LAMR:移动 Ad hoc 网络位置匿名的多路径路由协议*

张艳芬, 刘文菊, 王 赜, 刘 伟, 彭 松
(天津工业大学 计算机科学与软件学院, 天津 300387)

摘 要: 为有效减少移动 Ad hoc 网络路由协议开销并且实现网络路由的鲁棒性,引入位置匿名性和 LAR 局部定向洪泛机制。对 Ad hoc 网络中的 ARMR 协议(anonymous routing protocol with multiple routes)进行改进,提出一种新的基于匿名位置的多路径路由协议 LAMR(location-based anonymous route protocol), LAMR 与 ARMR 的不同之处有两点:a)融入匿名性的位置可减少路由分组在网络的全局洪泛;b)定向洪泛思想可避免路由回路产生。仿真实验结果表明,LAMR 能比 ARMR 有效地提高路径请求成功率和降低路由请求时延。

关键词: 路由协议; 位置; 匿名性; 多路径
中图分类号: TP393.17 **文献标志码:** A **文章编号:** 1001-3695(2012)10-3831-04
doi:10.3969/j.issn.1001-3695.2012.10.060

Location-based anonymous multiple routes protocol in Ad hoc mobile network

ZHANG Yan-fen, LIU Wen-ju, WANG Ze, LIU Wei, PENG Song
(*School of Computer Science & Software, Tianjin Polytechnic University, Tianjin* 300387, *China*)

Abstract: In order to reduce routing overhead and ensure routing robustness in mobile Ad hoc network, this paper introduced location anonymity and the idea of directional flooding in local zone originated from LAR. It proposed a location-based anonymous multiple routes protocol (LAMR) based on the improved version of anonymous routing protocol with multiple routes (ARMR). There were two mainly differences between the new LAMR protocol and the traditional ARMR protocol: a) locations of nodes could effectively reduce route packets flooding in the entire network; b) directional flooding could avoid the result of loop. The simulation results show that the LAMR protocol is more effective than the ARMR protocol in improving the successful rate of routing request delivery and reducing the delay of routing request.

Key words: routing protocol; location; anonymity; multiple routes

0 引言

移动 Ad hoc 网络(MANET)可以在不受固定或有限的基础设施限制的环境下运行,它的主要特点是自组织、快速装备、无基础设施。随着近些年研究深入,MANET 已经广泛应用于军事、科研、民用等领域。

目前的匿名路由协议有两类:基于身份的路由协议如 ARMR[1]、ANODR(anonymous on demand routing)[2]、SDAR(secure distributed anonymous routing)[3]、AnonDSR(anonymous dynamic source routing)[4]和基于纯粹位置的 PPBR(privacy-aware position-based routing)[5]、ALARM(anonymous location-aided routing)[6]、PRISM(privacy-friendly routing in suspiciousMANETs)[7],即节点的标志用假身份或者位置。基于身份的路由协议是在路由发现过程中,以目的节点的假身份作为路由请求分组的一部分,在路由发现过程中寻找的是节点;基于纯粹位置的匿名路由协议,在路由发现过程中,以目的位置作为路由请求的一部分,在路由发现过程中寻找的是位置,把路由请求信息传给此位置的节点或者此位置附近的节点。

基于身份匿名的路由协议一般在路由发现阶段采用广播路由请求信息,造成不相关的节点也去广播路由请求信息,而使路由开销过大;基于身份和位置的路由协议有 PPBR,PPBR 是在 GPSR(greedy perimeter stateless routing)[8]的基础上加入匿名性而进行的改进,但它是单路径的路由协议,当路径遭到破坏时,只能重新发送路径请求信息,易造成过多的路径请求时延;基于纯粹位置的有 ALARM 和 PRISM。ALARM 中目的节点的位置在路由请求信息中没有加密,容易被恶意节点攻击,并没有达到安全性要求;PBISM 中虽然对目的位置进行保护,但路由请求信息是广播的,造成不必要节点能量的消耗。

本文提出的新路由协议 LAMR 是一种新的、密度足够大、基于地理位置的、具有鲁棒性的身份位置路由协议,此路由协议是双向的。在 ARMR 的基础上,融入基于位置路由协议的

收稿日期: 2012-03-11; **修回日期:** 2012-04-25 **基金项目:** 国家自然科学基金资助项目(60970016);天津市自然科学基金资助项目(11JCYBJC00800)

作者简介: 张艳芬(1986-),女,河北石家庄人,硕士研究生,主要研究方向为网络安全(zyfzyf121121@163.com);刘文菊(1961-),女,教授,硕士,主要研究方向为企业信息化、自动化网络安全;王赜(1976-),男,副教授,博士,主要研究方向为计算机网络与安全、企业信息化、多媒体通信;刘伟(1987-),男,硕士研究生,主要研究方向为 MBR 模拟仿真;彭松(1986-),男,硕士研究生,主要研究方向为网络安全.

思想 LAR(location-aided routing)[9],在路由发现阶段采用多播路由请求信息,故此路由协议 LAMR 是基于身份和位置相结合的路由协议。与 ARMR 相比,LAMR 的优点有:a)有效减少了路由开销;b)采用基于位置路由机制,避免了路由回路并提高了路由效率;c)同时 LAMR 也是多路径协议,增强了路由协议的鲁棒性。

1 相关工作

1.1 攻击模型

Ad hoc 网络的攻击有外部攻击和内部攻击,外部攻击和内部攻击又分别分为主动攻击和被动攻击。一般认为外部攻击不如内部攻击,被动攻击不如主动攻击,故本文主要考虑内部主动攻击。

1)女巫攻击 敌手产生一个或多个伪节点。敌人通过产生路由请求信息,在控制信息中有多个节点的假名,让别的节点误以为这些假名的节点存在。

2)位置欺骗 敌手对自己的位置说谎,这个对基于位置的匿名路由协议危害很大。例如敌人对自己的位置说谎,导致路由中的很多流量流向此节点,造成网络瘫痪,不能进行正常的通信。

1.2 定向洪泛思想

在目前路由协议中,根据何时和怎样进行路由发现阶段,Ad hoc 网络分为三种:路由表驱动协议,每个节点的路由表里含有多个邻近节点的路由信息并周期性进行更新;按需路由协议,当节点有路由请求时才进行路由发现阶段;混合式路由协议,既有路由表驱动又有按需(反应式)路由,两者的结合。LAR 就是混合式路由协议,当节点初次收到某节点的请求信息时,路由表里没有与之相关的路由信息,它是反应式路由协议;当节点收到邻近节点的路由请求信息时,路由表含有与之相关的路由信息,会按照路由表的信息进行路由发现,这时会采用表驱动路由。

本文是在 LAR 局部转发策略的基础上,融入匿名性,形成本协议 LAMR。LAR 局部转发策略如图 1 所示,节点 I 是源节点 S 的一跳邻近节点,圆是以目的节点 D 为圆心,$R = v_{\max}(T_1 - T_2)$ 为半径,其中,$v_{\max}$ 为目的节点的最大移动速度,路由请求分组在 T_0 时刻从源节点向目的节点定向洪泛,在 T_1 时刻到达目地。与 LAR 不太相同的是:为了保护目的节点的位置匿名性,在路由请求分组中不包含目的节点的位置,只是包含目的节点的伪名;为了保护源节点的位置匿名性,由于源节点是请求域(矩形)四个顶点之一,源节点在获得目的节点位置信息后,会以本节点的一跳邻近节点作为本节点的模糊位置,如图 2 所示。路由请求分组中包含此模糊位置和其余三个顶点。

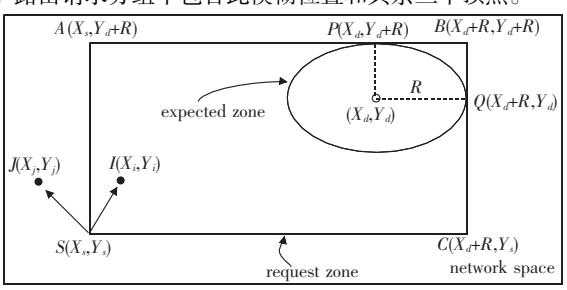

图 1 LAR 局部转发策略

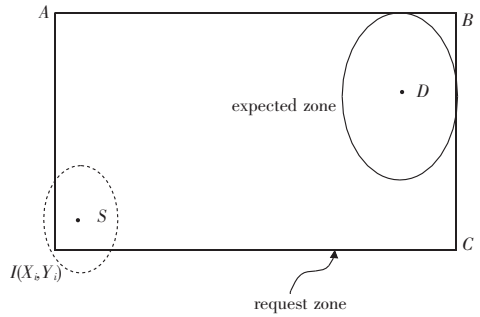

图 2 增加模糊机制的 LAR 局部转发策略

2 LAMR 协议过程

在路由协议 LAMR 中存在可信赖的第三方,有两个作用:

a)携带位置服务器,每个节点周期性地更新匿名和地理位置,并告诉第三方。每个节点可以通过安全的通道与位置服务器通信,获得目的节点的位置和匿名。

b)每个节点通过公钥基础设施获得公私钥对。

与其他路由协议一样,此路由协议分为路由发现和数据传输阶段,路由发现阶段分为路由请求和路由回复阶段。

2.1 路由请求阶段

2.1.1 源节点发送路由请求信息

源节点要与目的节点通信,通过可信赖的第三方获得目的节点所在的区域和匿名。在本阶段目的节点的公钥作为目的节点的匿名,在路由回复阶段作为目的节点的验证(会在路由回复阶段详细说明),通过 LAR 定向洪泛思想,定向多播路由请求信息,其分组形式如下:

$$\langle \mathrm{ARREQ}, \mathrm{AREA}_{cd}, H(N), y_s, y_d, E_{PK_d}(\mathrm{ID}_d, \mathrm{ID}_s, K_s), E_{K_s}(N) \rangle$$

其中:ARREQ 是匿名路由请求标志;AREA_{cd} 是请求区域,当源节点通过位置服务器获得目的节点的位置时,源节点通过计算本节点和目的节点的位置,求出请求域(此请求域是矩形,如图 2 所示);$H(N)$ 是此次路由请求标志,N 是源节点产生的随机数,如果在协议设定的时间范围内,源节点没有收到路由回复信息,则源节点重新产生新的随机数 N,$H(N)$ 作为新的路由请求标志,源节点再次发送路由请求信息;y_s 是源节点的伪身份;y_d 是中间第 d 个节点的伪身份;$E_{PK_d}(\mathrm{ID}_d, \mathrm{ID}_s, K_s)$ 是源节点与目的节点的真实身份用目的节点的公钥进行加密,K_s 为源节点的对称密钥;$E_{K_s}(N)$ 是随机数 N 用源节点的对称密钥加密。

2.1.2 中间节点收发路由请求信息

中间节点收到路由请求信息,会进行以下操作,如图 3 所示。

a)该节点根据路由请求信息中的位置信息判断该节点是否在请求域内。如果该中间节点处于请求域内,则执行 b),否则丢弃该包。

b)本节点根据路由表信息和路由请求信息中的 $H(N)$ 校验该路由请求包是否为重复包。如果该路由请求信息未被该节点接收过,则进行 c),否则丢弃该包。

c)本节点将路由请求包中的 y_i、y_d、$H(N)$ 等信息写入本节点的路由表中。本节点查找路由表中是否含有目的节点的路

由信息,如果有则发送路由回复信息包 ARREP,否则进行 d)。该机制与 AODV 的路由机制相似。

d)对比本节点的匿名信息 y_i 与路由请求分组中的目的节点匿名信息 y_d 是否一致,如果一致,则该节点就是目的节点,执行 e);否则用该节点的匿名信息 y_{i+1} 替换路由请求分组中的 y_i,再次定向洪泛该路由请求信息。

e)该节点使用本节点的公钥解密 $E_{PK_d}(\mathrm{ID}_d,\mathrm{ID}_s,K_s)$ 获得 K_s;再使用 K_s 解密 $E_{K_s}(N)$,获得随机数 N,对 $H(N)$ 进行验证。并回复 ARREP。通过该步骤可以避免收到重复的路由请求信息,减少路径开销,又能确保路径请求过程中抵御一定程度的恶意攻击。

f)其他节点如果接收到步骤 d)发出的路由请求信息,则重复执行步骤 a)~e)。

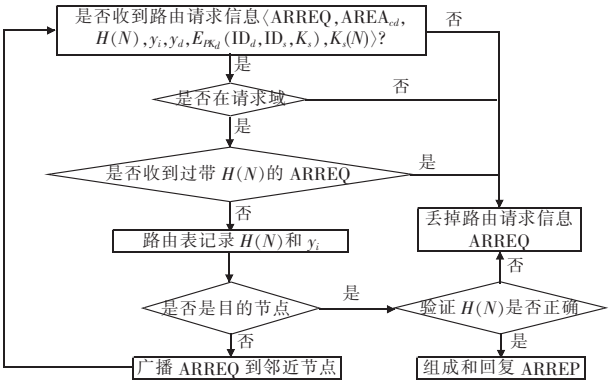

图 3　中间节点或者目的节点转发路由请求分组过程

中间节点 y_{i+1} 路由表中存在以下信息:

$$\langle(x_{i+1},y_{i+1}),H(N_0),y_i;H(N_1),y'_i;H(N_2),y''_i;H(N_3),y'''_i;\cdots\rangle$$

其中:(x_{i+1},y_{i+1}) 表示此中间节点的公钥和私钥,公钥 y_{i+1} 是此节点的匿名,代替真实身份 ID,从而避免真实身份的暴露;$H(N_0),H(N_1),H(N_2),H(N_3),\cdots$ 表示不同的路由请求分组标志,每个节点把上一跳节点的匿名 $y_i,y'_i,y''_i,y'''_i,\cdots$ 写在路由表中,在路由回复中,会把路由回复分组 ARREP 转发给上一跳节点。

2.2　路由回复阶段

当目的节点收到路由请求信息,目的节点会把本节点的匿名加到路由回复信息 ARREP 中,ARREP 格式为

$$\langle\mathrm{ARREP},H(N),y_d,E_{PK_s}(K_{\mathrm{ses}},\mathrm{ID}_s)\rangle$$

其中:ARREP 是路由回复信息标志;$H(N)$ 作为本次路由回复信息与路由请求信息相对应;y_d 是目的节点的公钥,作为目的节点的匿名,源节点在路由请求阶段前就已经知道目的节点的匿名,如果源节点收到的路由回复信息的匿名与本节点路由表中的目的节点的匿名相匹配,则证明此路由信息没有被恶意节点攻击;$E_{PK_s}(K_{\mathrm{ses}},\mathrm{ID}_s)$ 表示数据传输的会话密钥和源节点的真实身份用源节点的公钥进行加密,此公钥只有源节点的私钥能解密,其余节点不能解密获得会话密钥和源节点的真实身份。

中间节点收到回复信息后,作出如下的操作,如图 4 所示。

a)中间节点收到路由回复信息时,首先用本节点路由表中的 $H(N)$ 匹配 ARREP 中的 $H(N)$,如果匹配成功,则进行 b),否则丢弃该回复包。

b)更新路由表中的 $H(N)$,并用本节点的私钥去解密 $K_{PK_s}(K_{\mathrm{ses}},\mathrm{ID}_s)$,如果解密成功,执行 c),否则,执行 d)。

c)本节点成功解密并获得 K_{ses} 和 ID_s,此节点就是潜在的源节点,源节点通过比较本节点先前存在的匿名和 ARREP 中目的节点的匿名是否匹配,以此验证恶意节点是否攻击过该路由回复信息。如果不匹配,则该包受到恶意节点攻击而被窜改,丢弃该回复包;如果匹配,源节点用获得的 K_{ses} 加密将要传输的数据,进行数据传输阶段。

d)本节点根据路由表中存在的上一跳节点匿名将 ARREP 转发给上一跳节点。重复执行 a)b)。

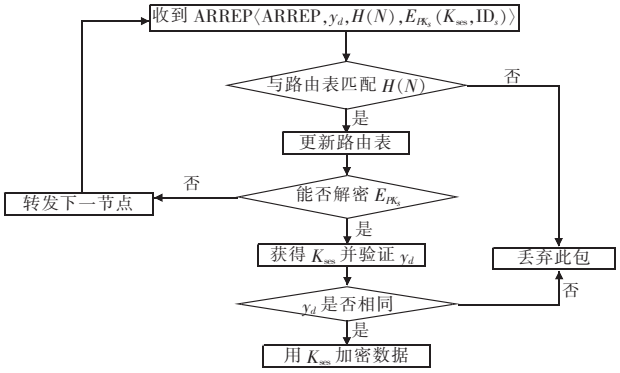

图 4　中间节点的回复过程

2.3　数据传输阶段

源节点用目的节点发来的会话密钥对数据进行加密,此密钥只有目的节点能解密,保证了数据传输的安全性。

数据传输可以用路径请求阶段建立的全部路径进行数据传输,也可以选择跳数比较少的路径进行传输,还可以选择路由回复分组先到达源节点的路径进行数据传输。

2.4　路由维护阶段

a)在路由协议 LAMR 中,每个节点周期性更新位置和匿名,并告诉可信赖的第三方。但位置的更新与节点的移动速度有关。LAMR 认为匿名和位置的更新时间远远高于路径请求的时间,这样保证在每次路径请求和路由回复时,每个节点的匿名即公钥不会发生变化;如果匿名和位置的更新时间低于路径请求的时间,会造成源节点频繁发出路径请求,加大端到端的路径请求时延。

b)路由错误机制,本文的 LAMR 在路由协议仿真中还用到路由错误机制,当链路发生断裂或者节点找不到下一跳节点或者目的节点时,此节点会向源节点发送路由错误分组,表明此路径行不通。源节点在计时器规定的时间内,如果也收到正确的路由回复分组,表明源节点可以在其他路径上进行数据传输;源节点在计时器规定时间内,全部收到错误路由分组,表明源节点在这个时间段内没有到达目的节点的路径,需要等待动态网路拓扑结构发生变化(在足够密度的网络中,源节点找不到到目的节点的路径的概率非常低)。

3　LAMR 路由协议分析

3.1　LAMR 安全性分析

本文 LAMR 与 ARMR 达到相同的安全性要求,通过节点周期性更新公钥,即伪名,能有效地抵御女巫攻击和位置欺骗。

由于 ARMR 采用全局洪泛,基于伪身份进行路由请求,在身份和路由匿名性上达到有效匿名性,但在位置匿名性上并没有显著地体现出匿名性。本文的 LAMR 也采用伪身份代替真实身份的机制,使其他恶意或者妥协的节点不能把路径上的活动节点的真实身份与位置联系在一起,所以恶意节点即使偷听路径上的信息,也不能确定某个节点的确切位置。

本文 LAMR 是基于位置的匿名路由,所以要强调节点在传输路径上的位置的匿名性。由于采用 LAR 的思想,所以路由请求分组中携带请求域的位置信息,即矩形的四个顶点坐标,其中一个坐标是源节点,为了保护源节点的位置信息,本文采用模糊位置信息,即把源节点的一跳节点的坐标信息代替源节点的位置信息携带在路由请求分组中,分组中其余三个坐标信息与目的节点位置有关,但恶意节点不能通过这三个节点定位目的节点的确切位置,由此提高了网路的安全性,也达到了各个节点位置的匿名性。

3.2 LAMR 路由性能分析

ARMR 在全网络中是洪泛的,容易产生回路(多播树),其采用布隆过滤器机制避免回路。LAR 本身就是免回路的路由,因为请求域中的节点都是定向向目的节点方向转发,因此不会产生回路。本协议 LAMR 含有 LAR 的思想,故也是免回路的路由协议,无须采用其他机制来避免路由的回路问题,使路由协议的复杂性降低,易于扩展。

为了验证协议的性能,采用 NS2[10] 仿真软件进行仿真实验,网络场景中的参数如表 1 所示。

表 1 LAMR 的仿真参数

仿真参数	数值
模拟区域大小	500 m × 500 m
节点速度	20/m/s
节点的运动方式	随机
MAC 层协议	IEEE 802.11b
数据流	CBR
封包大小	512/Byte
缓冲区大小	64 packets

通过实验对比 AODV、ARMR 和 LAMR 三种路由协议性能,两个指标是路径请求成功率和路径请求时延。路径请求成功率的定义是成功建立请求路径与全部请求路径的百分比;路径请求时延的定义是节点收到路径回复包与路径请求包之间的延迟时间。图 5、6 是在节点数为 10、20、30、40、50 的情况下,三种路由协议的路径请求成功率和路径请求时延。图 7、8 是在网络负载为 10、20、30、40、50 个节点的情况下,三种协议的路径请求成功率和路径请求时延。

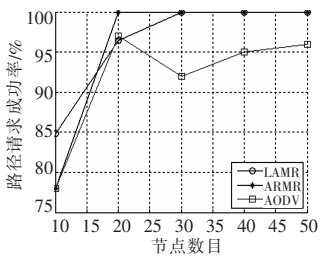

图 5 路径请求成功率

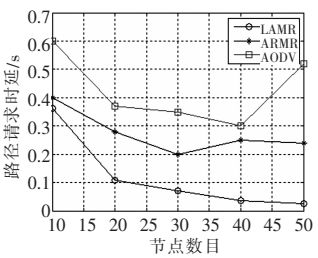

图 6 路径请求时延

LAMR 与 AODV、ARMR 相比,无论是随着节点数还是网络负载的增加,路径请求时延有很大的提高。LAMR 远低于 AODV 和 ARMR 的路径请求时延。LAMR 随着节点数或者网络负载而降低。

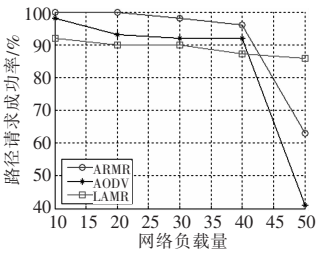

图 7 路径请求成功率

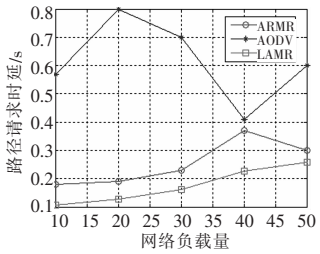

图 8 路径请求时延

随着节点数的增加,LAMR 与 ARMR 的路径请求成功率持平;随着网络负载量的增加,LAMR 的路径请求成功率略低于 ARMR,但当负载量是 50 时,LAMR 的路径请求成功率仍能维持在 85% 以上,表明 LAMR 在较大负载情况下,仍有较高的路径请求成功率。

4 结束语

本文详细阐述了基于位置的多路径匿名路由协议 LAMR,融入局部洪泛的思想和模糊位置机制,这样有利于减少路由协议开销,仿真实验也表明了 LAMR 路由协议的路径请求成功率优于 ARMR 路由协议。

参考文献:

[1] DONG Ying, CHIM T W, LI V O K, *et al*. ARMR: anonymous routing protocol with multiple routes for communications in mobile Ad hoc networks [J]. Ad hoc Networks, 2009, 7(8): 1536-1550.

[2] KONG K, HONG X. ANODR: an anonymous on demand routing with untraceable routes for mobile Ad hoc networks [C]//Proc of the 4th ACM International Symposum on Mobile Ad hoc Networking and Computing. 2003: 291-302.

[3] BOUKERCHE A, EL-KHATIB K, XU Li, *et al*. SDAR: a secure distrbuted anonymous routing protocol [C]//Proc of IEEE International Conference on Local Computer Networks. 2004: 618-624.

[4] SONG R, KORBA L, YEE G. AnonDSR: efficient anonymous dynamic source routing for mobile Ad hoc networks [C]//Proc of ACM Workshop on Security of Ad hoc and Sensor Networks. 2005: 33-42.

[5] ZHANG Chen-xi, LIN Xiao-dong. PPBR: Privacy-aware position-based routing in mobile Ad hoc networks [C]//Proc of Military Communications Conference. 2007: 1-7, 29-31.

[6] El DeFRAWY K, TSUDIK G. ALARM: anonymous location-aided routing in suspicious MANETs [C]//Proc of IEEE International Conference on Network Protocols. 2007: 304-313.

[7] El DeFRAWY K, TSUDIK G. PRISM: privacy-friendly routing in suspicious MANETs (and VANETs) [C]//Proc of IEEE International Conference on Network Protocols. 2008: 258-267.

[8] KARP B, KUNG H T. GPSR: greedy perimeter stateless routing for wireless networks [C]//Proc of the 6th Annual International Conference on Mobile Computing and Networking. 2000: 243-254.

[9] KO Y B, VAIDYA N H. Location-aided routing (LAR) mobile Ad hoc networks [C]//Proc of the 4th Annual International Conference on Mobile Computing and Networking. 1998: 66-75.

[10] http://www.isi.edu/nsnam/ns/[EB/OL].