第 36 卷 第 1 期 计 算 机 工 程 2010 年 1 月
Vol.36 No.1 Computer Engineering January 2010
·安全技术· 文章编号：1000—3428(2010)01—0157—04 文献标识码：A 中图分类号：TP309

# 基于 AODV 的安全高效路由方案设计

杨成云，张明清，唐 俊
(解放军信息工程大学电子技术学院，郑州 450004)

**摘 要：**路由协议的安全性是移动自组网络安全中最重要的一环，极易受到各种攻击。分析 AODV 路由协议存在的主要安全隐患，探讨现有安全路由方案的不足，提出一种新的基于椭圆曲线密码体制、自证明公钥、单向哈希链等技术的安全高效路由方案，同时完成会话密钥的交换。仿真结果表明，改进后的协议以较少的开销得到较高的安全性。

**关键词：**Ad hoc 网络；AODV 协议；椭圆曲线密码；自证明公钥；网络仿真

# Design of Secure Efficient Routing Scheme Based on AODV

YANG Cheng-yun, ZHANG Ming-qing, TANG Jun
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

**【Abstract】**Mobile Ad hoc networks usually use Ad hoc On-demand Distance Vector(AODV) protocol for lower overhead, but vulnerable to attacks for the lack of security mechanism. A security enhancement scheme based on Elliptic Curve Cryptography(ECC), self-certified pubic key, one-way Hash-chain is proposed, it establishes the session key between source and destination. Experimental results show that the proposed protocol is secure and efficient.

**【Key words】**Ad hoc networks; AODV protocol; Elliptic Curve Cryptography(ECC); self-certified pubic key; network simulation

## 1 概述

移动 Ad hoc 网络是由一组动态节点组成的多跳临时性自组织网络，广泛应用于军事和民用领域，其安全问题受到广泛关注。由于动态拓扑、资源受限、无线通信等特点使得路由协议的安全比传统网络要复杂得多。AODV(Ad hoc On-demand Distance Vector)[1]路由协议因简单和控制开销小而广泛应用于自组网络，但它没有任何安全机制保障，很容易受到各种恶意节点的攻击，常见的针对 AODV 协议的攻击[2]主要有篡改、假冒、伪造、黑洞、rushing 攻击、wormhole 攻击、拒绝服务攻击等。考虑到移动自组网中节点、网络资源有限的特点[3]，本文设计了一个安全高效的路由方案，以尽量少的占用资源，减少网络的延时。

## 2 相关工作

目前，已经提出的基于密码体制的安全路由协议，概括来说，可以分为以下 3 类：

(1)基于共享密钥的消息认证码 HMAC(Keyed-Hash Message Authentication Code)，如 SRP 等。HMAC 中哈希函数的计算开销低，对称密码系统中的加解密操作效率比较高，但它只能被确定的目的接收者验证，不适合于广播消息认证；任意 2 个 节点间共享密钥的建立比较困难，密钥的新鲜性难以保证；密钥的存储开销会随着新节点的加入显著增加；而且，如果一个节点被俘获，则它与所有节点的共享密钥都将被暴露。

(2)基于非对称密钥的数字签名，如 SAODV 和 ARAN 等。数字签名能够被任何知道签名者公钥的节点验证，适用于广播消息认证，并且适合于大型网络，因为它不需要大量对密钥。但是，目前所提出的基于数字签名的安全路由方案中，所使用的公钥密码体制引入大量的计算开销，并且需要证书对公钥进行验证，每个节点都维持一个证书撤销列表来记录撤销的证书，因此，要花费较大的处理、存储和通信开销。

(3)基于单向哈希链的消息认证码，如 SEAD, Ariadne 等。TESLA 是使用这种方法的广播认证协议，用单向哈希链来构造密钥，但是它需要时钟同步，这在移动 Ad hoc 网络中很难实现，而且引入了较大的存储开销和延时，SEAD, Ariadne 就是基于 TESLA 而提出的安全路由协议。

在基于 AODV 协议的安全路由方案中，最典型的就是 SAODV 和 ARAN。SAODV 协议采用数字签名和哈希链来保护路由发现和路由维护过程。ARAN 协议采用逐跳认证的方式对邻居节点进行鉴别。这 2 种协议都是基于 RSA 公钥密码体制，在增强安全性的同时引入了大量的计算开销；都需要证书对公钥进行验证，因而引入了大量存储、计算和通信开销；用户的私钥由密钥分发中心(KGC)产生与分发，因此，KGC 可以伪装成任何合法用户而不被发现，并且一旦 KGC 被俘获，所有其他节点的私钥将被暴露。此外，在 SAODV 协议中，使用单向哈希链来防止恶意节点减少跳数值时，不能阻止“同距离伪造”攻击，即恶意节点可以不按照协议规则增加跳数值，同时也不改变哈希值，直接将收到的跳数值和相应的哈希值转发出去。

## 3 安全路由方案设计

### 3.1 方案设计的基本原理

为适应 Ad hoc 网络中节点和网络资源有限的特点，本文引入了一个安全高效的数字签名方案。椭圆曲线密码体制非

**作者简介：**杨成云(1983－)，男，硕士研究生，主研方向：Ad hoc 网络安全，网络仿真；张明清，副教授；唐 俊，讲师
**收稿日期：**2009-08-30 **E-mail：**yangchengyundemail@163.com

常适用于无线通信这种资源有限环境，和其他公钥体制如 RSA, DSA 等相比，能够提供更好的加密强度、更快的执行速度和更短的密钥长度。自证明公钥密码系统也非常适合于移动 Ad hoc 网络，它有以下优点：验证用户身份不需要证书和基于身份的公钥密码系统相比更安全，因为系统中心只分发用户的公钥而不产生用户的私钥。文献[4]进一步提出了基于椭圆曲线的自证明公钥密码系统，它运行效率高，验证签名和公钥的有效性能一步同时完成，不需要证书服务，并且用户的私钥由用户自己产生，因此，具有更高的安全性。本文所设计的安全路由方案就利用一个基于椭圆曲线自证明公钥密码系统的数字签名方案，对 AODV 协议中的固定域部分进行保护。

对于 AODV 路由协议的可变域部分，利用单向哈希函数同时对跳数值和序列号进行保护。为了讨论方便，假设 $m$ 为网络中节点之间的最大跳数，$n+1$ 为哈希链的长度，哈希链 $\{h_0, h_1, \cdots, h_n\}$ 利用哈希函数 $H$，通过递归式 $h_{j+1} = H(h_j)$ 产生。哈希链中的哈希值被分成多段，每段包含 $m$ 个哈希值，并且根据所要保护路由信息的序列号和跳数值，按照与哈希链产生相反的方向进行使用。由于哈希函数的单向性和哈希值的分段使用，因此使得具有较小序列号的节点不能产生与较大序列号对应的哈希值，对于同一序列号中的哈希值，具有较大跳数值的节点不能产生与较小跳数值对应的哈希值，哈希链的结构如图 1 所示。

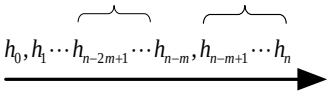


**图 1　哈希链结构**

为防止恶意节点的“同距离伪造”攻击，本方案借鉴了安全路由协议 SEAD[5]的思想，每个节点在进行哈希操作时要将自己的身份信息编码到哈希值中构成哈希树链。因此，节点就不能直接转发包含有其他节点身份信息的哈希值，而必须增加路由报文的跳数值，同时将自己的身份信息通过哈希操作编码到哈希值中，克服了 SAODV 协议无法防止“同距离伪造”攻击的缺陷。

此外，为了在数据传输阶段利用高效的对称加密算法进行大量的实时数据安全传输，所设计的安全路由方案同时完成了会话密钥的协商，密钥协商过程也是基于椭圆曲线的自证明公钥密码系统。

### 3.2　基于椭圆曲线的自证明数字签名方案

基于 Tsaur 提出的公钥密码系统，每个节点能够分别获得自己的公私钥对。以下先定义数字签名方案中所用到的符号，然后再描述具体的数字签名方案。

符号定义：

$ID_i$：节点 $i$ 的身份信息。

$P$：有限域的大小，是一个素数或 2 的幂，长度大约为 160 bit。

$E$：基于有限域 $F_p$ 上的椭圆曲线，$E$: $y^2 = x^3 + ax + b \pmod p$，域元素 $a,b \in F_p$ 且 $4a^3 + 27b^2 \pmod p \neq 0$，由所有的点$(x, y)$，$x \in F_p$，$y \in F_p$ 及无限远点 $O$ 构成 $E(F_p)$。

$B$: $E(F_p)$ 上阶为 $n$ 的基点，其中 $n$ 是一个大素数(160 bit)。

$X(G)$：取点 $G$ 的横坐标值。

$S_u$：节点 $u$ 的私钥。

$P_u$：节点 $u$ 的公钥。

$M$：待签名的路由信息。

$A$：对路由信息进行签名的节点。

$B$：验证签名的节点。

$SA$：颁发节点公钥的系统授权中心。

签名过程：

(1)$A$ 随机选择一个整数变量 $k$，$k \in [2, n-2]$，并计算 $k \cdot B = G$。

(2)$A$ 计算：

$r = X(G) \pmod p$, $s = k + S_a \cdot h(M \| r) \pmod n$。

(3) $A$ 传输签名$(r,s)$和 $M$ 给 $B$。

验证过程：

(1) $B$ 计算：

$V_a = P_a + h(ID_a) \cdot B + [(X(P_a) + h(ID_a)) \bmod n] \cdot P_{SA}$，

$s \cdot B - h(M \| r) \cdot V_a = k \cdot B + S_a \cdot h(M \| r) \cdot B - h(M \| r) \cdot (S_a \cdot B) =$

$k \cdot B = (x_1, y_1)$

(2)如果 $x_1 = r \pmod p$ 成立，则签名是有效的。

### 3.3　初始化阶段

系统 CA 定义系统参数并产生公、私钥对以便以后为注册用户产生自证明公钥。用户向系统 CA 提交自己的身份信息和受保护的随机密钥，由于随机密钥受到保护，CA 不知道用户的随机密钥，因此不能化装成其他合法用户。根据用户提交的身份信息和受保护的随机密钥，CA 将返回一个自证明公钥和公钥的证明，然后注册用户可以用自己的随机密钥和 CA 分发的公钥证明产生自己的私钥，同时用户也可以用自己产生的私钥验证 CA 分发的公钥的真实性。表 1 是改进协议使用的符号定义。

**表 1　协议符号定义**

| 符号 | 定义 |
|---|---|
| RREQ | 路由请求数据包 |
| RREP | 路由回复数据包 |
| RERR | 路由错误数据包 |
| $u$,$v$ | 用户节点 |
| $k_u$ | 节点 $u$ 的公钥 |
| $k^{-1}_u$ | 节点 $u$ 的私钥 |
| FF | 路由信息中的固定域(Fixed Field)部分 |
| CF | 路由信息中的可变域(Changeable Field)部分 |

### 3.4　路由发现阶段

AODV 路由协议的路由过程主要依赖 RREQ、RREP 和 RRER 报文，必须对这些报文进行保护，防止恶意节点篡改或伪造。本方案用上面给出的安全高效的数字签名方案对路由报文中的固定域部分进行数字签名；对报文中可变域部分，如跳数值和序列号，采用以上提出的单向哈希树链方法进行保护。为了对中间节点进行认证，引入逐跳签名即每个中间节点都要用上一跳节点公钥来验证签名，并用自己的私钥对收到报文重新签名，以防止来自中间节点的攻击。为描述方便，安全后缀中与哈希信息相关的不变部分用 $hash\_inf$ 表示，即：

$hash\_inf =< Hash\_Function,\ Max\_Hop\_Count, Top\_Hash >$

假设源节点为 $S$，目的节点为 $D$，中间节点为 $N_i$。当 $S$

Seq1 Seq0

有数据需要发送又没有到达目的节点的路由或路由已经过期时，$S$ 随机选择一个整数 $X_s \in [2, n-2]$，并计算 $T_s = X_s \cdot B(\bmod p)$，广播路由请求信息：

$S \to *$ :[ $RREQ$ , $hash\_inf$ , $RREQ\_CF\_Hash$, $RREQ\_FF\_Sig_s$, $RREQ\_FF\_SigN_i$, $E_{K_d}(T_s)$ ]

$RREQ\_CF\_Hash$ 是源节点 $S$ 根据路由请求信息中的跳数值和序列号计算的哈希值，$RREQ\_FF\_Sig_s$ 是源节点 $S$ 对固定域部分的签名，以便进行源认证和信息完整性认证，$RREQ\_FF\_SigN_i$ 是中间节点对固定域部分的签名，以便对中间节点进行认证。对于源节点而言，$RREQ\_FF\_SigN_i$ 为空。$E_{K_d}(T_s)$ 是 $S$ 用目的节点 $D$ 的公钥对会话密钥交换参数的加密保护。当中间节点 $N_i$ 收到上一跳节点 $N_{i-1}$ 的路由请求包时，将进行以下处理：(1)根据 $RREQ\_CF\_Hash$ 和 $hash\_inf$ 验证跳数值和序列号是否被恶意修改；(2)以源节点 $S$ 的公钥验证源节点的签名 $RREQ\_FF\_Sig_s$；(3)验证上一跳节点 $N_{i-1}$ 的签名 $RREQ\_FF\_SigN_{i-1}$。验证成功后，跳数值增加 1，更新 $RREQ\_CF\_Hash$，然后用自己的私钥对要转发的报文进行签名并更新 $RREQ\_FF\_SigN_{i-1}$，继续转发报文直至到达目的节点 $D$。目的节点收到路由请求包后，进行同样的处理，验证成功后用自己的私钥解密出 $T_s$，并随机选择一个整数 $X_d \in [2, n-2]$，计算 $T_d = X_d \cdot B(\bmod p)$，单播路由回复到上一跳节点，设为 $N_j$：

$D \to N_j$ : [ $RREP$ , $hash\_inf$ , $RREP\_CF\_Hash$ , $RREP\_FF\_Sig_d$ , $RREP\_FF\_SigN_i$ , $E_{k_s}(T_d)$ ]

$N_j$ 收到报文后同样先进行相关验证，其过程与路由请求过程相同。最终源节点 $S$ 收到 $RREP$ 报文，所有验证通过后，同样以自己的私钥解密出 $T_d$，路由发现过程结束。

源节点与目的节点分别收到 $T_d$ 和 $T_s$ 后，就可以计算它们的共享会话密钥，其过程如下：

$$S:\ V_d = P_d + h(ID_d)\cdot B + \left[(X(P_d) + h(ID_d)) \bmod n\right]\cdot P_{SA}$$

$$SK = X_s \cdot V_d + S_s \cdot T_d = (x_s s_d \bmod n)\cdot B + (s_s x_d \bmod n)\cdot B$$

同样，计算 $D$：

$$V_s = P_s + h(ID_s)\cdot B + [(X(P_s) + h(ID_s)) \bmod n]\cdot P_{SA}$$

$$SK = X_d \cdot V_s + S_d \cdot T_s = (X_d S_s \bmod n)\cdot B + (S_d X_s \bmod n)\cdot B$$

这样，源节点 $S$ 与目的节点 $D$ 有了共享会话密钥 $SK$，可用对称加密算法来保证大量实时数据的安全传输。

### 3.5 路由维护

当路径中由于节点移动或节点能量耗尽而出现链路中断时，链路的上游节点会发送路由错误信息 $RRER$ 通知其他节点。为了防止恶意节点通过伪造 $RRER$ 报文来破坏路径，必须对发送 $RRER$ 报文的节点进行身份认证。因此，中间节点必须用自己的私钥对 $RRER$ 报文进行签名，收到 $RRER$ 报文的其他节点只有通过对 $RRER$ 报文的源认证后，才从路由表中删除相应路由条目。

## 4 分析与仿真实验

### 4.1 效率与安全性分析

本文所提的安全路由方案对于路由信息的固定域部分采用基于椭圆曲线自证明公钥的数字签名加以保护，与 SAODV、ARAN 等基于 RSA 公钥体制相比，能够提供更好的加密强度、更快的执行速度和更短的密钥长度，而且不需要引入证书，因此，节省了大量了计算、通信、存储开销；对于可变域部分，利用高效的哈希函数加以保护。因此，本方案相对于其他的安全路由协议效率更高，能更好地适用于存储能力及 CPU 计算能力等资源有限的 Ad hoc 网络。

在安全性方面，采用了基于椭圆曲线自认证公钥的数字签名，安全强度更高，同时由于用户的私钥由用户自己产生，系统 CA 不知道用户的私钥，因此无法伪装成其他合法用户，而且也解决了用户私钥的安全分发问题；对可变域，利用单向哈希链同时对跳数值和序列号进行保护，并且将节点的身份信息编码到哈希值中构成哈希树，防止了“同距离伪造”攻击，因此，安全性更好。

### 4.2 仿真实验

本文使用源代码公开、具有良好扩展性的网络仿真软件 NS2 搭建网络仿真平台，通过仿真与评估来验证所提安全路由方案的有效性，其编译环境为 Windows 下的 cygwin。仿真实验参数如表 2 所示。

**表 2 仿真参数**

| 参数 | 对应值 |
|---|---|
| 节点数 | 40 |
| 仿真空间 | 1 000×1 000 |
| 仿真时间/s | 800 |
| 流量类型 | CBR |
| 分组传输速率/(packer·s$^{-1}$) | 4 |
| 分组大小/Byte | 512 |
| 移动模型 | Random waypoint |
| 最大移动速率/(m·s$^{-1}$) | 0~20 |
| 带宽/(Mb·s$^{-1}$) | 2 |
| 节点通信范围/m | 200 |

仿真实验选择以下性能指标进行比较：

(1)数据包递交率：成功到达目的节点的分组数与源节点所发送的分组数之比。

(2)平均路由请求时延：源节点从发出路由请求包(*RREQ*)到接收到第 1 个相应的路由回复包(*RREP*)之间的平均时延。

(3)网络吞吐量：表征网络传输速率。

仿真实验分 2 种情况进行：

(1)正常情况下改进后的协议与原 AODV 协议的性能比较。由图 2、图 3 可以看出，改进后的 AODV 协议在数据包递交率、网络吞吐量方面的性能均与原协议非常接近，这说明改进后的协议仍然保持了原协议高效的路由发现和路由维护能力。从图 4 可以看出，改进后协议的平均路由请求时延比原协议略高，这是由于路由报文在收发时要进行安全操作而耗费一定时间。但是由于本方案采用了高效的数字签名和单向哈希链，因此只引入了少量的时延。

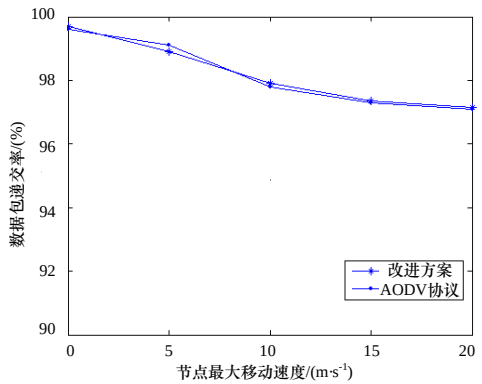


**图 2 正常情况数据包递交率**

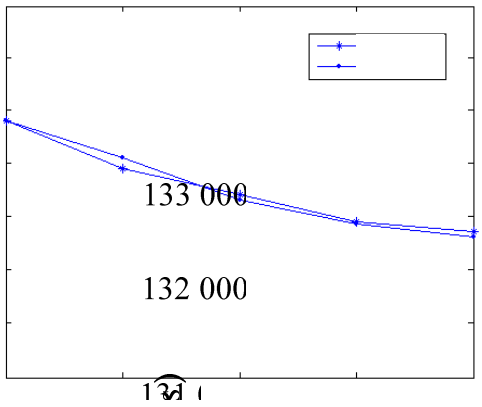


图 3　正常情况下网络吞吐量

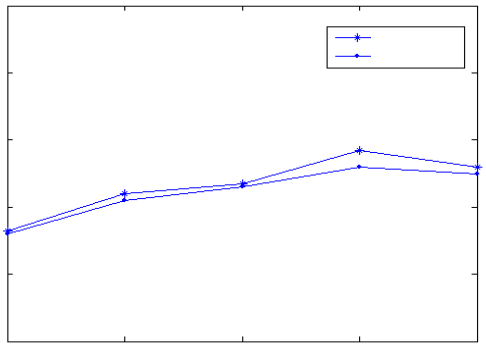

图 4　正常情况下平均路由请求时延

(2)在存在攻击节点情况下改进后协议与原协议安全性比较。为此在仿真实验中实现了最常见的简单黑洞攻击(blackholes)模型，执行黑洞攻击的恶意节点在收到邻居节点的 *RREQ* 报文后立刻冒充目的节点回复 *RREP*，同时置跳数为 0，当攻击节点出现在路由路径上时，所有经过此节点的数据包都将被丢弃。图 5 表明存在黑洞攻击的恶意节点时，原 AODV 协议的网络吞吐量明显降低，这是由于 AODV 协议没有安全措施的保护。相反所提的安全路由协议网络吞吐量始终维持较高水平，说明改进后协议能有效抵制黑洞攻击。

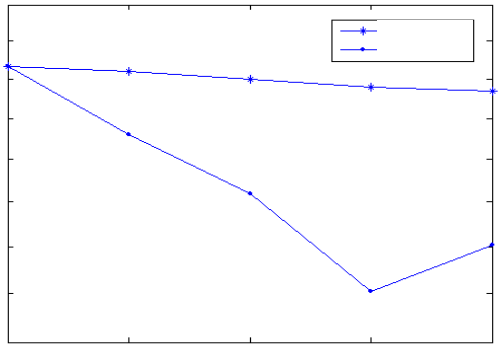

图 5　有攻击时网络吞吐量

## 5　结束语

本文提出了一种安全高效的路由方案，并同时完成了通信双方会话密钥的协商。分析和仿真结果表明，该方案在没有引入较大协议开销的基础上，大大提高了协议的安全性。本文只构建了简单的黑洞攻击模型，下一步将进一步研究改进协议在存在其他攻击情况下的工作效能。

## 参考文献

[1] 袁培燕, 庄新豪, 赵慧娜. 移动 Ad hoc 网络 AODV 路由协议的研究进展[J]. 许昌学院学报, 2007, 26(2): 91-94.

[2] 季晓君, 田　畅, 张毓森. Ad hco 网络路由安全[J]. 解放军理工大学学报, 2006, 7(4): 341-345.

[3] 戈文燕, 张修如. 一种基于 AODV 改进的安全路由方案[J]. 计算机与数字工程, 2008, 36(2): 75-78.

[4] Tsaur W J. Several Security Schemes Constructed Using ECC-based Self-certified Public Key Cryptosystems[J]. Applied Mathematics and Computation, 2005, 168(1): 447-464.

[5] Hu Yih-Chun, Johnson D, Perrig A. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks[J]. Ad Hoc Networks, 2003, 1(1): 175-192.

编辑　索书志

（上接第 156 页）

某些组件提取出来，分别对其进行分析，并在此基础上进一步综合分析整个密码算法。如果事先已经定义好了各种通用组件的分析接口，那么对 Camellia 算法的分析就转化为对这些分析接口的调用就可以了，大大简化了分析的难度和复杂度，方便了人们对 Camellia 算法的研究。由此及彼，对其他的分组密码算法也可以采用类似的方法，为分组密码自动化分析技术的实现提供了可能。

## 4　结束语

本文从许多现有分组密码算法的组建关系与流程特点入手，提取了分组密码统一描述模型的组件关系形式和算法流程形式，并给出实例验证了模型，阐述了模型带来的理论价值和实际意义。另外，关于分组密码的统一描述模型的研究符合现代密码技术的发展趋势，它将为分组密码的设计与分析带来方便。本文所建立的统一描述模型只适用于大多数常用的分组密码，因此，还需要作进一步的研究，直至建立能描述所有分组密码的统一模型。

## 参考文献

[1] Bibliowicz A, Cohen P, Biham E, et al. A System for Assisting Analysis of Some Block Cipher[EB/OL]. (2003-02-20). https://www.cosic.esat.kuleuven.be/nessie/reports/phase2/definition.pdf.

[2] Daemen J, Knudsen L, Rijmen V, et al. The Block Cipher Square[EB/OL]. (1997-10-20). http://homes.esat.kuleuven.be/~cosicart/pdf/VR-9700.

[3] Schneier B. 应用密码学——协议、算法与 C 源程序[M]. 吴世忠, 祝世雄, 译. 北京: 机械工业出版社, 2000.

[4] Biham E. A Note on Comparing the AES Candid-ates[EB/OL]. (1999-03-12). http://www-08.nist.gov/archive/aes/round1/conf2/pa-