基于有限惩罚建立无线自组网的激励机制 *

魏 华, 孙 浩, 周雪梅
(西北工业大学 理学院, 西安 710129)

摘 要: 首先基于博弈理论建立网络模型来描述自组网中节点的行为特征,并结合改进的 AODV 路由协议算法,给出了一种基于有限惩罚的激励机制,对防止节点的自私性和欺诈性起到了重要作用;最后通过理论证明和实验验证其合理性、有效性。

关键词: 自组网; 激励机制; AODV 路由算法; 有限惩罚; 博弈论
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2009)11-4248-03
doi:10.3969/j.issn.1001-3695.2009.11.070

Incentive mechanism based on limited punishment in wireless Ad hoc network

WEI Hua, SUN Hao, ZHOU Xue-mei
(*School of Science*, *Northwestern Polytechnical University*, *Xi'an* 710129, *China*)

Abstract: Based on Nash equilibrium and Ad hoc network model, this paper put forward the current AODV routing algorithm and a new incentive mechanism of the limited punishment, which was more important to avoid the selfish and cheating. At the end, provided the experiment to verify the incentive mechanism rational and effective.

Key words: Ad hoc network; incentive mechanism; AODV routing algorithm; limited punishment; game theory

近年来,移动 Ad hoc 网络以其组网灵活性强、支持移动性、易于迅速展开、系统整体抗毁能力强、系统成本低等优点,成为通信领域中的一个热点。但是由于无线移动自组网络其通信介质的开放性、缺少固定的基础设施的支持及拓扑的动态变化等特性,易遭受安全威胁,尤其存在敌意对手的环境中,安全信任变得更为严重。在 Ad hoc 网络中,节点既是终端又是路由器,这种双重功能决定了节点既要保证自身的通信需求,又要为其他节点提供选路和转发数据的服务;然而考虑到自身能量和宽带有限等因素,节点往往表现出不合作的自私行为。以网络路由为例,由于 Ad hoc 网络的路由算法通常采用分布式的处理方式,网络中的自私节点可以通过丢弃转发给它的数据包来拒绝服务,影响网络的正常运行。文献[13]用博弈理论的方法分析 Ad hoc 网络中节点的自私行为,寻找一种对所有节点均有利的策略,使网络达到纳什均衡。

Ad hoc 网络中的节点可以分为四种不同的类型:a)节点的行为良好,严格遵照事先定义的算法和协议运行;b)节点出现了某种故障,不能正常运行;c)自私节点,这类节点参与系统是为了最大程度地满足自己的利益,只对自己有益的数据感兴趣,不愿为其他节点提供转发数据包的服务;d)蓄意破坏系统的节点,并以此为目的来确定自己的策略。无论是自私节点还是恶意节点,它们的行为都将导致网络性能的下降和网络稳定性的恶化。文献[4]用贝叶斯博弈理论去分析恶意节点与防御节点之间的行为,在不同的情况下,双方均选择对自己有利的策略。

仿真分析表明[5],当 c)种节点达到一定数量时,网络的整体性能会严重下降,所以需要相应的机制去激励节点之间的合作。Ad hoc 网络中激励机制的目标就是建立起一种适当的机制和环境,促使网络中的节点都采取合作和负责的行为,从而使整个网络得到稳定性的发展。然而随着 Ad hoc 网络的应用越来越广,激励机制的缺乏严重影响了网络的稳定性和公平性。目前研究激励机制的重要方法就是将博弈论引入 Ad hoc 网络的研究中,将节点看做独立的代理,主要有三种类型,即信誉机制[6]、价格机制[7]和拍卖机制[8]。

本文给出的激励机制是基于博弈论中的有限惩罚,在网络达到纳什均衡下,为了防止节点的欺诈和自私行为影响网络的稳定性和公平性,对这些节点进行有限惩罚,对网络整体的吞吐量影响较小,并且保证网络最终是帕累托最优的。

1 基于有限惩罚建立激励机制

1.1 节点行为策略的理论分析

假设无线自组网络中共有 N 个节点分布在 K 种不同的能量等级,每种能量等级的上限值为 E_i,在等级 i 上节点的生存时间为 L_i,平均能量为 $\rho_i = E_i/L_i$,且 $\rho_1 > \rho_2 > \cdots > \rho_K$,节点作为收发端点或中间节点的概率均为 $1/N$,某条路径上需要参与转发的节点数目为 x,概率为 $q(x)$,路径上中间节点的最大数目为 M,则 $x \leqslant M$。定义从源端到目的端的一次通信称做一个会话。在通信过程中,节点发送、接收和处理数据都需要消耗能量。其中发送所耗的能量占主导。为简化起见,这里只考虑发送所消耗的能量并定义该值为常量 1。

如果在每次会话中节点的最小能量等级为 ρ_j,则称这次会话为会话 j。对给定的节点,称 $B_h^j(k)$ 为在会话 j 中节点 h 到时间 k 时发送出的转发请求的数目,$A_h^j(k)$ 为在会话 j 中节点 h

收稿日期: 2009-01-01; **修回日期**: 2009-02-23 **基金项目**: 国家自然科学基金资助项目(70871098)

作者简介:魏华(1986-),男,河南安阳人,硕士研究生,主要研究方向为博弈论、下一代无线网络(wh860127@163.com);孙浩(1967-),男,副教授,硕导,博士,主要研究方向为博弈论及其应用等;周雪梅(1985-),女,硕士研究生,主要研究方向为博弈论、下一代无线网络.

到时间 k 时发送出的转发请求被接收的数目,$D_h^j(k)$ 为在会话 j 中节点 h 到时间 k 时其邻节点给自己发出的转发请求的数目,$C_h^j(k)$ 为在会话 j 中节点 h 到时间 k 时节点 h 接收邻节点的转发请求的数目。对 $1\leqslant j\leqslant K, 1\leqslant h\leqslant N$ 时 $\phi_h^j(k)=A_h^j(k)/B_h^j(k)$,$\psi_h^j(k)=C_h^j(k)/D_h^j(k)$,则 $NAR=\lim\limits_{k\to\infty}\phi_h^j(k)$ 为节点 h 的标准化吞吐量。

下面分别讨论在会话 j 中,节点 P 作为源节点和转发节点所消耗的平均能量(忽略接收所消耗的能量)。如果 P 为源节点,消耗的能量记为 $e_{pj}^{(s)}$,则有

$$e_{pj}^{(s)}=(1/N)\times NAR=(1/N)\sum_{x=1}^{M}\sum_{h_1\cdots h_j}q(x)\Gamma(l;h_1\cdots h_j)\tau_{1j}^{h_1}\cdots\tau_{jj}^{h_j}\quad(1)$$

其中:$\Gamma(l;h_1\cdots h_j)$ 是一个多元函数,表示在参与转发的 x 个节点中能量等级为 ρ_i 的节点数目为 h_i 的概率;$\tau_{1j}^{h_1}\cdots\tau_{jj}^{h_j}$ 表示节点愿意提供转发服务的概率,简称转发概率。同样,如果 P 作为转发节点,消耗的平均能量记为 $e_{pj}^{(r)}$,则有

$$e_{pj}^{(r)}=(1/N)\sum_{x=1}^{M}xq(x)\sum_{h_1\cdots h_j}\Gamma(l-1;h_1\cdots h_j)\tau_{1j}^{h_1}\cdots\tau_{jj}^{h_j}\tau_{\mathrm{class}(p)j}\quad(2)$$

其中:class(p)表示 P 所属的能量等级。根据式(1)(2)得出

$$\sum_{j=1}^{K}(e_{pj}^{(s)}+e_{pj}^{(r)})\leqslant\rho_{\mathrm{class}(p)};1\leqslant\rho\leqslant N\quad(3)$$

$$\tau_{\mathrm{class}(p)j}\in[0,1];1\leqslant j\leqslant K;1\leqslant\rho\leqslant N\quad(4)$$

由式(1)可知,自组网络中节点的标准化吞吐量不仅与自己的转发概率有关,还受到其他节点的转发概率的限制。令节点的收益函数 $u_{hj}=NAR=\lim\limits_{k\to\infty}\phi_h^j(k)$,策略就是节点的转发概率,有以下定义。

定义 1　在会话 j 中,若一个策略组合 $\tau^*=(\tau_{1j}^*,\tau_{2j}^*,\cdots,\tau_{jj}^*)$ 是博弈 $G=\{\tau,u\}$ 的一个纳什均衡,那么式(5)成立:

$$u_{ij}(\tau_{ij}^*,\tau_{-ij})\geqslant u_{ij}(\tau_{ij},\tau_{-ij});1\leqslant i\leqslant j\leqslant K\quad(5)$$

例如假设节点 A 与 B 组成一个自组网,它们同属于一个能量等级,平均能量为 ρ,如果节点 A 和 B 其中之一要与外部接入点进行通信,则另外一个节点必须提供转发服务。因此,转发节点数目为 $x=1$,概率 $q(1)=1$。由式(3)和(4),求得节点 A 所消耗的能量为 $e_A^{(s)}+e_A^{(r)}\leqslant\rho,\tau_B/2+\tau_A/2\leqslant\rho$。同理节点 B 所消耗的能量为 $e_B^{(s)}+e_B^{(r)}\leqslant\rho,\tau_A/2+\tau_B/2\leqslant\rho$。

如图 1 所示,横轴为节点 A 的收益 u_A,纵轴为节点 B 的收益 u_B,可以通过以下三种情况分析网络的纳什均衡点:

a)当 $\tau_A^*>\rho$ 或 $\tau_B^*>\rho$ 时,因为当 $\tau_A<\tau_A^*$ 时,$u_A(\tau_A,\tau_B)\geqslant u_A(\tau_A^*,\tau_B)$,所以 (τ_A^*,τ_B^*) 不是纳什均衡点。

b)当 $\tau_A^*=\tau_B^*=\rho$ 时,由图 1 可知 $u_A(\rho,\tau_B)\geqslant u_A(\tau_A,\tau_B)$ 和 $u_B(\rho,\tau_A)\geqslant u_B(\tau_B,\tau_A)$ 同时成立,所以 (τ_A^*,τ_B^*) 是纳什均衡点。

c)当 $\tau_A^*<\rho,\tau_B^*<\rho$ 时,只需将直线 $\tau_A+\tau_B=2\rho$ 沿方向 $(-1,-1)$ 移动,由式(1)(2)可知,当 $\tau^*=(\rho_1,\rho_1),\rho_1<\rho$ 时,网络也是达到纳什均衡的。

由以上的分析可知,在线段 $(0,0)(\rho,\rho)$ 上的点都是纳什均衡点,在点 (ρ,ρ) 处是帕累托最优的。当一个节点的策略大于理性策略时,该节点的收益也不会超过该节点采取理性策略的收益,有以下的推论。

推论 1　在会话 j 中节点的理性策略为 $\tau_{ij}=\tau_{jj};1\leqslant i\leqslant j\leqslant k$。

1.2　*GTFT* 算法

在一个有自私节点的网络中,每个节点都想使自己的收益达到最大,因为节点的收益不仅取决于自己的策略,还取决于其他节点的策略,这就需要节点通过合作来得到。GTFT 策略就是节点模仿对手的策略,在 $t>1$ 的任意阶段选择的策略等于对手在 $t-1$ 阶段选择的策略。可以用图 2 形象地表示出来。(x,拒绝)表示对手拒绝转发,我方也将选择拒绝;(x,接收)表示对手接收转发请求,我方也回到接收请求状态,x 表示任意的行动。

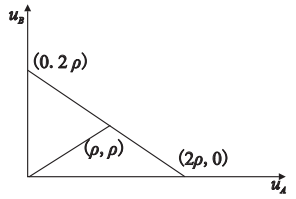

图1　节点*A*与*B*的Nash均衡点

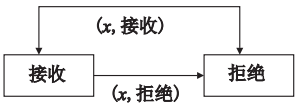

图2　GTFT策略

下面给出基于自组网模型的 GTFT 算法[9]:

a)当 $\psi_h^j(k)>\tau(\tau\leqslant\tau_j)$ 或 $\phi_h^j(k)\leqslant\psi_h^j(k)-\varepsilon$ 时,节点 h 拒绝转发,τ 为节点 h 初始设定的行为策略;

b)其他情况时,为其他节点转发。

$\psi_h^j(k)>\tau(\tau\leqslant\tau_j)$ 表示节点 h 接收其他节点的转发请求已经超过了自己的意愿;$\phi_h^j(k)\leqslant\psi_h^j(k)-\varepsilon$ 表示节点 h 接收其他节点的转发请求超过了其他节点接收自己的转发请求。由于节点的自私性,节点 h 在这两种情况下的策略就是拒绝其他节点的转发请求。

定理 1[9]　如果网络中有 N 个节点,K 个能量等级,$\rho_1>\rho_2>\cdots>\rho_K$,每个能量等级 i 有 n_i 个节点,设 $q(1)=1,M=1$,则

a)如果除了节点 h 外,其他节点均采用 GTFT 策略,那么 $\lim\limits_{k\to\infty}\sup\phi_h^j(k)\leqslant\tau(\tau\leqslant\tau_{jj})$。

b)如果所有节点均采用 GTFT 策略,则所有的 $\lim\limits_{k\to\infty}\phi_h^j(k)\to\tau(h=1,\cdots,N)$。

推论 2　若定理 2 中的两个结论成立,则 GTFT 策略收敛到一个纳什均衡。

推论 3　若定理 2 中的两个结论成立且当 $\tau=\tau_{jj}$ 时,则 GTFT 策略收敛到一个纳什均衡且是帕累托最优的。

1.3　AODV 路由协议的改进

在上面的网络模型中会遇到新的问题,即在每次会话中,中间节点如何获知本次会话的类型,从而得知本次会话的理性策略。笔者将用改进的 AODV 路由协议来确保中间节点都能得知每次会话的类型。文献[10]给出了 AODV 路由协议的路由发现过程,为了确定每次会话的类型 j,可以把 AODV 路由协议的路由发现过程进行修改。路由发现过程如下:

a)源节点首先发起路由请求过程,在发起的路由请求报文中携带以下信息字段:〈源地址,源序列号,广播 ID,目的地址,目的序列号,跳数计数器,会话的类型 j〉。其中,序列号〈源地址,广播 ID〉惟一标志一个路由请求。

b)中间节点 i 在收到路由请求报文时,比较本节点和目的节点的地址:

(a)若自己是目的节点,则回复路由响应报文;否则转(b)。

(b)根据〈源地址,广播 ID〉判断是否收到过该请求消息,如果收到过则丢弃该请求消息;否则转向(c)。

(c)记录相应的信息以形成反向路由。记录的信息包括上游节点地址(即向本节点发送路由请求消息的节点)、目的地址、源地址、广播 ID、反向路由超时时长和源序列号等。同时跳数计数器加 1,且

$$j \Leftarrow \begin{cases} \text{class}(i) & \rho_{\text{class}(i)} < \rho_j \\ j & \text{其他} \end{cases}$$

c)向邻节点转发该路由请求报文。

经过改进的 AODV 路由协议,在路由发现的过程中,同时可以确定本次会话的类型,中间节点就可得知本次会话的理性策略。

1.4　基于有限惩罚的激励机制

在 1.1 节中给出了一种基于博弈论的网络模型,当节点在每次会话中诚实地报出自己的能量等级,且当节点采取 GTFT 策略时,网络是收敛到纳什均衡状态的。然而在实际中的自组网,由于节点是受能量限制的,节点都想尽量降低自己为其他节点转发数据所消耗的能量,提高其他节点为自己转发数据所消耗的能量。这样就会出现下面两种欺骗行为:

a)若源节点 P 的能量等级为 ρ_7,中间节点的能量等级分别为 ρ_3、ρ_5、ρ_6、ρ_4,由前面的知识可知,本次会话的类型为 7,且中间节点的理性策略为 τ_{77},源节点 P 的收益为 u_{p7}。若源节点报出自己的能量等级为 ρ_6,则中间节点的理性策略就为 τ_{66},源节点 P 的收益就会增大到 u_{p6}。

b)若节点 P 作为中间节点且会话类型为 7,则节点 P 就可以降低自己的能量等级为 ρ_8 或更低,这样节点 P 就减少了为其他节点转发数据所消耗的能量。

本文给出的激励机制主要借鉴博弈论中的有限惩罚策略[11]。有限惩罚就是惩罚只会持续一段时间,而不会永远持续下去,这样的好处就是对网络整体的吞吐量影响较小。假设网络中的节点都装备了对邻节点进行监测的监测器 watchdog 和时间计时器 timer,给定的初始值为 t。另外,在每次会话中,所有节点采取的策略均为理性策略,这样给出下面的激励机制:

a)若节点 P 的邻节点的监测器 watchdog 发现节点 P 两次汇报的能量等级不相符时,就把这些信息发送给其他节点。

b)当节点 P 在会话 j 中作为源节点时,中间节点的策略为 $\lambda\tau_{jj}(0 \leqslant \lambda \leqslant 1)$,$\lambda$ 称为惩罚的系数,且时间计数器 timer 减 1。

c)若又有其他节点发现节点 P 出现欺骗行为时,时间计数器 timer 恢复初值。

d)当时间计数器为零时,则取消对节点 P 的惩罚。

笔者所给出的激励机制是以有限惩罚为基础的,假如有节点谎报了自己的能量等级,在它作为源节点的会话中,其他节点就减少自己对该节点的服务,以对该节点进行惩罚。笔者认为网络中的所有节点均装备了时间计时器 timer,这是给犯错误节点悔过的机会,这样对网络的整体性能影响不太大。当节点在一次会话中欺骗了其他节点,它就会得到相应的惩罚;当该节点在以后的时间 t 中没有再欺骗其他节点,其他节点就不再惩罚该节点。

2　仿真实验和分析

实验 1 的条件是:若节点 A、B 和 C 组成一个无线自组网,它们的真实能量等级分别为 $\rho_A = \rho_B = 0.51$ 和 $\rho_C = 0.58$。由推论 1 可知节点的理性策略为 0.51,如果其中之一要与外部接入点进行通信,则另外一个节点必须提供转发服务,因此,转发节点数目为 $x = 1$,概率 $q(1) = 1$。

由推论 1 可知节点 C 的理性策略为 0.51,若节点 C 想通过将自己的策略 τ 增大来提高自己的标准化吞吐量,也就是说增大自己对其他节点转发请求的接收率,使其他节点也增大对自己的转发请求的接收率。但图 3 表明,当节点 C 通过采取策略 $\tau > 0.51$ 时得到的标准化吞吐量仍为 0.51,也就是说当其他节点采取策略 τ_{jj} 时,节点 C 的理性策略也为 τ_{jj}。

实验 2 的条件是:若节点 A、B 和 C 组成一个无线自组网,它们的真实能量等级分别为 $\rho_A = \rho_B = 0.56$ 和 $\rho_C = 0.46$。由推论 1 可知节点的理性策略为 0.51,如果其中之一要与外部接入点进行通信,则另外一个节点必须提供转发服务,因此,转发节点数目为 $x = 1$,概率 $q(1) = 1$,$n = 20$,时间计时器的初值 $t = 500$。

图 4 给出的是节点 C 欺诈与诚实时节点 C 的收益。由图 4 可知,节点欺诈时的收益明显要高于节点诚实时的收益。为了网络的公平性,要对这些节点进行惩罚。

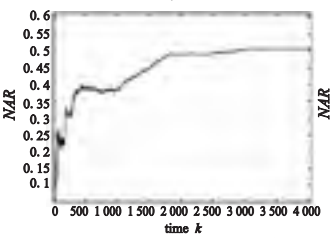

图3　节点收益的收敛曲线

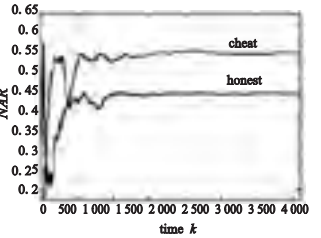

图4　节点欺诈与诚实的收益对比

若节点 A 的监测器 watchdog 发现节点 C 两次汇报的能量等级不相符时,就把这些信息发送给节点 B。节点 B 知道节点 C 欺骗了自己,则节点 A 和 B 就会在节点 C 作为源节点时对其进行惩罚。在惩罚过程中,节点 B 的吞吐量变化过程如图 5 所示。

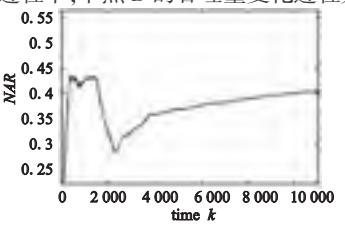

图5　节点受到有限惩罚的收益曲线

由图 5 可知,在节点 C 受惩罚的过程中,节点 C 的吞吐量在急剧下降,当惩罚结束时它的吞吐量开始上升。节点 C 为了使自己总的吞吐量最大,在惩罚结束后,为了自己总的吞吐量就不会第二次欺骗其他节点,除非这种节点是恶意的。

3　结束语

Ad hoc 网络中的激励机制是 Ad hoc 网络研究领域中一个很有意义的课题,对于 Ad hoc 网络的可持续发展起到了重要作用。本文结合当前的研究现状,提出了基于博弈理论的一种惩罚性的激励机制,并从实验中验证了该激励机制的有效性,对节点的自私性和欺诈性起到了一定的作用,且 Ad hoc 网络是收敛到纳什均衡状态的,并且是帕累托最优的。

参考文献:

[1] NURMI P. Modeling energy constrained routing in selfish Ad hoc networks[C]//Proc of GameNets'06. Pisa:[s. n.],2006.

[2] FELEGYHAZI M, HUBAUX J P, HUBAUX J P, *et al*. Nash equilibria of packet forwarding strategies in wireless Ad hoc networks[J]. IEEE Trans on Mobile Computing, 2006,5(5):463-476.

[3] YAN Lu, HAILES S. Cooperative packet relaying model for wireless Ad hoc networks[C]//Proc of FOWANC'08. Hong Kong:[s. n.], 2008:88-93.

[4] LIU Yu, COMANICIU C, MAN Hong. A Bayesian game approach for intrusion detection in wireless Ad hoc networks[C]//Proc of GameNets'06. Pisa:[s. n.],2006.

(下转第 4288 页)

是随机变化的,S 也是随机的,所以整个签名中没有任何真实签名者的信息,所以签名具有完全匿名性。

4.3 存在不可伪造

在 model2 下存在不可伪造的证明类同文献[15]中存在的不可伪造证明,不同的是在签名提问中 σ 的构造和 g^{ab} 的计算,具体如下:

B 采用如下方法构造 R 和 m 的签名:选择 u_i,令 $F(u_i)\neq 0 \pmod{l_u}$,选择 $r_1, r_2, \cdots, r_n \in_R Z_p$,对 $F(u)=0 \pmod{l_u}$,令 $U_u = g^{J(u)}$,$u'' = J(u)$,计算 $R_j = g^{u^{n_{rj}}}$,$j \in \{1,2,\cdots,n\} \setminus \{i\}$,$R_i = g^{u^{n_{ri}} r_{ui}} g^{r_{ui}}$,$h = H_m(R, m, R_1, R_2, \cdots, R_n)$,$S = g_2^a (U_{u_i})^{r_{ui}} g^h \left(\prod_{j=1}^{n} (U_j)^{r_j}\right)$,$R$ 关于 m 的签名为 $\sigma = (S, R_1, R_2, \cdots, R_n)$。

如果 $F(u_j^*)\neq 0 \pmod p$,B 中断;如果对于所有的 $j \in [1, n]$,$F(u_j^*)=0 \pmod p$,B 计算输出:

$$S/(R_1^{J(u_1^*)} \cdots R_n^{J(u_n^*)} \cdot g^h) = [g_2^a (U_{u_i})^{r_{ui}} g^h (\prod_{j=1}^{n} (U_j)^{r_j})]/$$
$$(g^{u'' r_1 J(u_1'')} \cdots g^{u^{n_r} r_n J(u_n^*)} \cdot g^{r_{ui} J(u_i^*)} \cdot g^h) = g_2^a = g^{ab}$$

输出为 CDH 问题实例的解。改进后的方案在 model2 下是存在不可伪造的。

在 model3 下,假设攻击者在已知环 R 关于消息 m 的签名 $\sigma = (S, R_1, R_2, \cdots, R_n)$ 时,伪造签名 $\sigma' = (S', R'_1, R'_2, \cdots, R'_n)$,由于 H_m 是无碰撞的,则 $h' \neq h$,要使 $e(S', g) = e(g_1, g_2)\, e(g, g)^{h'} \left(\prod_{i=1}^{n} e(U_i, R'_i)\right)$ 成立,概率为 2^{-n_m},因而伪造成功的概率是可忽略的。改进后的方案在 model3 中是存在不可伪造的。

4.4 效率分析

本文提出的方案与已有方案进行的效率与安全性分析如表 1 所示。

表 1 效率与安全分析

方案	效率		安全模式		
	签名长度	验证	M_1	M_2	M_3
文献[11]	$n+2$	$n+2$		√	
文献[15]	$n+1$	$n+1$		√	
文献[16]	$n+2$	$n+2$			√
本文方案	$n+1$	$n+1$			√

在效率分析中,只考虑双线性对的运算量。从表 1 可以看出,本文提出的方案结合了高效率和高安全性两个优点。

5 结束语

本文提出的基于身份的环签名方案的安全性是基于标准模型下的 CDH 假设。该签名与已有签名相比,签名效率和安全性均较高。

参考文献:

[1] SHAMIR A. Identity based cryptosystems and signature schemes [C]// Lecture Notes in Computer Science, vol 196. Berlin: Springer-Verlag, 1984: 47-53.

[2] RIVEST R, SHAMIR A, TAUMAN Y. How to leak a secret [C]// Lecture Notes in Computer Science, vol 2248. Berlin: Springer-Verlag, 2001: 552-565.

[3] ABE M, OHKUBO M, SUZUKI K. 1-out-of-*n* signatures from a variety of keys [C]// Proc of ASIACRYPT'02. Berlin: Springer-Verlag, 2002: 415-432.

[4] LIU J K, WONG D S. On the security models of (threshold) ring signature schemes [C]// Proc of ICISC 2004. Berlin: Springer-Verlag, 2004: 204-217.

[5] ZHANG Fang-guo, KIM K. ID-based blind signature and ring signature from pairing [C]// Lecture Notes in Computer Science, vol 2501. Berlin: Springer-Verlag, 2002: 533-547.

[6] HERRANZ J, SAEZ G. Forking lemmes for ring signature schemes [C]// Lecture Notes in Computer Science, vol 2904. Berlin: Springer-Verlag, 2002: 266-279.

[7] BAEK J, RON S, ZHENG Yu-liang. Formal proofs for the security of signcryption [C]// Lecture Notes in Computer Science, vol 2274. London, UK: Springer-Verlag, 2002: 80-89.

[8] AWASTHI A K, LAL S. ID-based ring signature and proxy ring signature schemes from bilinear pairings [EB/OL]. (2004). http://eprint.iacr.org/2004/184.pdf.

[9] HERRANZ J, SAEZ G. A provable secure ID-based ring signature scheme [EB/OL]. (2003). http://eprint.iacr.org/2003/261.pdf.

[10] BONEH D, BOYEN X. Short signatures without random oracles [C]// Proc of EUROCRYPT'2004. Berlin: Springer-Verlag, 2004: 56-73.

[11] AU M H, LIU K, YUEN T H, *et al*. ID-based ring signature scheme secure in the standard model [C]// Proc of IWSEC 2006. Berlin: Springer-Verlag, 2006: 1-16.

[12] CHOW S S M, WEI U K, LIU J K, *et al*. Ring signatures without random oracles [C]// Proc of ACMSICCS. New York: ACM Press, 2006: 297-302.

[13] SHACHAM H, WATERS B. Efficient ring signatures without random oracles [EB/OL]. (2006). http://eprint.iacr.org/2006/289.pdf.

[14] BENDER A, KATZ J, MORSELLI R. Ring signatures: stronger definitions, and constructions without random oracles [C]// Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2006: 60-79.

[15] 张跃宇,李晖,王育民. 标准模型下基于身份的环签名方案[J]. 通信学报,2008, 29(4):40-44.

[16] 王化群,于红,吕显强,等. 两个标准模型中可证安全的环签名方案的安全性分析及其改进[J]. 通信学报, 2008, 29(8):57-62.

(上接第 4250 页)

[5] MARTI S, GIULI T J, LAI K, *et al*. Mitigating routing misbehavior in mobile Ad hoc networks [C]//Proc of the 6th IEEE International Conference on Mobile Computing and Networking. Massachusetts, BA: [s. n.], 2000: 255-265.

[6] HE Qi, WU Da-peng, KHOSLA P. SORI: a secure and objective reputation based incentive scheme for Ad hoc networks [C]//Proc of IEEE Wireless Communications and Networking Conference. Atlanta, GA: [s. n.], 2004: 825-830.

[7] BUTTYÁN L, HUBAUX J P. Stimulating cooperation in self-organizing mobile Ad hoc networks [J]. ACM Mobile Networks and Applications, 2003, 8(5): 579-592.

[8] CAI Jian-feng, POOCH U. Play alone or together-truthful and efficient routing in wireless Ad hoc networks with selfish nodes [C]//Proc of IEEE International Conference on Mobile Ad hoc and Sensor Systems. Fort Lauderdale: [s. n.], 2004: 457-465.

[9] SRINIVASAN V, NUGGEHALLI P, CHIASSERINI C F, *et al*. Cooperation in wireless Ad hoc networks [C]//Proc of IEEE Inocom Conference. 2003.

[10] 郑少仁,王海涛,赵志峰,等. Ad hoc 网络技术[M]. 北京:人民邮电出版社,2005.

[11] 姚国庆. 博弈论[M]. 北京:高等教育出版社,2005.