增强安全性的IEEE802.15.4协议研究

杨 剑,杨铭熙,李腊元
(武汉理工大学 计算机科学与技术学院,湖北 武汉 430070)

摘 要:IEEE 802.15.4标准因其低速率、低成本、低功耗、高质量,被认为是无线传感器网络和无线个人域网络的理想实现技术。简要介绍了无线传感器网络及其主要特点和问题,及无线传感器网络的安全需求。提出了增强安全性的IEEE802.15.4协议SE-IEEE802.15.4研究,其中使用公钥加密算法ECC来实现IEEE802.15.4协议的数字签名。最后采用NS-2平台对其进行仿真,并进行了性能和安全性的分析。

关键词:无线传感器网络;IEEE802.15.4;仿真;ECC;安全
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2007)12-0136-04

Research of Security Enhanced IEEE802.15.4 Protocol

YANG Jian, YANG Ming-xi, LI La-yuan
(School of Computer Sci. & Tech., Wuhan Univ. of Tech., Wuhan 430070, China)

Abstract: With the characteristics of low rate, low cost, low power and high quality, IEEE 802.15.4 standard is considered to be the ideal technology to implement wireless sensor networks and wireless personal area networks. In this paper, at first introduce the main characters and problems of wireless sensor network. Then introduce security demands of wireless sensor network. And then propose a new security enhanced IEEE802.15.4 protocol. In the new protocol, use ECC to realize digital signature, which encryption key is smaller than RSA. At last adopt NS-2 platform to simulate them and make performance and security analysis.

Key words: wireless sensor network; IEEE802.15.4; simulation; ECC; security

0 引 言

无线传感器网络[1]综合了传感器技术、嵌入式计算技术、分布式信息处理技术和无线通信技术。它能够实时监测、感知和采集各种环境或监测对象的信息,并对其进行处理,然后把信息传送到用户。这种网络系统是计算机科学技术的一个新的研究领域,具有十分广阔的应用前景,可以广泛应用于国防军事、国家安全、环境监测、交通管理、医疗卫生、制造业、反恐抗灾等领域。

无线传感器网络的主要特点与问题[2]是:

(1)通信能力有限:传感器的通信带宽窄且经常变化,通信覆盖范围只有几十到几百米。传感器之间的通信断接频繁,如何在有限通信能力的条件下提高质量,这对信息的处理与传输是个挑战。

(2)电源能量有限:传感器的电源能量极其有限,是约束其应用的严重问题。

(3)计算能力有限:传感器网络中的传感器都具有嵌入式特性的处理器和存储器,但是由于嵌入式处理器的能力和存储器的容量有限,使得传感器的计算能力十分有限。

(4)传感器数量大、分布范围广:传感器网络中传感器节点密集,数量巨大,可能达到几百、几千,甚至更多。

(5)感知数据量大:传感器网络中的每个传感器通常都是产生较大的流式数据,并具有实时性。每个传感器仅仅具有有限的计算资源,难以处理巨大的实时数据流。

1 无线传感器网络安全协议需要解决的问题

从消息安全角度看,传感器网络安全和一般网络安全的出发点是相同的,都要解决如下问题[3]:

(1)机密性(Confidentiality)。所有敏感数据在存储和传输的过程中都要保证其机密性,让任何人在截获物理信号的时候不能直接获得消息的内容。

收稿日期:2007-07-21
基金项目:国家自然科学基金资助项目(60672137);教育部博士点基金(20060497015)
作者简介:杨 剑(1980-),男,湖北武汉人,硕士研究生,研究方向为网络安全;杨铭熙,副教授,研究方向为网络技术与网络安全;李腊元,教授,博导,研究方向为高性能网络技术、通信协议。

(2)点到点的消息认证(Authentication)。网络节点在接收到其它节点发来的消息时,能够确认这个数据包确实是从该节点发送出来的,而不是别人冒充的。

(3)完整性(Integrity)。网络节点在接收到一个数据包的时候,能够确认这个数据包和发出来的时候一样,没有被中间节点篡改。

(4)新鲜性(Freshness)。数据本身具有时效性,网络节点能够判断最近接收到的数据包是发送者最新产生的数据包。

(5)广播认证。解决单一节点向多个节点发送统一通告的认证安全问题。认证广播的发送者是一个,而接收者是多个,所以认证方法和点到点通信认证方式完全不同。

2　无线传感器网络安全设计协议设计

2.1　IEEE 802.15.4 简介

IEEE802.15.4 标准,是针对低速无线个人区域网络(low - rate wireless personal area network, LR - WPAN)制定的标准,该标准把低能量消耗、低速率传输、低成本作为重点目标,旨在为个人或家庭范围内不同设备之间低速互连提供统一标准。LR - WPAN 网络是一种结构简单、成本低廉的无线通信网络,它使得在低电能和低吞吐量的应用环境中使用无线连接成为可能。

传感器网络需要低功耗短距离的无线通信技术。由于 IEEE802.15.4 标准的网络特征与无线传感器网络存在很多相似之处,所以很多研究机构把它作为无线传感器网络的无线通信平台。因此,IEEE 802.15.4 中的 MAC 协议是一种重要的无线传感器 MAC 层协议。

IEEE 802.15.4 的 MAC 层采用 CSMA/CA 机制,由于在一个时间内只能有一个设备进行传输,因此所有想要传输的节点设备就会通过 CSMA/CA 机制来竞争传输媒体的使用权。所有准备传输数据的设备,会监测目前的无线传输媒体是否有其他设备在使用中,如果为空闲,则可以开始发送数据,若目前的无线传输媒体是忙碌中的,则这些设备将会在监测到媒体为空闲后,再进行 CSMA/CA 的竞争。

2.2　IEEE 802.15.4 的安全性分析

安全性[3,4]是 IEEE 802.15.4 的一个重要问题。为了提供灵活性和支持简单器件,IEEE802.15.4 在 MAC 层数据传输中提供了三级安全性。第一级实际是无安全性方式,对于某种应用,如果安全性并不重要或者上层已经提供足够的安全保护,器件就可以选择这种方式来转移数据。对于第二级安全性,器件可以使用接入控制清单(ACL)来防止非法器件获取数据,在这一级不采取加密措施。第三级安全性在数据转移中采用属于高级加密标准(AES)的对称密码。

我们重点考虑其中的第三级安全性的特性,它可以用来保护数据和防止攻击者冒充合法器件,但也存在着明显的缺陷,包括:

1) 进行安全通信前需要以安全方式进行密钥交换。这一步骤,在某种情况下是可行的,但在某些情况下会非常困难,甚至无法实现。不能防止攻击者在通信双方交换密钥时通过窃听来截取对称密钥。因此该安全性能无法保证数据的保密性,这可以通过采用公钥加密方式来解决。

2)不具有抗否认性。为了确保其发出的信息事后无法抵赖,使其具有抗否认性,可以通过数字签名实现。

3)不能保证数据的完整性。为了保证数据的完整性,可以通过数字签名实现。

4)规模复杂。对于对称密钥,A 与 B 两人之间的密钥必须不同于 A 和 C 两人之间的密钥,否则给 B 的消息的安全性就会受到威胁。在有 1000 个用户的团体中,A 需要保持至少 999 个密钥(更确切地说是 1000 个,如果他需要留一个密钥给他自己加密数据)。对于该团体中的其它用户,此种情况同样存在。这样,这个团体一共需要将近 50 万个不同的密钥! 推而广之, n 个用户的团体需要 $n^2/2$ 个不同的密钥。

综上所述,提出采用公钥加密算法。无线传感器网络节点的内存和计算能力都非常有限,因此诸如 RSA 等密钥过长、空间和时间复杂度大的算法不适用。经过与其他公钥加密体制比较,选取椭圆曲线公钥算法 ECC。

ECC 公钥算法的优点[5]:

(1)计算速度。在相同的计算资源条件下,虽然在 RSA 中可以通过选取较小的公钥的方法提高公钥运算的速度,即提高加密和签名验证的速度,使其在加密和签名验证速度上与 ECC 有可比性,但在私钥运算的速度(解密和签名)上,ECC 远比 RSA,DSA 快得多。另外,ECC 系统的密钥生成速度比 RSA 快百倍以上。

(2)存储需求。对于相同的安全强度,ECC 只需较短的密钥长度。比如当取 RSA 的密钥长度为 1024bit,相同安全强度的 DSA 的密钥长度也为 1024bit,而相同安全强度的 ECC 的密钥长度仅为 163bit,ECC 的密钥和系统参数所需的存储空间与 RSA,DSA 相比要小得多。

(3)带宽需求。由于密钥长度较小,所需的带宽要求低。带宽需求低使 ECC 在无线网络领域具有广阔

的应用前景。

3 增强安全性的 IEEE802.15.4 协议—SE－IEEE 802.15.4

3.1 椭圆曲线密码体制

椭圆曲线密码体制(ECC)自 1997 年以来成为研究热点,其安全性基于有限域上椭圆曲线离散对数问题(ECDLP)的难解性。在有限域 K 上椭圆曲线方程有如下形式[6]:

$$y^2 = x^3 + Ax + B \qquad A,B \in K$$

ECDLP 难解性是指:对于曲线上给定的离散点 P 和 Q,难于找到整数 l,使得 $lP = Q$。将椭圆曲线应用于密码体制时,设 P 为公钥,Q 为私钥,其安全性就表现为知道 P 无法推导 Q。对于有限群上的 a 和 b,若存在正整数 n,使得 $an = b$,求解 $n = \log ab$ 的问题称为有限群上离散对数问题;而对椭圆曲线上的离散点 P,Q,求解 l 使得 $lP = Q$ 称为椭圆曲线离散对数问题。椭圆曲线密码体制的诱人之处在于安全性相当的前提下,其密钥的长度更短。如前所述,RSA 使用 1024 bit 模长获得的安全性,在椭圆曲线密码体制中使用 160 bit 模长就可以获得等同的安全性。

3.2 ECC802.15.4 协议描述

新的 802.15.4 协议 ECC802.15.4 采用 ECC 公钥算法增强其 MAC 层安全性能,使网络内所有节点都有自己的密钥对,各个节点的公钥可以采用离线预设置的办法使其它节点获得,在此基础上利用 ECC 来对源和目的节点等信息进行数字签名。安全椭圆曲线的选取是建立椭圆曲线密码体制的难点,此外 ECC 的签名长度也是要重点考虑的问题。对于安全椭圆曲线的选取采用随机选取[7]的方法,ECC 的签名长度为 163bit。表 1 和表 2 是该协议的 MAC 帧格式,由帧头(MAC header, MHR)、负载和帧尾(MAC footer, MFR)三部分组成:

表 1 IEEE802.15.4 协议 MAC 帧格式

<table>
<tr><td>字节数:2</td><td>1</td><td>0/2</td><td>0/2/8</td><td>0/2</td><td>0/2/8</td><td>可变</td><td>2</td></tr>
<tr><td rowspan="2">帧控制信息</td><td rowspan="2">帧序列号</td><td>目的设备PAN标识符</td><td rowspan="2">目标地址</td><td>源设备PAN标识符</td><td rowspan="2">源设备地址</td><td rowspan="2">帧数据单元</td><td rowspan="2">FCS校验码</td></tr>
<tr><td colspan="3">地址信息</td></tr>
<tr><td colspan="6">帧头</td><td>MAC负载</td><td>MFR帧尾</td></tr>
</table>

表 2 SE－IEEE802.15.4 协议 MAC 帧格式

<table>
<tr><td>字节数:2</td><td>1</td><td>0/2</td><td>0/2/8</td><td>0/2</td><td>0/2/8</td><td>20</td><td>可变</td><td>2</td></tr>
<tr><td rowspan="2">帧控制信息</td><td rowspan="2">帧序列号</td><td>目的设备PAN标识符</td><td>目标地址</td><td>源设备PAN标识符</td><td>源设备地址</td><td rowspan="2">ECC签名</td><td rowspan="2">帧数据单元</td><td rowspan="2">FCS校验码</td></tr>
<tr><td colspan="4">地址信息</td></tr>
<tr><td colspan="6">帧头</td><td>签名</td><td>MAC负载</td><td>MFR帧尾</td></tr>
</table>

该协议的具体流程如下:

1)密钥初始化。

假设一组椭圆曲线的参数组为(q,FR,a,b,G,n,h)。其中 q 是域的阶,FR 指示域中元素的表示方法,a,b 是两个系数,G 是基点,G 的阶为 n,余因子 $h = \#E(Fq)/n$,它是一个小的素数。密钥对生成过程如下:

(1) 选择一个随机数 d,$d \in (1,n-1)$。

(2) 计算 Q,$Q = dG$。

(3) 那么公钥为 Q,私钥为整数 d。

按照此方法选取的密钥必然为椭圆曲线上的点。

(4) 各个节点的公钥可以采用离线预设置的办法使其它节点获得,把公钥预存储在各传感节点中,私钥存储在自己的内存中。

2) 发送节点签名和传输。

在域 K,椭圆曲线 E/K,曲线阶数 n 及线上基点 $G \in E(K)$ 参数确定好的前提下,源节点 A 使用椭圆曲线数字签名算法对报文签名过程如下[8]:

(1) 选择一临时ECC密钥对(k,R),其中 $k(1 < k < n-1)$,$R = (x,y) = kG$;

(2) 设 $r = x \bmod n$;如果 $r = 0$,返回到步骤 1;

(3) 计算待签名消息的散列值 $e = \mathrm{Hash}(M)$;

(4) 利用 A 的私钥 KA^-,计算 $s = k^{-1}(e + rKA^-) \bmod n$;如果 $s = 0$,返回到步骤 1;

(5) 源节点 A 发送报文及其签名(r,s)。

源节点 A 用私钥 KA^- 对报文签名后广播:

$A \rightarrow$ broadcast:[MHR,M,MFR] || [MHR,M,MFR]$_{KA^-}$。

3) 接收节点接受和验证:目的节点 B 收到源节点 A 的签名报文后,利用椭圆曲线验证算法进行验证,具体验证过程如下:

(1) 如果 $r,s \notin [1,n-1]$,则签名无效;

(2) 计算待签名消息的散列值 $e = \mathrm{Hash}(M)$;

(3) 计算 $u_1 = s^{-1}e \bmod n$ 和 $u_2 = s^{-1}r \bmod n$;

(4) 利用 A 的公钥 KA^+ 计算 $R = (x,y) = u_1P + u_2KA^+$;如果 $R = 0$,签名无效;

(5) 令 $v = x \bmod n$,比较 v 和 r,如果 $v = r$,签名有效。目的节点 B 接受源节点 A 对报文的签名。目的节点 B 使用源节点 A 的公钥 KS^+ 认证通过后,确认该签名有效。

改进后的协议应用数字签名,可以增加数据的完整性、身份的真实性和抗否认等三种安全服务,具有更高的安全性。比起 RSA 算法,ECC 具有更短的密钥和相同的安全级别,因此改进后的协议具有更好的网络性能。

4　网络性能仿真及分析

4.1　NS－2 仿真平台

NS[9](Net Simulator)起源于 1989 年的实时网络仿真器(REAL Network Simulator),在这几年中,不断地进行改进。在 1995 年,DARPA 通过 VINT(Virtual InterNet Testbed)支持了这个项目,并开发了通用的多协议网络模拟工具 NS－2。NS－2 是一个仿真的环境,用计算机程序对通信网络进行模型化,通过程序运行,模拟真实环境中节点在网络中的状态。NS－2 软件是公开源代码的,可以免费从网上下载。许多协议已经实现,有较好的文档使用手册,NS－2 具有相当大的用户群。所以 NS－2 成为了目前学术界广泛使用的一种网络仿真软件。

4.2　仿真环境及结果

利用 NS－2 仿真平台在 LINUX 环境下进行仿真试验。进行仿真前,对于 NS－2 仿真软件进行了扩展。在相关 C＋＋源程序文件中修改了相关的代码,并进行重新编译,扩展 NS－2 仿真平台。以下的仿真就是在已扩展的 NS－2 仿真平台下进行的。

下面是 ECC163 和 RSA1024 的一个性能对比表[10]:

算法	密钥大小	密钥生成	认证	签名
RSA	1024	4708.3ms	12.7ms	228.4ms
ECC	163	3.8ms	10.7ms	3.0ms

设置一个 500m * 500m 的区域,结点的移动速度为 0m/s(静止),仿真时长设为 200s。对于不同的结点数,分别用 ECC 和 RSA 来实现数字签名,Hash 函数选择 SHA－1。采用 ECC 签名,签名延迟设为 3.0ms,认证延迟设为 10.7ms, SHA－1 做 Hash 处理的时间为 0.0009ms;采用 RSA 签名,签名延迟设为 228.4ms,验证延迟设为 12.7ms, SHA－1 做 Hash 处理的时间为 0.0036ms。采用 CBR 数据源,设定发送速率为每秒 1 个数据包,对于无签名的 802.15.4 协议,CBR 数据源生成的数据包的长度取值为 44 字节,采用 ECC 签名,CBR 数据源生成的数据包的长度取值为 64 字节,采用 RSA 签名,CBR 数据源生成的数据包的长度取值为 256 字节。然后进行多次仿真,计算出数据包的端到端延迟时间的平均值。如图 1 所示,可以明显地看出,由于 ECC 的签名速度比 RSA 快很多,使用 ECC 算法来实现数字签名比使用 RSA 算法的端到端延迟有明显的减少;而由于 ECC 算法密钥很短,比起无签名的情况,使用 ECC 算法来实现数字签名并未产生很明显的端到端延迟,开销小,因而能耗少,拥有很好的网络性能。

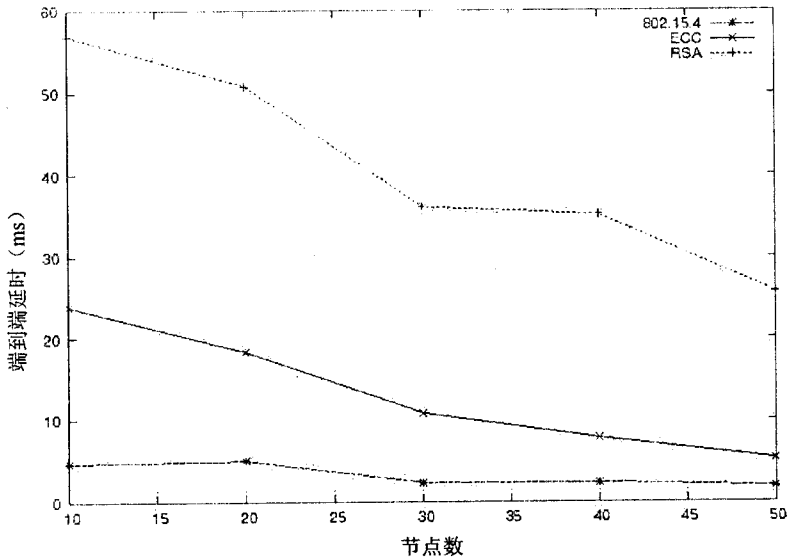

图 1　端到端延迟

5　结　论

对 802.15.4 协议的安全进行了研究,提出了一个新的增强安全性的 IEEE 802.15.4 协议并用 NS－2 进行网络仿真。该协议通过使用公钥加密算法 ECC 来实现数字签名,可以增加数据完整性、身份真实性和抗否认三种安全服务。与一般的用 RSA 算法实现数字签名相比,ECC 算法产生的端到端延迟明显减少,此外,ECC 密钥很短,比起无签名的情况,使用 ECC 算法来实现数字签名并未产生很明显的端到端延迟,开销小,因而能耗少,拥有很好的网络性能。

参考文献:

[1] 任丰原,黄海宁,林　闯. 无线传感器网络[J]. 软件学报,2003,14(7):1282－1291.

[2] 王安东,张方舟,秦　刚,等. 无线传感器网络安全协议的研究[J].计算机工程,2005,31(21):10－13.

[3] 孙利民,李建中,陈　渝,等. 无线传感器网络[M].北京:清华大学出版社,2005:109－132,

[4] IEEE Standards 802.15.4－2003. Wireless Medium Access Control(MAC) and Physical Layer(PHY) Specifications for Low2Rate Wireless Personal Area Networks(LR2WPANs)[S].[s.l.]:[s.n.],2003.

[5] 范恒英,何大可,卿　铭. 公钥密码新方向:椭圆曲线密码学[J].通信技术,2002(7):82－84.

[6] Miller V. Use of elliptic curves in cryptography[M].[s.l.]: Springer－Verlag,1998:418－425.

[7] Stallings W. 密码编码学与网络安全[M].刘玉珍,王丽娜,

(下转第 143 页)

比四维树减少 19.46%(为偶数)、33.5%(为奇数)。另外,概率树、二叉树、星型结构其加密次数均随着 k 的增长呈 2 倍增长;而四维树其加密次数随着 k 的奇数(或偶数)增长呈 4 倍增长。

文献[7]中指出成员在某些多播组中或者停留极短的时间或者待满整个多播会话过程。故假设有一半成员属于 C_1,即在星型结构中,而另一半成员处于其它子树中。

实验二:假设 $N/2$ 成员属于 C_1,$N/4$ 成员属于 C_2,$N/8$ 成员属于 C_3,$N/16$ 成员属于 C_4,$N/32$ 成员属于 C_5,$N/64$ 成员属于 C_6,比较上述四种密钥组织结构在批量密钥更新时管理者的密钥更新开销。

图 3(a) ~ (d) 分别绘制了 k 取[10,15]、[16,20]、[21,25]、[26,30]时四种密钥组织结构各自的 $\bar{E}$。如图所示,无论 k 取何值,概率树均优于其它三种密钥组织结构。在一次批量密钥更新中,其平均加密次数比星型结构减少 21%,比二叉树减少 34.8%,比四维树减少 22%(k 为偶数)、14.4%(k 为奇数)。概率树、二叉树、星型结构其加密次数均随着 k 的增长呈 2 倍增长;而四维树其加密次数随着 k 的奇数(或偶数)增长呈 4 倍增长。

综上实验,无论 k 取何值,概率树效率较其它三种密钥组织结构都有较大的优势,尤其是相对于普通的平衡二叉树,显著地减小了管理者的密钥更新开销。

在实验一的条件下,四维树优于星型结构;而在实验二的条件下,k 为奇数时,四维树较好,k 为偶数时,星型结构较好。这也符合表 1 的结果,成员变动概率越大,星型结构越有优势;成员变动概率越小,树型结构越有优势。如果成员变动概率均很大(趋向 1),二叉树的密钥更新开销接近概率树(此时即为星型结构)的 2 倍;如果成员变动概率均很小(趋向 0),星型结构的密钥更新开销接近概率树(此时即为树型结构)的几百倍。

3 结　论

对多播密钥树的组织结构进行理论研究,综合星型结构和树型结构,给出了密钥树的一种概率组织方法,较传统的平衡二叉树显著地减小了密钥更新开销。概率组织方法的关键是对成员依据其变动概率进行分类,尤其是将属于 C_1 的成员与属于其它类的成员划分开。关于成员变动概率的计算问题,文中没有涉及,是下一步的研究工作。简单的可以用附权值的方法,也可尝试采用赌轮等智能方法进行分类。另外,如果成员的变动概率呈现两极化或大多数成员的变动概率较大时,可以牺牲小部分的效率,将简化树再次简化为两分树的形式——星型结构和 $a = 1,2$ 的优化树,这在成员变动概率难以获得(或代价过高)时,具有更高的实际意义。

参考文献:

[1] Wallner D, Harder E, Agee R. Key Management for Multicast: Issues and Architecture[EB/OL]. 1998 - 09. Internet Draft, ftp://ftp.ietf.org/internet - drafts/draft - wallner - key - arch - 01.txt.

[2] Wong Chung Kei, Gouda M, Simon S. Lam Secure Group Communications Using Key Graphs[J]. IEEE/ACM Transactions on Networking, 2000, 8(1): 16 - 30.

[3] Steve L X, Richard Y Y, Gouda M G, et al. Batch Rekeying for Secure Group Communications[C]//Proceedings of the 10 th International World Wide Web Conference. Hong Kong, China: [s.n.], 2001: 525 - 534.

[4] Zhu F, Chan A, Noubir G. Optimal Tree Structure for Key Management of Simultaneous Join/Leave in Secure Multicast [C]//IEEE Military Communications Conference. Boston: [s.n.], 2003(2): 773 - 778.

[5] Selcuk A, McCubbin C, Sidhu D. Probabilistic Optimization of LKH - based Multicast Key Distribution Schemes[EB/OL]. 2000. http://www.ietf.org/internet - drafts/draft - selcuk - probabilistic - lkh - 01.txt, Internet Draft.

[6] Zhu S, Setia S, Jajodia S. Performance Optimizations for Group Key management Schemes for Secure Multicast[C]//Proceedings of the 23rd IEEE International Conference on Distributed Computing Systems. Rhode Island, USA: [s.n.], 2003: 163 - 171.

[7] Almeroth K, Ammar M. Multicast Group Behavior in the Internet's Multicast Backbone (MBone)[J]. IEEE Communications Magazine, 1997, 35(6): 224 - 229.

[8] 许　勇. 批量密钥更新中密钥组织方法的研究与实现[J]. 东南大学学报:自然科学版, 2006, 36(3): 488 - 492.

(上接第 139 页)

傅建明等译. 北京:电子工业出版社, 2005: 218 - 227.

[8] Stinson D R. 密码学原理与实践[M]. 第 2 版. 冯登国译. 北京:电子工业出版社, 2003: 245 - 246.

[9] 徐雷鸣, 庞　博, 赵　耀. NS 与网络模拟[M]. 北京:人民邮电出版社, 2003: 1 - 8.

[10] Certicom Corp. The Elliptic Curve Cryptosystem[EB/OL]. 1998 - 03. http://www.certicom.com.