一种不可信环境下的匿名位置辅助路由激励机制

钟 远[1],郝建国[2],戴一奇[1]
(1.清华大学计算机科学与技术系,北京 100084;2.军事科学院军事运筹分析研究所,北京 100091)

摘 要: 不可信环境下的路由性能问题,是移动自组织网(mobile ad-hoc networks,MANET)匿名路由协议面临的主要问题之一.本文为在不可信环境下通过对自私节点进行高效的协作激励,提高匿名路由协议的性能,提出了一种基于哈希链的匿名位置辅助路由激励机制.该机制利用哈希链在计算上的高效性和安全上的不可逆性,达成了对匿名数据转发节点的即时激励;通过基于支付代价的路由选择机制,优化了现有位置辅助路由机制的路由发现过程.匿名性分析证明,该机制能保证参与路由节点的匿名性.效率评价表明,在数据传输总量较大时,该机制对路由性能的影响很小,且该机制在较小规模的网络中有更好的性能.

关键词: 移动自组织网; 不可信环境; 位置辅助路由; 匿名节点激励; 微支付
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2013)03-0475-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.03.010

An Anonymous Incentive Mechanism for Location-Aided Routing in Untrusted MANET Scenarios

ZHONG Yuan[1], HAO Jian-guo[2], DAI Yi-qi[1]
(1. *Department of Computer Science and Technology, Tsinghua University, Beijing* 100084, *China*;
2. *Institute of Military Operations and Analysis, Academy of Military Science, Beijing* 100091, *China*)

Abstract: The routing performance issues in untrusted environments are the serious challenges for the privacy protection routing protocols in mobile ad-hoc networks (MANET). In order to encourage the selfish nodes and improve the routing performance in untrusted environments, this paper proposes an anonymous incentive mechanism based on hash-chain for the location-aided routing protocols. By using the efficiency and irreversibleness of hash-chain to the location-aided routing protocols, this mechanism can realize immediate incentive to the anonymous forwarders. Moreover, this mechanism can optimize the routing discover process through a route selection mechanism based on the payment price. The anonymity analyses indicate this mechanism can guarantee the anonymities of the nodes involved in routing. The performance evaluation shows that this mechanism has little effect on the routing performance when large amounts of data are transferred, and it is more efficient in small scale networks.

Key words: mobile ad-hoc networks (MANET); untrusted scenarios; location-aided routing; anonymous incentive; micro-payment

1 引言

不可信 MANET 环境[1~3]中的节点间信任关系复杂,在路由机制设计时,必须假设节点是自私的.由于自私节点出于自身利益最大化原则,趋向于拒绝为其他节点转发数据,所以不可信环境下的匿名路由机制面临严重的路由性能挑战.现有 MANET 匿名路由机制[4~6]通常假设网络节点是可信的,即节点间的协作关系是有保证的,因此在设计时很少考虑自私节点对路由机制性能的影响,且多数协议对节点参与路由协作的要求较高,难以保证不可信 MANET 环境下匿名路由机制的性能要求.

针对上述问题,本文着眼于不可信 MANET 环境下匿名路由机制的性能问题,在位置辅助路由机制之上设计了一种匿名路由激励机制,并对该机制的效率进行了实验验证和评价.本文提出的匿名位置辅助路由激励机制,采用基于哈希链的微支付机制,实现了对位置辅助路由机制中匿名数据转发节点的即时激励.该机制不仅能有效降低自私节点对路由性能的影响,提高匿名路由机制的性能;而且能优化位置辅助路由机制的路由发现,获得距离最短的最优路径.安全性分析和效率评价表明,该机制不仅能保证参与路由节点的匿名性,而且能以合理代价实现对匿名转发节点的支付激励.

2 研究背景

位置辅助路由协议是利用节点位置信息对基于拓扑路由协议的改进,这类协议中路由请求消息的发送

收稿日期:2011-12-09;修回日期:2012-05-03

不需全面泛洪,而是在目的节点位置的导向下进行有限泛洪,从而提高了路由效率.典型的位置辅助路由协议主要包括 LAR[7]等.本文的匿名位置辅助路由激励机制就建立在该路由机制上.本文假设在该路由机制上已部署了能有效保护节点匿名性的隐私保护机制.

本文的匿名位置辅助路由激励机制基于微支付.微支付(micro-payment)[8]是与宏支付(macro-payment)相对的小额电子支付机制.由于微支付中单次支付的金额通常低于宏支付单次支付的成本,因此微支付需要专门的支付机制来提供较高的效率和低成本的安全性.微支付机制的上述特点,使其多用来对卖方的多次重复小额支付,适合用来对参与 MANET 路由的节点进行转发激励.利用哈希函数的单向性及高效计算性,Rivest 和 Shamir 提出了基于哈希链的微支付方案 PayWord[9]. PayWord 在买方、卖方、可信第三方(Trusted Third Party,TTP)信任关系基础上,采用哈希链生成电子货币并进行支付,并将决定支付方案安全性的计算离线进行,减少了支付中的公钥运算次数.文献[10]将 PayWord 机制应用于 MANET,提出了一种基于哈希树的轻量级支付方案,使节点能实时支付为其提供网络访问服务的转发节点.该方案能适应节点移动引起的路由变化,但没有考虑对节点的匿名性保护,因此无法用于 MANET 匿名路由中的节点激励.

3 机制设计

3.1 符号和隐私攻击模型

本文机制描述中所用符号的含义如表 1 所示.

表 1 符号及其含义

符号	含义
$\{\text{pseud}_{i,k}\}_{k=1}^{w}$	节点 N_i 的 w 个假名
$K_{\text{pseud}_{i,k}}, K^{-1}_{\text{pseud}_{i,k}}$	N_i 的假名 $\text{pseud}_{i,k}$对应的公私钥对
$\text{Cert}(K_{\text{pseud}_{i,k}})$	$\text{pseud}_{i,k}$的公钥证书
$(\text{msg})_{K_{PS}}$	用 K_{PS}对消息 msg 加密后的密文
$H(\text{msg})$	用哈希函数 H()对 msg 进行哈希运算
$W_0 = H^N(W_N)$	对哈希根 W_N 进行 N 次运算得到哈希锚 W_0
$(\text{msg})\text{Sig}_{TTP}$	TTP 用其私钥对消息 msg 的签名

根据 Dolev-Yao 模型[11],本文采用了如下的隐私攻击模型:攻击者拥有合法的公私钥对,熟悉加密、解密、签名、哈希等密码算法,具有密码分析的能力;攻击者知道参与机制运行的各节点的假名公钥,但无法获得节点身份与其假名公钥的对应关系;由于节点频繁变换其假名,攻击者不具备追踪攻击的能力.

3.2 机制概述

匿名位置辅助路由激励机制建立在位置辅助路由机制之上,利用源节点生成的、经 TTP 签证的哈希链,通过在位置辅助路由消息中附加相应的字段,完成了对转发节点的即时支付.按照路由进程,该机制分以下 3 个子机制:(1)支付链建立机制:即在路由发现前,由 TTP 对源节点生成的一系列哈希链进行签证;然后在路由发现过程中,完成源节点对路由路径上转发节点的支付链建立.(2)动态转发激励机制:源节点在数据转发过程中,对转发节点进行数据转发激励,并针对 MANET 路由动态变化,进行支付链修复.(3)离线支付兑现机制:路由完成后,对转发节点进行支付兑现和账户结算.

通过上述三个子机制,匿名位置辅助路由激励机制能在不改变基本路由机制的情况下,高效地完成对自私节点的即时激励.3.3 ~ 3.5 节分别介绍了支付链建立机制、动态转发激励机制和离线支付兑现机制.

3.3 支付链建立机制

以下介绍了源节点 N_i 建立支付链的过程.

步骤 1 哈希链生成

N_i 用 m 个随机数(哈希根) Wi_n($i \in \{1,2,\ldots,m\}$),生成 m 条哈希链 Wi_j($i \in \{1,2,\ldots,m\}$,$j \in \{0,1,2,\ldots,n\}$),其中哈希根 Wi_n($i \in \{1,2,\ldots,m\}$)必须对其他网络实体保密.

为防止自私节点通过虚假支付欺骗转发节点,也为防止转发节点兑现其伪造或窃取的虚假支付,在发起路由前,需由 TTP 完成对源节点生成哈希链的签证.

步骤 2 签证请求

N_i 生成如下签证请求消息并发送给 TTP:

$$\{[N_i, (W1_0, W2_0, \ldots Wm_0), L, \text{Val}, \text{Amt}]\text{Sig}_{\text{pseud}_{i,k}}, \text{Cert}(K_{\text{pseud}_{i,k}})\}_{K_{TTP}} \quad (1)$$

式(1)所示的消息中,$(W1_0, W2_0, \ldots Wm_0)$为 m 条哈希链的哈希锚,$\text{pseud}_{i,k}$是 N_i 选择的假名,L、Val、Amt 分别为哈希链长度、每个哈希值代表的支付额、节点为使 TTP 签证上述信息而须向 TTP 支付的总额.

步骤 3 签证生成

TTP 收到式(1)所示的消息后,先通过解密和签名验证获得其中信息后,为每条哈希链生成一个签证.如对哈希链 $W4_j$($j \in \{0,1,2,\ldots,n\}$),TTP 的签证 Visa_4 是:

$$(W4_0, R_4, L, \text{Val}, \text{pseud}_{i,k}, \text{Expiry})\text{Sig}_{TTP}. \quad (2)$$

式(2)中,$W4_0$ 是哈希链 $W4_j$($j \in \{0,1,2,\ldots,n\}$)的哈希锚,随机数 R_4 是 TTP 为该哈希链生成的签证值,Expiry 是 TTP 设置的哈希链失效时间进行签名.

步骤 4 签证应答

TTP 将如下签证应答消息发送给 N_i:

$$\{[\text{Visa}_1, \text{Visa}_2, \ldots \text{Visa}_m]_{K_{\text{pseud}_{i,k}}}, \text{Receipt}\}. \quad (3)$$

其中的收据 Receipt 用来在随后的支付兑现中,防止 TTP 抵赖,其内容为:

$$[\text{pseud}_{i,k}, (W1_0, W2_0, \ldots Wm_0), L, \text{Val}, \text{Expiry}]\text{Sig}_{TTP}. \quad (4)$$

为在数据转发中为转发节点提供所需支付,源节点需获得路径上所有转发节点的转发要价.

步骤 5　要价请求

N_i 将以下要价请求字段附加在路由请求消息中进行广播:

$$\{S, D, \mathrm{Cert}(K_S), \mathrm{Cert}(K_D)\}. \tag{5}$$

其中 S、D 分别为源节点 N_i 和目的节点标识.

步骤 6　要价应答

转发节点收到带有要价请求字段的路由请求消息后,根据其距下跳节点的距离,提出为源节点转发单位数据的要价,并在路由应答消息中,附加如下要价应答字段:

$$\{S, D, [(A, x)\mathrm{Sig}_A, \mathrm{Cert}(K_A)], [(B, y)\mathrm{Sig}_B, \mathrm{Cert}(K_B)], \ldots\}. \tag{6}$$

其中 x、y…分别为转发路径上的节点 A、B…的要价.

步骤 7　支付链建立

N_i 根据各转发节点要价,从多条路由中选择总要价 $x + y + \cdots$ 最小的路由,为其分配相应数量的哈希链签证,然后将发送给路径上所有转发节点的签证封装到如下签证发布字段,将该字段随最初数据包发送给各转发节点,从而建立支付链:

$$\{[A, (\mathrm{Visa}_1, \ldots, \mathrm{Visa}_x)_{K_A}], [B, (\mathrm{Visa}_{x+1}, \ldots, \mathrm{Visa}_{x+y})_{K_B}], \ldots\}. \tag{7}$$

上述支付链建立机制中,由于节点要价反映了其与下一跳节点间的距离,因此总要价较小的路由通常较短.通过上述基于支付代价的路由选择机制,可优化现有位置辅助路由机制的路由发现过程,从而可利用转发节点间的位置关系,获得距离最短的最优路径.

3.4　动态转发激励机制

在路由的数据发送阶段,源节点通过数据转发激励机制,对路径上节点的转发行为进行激励.此外,转发激励机制必须能高效处理 MANET 路由变化引起的支付链中断问题.为此,本文利用位置辅助路由的局部搜索路由维护机制,设计了支付链修复机制.上述两种机制共同构成了动态转发激励机制.下面以源节点 S 向目的节点 D 发送数据为例,介绍动态转发激励机制.

(1)数据转发激励机制

如图 1 所示,路由路径建立后,S 通过在每个分组中附加的支付链,对路径上节点的转发行为进行激励.图中转发节点 A、B、C…的要价分别为 x、y、z…,则源节点在第 k 个分组附加的支付链为 $\{W1_{kx}, W2_{ky}, W3_{kz}\cdots\}$,其中 $W1_{kx}$、$W2_{ky}$、$W3_{kz}$…分别用于对 A、B、C…进行支付.A、B、C…收到分组后,对支付链中对应的支付值分别进行 x、y、z…次哈希运算,将得到的哈希值与前一次支付验证得到的哈希值进行比较.若二者相等,则支付验证通过,转发节点转发带有该支付链的分组.

(2)路径变化时的支付链修复机制

如图 2 所示,若 S 发送 k 个分组后,由于节点 C 的移动,路径发生中断,节点 B 发起局部搜索来维护路由.在局部搜索过程中,B 在路由请求消息中附加要价请求字段.在通过路由响应消息获得路径上新节点 E 的要价应答后,B 将该要价应答随路由维护成功消息发送到 S.S 在新路由的最初数据包中,根据要价向 E 发布相应签证,完成对支付链的修复.同时,S 继续路由维护前的支付状态,用旧哈希链对 A、B…进行支付;用新哈希链对 E 进行支付.利用上述机制,当路径发生变化时,只需对新路径上的少量新节点发送新签证,从而可高效完成支付链修复.

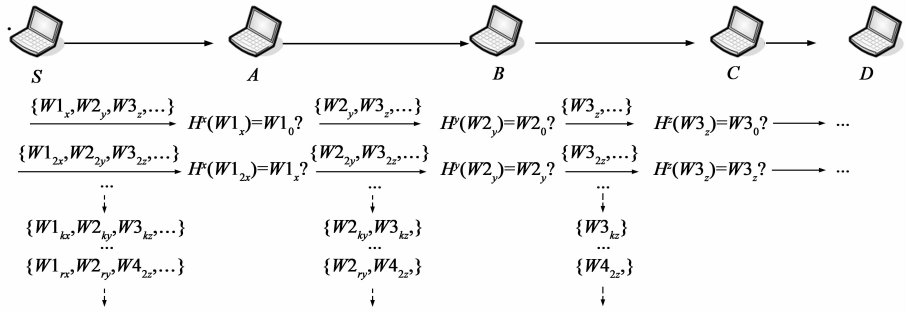


图1　数据转发激励机制

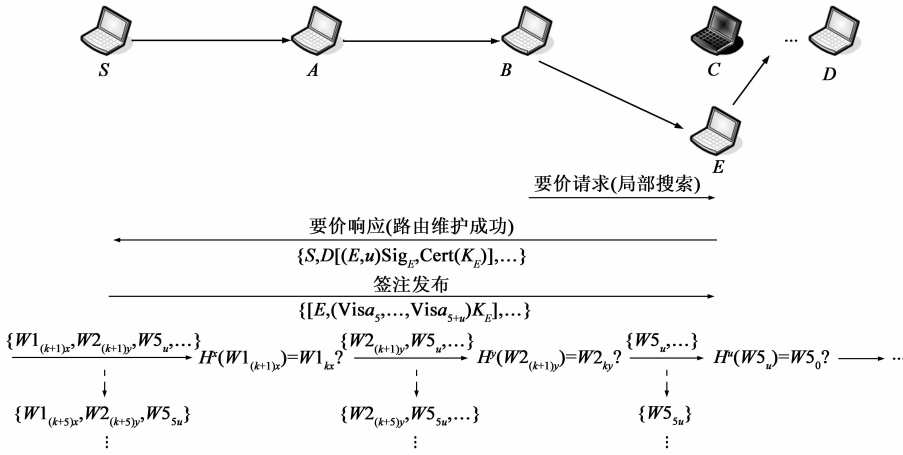


图2　支付链修复机制

3.5 离线支付兑现机制

数据转发完成后,转发节点可在空闲时将获得的支付值进行离线兑现.以下描述了转发节点 C 的兑现过程.

步骤 1 兑现请求

节点 C 发送的兑现请求消息内容为:

$$\{\mathrm{Cert}(K_C), W3_n, W4_n, (\mathrm{Visa}_3, \mathrm{Visa}_4)_{K_{\mathrm{TTP}}}\}\mathrm{Sig}_C. \quad (8)$$

其中 $W3_n$, $W4_n$ 为 C 获得的两条哈希链的最大哈希值,$(\mathrm{Visa}_3, \mathrm{Visa}_4)_{K_{\mathrm{TTP}}}$为用 TTP 公钥加密的哈希链签证.

步骤 2 兑现应答

TTP 验证后,向 C 的虚拟账户转入相应的支付值 Amt,并向 C 发出如下内容的兑现应答消息:

$$\{C, W3_n, W4_n, \mathrm{Amt}\}\mathrm{Sig}_{\mathrm{TTP}}. \quad (9)$$

4 匿名性分析

定理 1 匿名位置辅助路由激励机制能保证参与路由节点的匿名性.

证明 匿名位置辅助路由激励机制采用了基于公钥的假名机制.每个节点都有一系列与其身份对应的假名及其假名公钥证书,上述对应关系仅被公钥基础设施所知.节点在激励机制中用假名公钥证书发布其假名及假名公钥,并用假名公/私钥对各消息或字段进行加密或签名:在支付链建立机制中,式(1)中源节点身份标识及其假名公钥证书都用 TTP 公钥加密,故攻击者既无法知道源节点的身份,也无法获得其假名公钥证书;式(3)不包括节点的身份,攻击者仅能得到式(4)中的假名 $\mathrm{pseud}_{i,k}$;源节点在式(5)中发布源节点和目的节点假名公钥证书,转发节点在式(6)中发布其假名公钥证书,从而使参与路由节点在不同路由中使用不同假名.在离线支付兑现机制中,节点使用假名向 TTP 发出兑现请求并获得 TTP 的兑现应答.

根据本文隐私攻击模型,攻击者获得节点身份与其假名的对应关系在计算上是不可行的.因此,基于公钥的假名机制能保证参与路由节点对窃听攻击者的匿名性.

5 效率分析与评价

本文机制通过在路由消息中增加相应字段,能在不改变路由机制的情况下,激励自私节点参与路由协作,因此直观上具有较高效率.本节通过实验分析了本文机制在不同数据传输总量下的机制开销,评价了该机制的效率.

5.1 激励机制开销分析

实验采用激励消息比例(R_{im})和平均分组延迟(D_{ap})度量激励机制开销.激励消息比例

$$R_{\mathrm{im}} = \frac{L_{\mathrm{im}}}{L_{\mathrm{im}} + L_{\mathrm{dp}}} \times 100\% \quad (10)$$

反映了激励机制给路由机制带来的总开销,其中 L_{im}是发送 L_{dp}长度数据所需激励消息总长度,包括以下三部分的长度:签证请求、应答消息;要价请求、应答字段和签证发布字段;源节点附加在数据分组中的支付链字段.

平均分组延迟

$$D_{\mathrm{ap}} = \frac{D_{\mathrm{he}} + D_{\mathrm{cs}}}{N_{\mathrm{dp}}} + D_{\mathrm{pc}} + T_{\mathrm{vv}} \quad (11)$$

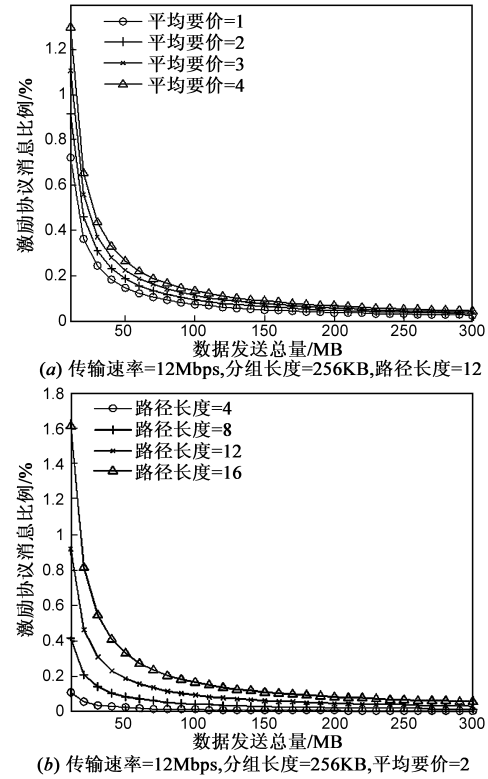
反映了激励机制对数据传输速度的影响,其中 D_{he}为哈希链签证延迟,D_{cs}为支付链建立延迟,D_{pc}为数据转发中支付链的传输延迟,T_{vv}为转发节点验证哈希值时间,N_{dp}为数据分组的数量.

实验参数如表 2 所示.

表 2 实验参数

参数	设置
哈希算法	SHA-256
加密/签名算法	1024bit RSA,采用 PKCS 填充模式
激励方式	基于每分组支付的即时激励
平均要价	1 ~ 4
路径长度	4 ~ 16 跳
分组长度	128K ~ 1024K
传输速率	6 ~ 27Mbps

5.2 实验结果及分析



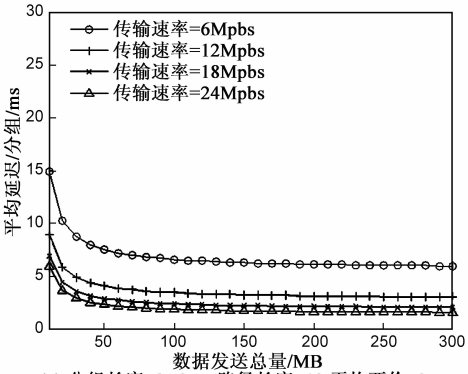
(*a*) 传输速率=12Mbps,分组长度=256KB,路径长度=12

(*b*) 传输速率=12Mbps,分组长度=256KB,平均要价=2

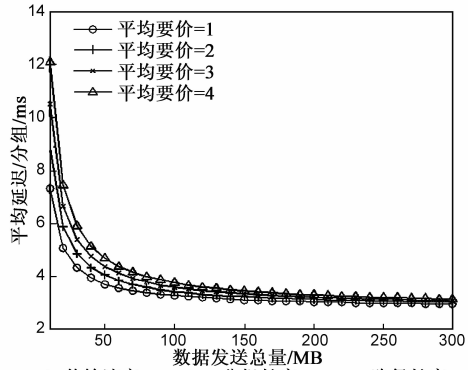
图3 激励消息比例随数据发送总量的变化

首先分析了不同数据发送量下的激励消息比例,实验结果如图 3 所示.从图 3 可见,随着数据发送总量的增加,激励消息比例快速下降:当数据发送总量为 300MB 时,无论分组长度、传输速率、平均要价、路径长度取值如何,激励消息比例都小于 0.1%.

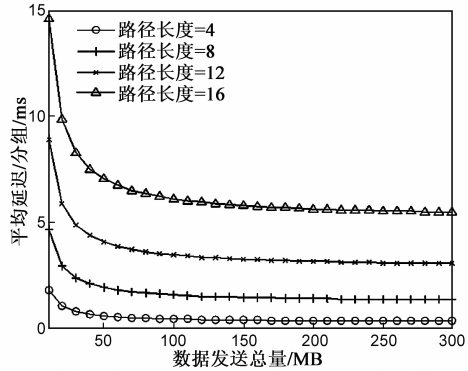
平均分组延迟随数据发送总量的变化如图 4 所示.从图中可见,数据发送总量越大,平均分组延迟越小.这是因为:本文激励机制带来的延迟主要在支付链建立机制,动态转发激励机制由于只需转发节点进行代价很小的哈希运算,因此引起的分组延迟相对前者很小.从图 4 还可看到,当传输速率、平均要价、路径长度等参数不变时,平均分组延迟在数据发送总量大于 100MB 后的变化很小.这说明当数据发送总量大于 100MB 后,支付链建立机制的开销对路由机制的影响很小.



(*a*) 分组长度=256KB,路径长度=12,平均要价=2



(*b*) 传输速率=12Mbps,分组长度=256KB,路径长度=12



(*c*) 传输速率=12Mbps,分组长度=256KB,平均要价=2

图4　平均分组延迟随数据发送总量的变化

综合图 3、图 4 的分析可知,随着数据传输总量的增大,不论是激励消息比例,还是平均分组延迟都迅速趋于较小的值.这说明,在数据传输总量较大(大于 100MB)的情况下,本文激励机制对路由性能的影响较小.此外,路径长度对本文激励机制的性能有较大影响,因此,本文机制在较小规模网络中有较好性能.

6　结论

本文提出的匿名位置辅助路由激励机制,采用基于哈希链的微支付机制,实现了对位置辅助路由机制中匿名数据转发节点的即时激励.该协议不仅能有效防止自私节点对路由性能的影响,提高不可信环境下匿名路由机制的性能;而且可优化现有位置辅助路由机制的路由发现过程,获得距离最短的最优路径.对该机制的开销分析和效率实验表明,它能以合理代价实现对匿名转发节点的支付激励,且数据传输总量越大,激励机制对路由性能的影响越小.

参考文献

[1] Defrawy K, Tsudik G. Alarm: Anonymous location-aided routing in suspicious MANET [A]. Proceedings of the IEEE International Conference on Network Protocols (ICNP07) [C]. Washington: IEEE Computer Society, 2007. 304-313.

[2] Defrawy K, Tsudik G. PRISM: Privacy-friendly routing in suspicious MANET (and VANET) [A]. Proceedings of the IEEE International Conference on Network Protocols (ICNP08) [C]. Washington: IEEE Computer Society, 2008. 258 – 267.

[3] Ardagna C, Jajodia S, Samarati P, Stavrou A. Privacy preservation over untrusted mobile networks [A]. Privacy in Location Based Applications [C]. Berlin: Springer-Verlag, 2009. 84 – 105.

[4] Kong J, Hong X, Gerla M. An identity-free and on-demand routing scheme against anonymity threats in mobile Ad Hoc networks [J]. IEEE Transactions on Mobile Computing, 2007, 6(8): 888 – 902.

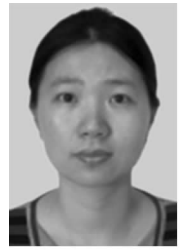
[5] Zhang Y, Liu W, Lou W. Anonymous communications in mobile ad hoc networks [A]. Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2005) [C]. New York: IEEE Press, 2005. 1940 – 1951.

[6] Wu X, Bhargava B. AO2P: Ad hoc on demand position based private routing protocol [J]. IEEE Transactions on Mobile Computing, 2005, 4(4): 335 – 348.

[7] Ko Y, Vaidya N. Location-aided routing (LAR) in mobile Ad hoc networks [A]. Proceedings of the 4th Annual International Conference on Mobile Computing and Networking (MOBI-

COM 1998)[C]. New York: ACM Press, 1998. 66 – 75.
[8] Micali S, Rivest R. Micropayments Revisited [A]. Proceedings of the Cryptography Track at RSA Conference 2002. LNCS 2271 [C]. Berlin: Springer-Verlag, 2002. 149 – 263.
[9] Rivest R, Shamir A. Payword and micromint: Two simple micropayment schemes [A]. Proceedings of the 4th Security Protocols International Workshop [C]. Berlin: Springer-Verlag, 1996. 69 – 87.
[10] Tewari H, O'Mahony D. Multiparty micropayments for ad hoc networks [A]. Proceedings of IEEE Wireless Communications and Networking Conference (WCNC 2003) [C]. New York: IEEE Press, 2003. 2033 – 2040.
[11] Dolev D, Yao A. On the security of public key protocols [J]. IEEE Transactions on Information Theory, 1983, 29(2). 198 – 208.
[12] 章洋,范植华,等. 移动自组网络中多径路由的匿名安全 [J]. 电子学报, 2005, 33(11): 2022 – 2030.
Y Zhang, Z H Fan, et al. Anonymous secure multipath routing in mobile ad hoc networks [J]. Acta Electronica Sinica, 2005, 33(11): 2022 – 2030. (in Chinese)

作者简介



钟 远 女,1973 年生于江西,清华大学计算机科学与技术系在读博士生,主要研究方向为无线网络安全和隐私保护.
E-mail: zhongy07@mails.tsinghua.edu.cn

郝建国 男,1976 年生于河北,博士,军事科学院军事运筹分析研究所在站博士后,主要研究方向为无线网络安全和隐私保护、移动电子支付、作战模拟.
E-mail: tigerzhh@gmail.com

戴一奇 男,1946 年生于浙江,清华大学计算机科学与技术系教授,博士生导师,主要研究方向为网络信息安全.
E-mail: dyq@mail.tsinghua.edu.cn.