移动自组织网络安全接入技术研究综述

乔 震[1] 刘光杰[1] 李 季[1] 戴跃伟[1,2]
(南京理工大学自动化学院 南京 210094)[1] (江苏科技大学 镇江 212003)[2]

摘 要 针对移动 Ad hoc 网络的特点对其中存在的主要安全威胁进行了分析,给出了 MANET 中安全接入的概念以及主要的性能要求。在此基础上,对 MANET 的主要安全接入技术进行了回顾,对各方案的优缺点进行了分析。最后对几类典型的安全接入方案进行了比较,并对未来值得进一步研究的问题进行了展望。

关键词 移动自组织网络,安全接入,认证,密钥管理,门限密码
中图法分类号 TP393 **文献标识码** A

Survey on Secure Access Technology in Mobile Ad-hoc Network

QIAO Zhen[1] LIU Guang-jie[1] LI Ji[1] DAI Yue-wei[1,2]
(School of Automation, Nanjing University of Science and Technology, Nanjing 210094, China)[1]
(Jiangsu University of Science and Technology, Zhenjiang 212003, China)[2]

Abstract In this paper, the main security threats were analyzed based on the characteristics of MANET. The concept and the performance demand of the secure access were presented. With that, the major secure access techniques of MANET were reviewed and the merits and demerits of each scheme were analyzed. Finally, the several typical kinds of secure access schemes were compared. And the problems which are worth studying further were forecasted.

Keywords MANET, Secure access, Authentication, Key management, Threshold cryptography

1 引言

1.1 MANET 基本概念和安全威胁分析

移动 Ad hoc 网络[1,2] (Mobile Ad hoc Network, MANET)是由一组带有无线收发信装置、逻辑上对等的移动节点组成的一类无线移动通信网络,它不依赖于预设的基础设施,通过传输范围有限的移动节点间的相互协作和自我组织保持网络连接和实现数据的传递,是无中心、自组织、多跳的移动无线网络。

MANET 可广泛应用于军事战场信息系统、民用紧急救助、传感器网络等众多领域,具有重要的研究意义和应用价值。作为一种新型的网络结构,MANET 具有无中心、分布式控制、自组织、对等性、拓扑动态性、链路带宽有限、有限的节点能量和计算能力、多跳性、有限的物理安全等诸多特点。MANET 的这些特点使其相比传统网络所面临的安全威胁以及采用的安全机制方面均有较大的不同[3-5]。具体分析如下:

(1)节点之间的无线通信,使得 MANET 更易受到窃听、假冒、篡改、重放和拒绝服务(DoS)等攻击。开放的广播信道环境也使得网络中的节点不可避免地受到各种直接或间接攻击。

(2)当节点工作于对抗环境中时,移动节点可能漫游到敌方区域而被俘获,节点内的密钥、报文等信息存在被破获的危险。更为严重的是被俘获节点仍以合法身份参与网络组建和活动,可被用来获取秘密或破坏网络的正常功能,使 MANET 面临来自网络内部节点的攻击。因此,MANET 不仅要防范来自网络外部的入侵,还要对付来自网络内部节点的攻击。

(3)由于节点经常移动或是加入/退出而导致的网络拓扑频繁改变使得 MANET 的安全边界模糊,导致传统防火墙技术难以实施,还会引起节点间信任关系的频繁变化,这就要求 MANET 的安全措施应具有动态适应性。

(4)MANET 网络的对等性,使得传统网络中为保障信息机密性、完整性、不可抵赖性等安全服务的公钥基础设施难以在 MANET 中部署。

(5)MANET 中移动节点的无线带宽、电池能量、计算能力均有限,这使其无法支持复杂的安全协议和加密算法。在设计 MANET 安全策略的过程中因为能耗问题,有时甚至只能采用有限的安全服务。同时能量的有限性使得攻击方也可通过增加额外的通信量和复杂的计算,对移动节点进行 DoS 攻击,通过耗尽其能源,而使其无法为其他节点提供服务。

(6)MANET 组网和通信过程中的各种运算和决策一般均依赖节点间的协作来完成,这种协作机制易遭到邻近的恶意节点和已被控制的内部节点的攻击。另外,网内节点的"自私"行为也会对网络通信性能产生影响。

1.2 MANET 安全接入基本概念

通过对 MANET 自身特点及其所面临安全威胁的分析

到稿日期:2013-02-06 返修日期:2013-07-02 本文受国家自然科学基金(61170250,61103201),江苏省自然科学基金(BK2010484)资助。
乔 震(1973—),男,博士生,主要研究方向为网络与信息安全,E-mail:qiaozhennust@163.com;刘光杰(1980—),男,博士,副研究员,主要研究方向为网络与信息安全;李 季(1985—),男,硕士,主要研究方向为网络与信息安全;戴跃伟(1962—),男,博士,教授,主要研究方向为复杂系统建模仿真与评估、信息安全。

发现，由于 MANET 存在网络拓扑的频繁改变和移动节点的加入/退出，若不采取可靠的安全接入控制机制，则无法有效阻止非法节点的侵入和攻击。MANET 安全接入技术是指在网络建立阶段或有新节点接入网络时，对申请接入节点所进行的一系列用于确保接入节点身份合法性的认证和相应的密钥协商机制。它一般采用密钥管理机制来实现节点身份的认证，并通过密钥协商生成会话密钥以保障通信的机密性。安全接入技术主要涉及以下性能指标：

(1)安全性：指网络能否为节点提供保障通信的机密性、完整性、不可否认性等安全服务，以抵抗窃听、假冒、篡改、重放、合谋和拒绝服务(DoS)等安全攻击。

(2)接入成功率：指节点成功接入网络的几率。

(3)易部署性：指网络初始化是否简便且易于实施。初始化工作具体包括：a)系统主密钥的生成、密钥的分发和存储；b)接入认证服务节点选举；c)节点数字证书生成、分配、存储及管理。

(4)密钥全生命周期管理：指是否支持密钥从产生、更新、销毁的全生命周期管理问题。

(5)通信负担：指安全接入所需的通信跳数、流量及次数等。

(6)计算复杂度：指安全接入算法所需要的 CPU 和存储消耗。

(7)可扩展性：指安全接入机制适应网络规模扩展的能力。

(8)抗毁性：指当部分网络节点损毁、失效、被俘，或者部分链路断开的情况下，网络还能为其节点提供可靠的安全接入服务的能力。

研究者已经提出了多种针对 MANET 网络特点的安全接入技术。根据安全机制中采用的密钥体制，可将它们分为基于单钥体制、基于双钥体制和基于单、双钥体制的安全接入技术；根据公钥密钥的不同管理方式，又可分为基于证书(PKC)、基于身份密码(IDC-PKC)和基于无证书的安全接入技术(CL-PKC)。本文对若干典型的安全接入技术进行回顾和分析，总结归纳方案的优缺点，对各类典型安全接入方法进行了综合比较，并对 MANET 安全接入技术未来需要进一步研究的问题进行了展望。

2 基于口令认证的安全接入

基于口令认证的安全接入的基本原理是通过网络中事先共享的接入口令来实现节点间的身份认证，并在完成身份认证后协商一个短期的会话密钥，以保障后续通信的安全。

Bellovin[6] 等人提出了一种基于口令的认证协议，该协议称为加密的密钥交换(EKE, Encrypted Key Exchange)。EKE 协议使用概率加密技术对口令进行随机的“加盐操作”，放大了口令的空间，从口令的字典变成某个随机的非对称密钥空间，它不仅可以抵抗对于口令的在线窃听，还可以抵抗离线字典攻击等被动攻击；通过引入相应的检测机制[7]，主动攻击可被诚实的协议参与者以很大的概率成功检测，并果断废止协议的运行。同时，EKE 协议还提供了一种完善的口令更新机制，网络节点间的安全连接通过不断变化的口令建立，这样即使攻击者破解了当前的口令，他也无法知道之前的口令，保证了之前的通信数据不会泄露[8]。在 EKE 协议中所有的节点都参与了密钥的生成，这使攻击者的干扰无法阻止会话密钥的生成。但对于较大范围的网络，会话密钥的生成将会非常复杂，可扩展性较弱。

在会话密钥协商方面，从传统的 Diffie-Hellman 密钥协商协议到椭圆曲线密码体制(elliptic curves cryptography，简称 ECC)下的密钥协商方案，国内外学者已经做了大量工作，如文献[9-11]中的方案等。王晓峰[12]等基于 ECC 提出了一种适用于 MANET 的具有口令认证和共享口令进化的多方密钥协商方案。其主要思想是采用共享口令进化机制来保证每次认证节点密钥和协商会话密钥时口令的新鲜性和安全性，从而既减轻了移动节点的计算量和存储负担，也实现了移动节点之间的密钥认证和信息加密。该方案具有抗中间人攻击、抗重放攻击、密钥独立和前向安全等多种安全特性。但该算法同样无法阻止攻击节点使用合法口令接入网络。

综上所述，基于口令的安全接入方法的缺陷在于节点之间仅依赖口令作为信任的凭证来实现相互的认证并以此为基础生成会话密钥，缺少对新接入节点的身份认证机制，且任何具有口令的节点均可以冒充合法节点接入网络。因此，基于口令的安全接入方法仅适合于对安全性要求不高的场合。

3 基于门限密码的分布式安全接入

在强对抗环境下，由于 MANET 节点容易受到攻击、损毁或由于强电磁干扰导致连接暂时不可用，基于单一认证中心的安全接入机制存在认证中心单点失效的风险。为增加网络的抗毁性和生存能力，可将原来集中的认证服务分散到若干可靠节点上，以实现分布式认证。在分布式认证中，有以下基本假设：即在自组网中，尽管没有任何一个单独的节点是值得信任的，但若干节点的集合是可信任的，系统中所有节点都已知系统公钥，并信任对任何节点的公钥证书用系统私钥的签名。

3.1 部分分布式安全接入

Zhou[13] 等提出了一种基于门限密码的异步的部分分布式密钥管理方案。部分分布式门限密码认证方案采用了门限密码(n,t)体制来进行密钥管理。门限密码(n,t)表示在 n 个服务节点的网络中，任意大于等于 t 个人协作都能恢复出密钥 key；而任意 $t-1$ 或更少的人协作对恢复密钥 key 没有任何帮助。该方案采用门限数字签名来保护路由信息、数据交换和节点的身份认证，它要求系统有一个公钥/私钥对，用来对每个节点的公钥证书进行签名和验证，以识别节点身份。每个节点还要有各自的公钥/私钥对，对交换的数据进行加密和签名。在网络中任选 n 个节点作为服务节点，把系统私钥 SK 分成 n 份分发给各个认证节点，使每个认证节点都有一份系统私钥，密钥管理服务由 n 个服务节点中的任意 k 个节点提供。其工作原理如图 1 所示，申请接入的合法节点向网络中其他节点发起接入申请，可提供认证服务的节点利用其分配到的系统私钥分量对申请接入节点的公钥进行门限签名，这些签名最终返回接入节点形成由系统私钥签发的公钥证书。

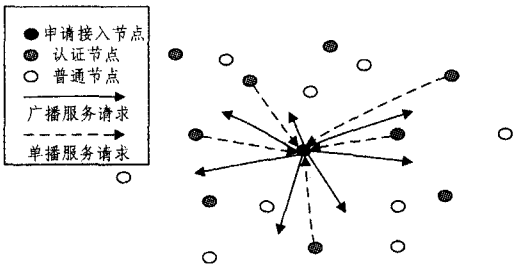

图1 部分分布式接入认证模型

系统的安全性基于这样的假设，即在一段时间内最多有 $t-1$ 个服务节点被占领。为了保证系统的安全性，还可采用认证节点私钥定时更新的方法，使攻击者更难同时获得 t 个认证节点的有效系统私钥分量。部分分布式门限密码认证技术的优点是将单一的认证服务分散到 n 个节点中，有效地防止了因单点失效而导致的 MANET 网络崩溃，提高了网络健壮性。但仍存在一些缺陷[14]：(1)新加入节点需要到 t 个认证节点去申请证书，这些节点可能遍布于网络各处，需要多跳通信才能达到，一定程度上增加了网络的通信负荷；(2)提供安全接入的认证节点的计算量和通信量都较大，容易造成通信瓶颈；(3)门限机制中的参数 n 体现了方案的可用性，t 体现了方案的安全性，如何选择合适的 n 和 t，以及如何"选举"可靠性高的节点充当认证节点是需要仔细考虑的问题。

熊焰、苗付友[15]等人提出了一种基于"多跳步加密签名函数"签名的分布式认证方法，该方法将 Sander 等[16]提出的移动密码学与门限加密分布式认证相结合，并采用了分布式容错处理技术中的 Lamport 协同一致算法解决被攻破认证节点的 Byzatin 攻击问题，以发现和避免认证节点被攻破后提供假私钥分量破坏认证私钥生成的行为；采用了私钥分量刷新技术来保护私钥分量和认证私钥不外泄，以提高门限加密的安全性。在该算法中，由于使用计数器对证书生成过程中跳数进行计数，使得攻击者可以通过篡改计数器跳数的方法来达到破坏数字签名证书生成的目的。

Dey[17]等人在部分分布式认证节点的基础上，设计一种安全接入方案。该方案规定如果节点 B 从节点 A 处得到一份认证分量，就在两个节点间画一条有向线段连接起来，方向由认证节点(节点 A)指向被认证节点(节点 B)。然后，通过文献中给出的信任权重计算方法计算各自的权重值。网络中的所有节点经过这样的处理后，形成一张带权重的信任图。最后，从所有的认证节点中选择一个信任权重最高的认证节点作为"临时代表"(Session Leader，SL)。当有新节点要接入网络时，一个离线管理器首先为该节点选择一个认证节点作为"介绍人"(Introducer)。然后，该节点联系为其推荐的介绍人节点，通过验证算法验证申请接入节点的 ID 是否有效。如果符合条件，介绍人节点使用申请节点的公钥对临时代表的 ID 进行加密，然后发给申请节点。最后，节点通过该临时代表对其身份进行认证以及密钥协商，从而达到接入网络的目的。该算法通过临时代表选举(Session Leader Election)的方式使得申请加入的节点仅能通过临时代表进行认证而无法获得其他认证节点的 ID，保护了其他提供认证服务的节点，使其免于来自恶意节点的针对性攻击(precision attack)。该算法的缺点是每次有新节点申请加入都要通过离线管理机构为其选择介绍人节点，这在很多情况下是不现实的。同时，算法本身过于复杂，每次有新节点成功加入网络都需要重新更新信任模型的数据，这对节点自身资源的消耗比较大。

大多数基于门限密码的分布式认证方案都默认 MANET 中的所有节点均是可信的，都可以被用来作为认证节点。然而事实却并非如此，有很多方法采用了过于复杂的传统公钥密码体制，使得 MANET 中，节点往往因为自身资源有限难以承受复杂的计算。针对上述问题，Seung 等[18]认为应该挑选自身能力强的节点来提供接入认证服务，而不是随意指定，并据此提出了一种基于门限密码的 MOCA(MObile Certificate Authority)分布式认证方案。该方案中以节点的电池容量、通信范围、计算能力以及安全性作为选择认证节点的标准，并通过一个基于门限密码体制的离线密钥处理装置生成系统公钥和私钥，然后把私钥分量分发给每个认证节点。这个离线密钥处理装置通过物理隔离的方法，有效地防止了恶意节点通过网络的攻击，保证了整个网络的认证安全。但是，由于该装置存有完整的系统私钥，因此离线密钥处理装置的保护对整个网络的安全起着至关重要的作用。MOCA 为了保证高效的通信还专门设计了相应的路由协议来支持认证协议，以改善提供认证服务的节点的通信性能。

3.2 完全分布式安全接入

在采用部分分布式安全接入机制的大规模 MANET 中，新加入节点经常需要多跳通信才能到达认证节点，这在一定程度上增加了网络的通信负担以及转发节点的资源消耗。Kong 等[19]针对这些问题，提出了一个基于门限密码的完全分布式安全接入认证方案。该方案假设节点与单跳邻节点之间的通信要比与多跳节点之间的通信可靠，且每个节点至少有 t 个合法的单跳邻节点。完全分布式认证方案的工作原理如图2所示，与部分分布式安全接入方案不同之处在于，完全分布式方案中认证服务由网络中的所有节点共同承担，系统私钥不只分为 n 份由 n 个节点持有，且网络中每个节点都持有一份系统私钥分量，这大大降低了请求节点得到足够数量证书的难度。当有新节点加入网络时，只要向周围 t 个邻居节点提出申请，便可获得 t 份邻居节点保存的系统私钥分量，有了这些系统私钥分量即可形成一份完整的证书，从而将分布式认证转化为本地认证，提高了认证方案的可用性，且增强了扩展能力，降低了接入认证对网络资源的消耗。

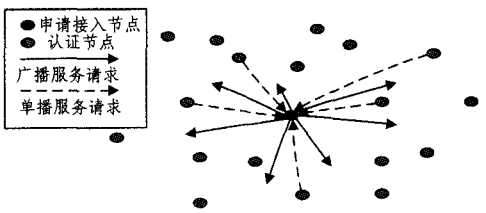

图2 完全分布式认证模型

在完全分布式安全接入方案中，为了防止由于部分节点被攻陷导致的私钥泄漏，节点的证书被设定了一个有效期，网络中的节点必须在有效期内对证书进行更新。这也是完全分布式与部分分布式安全接入方案的另一个区别。Luo 等在文献[20,21]中对文献[19]中方法做了进一步分析，增加了证书的更新与撤销机制，使得每个节点周围的邻节点不仅联合颁发证书，而且负责监视其行为。证书的更新与撤销机制的具体过程如下：

收到证书更新请求的邻居节点先检查请求节点的证书有

效期，如果还在有效期内，就检查自己保存的证书撤销列表CRL(Certificate Revocation List)，看请求节点是不是已经被自己的监视机制判定为恶意节点。同时，节点判定其某个邻居节点为恶意节点后，就把这个邻居节点的唯一标识符ID加入到自己的CRL列表中去，并广播一个控告信息来告知其他节点这个节点已经不可信。如果一个节点收到 t 个不同的节点针对同一节点的控告信息，则被控告节点就要被加入到本节点的CRL列表中。一个节点被系统所有的节点判定为恶意节点后将得不到证书更新，从而被隔离出整个网络。如果请求节点的证书既没有过期，ID也没有在被请求节点的CRL中，则其邻居节点就颁发一个用自己的部分私钥签名的证书给请求节点。收集到 t 份部分证书后，请求节点就可以把它们合并，得到用系统私钥SK签名的有效证书。

完全分布认证与部分分布认证相比，可扩展性更强，认证效率更高，并且能够提供证书的签发、更新和撤销等服务。该方案同样需要密钥管理设施来提供网络的初始化，每个节点在其加入到网络之前必须从管理机构处获得最初的有效证书，网络在初始化时管理机构选择 k 个节点共享密钥，再由这 k 个节点把各自分配到的系统私钥分量分发给其他节点，网络建成后由网络中的节点开始充当认证中心(CA)的功能[22]。这类方法的缺点是[14,23]：(1)认证私钥的初始化和更新过程比较复杂，如文献[21]中也没有介绍具体的初始化算法；(2)方案假设每个节点周围都至少有 t 个合法单跳邻节点，并不是任何时间任何地点都能满足这一假设，存在部分节点不能获得认证服务问题；(3)网络中的每个节点都是CA节点，攻击者只要攻击任意 t 个具有不同系统私钥分量的节点，就可以获得一份完整的系统私钥，从而降低了系统的安全性；(4)每个节点都拥有系统私钥分量，随着拥有系统私钥分量的节点数目的增加，对其管理和维护的费用也在增加。

Omar[24]等把信任图(trust graph)与门限秘密共享技术相结合构造了一种新的信任模型，并基于此模型提出了一种完全分布式安全接入技术。该算法使用节点分享到的系统部分私钥分量对证书进行签名，代替传统的使用节点本身私钥对证书签名。如果包含节点 B 的 n 个节点的集合中至少有 k 个节点信任节点 C，而 A 又信任 B，那么 A 就信任 C(如图3所示)。网络中的节点就是通过这种“信任传递”建立部分证书链(partial certificates chain)，并以此为根据形成信任图，从而最终建立信任模型。这种方法可以有效地抵抗恶意节点发布错误的公钥证书来欺骗证书服务系统。该方案仍存在密钥管理消耗大、系统安全性不高等缺点。

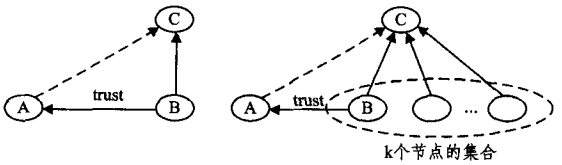

图3 信任关系模型

4 自组织式安全接入

分布式认证方法一般都需要离线的密钥生成器参与实现网络的初始化或是公认的CA来发布和维护证书。由于密钥生成器或是公认的CA拥有完整的系统私钥，因此对这些设备的保护对整个网络的安全起着至关重要的作用。Hubaux等人[25]为了消除这一安全隐患，提出了一种类似于PGP(Pretty Good Privacy)算法的自组织的密钥管理方案，并在文献[26]中对该算法进行了详细论述和模拟实验。该方案的实现主要是基于节点之间的信任关系，并且这种信任关系是可以传递的。网络初始化时，MANET中每个节点首先生成本节点的公钥和私钥，然后发布自己的证书并收集其他节点的证书，从而建立各自的证书数据库。其中，证书数据库中包含该节点颁发给其他节点的证书、其他节点颁发给该节点的证书、该节点转发给其他节点的证书。当有新节点要接入到MANET时，该节点与网络中的一些节点会合并它们各自拥有的证书数据库形成一张认证路径图，并希望从该图中发现一条认证链路，使得网络中的某一节点与申请接入节点间可达。如果存在这样一条认证路径，则认证成功；否则，认证失败。

上述方案不需要公认的CA来发布和维护证书，节点自己发布并维护证书，通过证书链来实现认证，防止了单点失败。与PGP不同的是，节点证书是靠节点自己分配并分布存储于其它节点的证书库中，而不是存储于认证服务器之中。同时，其缺点也是显而易见的[27,28]：认证基础是信任的可传递性，但是信任可传递性是有条件的，Hubaux的方案并不满足信任传递性的条件；没有CA来验证身份，任何能发布证书的节点均能加入网络，攻击者可假冒合法节点或编造节点标识发布证书加入网络；采用概率意义的认证方法，无法保证节点总能发现所需证书链(如果存在)；节点对证书库的维护会引入很大开销并影响扩展性；找到的证书链可能过长，安全性非常脆弱；方案进入正常运行前还需要经过一个预热的时间段。

Rafsanjani[29]等提出了一种改进的MANET自组织公钥管理策略，该算法的主要思想是：首先，每个节点生成自己的公钥/私钥对；然后，每个节点为其他邻节点提供自己的信任凭据，如果该节点的信任值达到邻节点的信任要求，它们之间就建立信任关系并通过秘密渠道交换公钥；最后，根据节点信任值生成证书并建立各自的证书库。密钥认证过程同文献[25]类似，都是合并各自证书库并试图找到一条可达认证链路。不同之处在于该算法的证书库中的证书只包含两类证书：节点颁发给其他节点的证书、其他节点颁发给该节点的证书。并且，发给使用者的每一个证书，其发布者也要存储。节点在下次发布证书给其邻节点时，会先搜索本地存储的证书，通过对比证书的ID决定是否发送，有效地避免了重复发送证书对网络资源的消耗。由于该算法主要是基于假设移动节点静止或是移动速度缓慢的情况，其适用性是该方案的主要局限。

刘世忠[27]等基于PGP的信任关系理论，利用门限秘密共享体制，提出一种基于MANET自组织密钥管理的节点安全接入方案。该方案通过对新节点的多点信任认证以及对身份标识的一致性、唯一性判断，保证了MANET中新节点的安全性。方案主要从节点转发能力和MAC的唯一且一致性对新节点的安全性进行验证，能很好地拒绝有“自私”行为的节点，且能很好地抵御假冒攻击。但当网络中节点移动速度过快时，可能导致申请接入节点在没被网络中已有节点认证成功就脱离节点的认证范围，从而使其在认证过程中获得的安全权值较低，安全节点反而不能加入到网络中。另外，大量

新节点在同一时刻向网络中同一节点申请接入时，很可能造成网络拥塞，使得节点接入申请因为得不到正常的服务而被拒绝。

董攀等[28]提出了一种新的自组织公钥管理方案 HPWKM(High Performance Web-of-trust Key Management)，HPWKM 把大规模 MANET 中的节点根据其任务、兴趣或目标的不同来划分安全域，以全新的域内节点证书预签发机制和异域节点证书签发机制为基础建立域内认证机制，同域节点可以利用域内证书链路径算法得到多条证书链路径。这样的设计使得该算法不但可挑选在开销、安全性上最有优势的证书链路径完成认证，还可使用多条证书链进行认证。HPWKM 继承信任网模型的自组织特点，不需要节点维护证书库，相比其他同类方案，具有更低的运行开销和更高的安全性。异域节点的认证设计为两次域内认证的合成，对漫游到其他域的节点的认证可能需要大量的远程通信，认证过程相对复杂，认证代价相对较高。

自组织认证机制更加符合移动自组织网络自组织特性，能够实现节点对系统安全设置的完全控制[30]。但是，缺乏证书撤销机制是这类方案存在的最大问题。由于证书的签发完全依赖于节点之间的信任关系，被俘获节点容易通过错误证书对网络造成危害，严重影响系统的容错性和安全性。且在网络构建初期，很可能因已签发证书数量不足导致在两个节点之间无法找到一条证书链，因此该方案比较适用于生存期较长的移动自组织网络。同时，由于缺乏可信任的第三方，因此通过证书链建立的信任的可靠性随着链长增加会迅速降低。所以，该类方法也不适用于对安全要求较高的、规模较大的 MANET。

5 基于身份的安全接入

基于证书的安全接入技术通过认证中心为用户签发公钥证书，以保证系统中节点身份的真实性。但是，新接入的节点要向 MANET 中所有的服务器节点注册自己的证书，而认证服务节点需要保存所有节点的公钥证书，并且当节点的证书更新或撤销时，认证服务节点的证书目录需要同步刷新。这使得网络消耗较大的计算、通信和存储资源来管理和维护各节点的公钥证书。

为了减少安全接入过程中节点间的通信次数和数据流量，降低 MANET 在证书维护和管理方面的开销，Khalili 等[31]将基于身份的密码体制[32]和门限密码技术相结合，提出了一种基于身份的 MANET 密钥管理方案。在网络初始化时，由离线的密钥生成器 PKG(Private Key Generation)生成系统的公钥/私钥对。然后，通过广播的方式将系统公钥告知网络中的所有节点。采用(n,t)门限秘密共享的方法为 n 个认证节点生成系统私钥分量。同时，每个节点都有一个具有唯一性的身份标识 ID(如名字、MAC 地址或 Email 等)作为节点的公钥，而与节点身份相应的私钥由 t 个 PKG 节点合作生成。两个节点间通信时，源节点使用系统公钥和目的节点的 ID 对信息进行加密，只有拥有与目的节点身份相应的私钥才能解密此信息。这种方案不需要公钥证书的存在，而且使用了由椭圆曲线构造的密码体制，与基于 RSA 公钥密码体制的管理方案相比，密钥长度更短，接入效率更高，降低了算法的复杂度和通信开销，但仍难以防止恶意节点通过发送假的系统公钥给新接入网络的节点使其拥有相应私钥的方式来实现中间人攻击的情况；网络初始化时，没有可信任第三方的参与，不适于对安全性要求较高的网络；新入网节点需要联系至少 k 个 PKG 节点认证身份，获得自己的私钥分量，如何安全可靠地实现此过程方案中也没有给出。随后，Deng 等[33]也给出了一种类似的基于身份的 MANET 密钥管理的方法。

上述两种方案中，都需要安全信道来传输用户私钥，而在 MANET 中预先建立和维护安全信道是十分困难的。李慧贤、王育民等[34]对上述两种方案进行了改进，提出了一种无需安全信道的安全接入方案。该方案通过门限技术，依靠 MANET 中的内部成员相互协作生成节点密钥；采用基于身份的密码技术实现对用户和分布式可信机构的双向认证；通过盲签名来实现对用户私钥在公开信道上的安全传输。该方案达到了较高的信任等级，具有良好的容错性，并能抵御网络中的主动和被动攻击，在满足 MANET 安全需求的情况下，极大地降低了计算和存储开销。

Zhang[35]等人从保护节点隐私的角度考虑，基于双线性映射提出了一种分布式匿名认证策略。该方法通过门限秘密共享和零知识证明(zero-knowledge proof)技术为 MANET 中节点在认证和密钥传递过程中提供匿名服务，使得恶意节点难以收集同一节点的位置、移动和通信方式等重要信息，从而达到保护网络中节点隐私的目的。同时，匿名性服务还可保护网络中的重要节点的安全，使其避免来自恶意节点的针对性攻击(precision attack)。

6 基于无证书的安全接入

基于身份的安全接入技术无需从数据库中查找节点公钥，也无需对公钥的真实性进行验证，有效地降低了节点终端计算和存储负担以及相应的通信开销。但是由于 PKG 知道任何节点的私钥，PKG 可对注册节点的通信信息进行窃听，或通过伪造任何注册节点的签名冒充合法节点加入网络并获取服务，即所谓的私钥托管问题。为了解决基于身份的密码系统中的私钥托管问题，Al-Riyami 和 Paterson[36]把基于证书的密码系统和基于身份的密码系统相结合，设计了一种无证书的公钥密码 CL-PKC(certificateless public key cryptography)系统。在无证书的公钥密码系统中，仍然存在一个可信的拥有系统主密钥的第三方密钥生成中心 KGC(key generation center)，KGC 的作用是根据用户的身份信息和系统的主密钥计算用户的部分私钥并安全地传送给用户。在安全地收到自己的部分私钥后，用户再使用该部分私钥和随机选择的一个秘密值生成自己完整的私钥，公钥由自己的秘密值、身份和系统参数计算得出，并以可靠的方式发布。通过这样的处理，用户就可以用自己的私钥进行解密和签名，而不必担心 KGC 对自己通信的窃听甚至伪造合法用户冒充自己的情况发生。与传统的公钥密码系统相比，无证书的公钥密码系统一方面保持了基于身份的公钥密码系统的身份易管理性，另一方面还解决了其固有的密钥托管问题，使得构建的安全接入协议在兼顾了基于证书的密码系统和基于身份的密码系统两者优点的同时，还从一定程度上克服了它们的缺点，进一步增强了系统的可靠性和可用性[37]。这类方法一经提出，就受到了相关研究人员极大的关注，成为密码学和信息安全领域研究的热点之一。

随着无证书密码学的快速发展，研究者们又提出了多种基于无证书认证密钥协商方案。Mandt 等[38]基于 Bilinear Diffie-Hellman 计算困难性假设提出了一种两方无证书认证密钥协商方案。Wang 等[39]也提出了一种类似的方案。Swanson 在文献[40]中定义了一种无证书两方认证协议的安全模型，并在定义的安全模型中对文献[38,40-41]中提出的方法的安全性进行了评估。结果表明，文献[36,38-39]的方法都是不安全的，方法主要不能抵抗密钥泄露伪装攻击或临时私钥泄露攻击。基于 Swanson 提出的安全模型，Lippold 等[41]提出了无证书两方认证协议的一个更强的安全模型，并给出了一个可证安全的无证书认证协议，但协议的计算复杂度较高。

葛爱军等[42]在文献[43,44]研究的基础上，利用 Schnorr 签名的思想，基于离散对数困难问题构造了一种新的不需要双线性对的无证书签名方案，使得方案效率要比其他现有的基于无证书签名算法效率更高。该方案虽然在公钥长度及签名长度等方面有所增加，但是在计算效率方面具有极大的优势。Samreen 等人在文献[45]中结合 RSA 算法和门限秘密共享技术提出了一种端到端的无证书安全认证策略。该方法依赖于大数分解的困难性来确保认证算法的安全性，同样达到了避免复杂双线性运算提高认证效率的目的。

7 MANET 安全接入中的其他问题

7.1 基于簇结构的安全接入

MANET 的网络结构一般分为平面结构和层次结构两种。如图 4 所示，在层次结构中，网络被划分为多个簇，每个簇由一个簇头和多个簇成员组成，由簇头节点负责簇间报文的转发。层次结构利用簇减少了网络管理的复杂度，提升了网络的可扩展性。

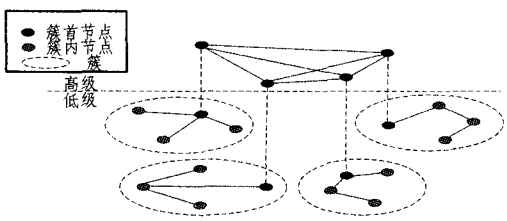

图 4 簇结构示意图

随着 MANET 的发展及其规模的扩大，基于簇结构的 MANET 因其具有更强的可扩展性、组网方式更灵活、网络综合性能高等优点，更适合应用于大规模 MANET，簇结构已成为未来 MANET 网络结构的主要组网方式。随着研究的不断深入，国内外研究者提出了最小节点分簇算法、最高节点度启发式算法、最低移动性分簇算法、限制簇尺寸的分簇算法、通用组合加权分簇算法等来形成和维护簇结构[46]。

Venkatraman 和 Agrawal 在文献[47]中针对簇结构的 MANET 提出一种安全接入方案。该方案在每个簇中选举一个簇首 CH(Cluster Head)提供安全管理功能，每个 CH 负责对新加入簇的节点进行认证、颁发证书以及生成簇内的共享密钥。该方案簇首存在单点脆弱性问题，一旦簇首被攻破，则整个簇中节点都将受到直接威胁。另外，由于簇首几乎提供所有安全管理和安全通信功能，因此簇首容易成为网络通信瓶颈。为克服这个问题，Bechler 等人在文献[48]中提出了另外一个基于簇结构 MANET 网络安全解决方案。在该方案中，多个 CH 一起构成一个逻辑网络，采用门限加密机制分配安全权限给每个 CH。CH 负责管理簇内安全，当簇首受到威胁时，可以把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首的单点威胁。当一个新节点加入簇时，簇内任何节点均可认证该节点并颁发许可，当一个新节点获得足够多的许可时，该簇就向该节点颁发一个合法身份的证书。当一个节点漫游到另外一个簇时，该簇将该节点当作网络的新节点，重新对其认证。该方案与文献[47]相比，具有更好的安全性和网络性能，但是网络中的 CH 需要承担证书中心 CA 的职责，包括在线证书发放、撤销等功能，大大增加了簇首的负担。其次，CH 虽然可以将职责转交给其他节点，但并没有从根本上解决单点脆弱性问题。最后，该方法没有考虑恶意节点的撤销和漫游问题，恶意节点即使被发现也仍然可以在网络中漫游，继续实施破坏网络的行为。

Li 等[49]将身份的密码体制与 MANET 的分簇结构相结合，提出了一种密钥管理方案。在网络初始化时，选择 n 个自身能力较强的节点充当簇首节点，这些节点在网络运行过程中一直充当簇首，负责簇内的安全管理，簇内成员节点与簇首协作，共同实现安全功能。在该方案中应用基于身份的密码体制，减少了网络的通信开销和计算量。但是，同文献[47]一样，该方案不具备通过簇首选举机制对簇首进行更换的功能，因此，仍存在单点脆弱性和网络瓶颈问题。

李涛在文献[50]中利用 Boyen[51]的签密体制，并结合门限密码体制，给出一种基于身份和簇结构的安全接入方案。首先把 MANET 中的所有节点分成多个簇，所有簇首构成一个逻辑网络，簇首间通信和簇内成员节点间通信采用不同的通信频率，构造成一个双频两级网络。然后，从簇首节点中选取 n 个性能优越的节点作为认证节点，通过门限密码技术为每个节点分配一份系统私钥分量。文献[50]中还增加了簇首选举机制，并给出了簇首持有的簇间私钥的产生和更新方法，与簇首节点持有系统私钥分量周期性更新机制共同保证了簇首的安全性和可用性，从一定程度上减轻了单点失效的威胁。同时，该方法还考虑到节点漫游到其他簇的情况，给出了相应的机制对漫游节点的身份进行验证。在该方案中，每个移动节点在加入网络之前，必须以离线方式向密钥生成机构(Private Key Generation，PKG)注册。这种方式可以很好地验证每个节点的身份真实性，提高 MANET 节点的可信度。但是，在很多情况下，不能保证能够找到可信的 PKG 进行离线注册。同时，该方案中缺少证书撤销机制，无法有效地抵抗内部攻击。最后，离线的 PKG 存有网络中所有节点的身份信息，一旦 PKG 被俘获，任何节点都可以进行离线注册并加入到网络中，使得整个网络面临致命的安全威胁。

吴旭光等[52]结合无证书的签密协议提出一种基于簇结构的 MANET 密钥管理协议。该方案不需要公钥证书，用户自己生成公钥，有效地降低了用户终端计算、存储能力的需求和系统密钥管理的通信开销。同时，密钥生成中心 KGC 为用户生成部分私钥，解决了基于身份密码体制中的密钥托管问题。最后，基于簇的结构将网络中的节点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，也便于对某些紧急情况快速做出反应。该算法的缺点是需要进行多次计算量大、耗时多的双线性对计算，对节点自身的资源和接入认证的效率有着一定的影响。

7.2 跨域认证问题

在实际应用中，通常把一些相互信任的节点联合起来形成一个具有某种独立功能的安全域，再由一个或多个安全域共同构成一个 MANET 网络。然而，MANET 是一个高度动态的拓扑网络，某个安全域中的节点经常会漫游到其他域中进行访问服务。并且，这些节点和被访问域的认证服务器之间事先并不存在信任关系。在这种情况下，被访问域就需要一种有效的支持跨域认证的安全接入策略，用以验证漫游节点的身份以及是否具有资格或是否足够安全，并以此为依据进一步判定是否为其提供服务或允许其访问域中的资源，从而避免对漫游节点重新进行复杂的身份认证，达到节省节点自身资源的目的[53-55]。

在早期的安全接入技术相关研究中，大部分研究者并没有意识到漫游节点的跨域认证问题，少部分注意到该问题的研究者也只是对漫游节点进行重新认证处理，并没有提出有效的跨域认证解决方案。随着 MANET 环境下节点漫游现象的日益增多以及对安全接入技术研究的深入，安全接入技术中的跨域问题成为了研究的焦点。设计合适的支持跨域认证的安全接入协议成为确保跨域通信安全的有效手段。由于对 MANET 的研究尚不成熟，只能借助于现有的有线通信中的跨域认证协议和密钥协商机制等较为成熟的方法来解决安全接入技术中的跨域问题。如图 5 所示，典型的跨域认证协议涉及到 3 类参与者[56]：漫游节点、漫游节点所属域(漫游节点的注册域，也称家乡域)认证服务器 HA(Home Authenticator)、被访问域认证服务器 FA(Foreign Authenticator)。为了使漫游节点能够安全地接入到其他安全域并访问域中的资源，MANET 中的各个安全域之间需要事先建立信任，构成一个联邦，而每个安全域相当于联邦中完成某一特定功能的一个联邦成员。当漫游节点访问其他域的资源时，被访问域的认证服务器 FA 需要联合漫游节点所属域的认证服务器 HA 对节点身份进行验证[59]。支持跨域认证的安全接入是比域内认证安全接入更复杂的安全问题，它涉及到的实体更多，认证及密钥协商过程也更加复杂。多信任域网络环境中共享资源的分散性以及支持跨域认证的安全接入技术的特点，决定了典型的跨域安全接入技术对被访问域身份的验证、对漫游节点所属域的验证，具有安全的密钥协商机制，同时，能够保证漫游节点的匿名性和不可跟踪性[58-60]。

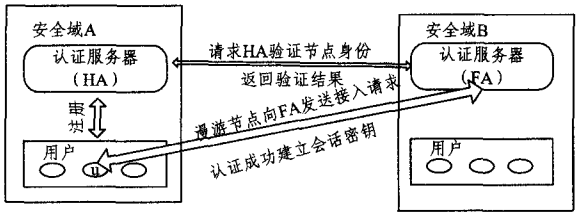

图 5 跨域认证系统结构

基于身份的安全接入方案相较于基于证书的安全接入方案存在着身份易管理以及无需对公钥证书进行维护和管理等优势，而基于无证书的安全接入方案能够有效地解决基于身份的安全接入技术中的密钥托管问题，但由于无证书密码系统被提出的时间较短，还没有比较成熟的基于无证书密码系统设计的支持跨域认证的安全接入技术，现有的支持跨域认证的安全接入技术主要是以基于身份密码系统为主。

文献[58]提出一种基于身份的跨域认证方案，认证服务器只需要在漫游节点首次跨域认证时进行域间通信，在之后的跨域认证过程中，被访问域的认证服务器为通过身份验证的漫游节点生成本安全域的临时合法身份，这样就不需要再进行域间通信，避免了域间通信造成的过大时间延迟。但是，该方案中漫游节点需要进行多次复杂的双线性对运算，用户计算开销较大。

文献[61]利用椭圆曲线加法群提出了一种基于身份的签名算法，算法中签名的验证结果相对于用户身份是一个常量，并且避免了复杂的双线性对运算。基于该算法设计了一种普适环境中的跨域认证方案，方案中用户利用该算法将时戳签名作为认证信息，在保证用户身份不被泄漏的前提下，实现了用户与访问域认证服务器间的安全认证，并减少了用户端计算开销，使得该方案可以满足双向认证、安全会话密钥的建立，在保证安全性的同时，还具有效率优势。

结束语 本文针对 MANET 无中心、网络拓扑快速变化、节点自身资源有限等诸多特点，对 MANET 中一些典型的安全接入技术进行了总结和归纳，详细分析了各种方案的优缺点。在本文前述工作的基础上，表 1 给出了几类典型安全接入方案在安全性、接入成功率、易部署性、密钥管理、通信负担、计算负担、可扩展性和抗毁性几个方面的性能比较。

表 1 典型安全接入方法性能比较

接入方案 \ 性能	安全性	接入成功率	易部署性	密钥全生命周期管理	通信负担	计算复杂度	可扩展性	抗毁性
基于口令认证的安全接入	较差	高	一般	支持	轻	较简单	较弱	较差
基于门限密码的分布式安全接入 部分分布式	较好	一般	一般	支持	较重	一般	一般	一般
基于门限密码的分布式安全接入 完全分布式	一般	高	复杂	支持	较轻	一般	较强	较差
自组织式安全接入	一般	一般	复杂	不支持	重	简单	较弱	差
基于身份的安全接入	较好	一般	简单	支持	一般	较复杂	一般	较好
基于无证书的安全接入	好	一般	一般	支持	较重	复杂	一般	好

安全接入技术作为 MANET 网络安全的第一道防线，是无线通信安全领域研究的重点，同时也是保证 MANET 网络安全的关键技术之一。关于自组织性、MANET 安全接入和认证技术的研究仍是未来无线通信领域研究的重点和难点，因此今后的研究工作以及可能面临的挑战主要表现为：

(1)低开销的安全接入方案。从基于公钥证书的方法到基于身份的方法再到基于无证书的方法，从平面结构到层次结构的安全接入方法，研究者们一直在寻找更简单、更高效的低开销安全接入方案来适应 MANET 应用的需求，如何减少接入过程中的通信次数，降低每次通信的数据流量，并在尽量保证安全的情况下，降低现有密码算法的复杂度和计算开销是 MANET 安全接入技术研究的主要方向之一。

(2)安全高效的系统私钥更新机制。密钥管理是安全管理中最困难、最薄弱的环节，历史经验表明，从密钥管理途径进行攻击要比单纯破译密码算法代价小得多。因此，在多种基于公钥证书的安全接入方法中，系统私钥起着至关重要的

作用，私钥的更新对保障系统的安全有着非常重要的作用，如何选择合适的更新周期，针对分布式和自组织式的密钥管理开发安全和高效的私钥更新机制，也是未来 MANET 安全接入技术研究的重点之一。

(3)具有抗毁性的可靠安全接入机制。MANET 网络常被应用于具有较强火力、电磁和信息对抗的战场环境，网络中的关键节点可能会由于对抗而无法通信、无法实现认证服务或被敌方控制。如何设计一套能感知网络态势并根据连接情况自组织地实现认证节点的选举分配、失连和不可信节点的隔离机制，并据此提供可靠性更高的安全接入方案，也是未来需要进一步研究的内容。

参 考 文 献

[1] 陈林星，曾曦，曹毅. 移动 Ad-hoc 网络——自组织分组无线网络技术(第二版)[M]. 北京：电子工业出版社，2012

[2] 于弘毅. 无线移动自组织网[M]. 北京：人民邮电出版社，2005

[3] Jain A, Jain A, Sagar P K. Various Security attacks and trust based security architecture for MANET[J]. Global Journal of Computer Science and Technology, 2010, 10(14): 32-36

[4] 易平，蒋嶷川，张世永，等. 移动 Ad Hoc 网络安全综述[J]. 电子学报，2005，33(5)：893-899

[5] Cayirci E, Rong C. 无线自组织网络和传感器网络安全[M]. 北京：机械工业出版社，2011

[6] Bellovin S M, Merritt M. Encrypted key exchange: Password-based protocols secure against dictionary attacks[C]// Proceeding of the 1992 IEEE Symposium on Research in Security and Privacy. 1992: 72-84

[7] 祁小波. Ad-hoc 网络端到端认证加密协议研究[D]. 西安：西安电子科技大学，2009：24-25

[8] 赵光胜. 混合式 Ad Hoc 网络中接入认证和安全通信技术研究[D]. 长沙：国防科技大学，2009：9-13

[9] Kim Y D, Perrig A, Tsudik G. Simple and fault-tolerant key agreement for dynamic collaborative groups[C]// Pierangela S. Proceedings of the 7th ACM Conference on Computer and Communications Security. New York, NY, USA: ACM Press, 2000: 235-244

[10] Horng G. An efficient and secure protocol for multi-party key establishment[J]. The Computer Journal, 2001, 44(5): 463-470

[11] 隋爱芬，杨义先，钮心忻，等. 基于椭圆曲线密码的可认证密钥协商协议的研究[J]. 北京邮电大学学报，2004，27(3)：28-32

[12] 王晓峰，张璟，王尚平，等. 基于口令认证的移动 Ad-hoc 网密钥协商方案[J]. 软件学报，2006，8：1811-1817

[13] Zhou L, Hass Z J. Securing Ad hoc networks[J]. IEEE Networks Special Issue on Network Security, 1999, 13 (6): 24-30

[14] 胡荣磊，刘建伟，张其善. Ad Hoc 网络保密与认证方案综述[J]. 计算机工程，2007，33(19)：134-137

[15] 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

[16] Sander T, Tschudin C F. Protecting mobile agents against malicious hosts[C]// Mobile Agents and Security. Lecture Notes in Computer Science, 1998, 1419: 44-60

[17] Dey H, Datta R. A Threshold Cryptography Based Authentication Scheme for Mobile Ad hoc Network[J]. Advances in networks and communication, 2011, 132: 400-409

[18] Seung Y, Robin K. MOCA: Mobile Certificate authority for wireless Ad hoc networks[C]// IEEE Proc of 2nd Annual PKI Research Workshop Program. Maryland: Gaithersburg, 2003: 65-79

[19] Kong J, Zerfos P, et al. Providing robust and uniquitous security support for mobile Ad Hoc networks[C]// IEEE 9th International Conference on Network Protocols (ICNP'01). California, 2001: 251-260

[20] Luo H, Kong J, et al. Self-securing Ad Hoc wireless networks [A]// Proc of the Seventh IEEE Symposium on Computers and Communications (ISCC'02)[C]. Italy, 2002: 567-574

[21] Luo H, Lu S. Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks[R]. Dept of Computer Science, UCLA, 2000: 13-23

[22] 李奕男. Ad-hoc 网络门限身份认证方案及入侵检测模型研究[D]. 长春：吉林大学，2010：63-68

[23] 麻晓园，陈前斌，李云. 移动 Ad-hoc 网络中的密钥管理[J]. 通信技术，2003，10：121-123，128

[24] Omar M, Challal Y, et al. Reliable and fully distributed trust model for mobile ad hoc networks[J]. Computers& Security, 2009, 28: 199-214

[25] Hubaux J, Buttyan L, Capkun S. The Quest for Security in Mobile Ad Hoc Networks[C]// Proc of the 2001 ACM International Symposium on Mobile ad hoc networking&computing 2001. Long Beach, CA, USA, 2001: 146-155

[26] Capkun S, Nuttyan 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

[27] 刘世忠，张宗云，贾小珠. 一种 Ad-hoc 网络自组织密钥管理方案的新节点加入安全算法[J]. 青岛大学学报：自然科学版，2008，21(4)：64-66，98

[28] 董攀，朱培栋. 一种新型 MANET 自组织密钥管理方案[J]. 计算机工程与科学，2009，31(4)：13-17

[29] Rafsanjani M K, Shojaiemehr B. Improvement of Self-organized Public Key Management for MANET[J]. Journal of American Science, 2012, 8(1): 197-202

[30] 李景峰. 移动自组织网络关键安全问题的研究[D]. 郑州：信息工程大学，2006：19

[31] Khalili A, Katz J. Toward secure key distribution in truly Ad Hoc networks [A]// Proceedings of the Symposium on Applications and the Internet Workshops (SAINT'03)[C]. Orlando, FL, USA, 2003: 342-346

[32] Boneh D, Frankkin M K. Identity-based encryption from the Weil pairing[J]. SIAM Journal of Computing, 2003, 32(3): 586-615

[33] Deng H, Mukherjee A, Agrawal D P. Threshold and identity-based key management and authentication for wireless ad hoc networks[A]// Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04)[C]. Las Vegas, USA, 2004: 107-110

[34] 李慧贤，庞辽军，王育民. 适合 ad hoc 网络无需安全信道的密钥管理方案[J]. 通信学报，2010，31(1)：112-117

[35] Zhang T, Yue K, Yao J K. A Distributed Anonymous Authentication Scheme for Mobile Ad Hoc Network from Bilinear Maps [A]// International Conference on Mechatronic Science, Electric Engineering and Computer[C]. Jilin, China, 2011: 314-318

(下转第 30 页)

[51] Moschakis I A, Karatza H D. Performance and Cost Evaluation of Gang Scheduling in a Cloud Computing System With Job Migrations and Starvation Handling, [C]// The 16th IEEE Symposium on Computers and Communications (ISCC 2011). 2011: 418-423

[52] Diaz J, Laszewski G V, Wang Fu-gang, et al. FutureGrid Image Management Framework to Support Cloud and HPC Dynamic Provisioning [R/OL]. http://cyberaide.googlecode.com/svn-history/r5739/trunk/papers/a-draft/draft-11-imagemanagement/draft-11-imagemanagement.pdf

[53] 过敏意. 绿色计算:内涵及趋势[J]. 计算机工程, 2010, 36(10): 1-7

[54] Garg S K, Yeo C S, Anandasivam A, et al. Energy-Efficient Scheduling of HPC Applications in Cloud Computing Environments[J]. Computer Science, Distributed, Parallel, and Cluter Computing, 2009

[55] Garg S K, Yeo C S, Anandasivam A, et al. Environment-conscious scheduling of HPC applications on distributed cloud-oriented data centers[J]. Journal of Parallel and Distributed Computing, 2011, 71(6): 732-749

[56] Kessaci Y, Melab N, Talbi E G. A pareto-based GA for scheduling HPC applications on distributed cloud infrastructures[C]// International Conference on High Performance Computing and Simulation (HPCS). 2011: 456-462

[57] Kommeri J, Niemi T, Helin O. Energy Efficiency of Server Virtualization[C]// The Second International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies, 2012

[58] BurnInSSE Benchmark[EB/OL]. http://www.roylongbottom.org.uk

[59] Coker R. Bonnie++ Benchmark [EB/OL]. http://www.coker.com.au/bonnie++/

[60] SARA HPC Cloud [OL]. https://grid.sara.nl/wiki/index.php/Using_the_HPC_Cloud/betaevaluation

[61] Amazon Elastic Compute Cloud[EB/OL]. http://aws.amazon.com/ec2/, 2007-01-01

(上接第 8 页)

[36] Al-Riyami S S, Paterson K G. Certificateless public key cryptography[C]// Laih CS, ed. Proc. of the ASIACRYPT 2003. LNCS 2894, Berlin: Springer-Verlag, 2003: 452-473

[37] Zhang F T, Sun Y X, Zhang L, et al. Research on certificateless public key cryptography[J]. Journal of Software, 2011, 22(6): 1316-1332

[38] Mandt T K, Tan C H. Certificateless authenticated two-party keyagreement protocols[C]// Advances in Computer Science-ASIAN 2006, Secure Software and Related Issues. Heidelberg: Springer-Verlag, 2008: 37-44

[39] Wang S B, Cao Z F, Wang L C. Efficient certificateless authenticated key agreement protocol from pairings[J]. Wuhan University Journal of Natural Sciences, 2006, 11(5): 1278-1282

[40] Swanson C M. Security in key agreement: Two-party certificateless schemes[D]. Waterloo: University of Waterloo, 2008

[41] Lippold G, Boyd C, Nieto J G. Strongly secure certificateless key agreement[C]// Proceedings of the Pairing 2009. Lecture Notes In Computer Science, 2009(5671): 206-230

[42] 葛爱军, 陈少真. 具有强安全性的不含双线性对的无证书签名方案[J]. 电子与信息学报, 2010, 32(7): 1765-1769

[43] Baek J, Safavi-Naini R, Susilo W. Certificateless public key encryption without pairing[C]// ISC 2005. LNCS 3650, Berlin: Springer-Verlag, 2005: 134-148

[44] Sun Y X, Zhang F T, Baek J. Strongly secure certificateless public key encryption without pairing [C]// CANS 2007. LNCS 4856, Berlin: Springer-Verlag, 2007: 194-208

[45] Samreen A, Ansari S. Certificateless ID-based Authentication using Threshold signature for P2P MANETs[A]// 2009 Information and Communication Technologies[C]. ICICT, 2009: 112-116

[46] 张彬连. 基于簇结构的分布式认证和密钥管理机制研究[D]. 长沙: 湖南师范大学, 2007: 16-18

[47] Venkatraman L, Agrawal P D. A novel authentication scheme for Ad Hoc Networks[J]. IEEE Wireless Com-munications and Networking Conference, 2000, 3: 1268-1273

[48] Bechler M, Hof H J, 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

[49] Li G S, Han W B. Cluster-Based key management in Ad Hoc Networks[J]. Computer Science, 2006, 33(2): 79-82

[50] 李涛. 移动 Ad-hoc 网络的安全性及密钥管理研究[D]. 济南: 山东大学, 2007: 41-56

[51] Boyen X. Multipurpose Identity-Based Signeryption: A Swiss Army Knife for Identity-Based Cryptography[C]// Crypto'03, Lecture Notes in Computer Science 2729. Berlin: Springer-Verlag, 2003: 383-399

[52] 吴旭光, 张敏情, 杨晓元, 等. 一种无证书的移动 Ad hoc 网络密钥管理方案[J]. 计算机工程与应用, 2009, 45(21): 74-76

[53] Lee D G, Kang S I, Seo D H, et al. Authentication for single/multi domain in ubiquitous computing using attribute certification[A]// International Conference on Computational Science and Its Applications[C]. UK, 2006: 326-335

[54] 王俊, 张红旗, 张斌. 新的基于角色的跨信任域授权管理模型[J]. 计算机工程与应用, 2010, 46(8): 106-109

[55] 樊蕊. 跨域身份认证系统的研究与实现[D]. 西安: 西安电子科技大学, 2007: 27-36

[56] 姜奇, 马建峰, 李光松, 等. 基于身份的异构无线网络匿名漫游协议[J]. 通信学报, 2010, 31(10): 138-145

[57] Yao L, Wang L, Kong X W, et al. An inter-domain authentication scheme for pervasive computing environment [J]. Computers and Mathematics with Applications, 2010, 59(2): 811-821

[58] 彭华熹. 一种基于身份的多信任域认证模型[J]. 计算机学报, 2006, 29(8): 1271-1281

[59] Chan Y Y, Fleissner S, et al. Single sign-on and key establishment for ubiquitous smart environments [A]// International Conference on Computational Science and Its Applications[C]. Glasgow, UK, 2006: 406-415

[60] Forne J, Hinarejos F, MarinA A, et al. Pervasive authentication and authorization infrastructures for mobile users [J]. Computers&Secutity, 2010, 29(4): 501-514

[61] 罗长远, 霍士伟, 邢洪智. 普适环境中基于身份的跨域认证方案[J]. 通信学报, 2011, 32 (9): 111-115, 122