第33卷 第23期 计 算 机 工 程 2007年12月
Vol.33 No.23 Computer Engineering December 2007
·博士论文· 文章编号：1000—3428(2007)23—0001—02 文献标识码：A 中图分类号：TP309

基于快速公钥签名的自组网QoS多播路由认证

杨铭熙，李腊元
（武汉理工大学计算机学院，武汉 430070）

摘 要：提出了一个新的具备安全功能的Ad hoc网多QoS约束的多播路由协议NSQMRAN。该协议采用新型公钥签名算法NTRUSign作为密码机制为路由报文签名，加强了安全性。NSQMRAN为Ad hoc网QoS多播路由协议增加了源认证机制，从而提供了QoS多播路由报文的来源真实性、数据完整性和抗否认等安全服务以抵御恶意节点的攻击。基于NS2的仿真结果表明，在Ad hoc网中，与采用RSA公钥算法的协议相比，采用NTRUSign的NSQMRAN协议网络性能较好，产生较少的端到端延迟。

关键词：QoS；多播；公钥；NTRUSign；认证

QoS Multicast Routing Authentication for Ad Hoc Networks Based on Fast Signing with Public Key

YANG Ming-xi, LI La-yuan
(School of Computer Science and Technology, Wuhan University of Technology, Wuhan 430070)

【Abstract】A novel secure multiple QoS guaranteed multicast routing protocol for Ad hoc networks NSQMRAN is presented, which uses NTRUSign as cryptographic mechanism to sign the route massages. NSQMRAN enhances the security with source authentication mechanism and provides such security services as reality, integrity and non-repudiation for the QoS multicast route messages in Ad hoc networks to guard against the attacks caused by malicious nodes. And the main simulating on results based on NS2 shows that compared with other protocols which use RSA as public key cryptographic algorithm, the performance of NSQMRAN protocol based on NTRUSign is better and it causes less delay of end to end.

【Key words】QoS; multicast; public key; NTRUSign; authentication

已有一些学者提出了适用于Ad hoc网的QoS多播路由协议，如HQMRP和AQM等。但这些协议都没有相关安全措施，相信所有的参与通信的节点，而恶意节点进行伪造、篡改路由信息的攻击是时时存在的。因此，构造安全QoS多播路由协议是十分必要的。

在诸多Ad hoc网安全路由协议中使用的密码机制，基本上都是对称密钥、RSA等传统公钥机制或Hash链机制[1]。其中对称密钥机制不能抵御接收方伪造和发送方否认攻击，RSA公钥机制计算开销太大，而Hash链机制也需借助于MAC机制且需时钟同步和链同步。

近年来涌现出了一些新的公钥密码算法，如NTRU, XTR, ECC等。经比较，NTRU是其中最快的一种。本文提出了一个以基于NTRU的签名算法NTRUSign为认证机制的移动自组网安全QoS多播路由协议NSQMRAN，意在寻求密钥较短且速度也较快的密码机制的支持。

1 NTRUSign简介

NTRUSign[2]是一种基于NTRU的签名算法。NTRU[3~4]是一种新型简单的快速公钥密码，它加密、解密一个长度为N的信息分组需要$O(N^2)$次操作，而RSA需$O(N^3)$次操作，所以，NTRU比RSA快。NTRUSign签名算法[2]是基于NTRU的安全性较强的签名算法，目前尚未发现针对其的有效攻击。其算法描述[4]如下所述。

1.1 定义与符号

与NTRU相同，NTRUSign也在环$R=Z[x]/(x^N-1)$上进行运算。一个多项式$a(x)\in R$可表示为 $a=\sum_{i=0}^{N-1}a_i x^i$。两个多项式的积可以简单记为$a*b=c(\mathrm{mod}x^N-1)$。其中，多项式系数要取模$q$, q为2的次幂。在$R_q^*=\{R_q-0\}$中单位元记为1，a在R_q^*中的逆元记为a^{-1}。

定义 设$a(x)$是环$R=Z[x]/(x^N-1)$上的一个多项式，$a(x)$的中心范数定义为

$$\|a(x)\|^2=\sum_{i=0}^{N-1}(a_i-\mu_a)^2=\sum_{i=0}^{N-1}a_i^2-\frac{1}{N}(\sum_{i=0}^{N-1}a_i)^2$$

其中，$\mu_a=\frac{1}{N}\sum_{i=0}^{N-1}a_i$，且有 $\|a*b\|\approx\|a\|\cdot\|b\|$。

公开参数：N为维数，是一个素数，如251；q为模数，通常为2的次幂；d_f, d_g为密钥参数；$NormBound$为验证时使用的确认边界范数。

1.2 密钥生成

(1)选择两个多项式f, g，它们分别有d_f, d_g个1，其余为0。其中，要求f, g满足：

$$\|f\|,\ \|g\|=O(\sqrt{N})$$

计算公钥：

$$h\equiv f^{-1}*g(\mathrm{mod}\,q) \tag{1}$$

(2)计算多项式(F,G)满足：

$$f*G-F*g=q \tag{2}$$

$$\|F\|\approx\|f\|\sqrt{N/12},\qquad \|G\|\approx\|g\|\sqrt{N/12} \tag{3}$$

基金项目：国家自然科学基金资助项目(60672137)；教育部博士点基金资助项目(20060497015)

作者简介：杨铭熙(1956－)，女，博士、副教授，主研方向：网络安全；李腊元，教授、博士生导师

收稿日期：2007-01-20 **E-mail：**yangmx@whut.edu.cn

1.3 签名

(1)对消息D使用Hash变换：$H(D)$，获得多项式(m_1,m_2)，m_1, m_2均为$R_q = Z_q[x]/(x^N-1)$上的多项式。

(2)计算多项式a, b, A, B，它们均属于环$R=Z[x]/(x^N-1)$：

$$G*m_1-F*m_2 = A+q*B \quad (4)$$

$$-g*m_1+f*m_2=a+q*b \quad (5)$$

其中，a 和 A 的各项系数均在$-q/2$~$q/2$ 之间。

(3)计算多项式 S 如下：

$$S \equiv f*B+F*b(\bmod q) \quad (6)$$

多项式 S 为消息 D 的关于公钥 h 的签名。

1.4 验证

(1)对消息D实行Hash变换$H(D)$，得到多项式(m_1,m_2)。

(2)由 S 及 h 得到

$$T\equiv S*h(\bmod q) \quad (7)$$

(3)计算(S,T), (m_1,m_2)之间距离$\|m_1-S\| + \|m_2-T\|$。若

$$\| S-m_1\|^2 + \| T-m_2\|^2 \le NormBound^2 \quad (8)$$

成立，则通过验证。

文献[2]指出：$(N, d_f, d_g, Normbound) = (251, 128, 73, 71, 1\ 300)$，密钥长度为 1 757bits的情况下其安全性等同于RSA1024。

2 NSQMRAN 协议描述

2.1 初始化阶段

(1)选择与RSA1024 安全强度相当的NTRUSign参数分别为: $N = 251$, q=128, d_f=73, d_g=71, $NormBound$=300。

(2)随机选择多项式 f和g，使其系数符合d_f和d_g的要求，根据式(1)计算公钥h。

(3)根据式(2)计算多项式 F 和 G，使其满足式(3)。它们和 f, g 共同组成私钥。

2.2 安全组的加入

假设: (1)网络中已有了合适的分布式访问控制和密钥管理机制可用于安全组；(2)网络中已有相关信号机制为各节点提供带宽、时延和抖动等链路参数。

每个加入安全 QoS 多播会话的成员都必须加入安全组，接受访问控制和密钥管理机制的约束和服务。

2.3 安全QoS多播树的创建

如果一个组成员t_s想安全地发送信息给组成员，可在开始时初始化一个安全QoS多播会话，即创建一个安全的对QoS敏感的多播树$T(s,M)$。因此，t_s广播一个序列号为 i 的创建声明$CTreq$如下（其中省略了对路由跳数的处理）：

(1)t_s: $m_{s,i}$ = [$CTreq$, IDt_s, $T(s,M)$, i, $Bandwidth$, B, $Delay$, D, $Delay\text{-}jitter$, J,…]

其中，QoS 约束指标为最小带宽 B、最大累计延迟 D、最大抖动 J。

(2)t_s：将Hash($m_{s,i}$)表示成向量的形式(m_1, m_2)，计算多项式a, b, A, B，满足式(4)和式(5)。其中，a和A的各项系数均在$-q/2$, $q/2$ 之间。则t_s创建QoS多播树的声明报文的签名为

$$Sig_{s,i} \equiv f*B+F*b(\bmod q)$$

(3)$t_s \rightarrow *$: $\{m_{s,i} \| Sig_{s,i}\}$。

若该多播树已被创建过，则t_s的邻居会发出拒绝创建的信息“Ctnak”给t_s，经签名验证后该组创建声明被丢弃。否则经过一段特定的时间后该安全QoS多播树创建成功。

2.4 安全 QoS 多播树的加入

(1)如果一个组成员同时也是接收者的t_u希望加入安全QoS多播会话，则广播一个加入QoS多播树的请求，其中，t_v为树上节点，具体为生成报文和签名：

1) t_u: $m_{u,i}$ =[$JTreq$, $IDtu$, $T(s,M)$, i, $Bandwidth$, B, $Delay$, D, $Delay\text{-}jitter$, J,…]

2)签名：操作同上节中的步骤(2)和步骤(3)，然后t_u向邻居发出广播包：

$t_u \rightarrow *$: $\{ m_{u,i} \| Sig_{u,i}\}$

(2)当中继节点并且也是树上节点的t_v收到这个请求信息以后，对t_u签名验证如下：

1)用t_u的公钥h根据式(7)算出T；

2)然后验证式(8)是否成立。若成立，则通过验证，否则不通过，丢包；

3)接着t_v检查该安全多播树能否满足t_u的QoS要求。

若$(d(t_s,*)+d(t_u,t_v) \leqslant D) \wedge (dj(t_s,*)+dj(t_u,t_v) \leqslant J) \wedge (bw(t_u,t_v) \geqslant B)$成立，其中，$d(t_s,*)$和$dj(t_s,*)$分别是从$t_s$到$t_u$的累计延迟和延迟抖动的和；$bw(t_u,t_v)$, $d(t_u,t_v)$和$dj(t_u,t_v)$分别是t_u和t_v两节点间沿路的带宽、延迟和抖动。

则 t_v发出一个回应信息JTack给t_u如下，表示接受t_u经由t_v加入此树。

$t_v \rightarrow t_u$: $\{[JTack, IDt_v, T(s,M), i] \| Sig_{v,i}\}$

否则，再检查：若 $bw(t_u,t_v)<B$，则从$T(s,M)$上移去t_u；

若$(d(t_s,*)+d(t_u,t_v)>D) \vee (dj(t_s,*)+dj(t_u,t_v)>J)$，则$t_v$转发$t_u$的请求给它的本地邻居为$t_u$搜索和计算满足条件的新的 路径。

若找不到，t_v发出拒绝报文$JTnak$给t_u：

$t_v \rightarrow t_u$: $\{[JTnak, IDt_v, T(s, M), i] \| Sig_{v,i}\ \}$

(3)当t_u收到回应信息$Jtack$后会验证t_v的签名$Sig_{v,i}$。验证通过则收下，t_u加入安全QoS多播树和路由成功；否则丢弃该报文。收到拒绝报文且签名验证通过，则加入安全QoS多播树和路由请求失败。

3 NSQMRAN 网络性能仿真

本文采用国际标准组织推荐的网络仿真平台NS2 来仿真NSQMRAN的网络性能，在不同的安全QoS多播树成员数目下的网络端到端的延迟时间如图 1 所示。为了比较，还实现了以RSA和HORSEI2[5]为基础进行认证的安全QoS多播协议，在图 1 中 3 条曲线分别标以HORSEI2, NTRUSign, RSA。

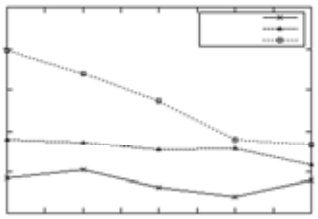

图 1 端道端延迟比较

仿真相关参数为：(1)区域：1 500m×300 m；(2)节点总数为 50，发送者数目为 1；(3)仿真时长：910s；(4)物理层/MAC层协议：802.11b；(5)发送速率为 2 包/s。(6)节点运动速度为随机 0～1m/s，没有停顿时间；(7)每个仿真数据经过 9 次CBR会话得出；(8)所采用的QoS约束为最小带宽 56Kb/s；(9)数据包长度为 256bits。(10)所采用的各种签名算法的延迟时 间[2]如下：HORSEI2 的签名延迟为 0.003 59ms，验证延迟为 0.003 59ms*R，R为 1～32 整数范围中的随机数。且设置t =1024, k =16, d =1024。RSA的签名延迟为 0.36ms，验证延迟为 9.54ms(据weidai网页测试数据)。NTRUSign的签名延迟

（下转第 15 页）