文章编号: 1005-3026(2006)06-0646-04

基于ECC的移动Ad hoc网络安全路由算法

陈书义, 王翠荣, 赵 宏
(东北大学 信息科学与工程学院, 辽宁 沈阳 110004)

摘 要: 研究了移动Ad hoc网络(MANET)的安全路由问题, 分析了现有MANET入侵检测和安全路由策略的优缺点. 针对MANET安全和路由问题的特殊性, 提出并实现了基于ECC的MANET安全路由算法. 算法吸收了表驱动路由和按需路由策略的优点, 具有能耗低、延迟小、递交率高等显著特点. 并且算法在路由过程中引入了ECC签名认证机制, 通过路由过程中的签名认证, 使得有害节点不能参与到路由中, 保证了路由的安全性、信息的完整性和不可抵赖性. 最后利用NS-2仿真器对算法的性能进行仿真分析, 结果显示所提出的安全路由算法是高效的.

关 键 词: 移动Ad hoc网络; 网络攻击; 椭圆曲线密钥体制; 安全路由协议; NS-2网络仿真器
中图分类号: TP 393 文献标识码: A

移动Ad hoc网络(MANET)是一组移动节点动态构成的临时无线自组网络, 具有有限的物理安全、有限的终端等特点, 因此需要高效、轻量级计算的安全路由算法.

本文提出一个基于ECC的MANET安全路由算法ECCSRP, 利用ECC密钥体制对路由信息签名和认证, 保证发现可信路由. 椭圆曲线上离散对数问题是指数时间复杂度的算法, 基于模运算的整数因式分解问题和离散对数问题都是亚指数时间复杂度的通用算法, 因此椭圆曲线算法的性能要优于其他算法[1]. ECC密钥系统特别适用于MANET这种节点的计算能力和电源、带宽受限的环境, 符合MANET网络对安全路由算法性能和效率的要求.

1 移动Ad hoc网络安全路由协议

MANET网络的安全问题不同于传统的有线和无线网络, 依据攻击的特点, 可以把针对MANET网络的攻击分为主动攻击和被动攻击[2]. 把当前提出的MANET安全路由策略根据安全性实现的方法不同划分为加密、检测和冗余路径三类.

加密策略利用公钥/私钥对或者哈希密钥链来进行加密解密, 密钥管理一般采用可信CA方案或者门限密码方案. 现在已经提出的基于加密的安全路由策略主要有SRP[3], ARAN[4]和SEAD[5]等. SRP要求每个路由发现的源和目的节点之间具有一个SA. ARAN利用RSA密码体制对路由消息进行签名认证, 需要可信的CA和时钟同步, 另外RSA计算开销大. SEAD利用单路哈希函数来保证路由的安全, 需要MANET中时钟同步, 这在MANET网络中是困难的.

检测策略要求网络中的节点进行分布式协作检测节点有害行为, 然后做出响应并隔离有害节点. 已经提出的基于检测的安全路由策略主要有SAR[6]和Nuglets[7]等. 这些策略提供有限的路由安全, 可能出现错误检测等问题.

冗余路径策略[8]的思想通过冗余信息来防止对信息完整性的破坏, 要求在进行通信的两个节点之间存在安全连接, 这种策略存在效率问题.

2 基于ECC的MANET安全路由算法(ECCSRP)

2.1 ECCSRP密钥管理

算法使用离线的CA和分布式管理相结合的密钥管理策略, 它不需要选择特殊的节点作为CA, 而是由离线的CA负责网络的密钥管理, 在运行过程中网络中的节点也具备一定的密钥管理的能力, 适应网络拓扑结构的变化. 密钥管理可以分为三个阶段: 初始化阶段、更新阶段和撤销

收稿日期: 2005-07-15
基金项目: 国家高技术研究发展计划项目(2004AA113020).
作者简介: 陈书义(1972-), 男, 河南平顶山人, 东北大学博士研究生; 王翠荣(1963-), 女, 河北唐山人, 东北大学教授, 博士; 赵宏(1954-), 男, 河北河间人, 东北大学教授, 博士生导师.

证书. 本文首先在表 1 中说明一些要用到的变量和符号.

表 1　标识符说明

Table 1　Denotation of identifiers

K_A^+	节点 A 的公钥	ID_A	节点 A 的惟一标识符
K_A^-	节点 A 的私钥	$Cert_A$	节点 A 的证书
e	证书到期时间	RCB	撤销证书广播消息标识符
$[d]K_A^-$	节点 A 私钥签名的信息	SNB	可疑节点广播消息标识符
t	时间戳	MAC	消息认证码

(1) 初始化阶段: 在这个阶段, 离线的 CA 负责为每个要进入网络的节点利用 ECC 算法生成证书. 为了减少在路由建立过程中需要传递证书的开销, 在网络初始化时建立证书库分发给每个节点. 这样在路由建立过程中发送信息的节点只需要用自己的私钥签名, 而不用传递证书, 接收节点从本地的证书库查找对应公钥就可以完成认证. 例如节点 S 的证书形式如下:

$$CA \rightarrow S: Cert_S = [K_S^+, t, e, ID_S]K_{CA}^- .$$

(2) 更新阶段: 如果在运行过程中有新的节点 N 要加入到网络, 该节点必须向离线的 CA 申请证书, CA 给符合条件的节点签发证书. CA 利用 ECC 算法产生公钥私钥对、证书, 证书形式如下:

$$CA \rightarrow N: Cert_N = [K_N^+, t, e, ID_N]K_{CA}^- .$$

CA 更新证书库, 将证书库和 N 的私钥发给节点 N, N 获得证书库和私钥后进入网络, 进入网络后广播包含证书 $Cert_N$ 的消息. 如果消息是有效的, 接收到信息的节点更新自己的证书库, 将证书 $Cert_N$ 作为一条新的记录添加到证书库.

(3) 撤销证书: 在节点持有的证书库中记录着每个节点的证书的到期时间, 超过这个时间, 证书被撤销. 在两种情况下需要更新证书库中的证书到期时间. 第一种情况是 CA 撤销证书. 如果 CA 需要撤销某个节点 X 的证书, CA 就向网络中广播一条撤销证书的消息, 该消息在网络中广播, 收到消息的节点撤销相应节点 X 的证书,

$$CA \rightarrow broadcast: [RCB, t, Cert_X]K_{CA}^- .$$

第二种情况中网络节点可以通过组签名消息的方式撤销网络中某个可疑节点的证书. 网络中节点 N 发现可疑节点 X, 可以发送消息通告其他节点, 消息格式如下:

$$N \rightarrow broadcast: [SNB, t, Cert_X]K_N^- .$$

当一个节点接收到节点 N 发送的消息, 利用节点 N 的公钥对消息签名进行认证, 鉴别消息的有效性. 如果一个节点接收到 K 个不同可信节点关于节点 X 的可疑消息通告, 就认为节点 X 是有害节点, 撤销节点 X 的证书. 这里 K 是撤销证书时收到认证有效的 SNB 消息的门限值.

2.2　ECCSRP 路由机制

路由包含两个不同的阶段: 路由发现阶段(路由请求、路由应答) 和路由维护阶段.

(1) 路由发现

没有数据需要发送的时候, 节点处于空闲状态. 需要传递数据的时候, 节点变为源节点, 源节点检查路由表中有没有到目的节点的有效路由. 路由表中有有效路由, 进行数据发送, 没有有效路由则发送路由请求消息(RREQ), 开始路由发现过程. 中间节点转发 RREQ, 如果是目的节点接收到 RREQ 则返回一个路由应答消息(RREP). 中间节点将这个 RREP 返回到源节点, 这样就找到了一条路由, 进入路由建立状态, 开始数据传输.

路由消息的完整性是通过在路由消息中添加消息认证码(MAC) 来实现, MAC 是对路由消息的摘要. 路由的认证和不可抵赖性是通过 ECC 签名认证实现. 假如源节点 S 经过中间节点 A, B 查找到达目的节点 D 的路由, 路由发现过程举例如下:

S: 源节点 S 生成路由请求消息 RREQ 和消息认证码 MAC= MD5[RREQ], 签名后广播

$$S \rightarrow broadcast: [RREQ, MAC]K_S^- ;$$

A: 中间节点 A 接收到 S 的签名消息, 用 S 的公钥认证该消息, 签名有效则去掉 S 的签名, 更新 RREQ, 重新生成 MAC, 用 A 的私钥签名后广播, 并更新本地路由表

$$A \rightarrow broadcast: [RREQ, MAC]K_A^- ;$$

B: 中间节点 B 接收到 A 的签名消息, 用 A 的公钥认证该消息, 签名有效则去掉 A 的签名, 更新 RREQ, 重新生成 MAC, 用 B 的私钥签名后广播, 并更新本地路由表

$$B \rightarrow broadcast: [RREQ, MAC]K_B^- ;$$

D: 目的节点 D 接收到 B 的签名消息, 用 B 的公钥认证该消息, 签名有效则去掉 B 的签名, 生成路由应答消息 RREP 和 MAC = MD5[RREP], 用 D 的私钥签名后发送给 B, 并更新本地路由表

$D \rightarrow B$: [RREP, MAC] K_{D^-};

B: 中间节点 B 接收到 D 的签名消息, 用 D 的公钥认证该消息, 签名有效则去掉 D 的签名, 重新生成路由应答消息 RREP 和 MAC, 用 B 的私钥签名后发送给 A, 并更新本地路由表

$B \rightarrow A$: [RREP, MAC] K_{B^-};

A: 中间节点 A 接收到 B 的签名消息, 用 B 的公钥认证该消息, 签名有效则去掉 B 的签名, 重新生成路由应答消息 RREP 和 MAC, 用 B 的私钥签名后发送给 A, 并更新本地路由表

$S \rightarrow A$: [RREP, MAC] K_{A^-};

S: 源节点 S 接收到 A 的签名消息, 用 A 的公钥认证该消息, 签名有效, 则发现了一条到达 D 的路由, 更新本地路由表.

(2) 路由维护

在数据传输过程中, 路由上的节点定时发送 HELLO 消息维护着这条路由. 如果发现路由中断, 发现路由中断的节点发送路由错误消息 (RERR), 通告源节点重新发起路由发现过程.

3 ECCSRP 安全性和性能仿真分析

3.1 ECCSRP 安全性分析

算法采用了椭圆曲线密钥体制, 从信息的完整性、不可抵赖性等方面保证发现可信路由.

路由过程中使用 MD5 算法对路由消息进行摘要生成消息认证码(MAC) 保证了信息的完整性. 路由过程中利用 ECC 密钥体制的签名认证保证了路由的认证和不可抵赖性要求, 防止欺诈和伪造攻击. ECC 签名和认证也可以防止路由请求泛洪攻击, 攻击者发送的路由请求包没有可信的签名, 因此会被丢弃, 不能在网络中继续传播引起泛洪攻击.

3.2 ECCSRP 网络性能分析

利用 NS-2 仿真器[9] 在 LINUX 环境下进行仿真试验. 仿真范围是 670 m × 670 m, 节点的最大运动速度分别是 0, 5, 10, 15, 20 和 25 m/s, 仿真的运行时间是 500 s, 分为 20 和 50 个节点两种仿真场景. 仿真结果如下图所示, 其中 AODV 代表没有安全机制的标准 AODV 路由协议, ECCSRP 代表基于 ECC 的安全路由算法.

(1) 平均数据包端到端延迟

图 1 和图 2 分别显示了 20 个节点和 50 个节点的网络环境平均数据包端到端延迟的仿真结果. 虽然 ECCSRP 的路由获得时延大于 AODV 的路由获得时延, 但是从图 1 和图 2 可以看到 ECCSRP 和 AODV 的数据包传输的端到端延迟几乎相等. 这是因为路由发现信息相对于数据信息只是很小的一部分, 所以两者的平均数据包端到端延迟差别不大.

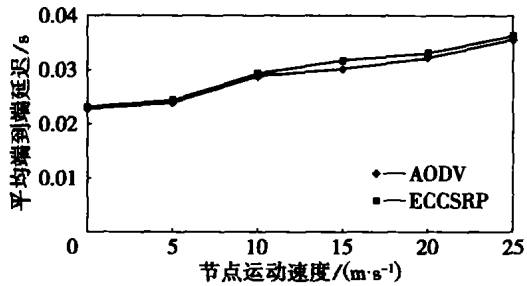

图 1 平均端到端延迟(20 节点)

Fig. 1 Average end-to-end delay (20 nodes)

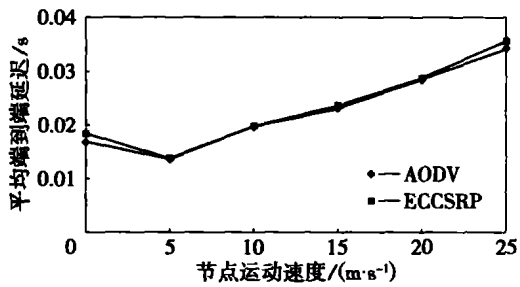

图 2 平均端到端延迟(50 节点)

Fig. 2 Average end-to-end delay (50 nodes)

(2) 数据包递交率

图 3 和图 4 分别显示了 20 个节点和 50 个节点的网络环境数据包递交率的仿真结果. 从图中可以看到随着速度的增加, 两个协议的数据包递交率下降, 但是都维持着较高的递交率. 两种情景下 ECCSRP 的包递交率和 AODV 的包递交率相似, 这说明 ECCSRP 在查找和维护路由方面是高效的.

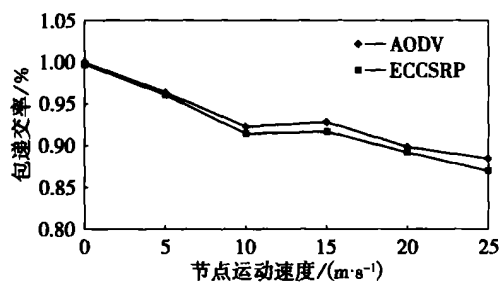

图 3 包递交率(20 节点)

Fig. 3 Average packet delivery (20 nodes)

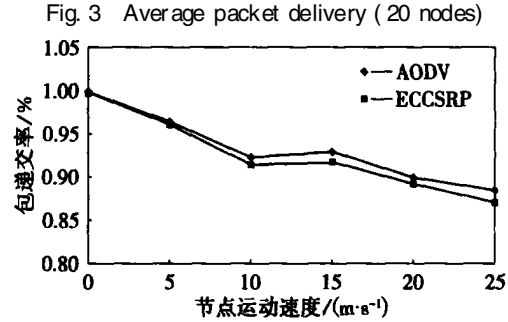

图 4 包递交率(50 节点)

Fig. 4 Average packet delivery (50 nodes)

(3) 平均节点能量消耗

图 5 和图 6 分别显示了 20 个节点和 50 个节点的网络环境平均节点能量消耗的仿真结果. 从图中可以看到 ECCSRP 和 AODV 并没有显著的差别, 这主要是因为 ECCSRP 算法并没有显著增加控制消息的数量.

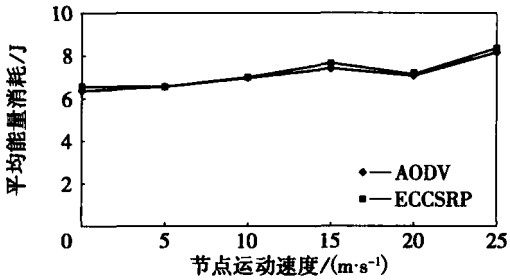

图 5　平均能量消耗(20 节点)

Fig. 5　Average energy consumption (20 nodes)

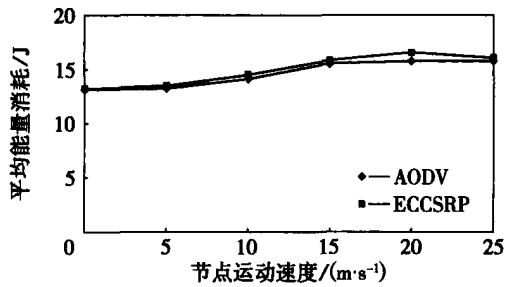

图 6　平均能量消耗(50 节点)

Fig. 6　Average energy consumption (50 nodes)

4　结　　论

MANET 可信路由的研究是一个非常有意义的研究方向, 有大量的问题需要解决. 本文提出并实现了一个基于 ECC 的 MANET 安全路由算法, 利用 ECC 密钥体制进行签名和认证, 保证了路由的可信性. 仿真结果也显示 ECCSRP 没有对路由性能带来显著影响, 因此适合 MANET 网络环境.

参考文献:

[1] Miller V. Use of elliptic curves in cryptography [A]. *Proceedings of Crypto* 85 [C]. Santa Barbara: Springer, 1985. 417- 426.

[2] 王翠荣, 高远. 移动 ad hoc 网络可信路由发现算法[J]. 东北大学学报(自然科学版), 2003, 24(11): 1045- 1048. (Wang C R, Gao Y. Discovery of trust routing for mobile ad hoc networks [J]. *Journal of Northeastern University (Natural Science)*, 2003, 24(11): 1045- 1048.)

[3] Papadimitratos P, Haas Z J. Secure routing for mobile ad hoc networks [A]. *Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS* 2002) [C]. San Antonio: Sage Science Press, 2002. 27- 31.

[4] Sanzgiri K, Dahill B, Levine B N, *et al*. ARAN: a secure routing protocol for ad hoc networks[A]. *Proceedings of* 2002 *IEEE International Conference on Network Protocols (ICNP)* [C]. Paris: IEEE Press, 2002. 78- 87.

[5] Hu Y C, Johnson D B, Perrig A. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks [A]. *The Fourth IEEE Workshop on Mobile Computing Systems and Applications*[C]. Callicoon: IEEE Press, 2002. 3- 13.

[6] Seung Y, Prasad N, Robin K. Security-aware ad hoc routing for wireless networks[A]. *The Second ACM Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc'* 01) [C]. Long Beach: ACM Press, 2001. 299- 302.

[7] Buttyan L, Hubaux J P. Nuglets: a virtual currency to stimulate cooperation in self organized ad hoc networks[R]. Lausanne: Swiss Federal Institute of Technology Lausanne, 2001. 43- 64.

[8] Lou W J, Fang Y G. A multipath routing approach for secures data delivery [A]. *Proceedings IEEE Military Communications Conference MILCOM* [C]. Washington: IEEE Press, 2001. 1467- 1473.

[9] Fall K, Varadhan K. NS notes and documents[EB/OL]. http://www.isi.edu/nsnam/ns/doc/ns_doc.pdf, 2004- 10- 22.

ECC-Based Secure Routing Algorithm for Mobile Ad Hoc Networks

CHEN Shu-yi, WANG Cui-rong, ZHAO Hong

(School of Information Science & Engineering, Northeastern University, Shenyang 110004, China. Correspondent: CHEN Shu-yi, E-mail: chen-sy@neusoft.com)

Abstract: The problem of secure routing for MANET (mobile ad hoc network) is studied. Analyzing the advantages and disadvantages of intrusion detection and secure routing policies, an ECC-based secure routing algorithm for MANET is presented and implemented according to the special secure routing requirements of the MANET. The algorithm has obviously the advantages of those of the on-demand and table driven routing policies such as low energy consumption, short delay and high delivery rate etc. The signature and authentication based on ECC are introduced in the process of routing to exclude the malicious nodes from joining the route, which can ensure the security of the route, the integrity of data and non-repudiation. The performance of the algorithm presented is analyzed with NS-2, and the simulative results show its high efficiency.

Key words: mobile Ad hoc networks; network attacks; elliptic curve cryptosystems; secure routing protocol; NS-2 network simulator

(*Received July* 15, 2005)