅议移动 Ad Hoc 网络路由协议中的安全性问题.计算机工程与应用.2002，22，28-29 页

[15] 赵志峰，郑少仁.Ad Hoc 网络体系结构研究.电信科学.2001,1,14-17 页

[16] 王海涛，郑少仁.移动 Ad Hoc 网络中的安全问题.中国数据通信.2002，(8)，65-68 页

[17] 周海刚，肖军模. Ad Hoc 网络中的安全问题和安全策略.电信科学.2001，(12).39-41 页

[18] 王海涛,郑少仁. Ad Hoc 网络面临的挑战及其对策. 中国数据通信.2002,(5)，73-77 页

[19] K.Raina，A.Harsh.战晓苏等译.移动商务安全实用指南.清华大学出版社，2003

[20] 赵英.移动互联网技术及移动电子商务.情报科学，2002，20(6)

[21] L.Stojmenovic. Handbook of Wireless Networks and Mobile Computing. John Wiley & Sons, Inc, 2002

[22] 谢新梅等.4G 无线通信系统及其关键技术分析.现代通信，2003，(1)

[23] 张禄林等.移动互联网的结构及其技术发展趋势.通信世界，2000，(10)

[24] Kärpijoki V, Security in Ad Hoc Networks. http://www.hut.fi/~vkarpijo/netsec00-manet-sec.ps.2000

[25] Khalili A, Arbaugh W A. Security of wireless ad-hoc networks. 2002

[26] 况晓辉，胡华平，吕世辉.移动 Ad-hoc 网络安全.小型微型计算机系统.2003,24(10),1861 一 1864 页

[27] 宁红宙, Ad Hoc 网络中 PKI 理论和技术的研究，北京交通大学博士学位论文，2006，6

[28] B Schoenmakers. A simple publicly verifiable secret sharing scheme and its application to electronic voting. CRYPTO'99. 1999：148-164 页

[29] 熊焰，苗付友，张伟超，王行甫.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.电子学报，2003.31.(2). 161-165 页

[30] Lamport， et al. The Byzantine Generals Problem. ACM Trans On Programming Languages and Systems. 1982. (4). 382-401 页

[31] R. Canetti. Studies on Secure multiparty computation. PHD Thesis. 1995

[32] 徐邦海，蒋泽军，刘晓婷.移动自组网信任模型研究综述.航空计算技术. 2005.35. (3). 117-120 页

[33] Audun Josang， Roslan Ismail， Colin Boyd.A Survey of Trust and Reputation Systems for Online Service Provision. Decision Support Systems，(to appear，preprint available online： http：//seccurity dstc.edu.au/staff/ajosang)， 2004

[34] S. Marsh. Formalising Trust as a Computational Concept. PhD Thesis. University of Stirling， UK， 1994

[35] Pradip Lamsal. Understanding Trust and Security . http：/www.cs.helsinki.fi/u/lamsal/asgn/trust/UnderstandingTrustAndSecurity.pdf. 2001

[36] 谢冬青，冷健.PKI 原理与技术.北京：清华大学出版社.2004.(1)

[37] 宋健.移动Ad Hoc网络信任模型研究.解放军信息工程大学硕士学位论文，2006，4

[38] 宁红宙, 刘 云, 何德全. 一种用于Ad Hoc网络的分布式证书撤消算法. 北京交通大学学报, 2005, 29(2): 44-46页

攻读硕士学位期间发表的论文和取得的科研成果

[1] 花向东，李阳，李慧.基于 MVC 模式的 Struts 框架的研究.信息技术.2005.7.103-105 页

致 谢

在论文完成之际，首先感谢我的导师李健利副教授，本文是在李老师的悉心指导下完成的。感谢他在我完成论文工作中给予的指导和启迪。

感谢哈尔滨工程大学计算机学院的领导和老师们，感谢你们一直以来对我的关心和支持，使我完成学业。

感谢我单位—哈尔滨铁道职业技术学院的领导和同事们，是你们的鼓励一直支撑着我。

感谢我的同学和朋友们，是他们让我在学习中得到了更大快乐。

感谢我的父母、妻子、女儿，感谢所有曾经关心支持我的师长和亲戚朋友。

个 人 简 历

1987 年 9 月 -1991 年 7 月　苏州铁道师范学院 数学系　　学生

1991 年 7 月 -1996 年 9 月　哈尔滨铁路工程学校　　助理讲师

1996 年 10 月-2001 年 9 月　哈尔滨铁路工程学校　　讲师

2001 年 10 月-2002 年 9 月　哈尔滨铁路工程学校　　高级讲师

2002 年 1 月 -2005 年 9 月　哈尔滨铁道职业技术学院　　高级教师

2005 年 10 月-现在　　哈尔滨铁道职业技术学院　　副教授

于2003年9月进入哈尔滨工程大学计算机科学与技术学院在职攻读硕士学位。

移动Ad Hoc网络中信任模型的研究

作者： 花向东
学位授予单位： 哈尔滨工程大学

相似文献(10条)

1.期刊论文 李柯.蒋理.蒋泽军.王丽芳.LI Ke.JIANG Li.JIANG Ze-jun.WANG Li-fang 异步移动Ad hoc网络信任模型的研究与设计 -计算机应用研究2006,23(11)

介绍并分析一些已经出现的安全策略,然后结合异步网络的特点,提出一个基于PKI的适合于异步移动Ad hoc网络环境的信任模型.

2.学位论文 胡雷 移动Ad Hoc网络中信任模型的研究 2008

移动Ad Hoc网络随时组网投入运行、抗毁坏的特性使它在战场、灾难救助等基础设施缺乏的场合有着广泛的应用前景。移动Ad Hoc网络的这种优点得益于它的不依赖基础设施的特性。但是,自组织的特性同时也带来安全问题。自组织性使得移动Ad Hoc网络允许网络节点自由加入和离开网络、在合理的速率范围内自由移动,同时使得敌对、恶意方有机可趁。

移动Ad Hoc网络中节点和信号传输范围外的节点的通信都必须寻求相邻节点的帮助,以这些相邻节点作为路由器转发自己想要交给接收方的数据,因此完成这些任务的包流经中间节点时,中间节点取得对包的完全控制权,移动Ad Hoc网络中的恶意行为节点利用这个便利可以对移动Ad Hoc网络发起多种攻击,使得移动Ad Hoc网络的安全问题显得尤为突出。

信任模型,利用移动Ad Hoc网络中无线链路开放的特性对节点行为进行监听,从而对节点行为进行判断,以此建立起对行为节点的经验,以区分合法节点和恶意节点。这种方法无需借助外部设备,可以在完全保持纯Ad Hoc特性的情况下工作。但是它在和各种Ad Hoc协议配合工作的时候,也存在不少的问题。

本文在分析了几种典型的Ad Hoc网络协议的脆弱性、信任模型在这几种协议下工作时存在问题的基础上,提出了一些对移动Ad Hoc网络信任模型的改进方法：利用上层协议的反馈信息辅助信任模型评估中间节点的行为,加快拉开合法节点和恶意节点的信任度的差距,减少恶意节点危害网络的时间；路由建立阶段的路由请求和应答包携带所有的路由积累信息帮助信任模型识别恶意行为,并且节点对路由积累信息进行扫描,可以在路由建立阶段排除恶意节点；改进信任度的计算方法,以合法行为/恶意行为对网络层任务的影响来分配事件权重。仿真结果显示,以上方法可以在适当增加路由开销和计算量的情况下,改善了文中提到的原信任模型的性能。

3.期刊论文 谭运宝.钟诚.张尊国.TAN Yun-bao.ZHONG Cheng.ZHANG Zun-guo 一种基于邻居合作监测的移动Ad hoc网络信任模型 -微电子学与计算机2008,25(10)

针对自私节点的恶意丢包行为,将节点和其邻居节点所监测的结果结合起来,计算出节点间的信任度,并以此作为路由选择的依据来促进节点间的相互合作,提出一种基于邻居合作监测的移动Ad hoc网络信任模型.将信任模型应用于DSR路由协议并在NS2中进行仿真实验,结果表明该信任模型可以有效地缓解自私节点造成的影响,提高了网络的分组投递率.

4.学位论文 张长伦 移动Ad Hoc网络自组织公钥管理研究 2008

移动Ad Hoc网络是一种新型的无线移动网络，它不需要预先铺设基础设施，组网快速灵活，具有广阔的应用前景。然而，网络拓扑结构动态变化、无线传输带宽有限和移动终端能源受限等特性也带来了许多新的安全问题，所以需要研究适合移动Ad Hoc网络的新的安全方案和安全策略。

保密性是许多安全服务的内在假设，而密钥管理是其成功实施的关键。由于不需要复杂的安全引导过程，自组织公钥管理已成为移动Ad Hoc网络密钥管理的一类重要可选方案。但是，现有的方案大多存在着认证成功率低、预热期长和扩展性差等问题。因此，分析移动Ad Hoc网络自组织公钥管理的特殊需求，给出合适的解决方案，对移动Ad Hoc网络安全技术的发展与应用都具有重要意义。

本论文对移动Ad Hoc网络自组织公钥管理方案重点关注的认证度量、认证成功率、预热期、证书存储和通信量等关键指标及其影响因素进行了研究，并提出了相应的解决方案。本论文的研究工作受到了国家自然科学基金项目“Ad Hoc网络中公钥管理与性能评估技术的研究（No. 60572035）”和通信与信息系统北京市重点实验室项目“智能化无线安全网关项目（No. JD100040513）”的资助。

论文的主要工作与创新点如下：

1．针对一些采用信任分级来度量信任关系的应用环境，提出了一种基于离散度量的云信任模型。模型引入信任基云和接受因子对实体之间的信任关系进行描述，将实体之间的信任程度和信任的不确定性统一起来，表达了信任表述和推理中存在的模糊性和随机性，相应的信任推理机制可以处理信任推荐和多路径信任综合，实现信任关系的传播。仿真实验表明：与现有模型相比，本模型的信任推理能产生较高的合作成功率及良好的抗攻击能力。

2．针对网络层数据等信任数据源多采用连续度量模式处理的应用环境，提出了一种基于连续度量的云信任模型。模型基于上下文环境等因素给出新的信任云的定义和计算方法，在充分考虑不同信任云的权重对信任结果的影响下，给出基于连续度量的信任云推理机制，并利用信任数乘处理不同上下文环境的信任综合。仿真实验表明：该模型能够很好的评估节点间的信任关系，有效的检测恶意节点。

3．提出了一种路由已知的信任路径查找方法。该方法充分利用局部信任信息以及可能存在的路由信息，缩小信任路径查找的范围，降低了通信量。

4．提出了一种产生小世界证书图的方法。该方法对移动Ad Hoc网络进行分簇，在随机选取的两个簇首之间以一定的概率签发少量的证书，使形成的证书图具有明显的小世界现象，从而提高了节点交换和收集证书信息的效率以及公钥认证的成功率。仿真实验表明：基于这种小世界特性的证书图认证成功率可以达到80％以上，比原有方案约50％的成功率有很大提高，同时也缩短了预热期。

5．提出了一种增强的移动Ad Hoc网络自组织公钥管理方案。该方案在证书库创建的过程中采用主要依靠局部信息交换的原则，同时把小世界特性和信任模型应用到公钥管理的证书颁发、证书维护和公钥认证等各个操作之中。分析表明：增强的自组织公钥管理方案较已有方案提高了认证度量的可靠性，减小了证书库创建的通信量，降低了算法的复杂性，具有良好的可扩展性。随着移动Ad Hoc网络的自组织公钥管理方案的性能不断改善，其应用领域也会逐步推广，研究工作会得到进一步发展。

5.会议论文 谭运宝.钟诚.张尊国 一种基于邻居合作监测的移动Ad hoc网络信任模型 2008

针对自私节点的恶意丢包行为,将节点和其邻居节点所监测的结果结合起来,计算出节点间的信任度,并以此作为路由选择的依据来促进节点间的相互合作,提出一种基于邻居合作监测的移动Ad hoc网络信任模型.将信任模型应用于DSR路由协议并在NS2中进行仿真实验,结果表明该信任模型可以有效地缓解自私节点造成的影响,提高了网络的分组投递率.

6.学位论文 宋健 移动Ad Hoc网络信任模型研究 2006

移动AdHoc网络是由一组带有无线收发装置的移动终端组成的多跳临时性自治系统。它具有无中心、自组织等许多不同于传统无线网络的特点，这使其在军事及民用领域中的应用前景非常广阔；但同时也使其比传统网络面临更多的安全威胁，其中，以路由安全问题最为突出。信任关系的建立是所有安全策略实施的基础，所以本文重点研究移动AdHoc网络的信任模型。

本文深入探讨了移动AdHoc网络所面临的安全威胁以及信任的概念和特点，并在此基础上对现有的移动AdHoc网络身份信任和行为信任模型进行了深入研究和分类介绍。通过比较我们发现，现有的信任模型存在很多仅依靠传统安全策略无法解决的问题，例如，身份信任关系的建立、撤销等机制缺乏决策标准，路由安全无法保障等。为了解决这些问题，本文将行为信任评估机制引入基于PKI的移动AdHoc网络身份信任模型，实现网络节点间的身份可信与行为可信。改进后的模型将行为信任作为身份信任关系更新、撤销的决策标准，并通过行为信任评估动态的改变CA节点集合，力求更好的兼顾网络的可用性与安全性。最后，我们对改进后的信任模型的安全性与可用性进行了分析和评估，并对其研究前景进行了展望。

7.会议论文 杨斌.路晖 基于动态信任模型的MANET安全路由方案 2007

移动Ad hoc网络安全问题受到广泛关注,现有安全方案都存在局限性。论文分析了路由协议的安全威胁,安全需求。提出一种基于动态信任模型的安全路由协议(DTM-based SRP),有机结合现有安全机制,提高路由协议的可用性及抗攻击能力。

8.学位论文 谢寿吾 移动Ad Hoc网络安全策略研究 2007

移动Ad Hoc网络作为一种新型的无线移动网络，是由一组带有无线收发装置的移动节点组成的一个多跳的临时自治系统。因其特有的无需架设网络设施、可快速组网等特点，成为了军事战地以及特殊需要紧急组网的情况下，比如地震，水灾、森林火灾等救援行动的首选。同时，移动Ad Hoc网络也逐步应用于商业环境中，比如传感器网络、移动会议、家庭网络、虚拟教室等。移动Ad Hoc网络在给我们的生活带来了极大的便利，但由于其节点具有充分的能动性，导致网络拓扑结构容易发生变化，安全性比较差，严重影响了其发展和应用，因此，迫切需要适合该网络特点的安全解决方案。

论文从结构上可以分为课题研究思路的提出、移动Ad Hoc网络安全机制的研究、引入分群策略的分布式信任模型的设计和模型的模拟与仿真四个部分。主要工作包括：

1、介绍了移动Ad Hoc网络的背景知识、特点。分析了目前该网络在安全方面的研究状况和存在的问题。

2、介绍了移动Ad Hoc网络的安全策略和需用到的相关密码知识。通过对基于不同密码体系签名算法的对比分析，采用了基于椭圆曲线的签名算法，从而使分布式信任模型在相同条件下，认证的效率及安全性有了明显的提高。

3、提出了一种有效的引入分群策略的分布式信任模型。结合秘密共享技术和PKI公钥解决方案，构建了一个建立在PKI之上的、适合于Ad Hoc网络环境的安全、可靠的信任关系模型。其内容包括群的形成、系统初始化、证书颁布、证书翻新和撤销等。

4、通过APE仿真平台对信任模型进行性能分析，重点模拟和分析了证书颁发过程。

论文针对移动Ad Hoc网络的安全策略问题，特别是密钥管理和证书认证方面做了深入的研究，并在信任模型的设计方面融入了分群策略。从结果上看，该模型减少了运算量，节省了存储空间和带宽，在一定程度上提高了移动Ad Hoc网络密钥管理的性能。

9.学位论文 沈颖 基于移动Ad Hoc网络的PKI/CA系统研究 2004

移动AdHoc网络(MANET，MobileAdhocNETworks)是由若干无线移动节点组成的不依赖于任何固定基础设施和集中式组织管理机构而通过节点间的相互协作进行网络互联的一种多跳自组织临时性自治网络系统。网络中每个节点兼备主机和路由器两种角色，通过无线信道实现移动节点之间的通信，主要用于军事战术通信、紧急情况下的快速组网及其它对安全敏感的环境。由于自身的特性和特殊应用使得移动AdHoc网络近年来逐步得到学术界的关注和研究，具有重要的战略意义和潜在的广阔的商业应用前景。

移动AdHoc网络所固有的大部分特性也正成为其潜在的脆弱点，使其更易遭受各种安全威胁。类似于传统有线网络，在移动AdHoc网络中同样需要解决网上身份认证、信息完整性和抗抵赖等安全问题。公钥基础设施和认证机构(PKI/CA，PublicKeyInfrastructureandCertificationAuthorities)体系是一种基于公开密钥理论和技术建立起来的安全体系，它的核心是要确认信息网络空间中的信任关系。PKI/CA体系在解决有线网络的这些安全问题方面已经成为一种比较有效和完善的安全解决方案。然而这种中心集中式PKI/CA体系无法直接应用于移动AdHo网络c。因此建立适合于移动AdHoc网络的PKI/CA系统是一个具有挑战性的任务，也是其未来应用必需要解决的问题。

本文是针对移动AdHoc网络面临的安全问题，致力于建立适合移动AdHoc网络环境的PKI/CA系统模型而开展的应用基础性研究。文章在介绍移动AdHoc网络背景、概念、特性的基础上，通过实施一个高层的安全风险分析，指出了移动AdHoc网络面临的安全问题和挑战。同时介绍了有关信息安全的基本理论和安全技术的相关知识，详细分析了公钥基础设施和数字认证机构的基本概念、功能及组成结构。针对移动AdHoc网络环境，提出了建立安全系统所要遵循的基本要素，并就国内外现有的安全解决方案进行了分析，指出了其中存在的问题。在对信任模型研究的基础上提出了局部分布式信任模型和扩展推荐信任模型，并就此提出了多域全分布式CA系统模型，建立了分布式系统管理和分布式证书服务机制，通过NS-2网络模拟器仿真模拟测试初步验证了模型的可行性和有效性。此外还进行了移动AdHoc网络的PKI/CA互操作技术和结构模型研究，提出了基于扩展推荐信任模型的CA互操作结构模型，通过动态信任路径管理模式和认证机构信任列表实现CA间信任关系的管理和维护。

10.期刊论文 陈怡.杨天怡.刘益良.黄勤.唐丹.CHEN Yi.YANG Tian-yi.LIU Yi-liang.HUANG Qin.TANG Dan 基于行为的Ad Hoc网络分布式CA推荐信任模型 -重庆大学学报（自然科学版）2007,30(1)

移动Ad Hoc网络是一组带有无线收发装置的移动节点组成的一个多跳的临时性自治系统,根据其通信具有局部性这一特点,可以建立移动Ad Hoc网络的多域全分布式CA系统.在研究如何建立不同域间的CA信任关系时,提出了基于行为的扩展推荐信任模型.它通过网络运行中的反馈信息,动态管理信任路径,提高了系统的安全性、可伸缩性和鲁棒性.