文章编号:1001 - 9081(2008)08 - 1916 - 04

基于 CPK 的高效移动 Ad Hoc 网络密钥管理方案

丁晓宇,刘建伟,邵定蓉,刘 淳
(北京航空航天大学 电子信息工程学院,北京 100083)
(ding_xiao_yu@163.com)

摘 要:移动 Ad Hoc 网络具有的动态网络拓扑、无线链路的弱安全性、节点的有限物理保护和无中心基础结构等特性,使得它面临严重的安全问题。因此鲁棒的密钥管理服务是移动 Ad Hoc 网络的安全基础。提出了一个基于椭圆曲线组合公钥方案和门限密码系统的移动 Ad Hoc 网络密钥管理方案。本方案的主要创新点是提出了三层密钥管理模型,并基于此模型,提出了节点密钥生成、密钥份额分发、节点密钥更新、密钥份额更新和密钥撤销的具体实现。三层密钥管理模型实现较高的安全性和较低的密钥管理开销。与基于证书的和基于身份的密钥管理方案相比,本方案在安全性和效率方面更加适用于移动 Ad Hoc 网络。

关键词:组合公钥;门限密码;移动 Ad Hoc 网络;椭圆曲线
中图分类号: TP393 **文献标志码**:A

Efficient key management scheme based on CPK for mobile Ad Hoc networks

DING Xiao-yu, LIU Jian-wei, SHAO Ding-rong, LIU Chun
(*School of Electronics and Information Engineering, Beijing University of Aeronautics and Astronautics, Beijing* 100083, *China*)

Abstract: Mobile Ad Hoc Networks (MANETs) face serious security problems due to their unique characteristics such as dynamic topology, vulnerability of weak-secure wireless link, limited physical protection of each node, and lack of central infrastructure. Robust key management services are central to ensuring security of mobile Ad Hoc networks. A novel robust key management scheme for MANETs is proposed based on Elliptic Curve Combined Public Key (ECCPK) scheme and the threshold cryptosystem. The major innovative point of this scheme was the proposal of three-tier key management model to provide high security, low key management load. Based on three-tier key management model, the node's key generation, secret share distributing, node's key updating, secret share refreshing and key revocation approaches are proposed. Compared with the security and efficiency of the certificate-based and the identity-based key management schemes, the new scheme is more suitable for the mobile Ad Hoc networks.

Key words: Combined Public Key (CPK); threshold cryptograph; mobile Ad Hoc networks; elliptic curve

0 引言

移动 Ad Hoc 网络作为一种新的无线通信模式,近来引起极大关注。为在需要全分布式网络的特殊地域环境,如战争,抢险,和灾难等建立通信提供了极其灵活的结构。但是,移动 Ad Hoc 网络的灵活性也带来了大量的研究难题,其中就包括安全的管理。

有效和鲁棒的密钥管理服务是移动 Ad Hoc 网络的安全基础。因此,门限秘密共享技术被提出应用于移动 Ad Hoc 网络。目前,此领域的大量研究可以分为两种门限密钥管理服务:基于证书的门限密钥管理和基于非证书的门限密钥管理。Zhou 和 Hass 首先提出了部分分布式认证授权方案[1],此方案定义一组特殊的节点,能够利用它们拥有的认证授权中心私钥份额为申请节点产生部分证书,一个节点的有效证书需要组合 t 部分证书。Kong 等人对文献[1]方案进行了扩展,他们在网络中不存在特殊节点的假设下,提出了一个全分布认证授权方案,此方案提出网络中的每一个节点都拥有认证授权中心的私钥份额[2-5]。Hubaux 等人提出了一种自组织公钥基础结构,这个结构和 PGP 概念类似。和以上的方案不同,本方案不需要一个可信认证中心,而是由每个节点为其他节点颁发证书。文献[7-9]提出了基于身份和门限的密钥分发方案。

在上述研究的基础上,本文提出一种新的基于椭圆曲线组合公钥(ECCPK)和门限技术的密钥管理方案,本方案属于基于非证书类的密钥管理方案。

1 椭圆曲线组合公钥的原理

椭圆曲线组合公钥是文献[10]中提出的一种密钥管理方法。设素数域椭圆曲线方程:

$$E: y^2 = (x^3 + ax + b) \bmod p \quad (1)$$

曲线参数为 $E:\{a,b,G,N,p\}$,G 是椭圆曲线 $E/F(p)$ 的基点,用 $G=(x_G,y_G)$ 来表示,N 是基点 G 的阶。假定私钥 sk 为整数 r,则对应的公钥为椭圆曲线 E 上的一个点 rG,用 (x_r,y_r) 标记。用 ***SSK*** 表示私钥种子矩阵,由整数矢量 (r_{ij}) 组成,如式(2)。***PSK*** 表示公钥种子矩阵,由对应的点 $(r_{ij}G)=(x_{ij},y_{ij})$ 组成,如式(3)。

收稿日期:2008 - 04 - 25;**修回日期**:2008 - 05 - 20。
基金项目:国家 863 计划项目(2006AA01Z422);国家自然科学基金资助项目(60672102)。
作者简介:丁晓宇(1977 -),男,河南洛阳人,博士研究生,主要研究方向:无线自组网络安全,密钥管理; 刘建伟(1964 -),男,山东莱州人,教授,主要研究方向:密码学、卫星信道编码调制、通信网络安全保密技术; 邵定蓉(1937 -),男,江苏宜兴人,教授,博士生导师,主要研究方向:通信与电子系统; 刘淳(1975 -),女,湖北罗田人,博士研究生,主要研究方向:无线自组网络安全、密钥管理。

$$\boldsymbol{SSK}=\begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1h} \\ r_{21} & r_{22} & \cdots & r_{2h} \\ \vdots & \vdots & & \vdots \\ r_{m1} & r_{m2} & \cdots & r_{mh} \end{pmatrix} \tag{2}$$

$$\boldsymbol{PSK}=\begin{pmatrix} (x_{11},y_{11}) & (x_{12},y_{12}) & \cdots & (x_{1h},y_{1h}) \\ (x_{21},y_{21}) & (x_{22},y_{22}) & \cdots & (x_{2h},y_{2h}) \\ \vdots & \vdots & & \vdots \\ (x_{m1},y_{m1}) & (x_{m2},y_{m2}) & \cdots & (x_{mh},y_{mh}) \end{pmatrix} \tag{3}$$

由 ***SSK*** 计算用户 A 私钥的步骤为:

1)假定有 h 个映射 $F_1,F_2,\cdots,F_h$,这些映射将 A 的身份信息(可以是身份证号等)映射为 h 个映射值,将 h 个映射值记为 $m_1,m_2,\cdots,m_h$。

2)用 $m_1,m_2,\cdots,m_h$ 作为行号从 ***SSK*** 的 h 列取出相应的矢量为 $r_{m_1 1},r_{m_2 2},\cdots,r_{m_h h}$,按式(4)来计算用户 A 的私钥。

$$sk_A=(r_{m_1 1}+r_{m_2 2}+\cdots+r_{m_h h})\bmod N \tag{4}$$

A 的公钥不需要通过证书传递,由通信对方 B 计算得到。步骤为:

1) B 由 A 的身份信息用相同的映射算法计算出行映射值 $m_1,m_2,\cdots,m_h$。从公钥种子矩阵 ***PSK*** 中取出相应的矢量,$((x_{m_1 1},y_{m_1 1}),(x_{m_2 2},y_{m_2 2}),\cdots,(x_{m_h h},y_{m_h h}))$。

2)按照式(5)计算公钥,pk_A 和 sk_A 构成一对椭圆曲线密码公/私钥对。

$$\begin{aligned} pk_A=&((x_{m_1 1},y_{m_1 1})+(x_{m_2 2},y_{m_2 2})+\cdots+\\ &(x_{m_h h},y_{m_h h}))\bmod p=\\ &(r_{m_1 1}+r_{m_2 2}+\cdots+r_{m_h h})G \end{aligned} \tag{5}$$

组合公钥技术的核心优势是由少量的种子密钥可以组合成海量的密钥空间。例如:假定系统公钥长度为 512 b,一个占存储空间 8KB 的公钥矩阵大约可以产生 10^{12} 个公钥,足够通常的 Ad Hoc 网络使用,而目前 Ad Hoc 网络节点一般有足够的容量保存 ***PSK***,这一点是组合公钥技术用于 Ad Hoc 网络环境的基础。而椭圆曲线密码的特性使得椭圆曲线组合公钥比其他形式的组合公钥更适合于移动环境的应用。

2　新的密钥管理方案

首先,本文首次提出三层密钥管理模型,此模型是本文的方案具有较高安全性和效率的基础。其次,我们将会给出系统初始化、秘密份额分发、节点密钥更新、秘密份额更新和密钥撤销过程的具体实现方法。

2.1　三层密钥管理模型

本文首先提出基于证书和基于身份的两层密钥管理模型,如图 1 所示。顶层是系统公/私钥对来提供节点密钥的生成和分发服务。底层是节点的公/私钥对。为了得到鲁棒的密钥管理服务,系统私钥被拆分并分发给特定的节点,同时,为了增强安全性,节点拥有的私钥份额定期进行更新。因为只需分享和更新系统私钥,计算量和通信开销较小,且安全性较高。

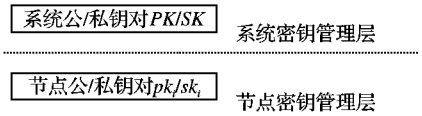

图 1　基于证书和基于身份的两层密钥管理模型

借鉴基于证书和基于身份的两层密钥管理模型的思路,设计基于椭圆曲线组合公钥的两层密钥管理模型,如图 2 所示。顶层是系统公/私钥矩阵,提供节点密钥的生成和分发服务。底层是节点的公/私钥对。为了得到安全和鲁棒的密钥管理服务,系统私钥矩阵需要拆分后分发给特定的节点,这些特定的节点定期更新拥有的私钥矩阵份额。

因为分享和更新的是私钥矩阵,计算量和通信负荷与私钥矩阵的大小成线性关系。与基于证书和基于身份的两层密钥管理模型相比,这个模型效率低,不适用于资源受限的移动 Ad Hoc 网络。

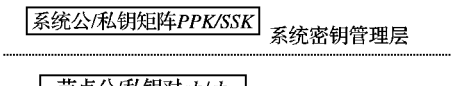

图 2　基于 ECCPK 的两层密钥管理模型

为了提高方案的安全性和效率,我们提出三层密钥管理模型,如图 3 所示。这个模型将密钥管理服务分为三层。顶层是系统安全管理层,是整个系统安全的核心,也就是系统公/私钥对。中间层是椭圆曲线组合公/私钥矩阵,提供节点密钥的分发服务。底层是节点的公/私钥对。这个模型的创新点在于提出了系统安全管理层。系统私钥的作用是保护椭圆曲线私钥矩阵。从而使系统安全保护的核心从私钥矩阵变为系统私钥。这个模型可以获得与基于证书和基于身份的模型几乎相同的管理效率。

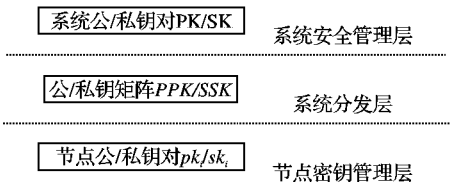

图 3　基于 ECCPK 的三层密钥管理模型

2.2　系统参数

利用椭圆曲线组合公钥机制和提出的三层密钥管理模型,我们给出一个新的移动 Ad Hoc 网络门限密钥管理方案。考虑一个移动 Ad Hoc 网络,其节点之间的通信基于带宽受限,易发生错误和不安全的无线信道。我们做出以下假设:

1)一个离线的认证中心只在初始化阶段提供服务;

2)在移动 Ad Hoc 网络的生命周期中每个节点具有一个唯一不变的身份标识;

3)网络中的节点是异构的;

4)在密钥更新周期时间范围内,攻击者只能攻破少于 t 个服务节点。

离线的认证中心选择一系列的系统安全参数,包括:1)RSA 系统公钥 e;2)RSA 系统私钥 d;3)椭圆曲线 E;4) h 个影射函数;5)私钥种子矩阵 ***SSK***;6)公钥种子矩阵 ***PSK***。系统私钥 d 和私钥种子矩阵 ***SSK*** 由认证中心产生并且必须是保密的,而其他参数是公开的。认证中心的组件还包括一个节点标识的数据库,数据库的大小依赖于网络的大小。认证中心保存所有存在节点的标识,节点标识数据库需要而且只能被认证中心保护。认证中心保证一个标识只会分配给一个节点,也就是说,一个标识只能使用一次。

2.3　安全初始化

安全初始化过程如图 4 所示。认证中心在网络生成时完

成安全的初始化操作。在初始化节点,所有的节点分为两类:普通节点 GN 和服务节点 SN。服务节点按照预先定义的标准进行选择。一般是具有较强计算能力,较多存储空间和较大传输距离的节点被选为服务节点。对于普通节点,认证中心给它分配一个有效标识,并且利用映射函数来将标识映射到私钥矩阵元素,根据式(4)计算节点私钥 sk。认证中心将标识映射到公钥矩阵元素,利用式(5)计算节点公钥 pk。于是,认证中心传输 ID,sk,pk,$\boldsymbol{PSK}$,e,映射函数,椭圆曲线参数到普通节点。注意,节点的私钥 sk 是通过安全通道传送的。服务节点的初始化过程和普通节点基本一样,但是,服务节点还包括两个重要的过程:认证中心根据式(6)利用系统公钥加密私钥矩阵,记作 $\boldsymbol{SSK}^e$。

$$\boldsymbol{SSK}^e = \begin{pmatrix} r_{11}^e & r_{12}^e & \cdots & r_{1h}^e \\ r_{21}^e & r_{22}^e & \cdots & r_{2h}^e \\ \vdots & \vdots & & \vdots \\ r_{m1}^e & r_{m2}^e & \cdots & r_{mh}^e \end{pmatrix} \tag{6}$$

认证中心传输 $\boldsymbol{SSK}^e$ 到每个服务节点。同时,认证中心把系统私钥 d 按照 (t,n) 门限方案拆分为 n 个份额,每个份额记为 d_i。于是,n 个份额安全地发送给 n 个服务节点。

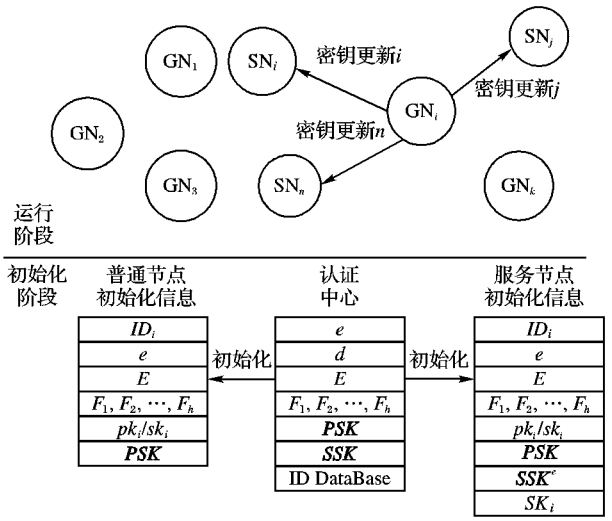

图 4 基于椭圆曲线组合公钥的密码管理方案

2.4 节点密钥更新

为了增强网络的安全性,我们介绍一个安全和有效的节点密钥更新方法,如图 4 所示。首先,移动 Ad Hoc 网络的整个生命周期被分为长度为 t 的时间间隔。在第 j 个时间间隔,一个节点的临时标识为 $ID_{tmp} = (ID \| j)$,ID 是节点的标识,$\|$ 表示字符串的连字符。所以,节点的新的公钥可以根据其临时标识计算。为了获得新的节点私钥,节点需要和至少 t 个服务节点联系。每一个服务节点都拥有加密的私钥种子矩阵和系统私钥份额。任何 n 个服务节点中的 t 个可以联合担当虚拟认证中心,根据节点的临时标识来生成节点新的私钥。

例如,在第 j 个时间间隔结束前,Alice 需要获得在第 $(j+1)$ 时间间隔内的节点公钥和私钥。

首先,Alice 可以根据她的临时身份标识获得新的公钥。利用 h 个映射函数和临时身份标识可以映射为 h 个值,m_1,m_2,$\cdots$,m_h,然后把 m_1,m_2,$\cdots$,m_h 作为行数从公钥矩阵中选择对应的元素。于是,Alice 就可以利用式(5)来计算新的节点公钥。

为了获得节点私钥,Alice 利用其当前的私钥对私钥更新请求(PKU_REQ)消息进行签名并发送给至少 t 个服务节点。当服务节点收到私钥更新请求(PKU_REQ),验证是否签名和声称的临时身份标识匹配。如果匹配,则根据临时身份标识 ID_{tmp} 和 h 个映射函数计算出 m_1,m_2,$\cdots$,m_h,然后把 m_1,m_2,$\cdots$,m_h 作为行号从加密的私钥矩阵中选择对应的元素,$r_{m_1 1}^e$,$r_{m_2 1}^e$,$\cdots$,$r_{m_h 1}^e$。于是,服务节点就可以利用式(7)来计算部分节点私钥。

$$r_{m_l i}' = (r_{m_l i})^{d_i e_i}; l = 1, \cdots, h \tag{7}$$

符号 $c_i = \prod_{1 \leqslant j \leqslant t, j \neq i} \frac{s_j}{s_j - s_i}$ 是拉格朗日系数。当 Alice 收到多于 t 个部分私钥时,它可以根据式(8)计算新的节点私钥。

$$sk_A = \sum_{l=1}^{h} \left(\prod_{i=1}^{t} r'_{m_i l} \right) \bmod N \tag{8}$$

于是,Alice 完成节点的密钥更新过程。

2.5 服务节点份额更新

为了使攻击者不能在足够长的时间内攻破超过 t 个服务节点,我们的密钥管理方案采用先应式秘密份额更新技术。整个生命周期被分为长度为 T 的时间段。每个时间段由两个阶段组成:服务阶段和更新阶段。在服务阶段,服务节点为所有的节点提供节点私钥更新服务。在更新阶段,所有的服务节点联合从旧的系统私钥份额产生新的份额。于是,攻击者为了破坏系统,需要在更新时间段 T 内攻破至少 t 个服务节点。

份额更新依赖于密码门限方案的私钥份额同态特性。假定有 n 个有效的服务节点,份额更新过程如下:

步骤 1 每个服务节点 SN_i 选择次数为 $t-1$ 的多项式,如 $g^{(i)}(x) = \sum_{j=0}^{t-1} a_j^{(i)} x^j$。设 $g^{(i)}(0) = 0$。因此 $g^{(i)}(0)$ 根据 (t,n) 门限共享方法,被拆分为 $k_1^{(i)}$,$k_2^{(i)}$,$\cdots$,$k_n^{(i)}$,$k_l^{(i)}$ 叫作子份额。服务节点 SN_i 保留子份额 $k_i^{(i)}$,同时其他 $n-1$ 子份额值通过安全信道分发给其他 $n-1$ 个服务节点。$k_l^{(i)} = g^{(i)}(ID_l)$ 应该被分发给服务节点 SN_l。

步骤 2 于是每个服务节点 SN_v 能够得到 n 个子份额 $k_v^{(i)}$,$i = 1, \cdots, n$。所以它能够计算新的系统私钥份额 $d_{\text{new}}^{(j)} = d_{\text{old}}^{(j)} + \sum_{l=1}^{n} k_j^{(l)}$。因此,$n$ 个服务节点能够在不改变系统私钥 d 的情况下更新拥有的私钥份额。

以上更新过程可能会遇到恶意的服务节点,或者信息包的丢失。但是只要有 t 个服务节点达成协议,更新过程就能成功执行。

2.6 节点撤销

为了隔离恶意节点和增强系统的安全性,密钥管理方案必须包括密钥撤销方法。许多密钥撤销方法已经被提出,但不是针对基于组合密钥管理的方案。我们设计了一个改进的密钥更新方案如下。

撤销的服务和计算由所有有效的服务节点提供。我们选择网络的固定参数集 (k,p)。这些参数根据网络的密度和系统的鲁棒需求来调整。符号 m_{GN} 表示普通节点控告者的数

量,m_{SN} 表示服务节点控告者的数量。控告值根据式(9)计算:

$$m = m_{GN} + p \times m_{SN};\ p \geq 1 \tag{9}$$

如果 m 值大于 k,则被控告的节点被认为是恶意的。因为,它在整个网络中被认为是恶意节点。

每一个服务节点有一个恶意节点表(MNL)。恶意节点表的 1 个条目是节点的标识,控告值和控告者列表。如果一个服务节点的控告者列表包括少于 k, 这个节点被标记为“怀疑”;否则,这个节点被认定是恶意的并且标记为“有罪”。

当一个服务节点收到控诉某个节点的消息时,它首先检查是否在恶意节点表中被标记为“有罪”节点。如果是,则这个消息被丢弃。否则,它更新它的恶意节点表记录,增加到控告者列表并更新控告值。如果被控告的节点的控告值超过 k,则被控告的节点被标记为“有罪”。当节点被标记为“有罪”,服务节点从控告者列表中删除此节点并更新控告值,如果一个节点的控告值低于 k,这个节点被标记为“怀疑”。

3　性能分析

3.1　安全性分析

本文提出了三层密钥管理模型。每一个节点的安全性基于私钥种子矩阵的安全性,私钥种子矩阵的安全性基于系统私钥的安全性。

系统私钥的安全性基于 RSA 困难问题。系统私钥是整个系统安全的核心,如果系统私钥被攻击者发现或破解,整个系统的安全被破坏。本方案采用了两种措施来保护系统的私钥安全,第一个措施:认证中心是离线的,因此可以采用物理方法保证私钥不会泄露。第二个措施:系统私钥按照 (t,n) 密码门限方法拆分,并且定期更新。我们假定攻击者在密钥更新周期内不能攻破超过 t 个服务节点,根据门限方法的特性,系统私钥不可能被推导出来。

私钥种子矩阵 ***SSK*** 的安全性基于椭圆曲线密码系统的安全性。目前,163 bit 的密钥长度已经被验证是足够安全的。所以,攻击者通过 ***PSK*** 不能得到 ***SSK*** 矩阵。同时,私钥种子矩阵 ***SSK*** 因为 RSA 困难问题,也不可能通过加密的 $\boldsymbol{SSK}^e$ 导出。

节点的安全性基于椭圆曲线加密系统,并且被节点密钥更新方法增强。

因为我们的方案整个系统的安全性基于系统私钥,所以它具有和基于证书和基于身份相同的安全性。

3.2　效率分析

基于证书的密钥管理方案需要管理证书,使得资源受限的移动 Ad Hoc 网络增加了计算,存储和通信负荷。基于身份的密钥管理方案和本文提出的基于椭圆曲线组合公钥方案属于非证书密钥管理方案,解决了基于证书管理方案的效率问题。因此,本文的方案在效率上比基于证书的密钥管理方案要高。

基于身份的密钥管理方案和新的方案都是在成员密钥更新过程中,对成员的标识进行指数运算;在服务节点份额更新过程中,都是进行多项式运算。因此,本文的方案在效率上和基于身份的方案是相当的。但是,基于身份密钥管理方案的算法主要是双线性对计算,比椭圆曲线算法复杂,而且实验数据可以定量说明这一点。在 MIRACL 提供的库函数的基础上,使用约 163 bit 长度椭圆曲线密钥,在 Pentium 1.5 GHz Windows 2000 平台下比较椭圆曲线和 IBE 加/解密算法时间,前者分别为:0.7 ms/1.1 ms,后者分别为:14.4 ms/65.3 ms,可见前者的计算效率远高于后者。所以,我们的方案比基于身份的密钥管理方案效率更高。

4　结语

本文提出了三层密钥管理模型,以及基于椭圆曲线组合公钥的高效鲁棒的密钥管理方案。此方案属于非证书管理方案,因此它明显比基于证书的方案效率高,能获得和基于身份方案相同的效率。同时,本文详细描述了节点密钥生成,份额分配,节点密钥更新,份额更新和节点撤销的实现方法。与基于证书和基于身份的密钥管理方案相比,我们的方案具有同样的安全性,并且管理上更加有效率,因此,更加适合于移动 Ad Hoc 网络。

参考文献:

[1] ZHOU LIDONG, HAAS Z J. Securing Ad hoc networks[J]. IEEE Network Magazine, 1999, 13(6): 24 – 30.

[2] KONG JIEJUN, ZERFOS P, LUO HAIYUN, *et al*. Providing robust and ubiquitous security support for MANET[EB/OL]. [2007 – 10 – 20]. http://irl.cs.ucla.edu/papers/ICNP01-haiyun.pdf..

[3] LUO HAIYUN, KONG JIEJUN, ZERFOS P, *et al*. URSA: Ubiquitous and robust access control for mobile Ad hoc networks[EB/OL]. [2007 – 10 – 20]. http://www.cs.ucla.edu/~lixia/papers/04TON_URSA.pdf.

[4] LUO HAI-YUN, LU SONG-WU. Ubiquitous and robust authentication services for Ad hoc wireless networks[EB/OL]. [2007 – 10 – 20]. http://camars.kaist.ac.kr/~hyoon/courses/cs710_2002_fall/2002cas/security/papers/%5B8%5D.pdf.

[5] LUO HAI-YUN, ZERFOS P, KONG JIE-JUN, *et al*. Self-securing Ad hoc wireless networks[EB/OL]. [2007 – 11 – 20]. http://www-sal.cs.uiuc.edu/~haiyun/publications/ISCC02.pdf.

[6] HUBAUX J P, BUTTYAN L, CAPKUN S. Self-organized public-key management for mobile Ad hoc networks[2007 – 11 – 23]. http://ic2.epfl.ch/publications/documents/IC_TECH_REPORT_200234.pdf.

[7] KHALILI A, KATZ J, ARBAUGH W A. Towards secure key distribution in truly Ad hoc networks[EB/OL]. [2007 – 11 – 25]. http://www.cs.umd.edu/~jkatz/papers/id_threshold.ps.

[8] DENG HONGMEI, MUKHERJEE A, AGRAWAL D P. Threshold and identity-based key management and authentication for wireless Ad hoc networks[C]// Information Technology: Coding and Computing. Washington: IEEE Computer Society, 2004: 107 – 111.

[9] LI JINGFENG, WEI DAWEI, KOU HONGZHAO. Identity-based and threshold key management in mobile Ad hoc networks[C]// Wireless Communications, Networking and Mobile Computing. New York: IEEE, 2006: 1 – 4.

[10] 南湘浩 陈钟. 网络安全技术概论[M]. 北京:国防工业出版社, 2003:56 – 61.