无线移动自组网混合式密钥管理方案研究

王 浩[1]，谢 颖[1]，郑 武[2]

(1. 重庆邮电大学自动化学院 重庆 南岸区 400065; 2. 电子科技大学计算机科学与工程学院 成都 610054)

【摘要】基于门限机制的密钥管理方案能提供高的安全性，但认证成功率较低，可扩展性差；基于证书链的密钥管理方案适合自组网的特点，但其安全性仅取决于证书链中节点的信任度，不能满足高安全要求的应用环境。该文提出了门限机制和证书链信任值方法相结合的混合式密钥管理和认证方案，在增加少量通信量的情况下，方案提高了自组网的认证成功率和系统的安全性，较好地平衡了自组网的安全性和认证成功率，满足自组网应用的安全要求。

关 键 词 自组网; 证书链; 密钥管理; 门限机制

中图分类号 文献标识码 A

A New Hybrid Key Management Scheme for Ad hoc Networks

WANG Hao[1]，XIE Ying[1]，ZHENG Wu[2]

(1. College of Automation, Chongqing University of Posts and Telecommunications Nan′an Chongqing 400065;

2. School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 610054)

Abstract Key management schemes based on threshold mechanism can provide high security, but lower certificate success rate and bad scalability; key management schemes based on certification chain satisfy self-organized features, but their security depends on trust degree of nodes and could not be applied high security environment. We advance hybrid key management scheme based on threshold mechanism and certification chain. Simulation shows that with less increment of communication overhead, our scheme can improve both certificate success rate and system security and better balances security and availability, and satisfies security needs of Ad hoc networks.

Key words Ad hoc; certification chain; key management; threshold mechanism

无线移动自组网是一种节点可任意移动、拓扑结构高度动态变化、没有预设网络基础设施的多跳无线网络。这种无线网络具有可临时组网、快速展开、无控制中心、抗毁灭等特点，在军事通信和民用系统中有着广泛的应用。然而，由于自组网的无线链路、动态拓扑、缺乏集中管理和资源受限等特点，其本身就是很脆弱的，容易遭受多种攻击，而且传统的安全机制不再适合于它，极大地阻碍了自组网的应用，特别是在关系到国防安全的军事领域。自组网的密钥管理和认证是自组网安全研究的核心问题之一，也是自组网安全研究中最困难的问题之一，是研究自组网安全通信和安全路由的基础[1]。

1 相关研究工作

文献[2-3]提出了基于门限机制的密钥管理方案，该方案利用(n, k)门限密钥共享体制把CA中心分散到n个服务器中，n个服务器中的任意k–1个合作就可以完成认证，而任意k–1个或者少于k个服务器就不能完成认证，系统具有较好的入侵容忍性。网络中的分布式CA作为信任中心共享密钥，要求共享密钥的CA中心具有较高的物理安全性、较强的计算能力和高的可信任度。基于门限机制的方案能够提供高的安全性，但仍有少部分节点不能获得密钥和认证服务，方案难以扩展到规模较大的网络中，可扩展性差，CA服务器也会引起通信瓶颈等问题[4]。

文献[5-6]提出了类似于PGP证书链的分布式自组织密钥管理方案，该方案是在每个节点存储并维护一个本地证书库，当需要鉴别时，合并两个鉴别节点的本地证书库，并在合并的证书库中寻找证书链(有向路径)来完成鉴别过程。这种基于证书链的方案适合于没有物理基础设施的自组网，不需要系统启动，也适合于自组织特性，但仍然需要时间依靠节点的行为和移动来形成证书图(信任网)；其次，不能保证证书图中存在有向可达路径，仍有可能因为

收稿时间：2007 – 09 – 09

作者简介：王 浩(1975 –)，男，讲师，主要从事网络安全协议和密码算法方面的研究.

找不到可达路径，无法完成鉴别，难以实现全部节点的鉴别和认证服务；最后，证书链的安全性取决于证书链中节点的信任度，在开放的网络中，这是困难的。依赖未知节点而缺少信任中心，使得证书链不能满足高安全要求的应用环境[7-8]。

利用上面两种方案的优点，本文提出自组网混合式密钥管理方案，采用多种密钥管理机制，包括门限式CA和证书链，结合这两种机制，混合式密钥管理方案能提高认证成功率，同时保证系统的安全性和可用性，如果一种机制失败时，另一种机制可继续工作，节点也可选择如何加入和使用服务。

2　方案的系统结构

在混合式密钥管理和认证方案中，有三种类型的节点：CA节点、证书链参与节点和服务请求节点。节点有可能同时属于多种类型。CA节点以门限机制的方式存储系统私钥分量，生成证书签名分量，联合其他CA节点提供认证服务，CA节点还参与证书的撤销、维护证书列表等证书管理活动；证书链参与节点必须能够监控和鉴别邻接节点、创建证书和给邻接节点签发证书、维护签发的证书列表等；服务请求节点通过门限CA机制和证书链完成认证，当服务请求节点收到门限k个证书签名分量时，合成k个证书签名分量并用系统公钥验证合成的证书签名，如收到小于k个的证书签名分量，则通过计算证书链的信任值来进行认证。

门限CA机制把可信第三方的功能分散到多个CA节点。设系统密钥对为<PK，SK>，其中，SK为系统的私钥，用于签发系统所有节点的证书；PK为系统的公钥，可验证由SK签发证书的有效性。通过Shamir门限密钥共享体制，每个CA节点获得密钥分量，CA节点CA_i获得的密钥分量用sk_i表示。同时，节点的密钥对为<pk_i，sk_i>，用于实现端到端的安全通信、信任值的安全传输、分量的生成以及消息的保密性、完整性和可用性等。节点j持有证书cert_j，$\mathrm{CERT}_j=\mathrm{cert}_j^{sk_i}$，$\mathrm{CERT}_j$为$CA_i$节点对证书$\mathrm{cert}_j$的证书签名分量。认证服务请求节点收到$t$个部分签名后，对于RSA签名体制，计算：$\mathrm{cert}_j^{SK}=\prod \mathrm{CERT}_j=\prod_{i=1}^{k}\mathrm{cert}_j^{sk_i}$，生成合成的证书签名并用公钥PK进行验证。

假设节点能够通过数据包转发等行为了解和监控周围邻接节点。每个节点维护一个信任值表，该表包括节点ID、公钥和信任值三个属性。当使用证书链进行认证时，认证服务请求节点依次轮询信任值表中的节点ID_i，并向节点ID_i发送信任值请求，收到请求后，节点ID_i在信任值表中查找认证节点的信任值，如果找到，节点ID_i用私钥pk_i加密后返回；收集到返回的信任值后，计算认证节点的信任值p，如满足信任值要求，则认证成功。证书链中的节点ID_i可以是CA节点，也可以是门限机制认证的节点，或是邻接节点。信任模型如图1所示。

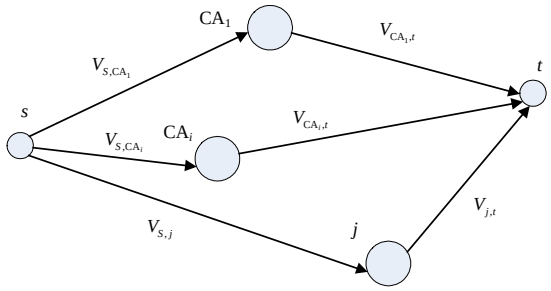

图1　证书链的信任模型

图中，s表示认证服务请求节点，t表示被认证的目标节点，CA_1、CA_i和j是证书链的中间节点，中间节点返回t的公钥pk_t和信任值为$V_{CA_1,t}$、$V_{CA_i,t}$和$V_{j,t}$，单条证书链的信任值为[9]：

$$V_{s,j,t}=V_{s,j}\odot V_{j,t}=1-(1-V_{j,t})^{V_{s,j}}$$

上式可以计算从s到t不同证书链路的信任值，每条证书链路的信任值通常是不同的，合并的信任值计算如下：

$$V_t=1-\prod_{k=1}^{n}(1-V_{s,j,t})$$

式中　n表示证书链路的条数。

3　认证过程

节点s对节点t的完整认证过程描述如下：

Step1　节点s向节点t发送一个认证请求；

Step2　节点t收到认证请求后，如果t有合成的签名证书，返回该签名证书，否则就返回无；

Step3　节点s收到请求响应后，如果返回的是签名证书，则用系统公钥PK验证该签名证书，如果验证成功，认证过程成功返回；否则，认证失败，隔离节点t；如果无合成的签名证书返回，跳转到Step4；

Step4　节点s查找信任值表中节点CA_i，发送信任值请求到节点CA_i，CA_i收到该请求后，如果存在$V_{CA_i,t}$，返回消息$m=\{PK_t,V_{CA_i,t}\}SK_{CA_i}$

Step5　节点s收到CA_i返回消息m后，用CA_i公钥解密消息m，计算信任值V_t；

$$V_{s,j,t}=V_{s,j}\odot V_{j,t}=1-(1-V_{j,t})^{V_{s,j}}$$

$$V_t = 1 - \prod_{k=1}^{n} (1 - V_{s,j,t})$$

Step6 如果V_t大于设定信任值p，则认证过程成功返回；否则，认证失败，隔离节点t。

4 仿真结果分析

本文使用网络仿真器ns-2模拟测试认证的性能。ns-2是面向对象的离散事件驱动网络仿真器，由美国UC Berkeley大学开发，为多种网络和路由协议仿真提供了充分的支持。使用C++和OTcl(Oriented Object Tool Command Language)两种面向对象的设计语言，分别完成具体协议的模拟实现和网络环境参数设置或改变。ns-2扩展性强，适用于大多数操作系统平台，因为它免费提供给用户的源码开放性，被广泛使用[10-11]。仿真参数的设置如表1所示。

表1 仿真参数值

参数	描述	设置值
NODE_NUM	总的移动节点数	200
SLM_TIME	模拟的时间长度/s	600
PAUSE_TIME	两次连续移动之间的停留时间/s	10
MAX_SPEED	最大移动速度/m·s^{-1}	25
TX_RANGE	无线传输距离/m	200
LENGTH	区域长度/m	1 500
WIDTH	区域宽度/m	1 500
CA node	CA节点数	50
Threshold k	门限值k	5、10、15、20、25、30

考察认证成功率性能参数，定义如下：

认证成功率S(成功率)：认证成功的节点数与请求认证的节点数之比，即

$$S = N_s / N_r$$

式中 N_s表示认证成功的节点数；N_r表示请求认证的节点数。当节点收到大于或等于k个CA节点返回数据包，或者合并的信任值大于设定值，表示节点认证成功。对仿真输出的跟踪文件中的数据进行整理，结果如图2～3所示。

首先固定门限值k=20，逐渐增加节点的移动速度，如图2所示，随着节点移动速度的增加，门限方案的认证成功率从90%下降到74%，混合式方案中基于证书链信任值的方法弥补了下降的认证成功率，使得认证成功率从98%上升到100%。同样的，固定节点移动的最大速度为15 m/s，逐渐增加门限值k，如图3所示，随着门限值k的增加，节点需要联系更多的CA节点来完成认证，门限方案的认证成功率从96%下降到63%，混合式方案中基于证书链信任值的方法弥补了下降的认证成功率。仿真结果说明，混合式方案能提高认证服务的可用性。在表2中对比了两种方案中通信的包数量，混合式方案的包数量略有增加。混合式方案是在门限认证失败时才启动证书链信任值的方法，所以包数量有较少的增加。

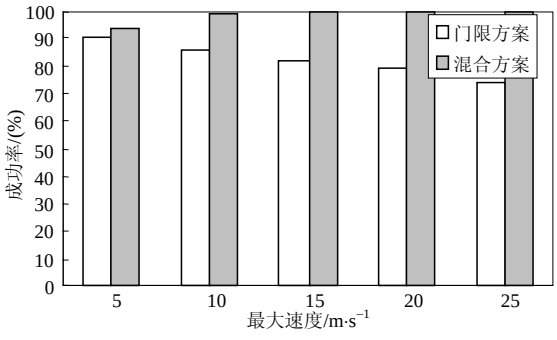

图2 移动速度与成功率的关系(k =20, p = 0.9)

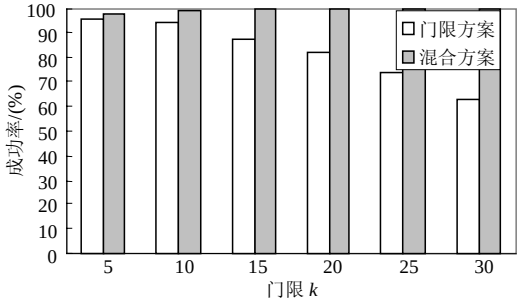

图3 门限与成功率的关系(最大速度=15 m/s，p = 0.9)

表2 通信量对比表 (k=20)

最大进度	门限方案的包数量	混合式方案的包数量	增加的百分比/(%)
5	112 059	112 683	0.6
10	116 362	117 269	0.8
15	129 374	131 702	1.8
20	152 841	156 203	2.2
25	170 351	174 609	2.5

5 方案的安全性分析

在本文方案中，分散可信第三方的CA节点可能由于不安全的存储、被攻击或俘获而造成秘密信息的泄漏。

(下转第1171页)

[2] GOLDWASSER S, MICALI S, RIVEST R. A digital signature scheme secure against adaptive chosen-message attacks[J]. SIAM Journal on Computing, 1988, 17(2): 281-308.
[3] CHAUM D. Blind signature for untraceable payment[C]// Crypto1982. Berlin: Springer-Verlag, 1983.
[4] ZHANG F, KIM K. ID-based blind signature scheme and ring signature from pairing[C]//ASIACRYPT 2002. Belin: Springer-Verlag, 2002.
[5] KIM J, KIM K, CHULSOO L. An efficient and provably secure threshold blind signature scheme[C]//ICICS 2001. Berlin: Springer-Verlag, 2001.
[6] ABE M， FUJISAKI E. How to date blind signatures[C]// Asiacrypt ’96. [S.l.]: Springer-Verlag, 1996.
[7] CHOW S S M, HUI L C K, YIU S M, et al. Two improved partially blind signature schemes from bilinear pairings[C]//In ACISP ’05. [S.l.]: Springer-Verlag, 2005.
[8] FAN C I, LEI C L. Low-computation partially blind signatures for electronic cash[J]. ICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 1998, E81- A(5): 818-824.
[9] ZHANG F, SAFAVI N R, SUSILO W. Efficient verifiably encrypted signature and partially blind signature from bilinear pairings[C]//In Indocrypt ’03. [S.l.]: Springer-Verlag, 2003.
[10] MAITLAND G, BOYD C. A provably secure restrictive partially blind signature scheme in public key cryptography[C]//PKC 2002. [S.l.]: Springer-Verlag, 2002.
[11] ABE M, OKAMOTO T. Provably secure partially blind signatures[C]. Crypto ’00. [S.l.]: Springer-Verlag , 2000.
[12] CAMENISCH J, KOPROWSKI M, WARINSCHI B. Efficient blind signatures without random oracles[C]// Forth Conference on Security in Communication Networks-SCN ’04. [S.l.]: Springer-Verlag, 2004.
[13] JUELS A, LUBY M, OSTROVSKY R. Security of blind digital signatures[C]//Crypto ’97. [S.l.]: Springer-Verlag, 1997.
[14] POINTCHEVAL D. Strengthened security for blind signatures[C]//In Eurocrypt ’98. [S.l.]: Springer-Verlag, 1998.

编　辑　熊思亮

(上接第1166页)

利用(n，k)门限密钥共享体制，认证请求节点仍可以通过获取其他k个合法节点的私钥分量或证书分量，完成认证，被攻破的节点不会影响整个系统的安全性，系统具有较好的入侵容忍性；在较长的一段时间周期内，有可能大于k个的CA节点被攻破或俘获而造成系统的不安全，可以利用Proactive方案周期性更新系统的密钥，从而有效地防止在一定时间周期内大于k个CA节点被攻击或俘获；证书链中的节点可能发布虚假证书进行欺骗攻击，方案中采用了两种方法来抵御这种攻击，一种是证书链认证的中间节点尽可能选取被分布CA中心或者是门限CA节点认证的节点，提高单条证书链认证的安全性。另一种是采用多条证书链，通过计算多条证书链的合并信任值来降低中间节点欺骗攻击的风险。对于非CA节点和非证书链中间节点的一般节点，它的安全性不会影响到整个系统的安全。本方案在提高认证成功率的同时保证了系统的安全性。

6　结　论

在总结分析门限机制方案和证书链方案的优势和存在的问题基础上，本文提出了混合式密钥管理方案，方案集成了门限机制和证书链机制，认证时首先采用门限机制，在门限机制失败时利用证书链信任值方法来完成认证。仿真结果表明，在增加少量通信量的情况下，提高了自组网的认证成功率，同时利用分布式CA和证书链保证了系统的安全性，较好地平衡了自组网的安全性和认证服务的可用性，满足自组网应用的安全要求。

参　考　文　献

[1] 于宏毅. 无线移动自组织网[M]. 北京: 人民邮电出版社, 2005.
[2] ZHOU L, HASS Z J. Secure Ad hoc networks[J]. IEEE Networks, 1999, 13(6): 24-30.
[3] LUO H, KONG J. Ubiquitous and robust access control for mobile Ad hoc networks[J]. IEEE/ACM Transactions on Networking (ToN), 2004, 12(6): 1049-1063.
[4] ASOKAN N, GINZBOORG P. Key agreement in Ad hoc network[J]. Computer Communications, 2000, 23: 1627-1637.
[5] 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.
[6] HUBAUX J P, BUTTYAN L, CAPKUN S. The quest for security in mobile Ad hoc networks[C]//In Proceedings of the ACM Symposium on Mobile Ad hoc Networking and Computing (MobiHoc). Long Beach: ACM Press, 2001.
[7] BROCH J. MALTZ D A, JOHNSON D B, et al. A performance comparsion of multi-hop wireless Ad hoc network routing protocol[C]//In ACM MOBICOM. Dallas: ACM Press, 1998.
[8] CANETTI R, HALEVI S, HERZBERG. A. Maintaining authenticated communication in the presence of break-ins[J]. Journal of Cryptology, 2000, 13(1): 61-105.
[9] REITER M K, STUBBLEBINE S G. Authentication metric analysis and design[J]. ACM Transactions on Information and System Security, 1999, 2(2): 138-158.
[10] KEVIN F, KANNAN V. The ns manual[J/OL]. [2007-07-10]. http://www.isi.edu/nsnam/ns/ns-documentation. html.
[11] PADMAPARNA H, JOHN H. Network simulator tutorial [J/OL]. http://www.isi.edu/nsnam/ns/ns-tutorial, 2007-07-10.

编　辑　税　红