第34卷 第14期 计 算 机 工 程 2008年7月
Vol.34 No.14 Computer Engineering July 2008
·安全技术· 文章编号：1000—3428(2008)14—0166—02 文献标识码：A 中图分类号：TP393.08

VANET中位置路由协议的安全和隐私保护

阮星华，徐敬东，于博洋
(南开大学网络与信息安全实验室，天津 300071)

摘 要：在车载Ad Hoc网络中，对地理位置路由的研究往往忽略安全和隐私保护问题，造成用户隐私受侵害，路由安全受威胁。该文通过笔名机制隐藏节点真实身份，保护节点位置隐私，采用群签名对消息进行认证，防止恶意节点破坏路由。分析表明，该方案在保护节点位置隐私的同时能有效抵御篡改、伪造和重放等多种攻击。

关键词：隐私保护；位置路由；群签名；笔名机制

Security and Privacy Protection for Geographic Routing Protocol in Vehicular Ad Hoc Networks

RUAN Xing-hua, XU Jing-dong, YU Bo-yang
(Laboratory of Computer Network and Information Security, Nankai University, Tianjin 300071)

【Abstract】 In Vehicular Ad Hoc Networks(VANET), position-based routing is more efficient. But most researches focus on the algorithm performance while the privacy and security issues are neglected. This paper proposes a scheme to protect the privacy and security. In the proposed scheme, position privacy is protected by using pseudonym and routing messages, which are authenticated with group signature algorithm. Security analysis shows that the scheme can effectively defeat the modification, forge and replay attacks while protecting the position privacy of nodes.

【Key words】 privacy protection; geographic routing; group signature; pseudonym mechanism

1 概述

近年来，随着Ad Hoc网络的发展和人们对智能交通的关注，出现了新型的Ad Hoc应用——车载Ad Hoc网络(Vehicular Ad Hoc Networks, VANET)。车载Ad Hoc网络的部署为车辆提供了相互通信的能力，在事故预警、保障交通安全以及为用户提供舒适的驾驶环境等方面起到了巨大的作用。在VANET中，节点数量多、计算能力强、运动速度快且具有一定的路径(公路)。许多研究表明，在这种网络环境中，基于地理位置的路由性能高于基于拓扑的路由[1-2]。因此，近几年针对VANET地理位置路由的研究逐渐成为热点，然而很多研究侧重于提高算法的性能，并未考虑隐私(节点位置)保护和路由安全问题。在地理位置路由协议中，地理位置信息是引导路由的主要依据，地理位置的暴露会导致用户被恶意节点跟踪，恶意节点还可以通过向网络中发布虚假的位置信息来扰乱路由，因此对用户隐私和路由安全构成严重的威胁，影响车载Ad Hoc网络的部署。

随着安全意识的增强，车载Ad Hoc网络的隐私保护和路由安全逐渐受到关注，一些解决方案相继被提出[3-4]。文 献[4]提出了一种使用环签名和匿名邻居表(ANT)来保护节点位置隐私的机制，有效地解决了隐私保护问题。但在该方案中，持有环签名私钥的恶意节点能够伪造和篡改位置信息从而扰乱路由；恶意节点还能收集信标数据包进行重放攻击。本文运用群签名[5]和笔名通信机制，提出了一种保护路由安全和位置隐私的地理位置路由方案。与文献[4]的方案相比，本文的方案能够在保护用户隐私的同时有效防止重放攻击，遏制恶意节点伪造和篡改位置信息的行为，从而保障路由 安全。

2 位置路由模型和攻击模型

大部分地理位置路由协议包括贪婪转发和恢复策略2个部分。以GPSR[2]为例，它是一种结合贪婪转发和周边转发的地理位置路由协议。为了转发数据包，节点需要知道自身位置、邻居位置和目的节点位置。本文假设节点自身位置可通过GPS获得，邻居位置可以通过Beacon信标机制[2]获得，目的节点位置可以通过位置信息服务获取。以图1为例，节点S有数据包需要发送，首先通过位置信息服务获得目的节点D的位置，再根据自身位置和所有单跳邻居的位置信息进行计算，选择一个距离目的节点D最近的邻居节点(图1中是节点$N5$)，把数据包转发给它。当出现局部最优[2]，也就是在需要转发数据包的节点本身距离目的节点最近的情况下，引入一种恢复机制(如周边转发)[2]来继续传递数据包。

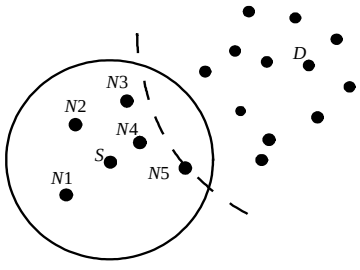

图1 贪婪转发

地理位置路由协议的通信模型概括如下：(1)邻居位置信

基金项目：天津市信息化项目基金资助项目(061084012)；微软亚洲研究院可信计算研究基金资助项目

作者简介：阮星华(1983－)，男，硕士研究生，主研方向：计算机网络与信息安全；徐敬东，教授、博士生导师；于博洋，硕士研究生

收稿日期：2007-08-20 **E-mail：**ruanxinghua@mail.nankai.edu.cn

息更新(NLU)，每个节点维护一张邻居位置信息表，并采用 Beacon 机制更新；(2)位置服务信息更新(LSU)，节点根据位置信息服务算法更新自身的位置到负责维护该节点位置信息的节点上；(3)目的位置请求(DLR)，需要发送数据的源节点根据位置信息服务算法发送请求，获取目的节点的位置；(4)数据包转发，根据贪婪转发或者周边转发把包传递给下一个节点，直到送达目的节点。

本文假设位置信息服务是安全的(安全位置信息服务的相关内容见文献[6])，重点讨论路由过程的隐私保护和安全保障。下面针对上文描述的通信模型，从被动攻击和主动攻击 2 个方面分析路由过程所面临的安全和隐私问题：

(1)被动攻击。本文假设敌手具有全网监听能力，能够轻易窃听全网中传递的数据包，获得 Beacon 信标中的位置信息，从而跟踪节点，使得节点隐私受侵犯。

(2)主动攻击。敌手能在 Beacon 机制中篡改和伪造 Beacon 信标，扰乱邻居位置信息表的更新，进而扰乱路由，并能收集合法的 Beacon 信标数据包，进行重放攻击，造成邻居位置表的更新错误，从而破坏路由。

3 带隐私保护的安全位置路由

对于敌手来说，由于节点身份和位置信息同时暴露的意义远大于单独的身份信息或者位置信息暴露，因此保护用户的位置隐私就是要保证敌手不能同时获得特定节点的身份和位置信息。另外，为了保障路由安全，相关数据(例如邻居节点发送的 Beacon 信标)必须是可验证和仲裁的。本文采用群签名算法和笔名机制，建立了可验证匿名邻居位置表(AANLT)，并基于 AANLT 提出了一种保障隐私和安全的匿名转发机制。群签名最早由 Chaumn 和 van Heyst 引入，在群签名算法中，任何群成员都可以使用自己的成员私钥代表整个群对消息进行签名而不暴露其身份，用户能够通过群公钥对产生的签名进行验证，但无法判断签名是哪一个群成员产生的，在必要的时候，群管理员能够使用群管理私钥打开签名，揭示签名者的身份。文献[5]提出了一种高效的适用于大规模网络的群签名方案。在该方案中，群管理员能够在不改变群公钥和原有成员私钥的情况下方便地添加新成员，并且群公钥和签名的长度都不受群规模的影响，因此，特别适用于车载 Ad Hoc 网络。

(1)AANLT 的建立维护机制

1)邻居节点发送结构为

$$<HELLO, PName, Loc, T_S, group\text{-}sig(PName, Loc, T_S)>$$

的 Beacon 信标，其中，*PName* 是邻居节点的笔名，它通过对邻居节点的身份 *ID* 和随机数 *RN* 进行哈希运算得到 $PName = H(RN, ID)$，节点定期更换使用的笔名；*Loc* 是邻居节点的位置信息；T_S 是信标发出时的时间戳；$group-sig(PName, Loc, T_S)$ 是邻居节点使用自己的群成员私钥实现的一个群签名。当节点收到邻居的 Beacon 信标后，使用群公钥对 Beacon 信标进行有效性验证，防止恶意节点篡改和伪造虚假的 Beacon 信标，同时对比时间戳 T_S 和当前时间，防止恶意节点进行重放攻击。

2)通过有效性验证后，节点根据其中的 *PName* 和 *Loc* 更新自己的邻居位置表，表项结构为：$<PName, Loc, T_r>$，其中，T_r 是该表项建立的时间，节点将根据收到的 Beacon 信标更新表项，删除过期的表项。

(2)基于 AANLT 的匿名转发过程

在匿名转发过程中，数据包的结构如图 2 所示，其中，*Loc-d* 是目的节点的位置；*PName* 是下一跳节点的笔名；*trapdoor* 是用目的节点的公钥 P_k 对源节点的身份 *SID* 和位置 *Loc-s* 加密得到的一段密文：$trapdoor = P_k(SID, Loc-s)$，只有目的节点能解开(假设节点即车辆在加入网络前必须向交通管理部门申请一对非对称密钥 (P_k, S_k))。

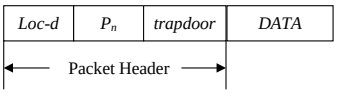

图 2 数据包格式

当节点收到数据包后：

步骤 1 对比 Packet Header 中的 *PName* 是不是自己使用的笔名(节点一般保存最近使用的 2~3 个笔名，以便处理使用这些笔名的数据包)，如果不是，丢弃这个包，否则转步骤 2。

步骤 2 节点检查自己是否属于 *Loc-d* 所在的目标区域(Destination Region, DR)，即节点的信号范围是否覆盖 *Loc-d* (如图 3 中 4 个灰色节点属于目标区域，而黑色节点不属于目标区域)，如果不是，节点查询自己的 AANLT，继续按照贪婪转发或者周边转发原则转发数据包，否则转步骤 3。

步骤 3 节点尝试解开 *trapdoor*，如果能正确解开，就接收这个包，传递过程结束，否则转步骤 4。

步骤 4 不能正确解开 *trapdoor*，说明该节点不是目的节点，于是继续寻找一个离 *Loc-d* 更近的节点进行转发，如能找到，则转发包到该邻居节点(如图 3 中节点 *B* 距离目的节点更近($d_2 < d_1$)，节点 *A* 把数据包转发给 *B*)，否则，转步骤 5。

步骤 5 如果该节点本身离 *Loc-d* 最近，则将 Packet Header 包头里的 *PName* 置为 0，然后单跳广播发送给它的邻居，邻居收到 *PName* 为 0 的包后，只是尝试着解密 *trapdoor*，不再继续传递，包传递过程结束。

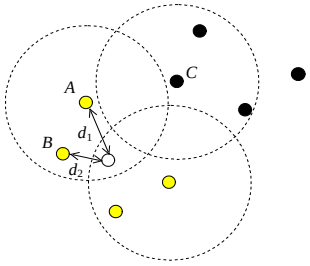

图 3 目标区域

4 安全性分析

本文的匿名转发方案在保护节点位置隐私的同时，能够有效防御伪造、篡改和重放等多种攻击，保障路由的安全。下面针对不同攻击方式分析方案的安全性：

(1)恶意节点窃听数据包，获取节点位置信息，侵犯用户隐私。在贪婪转发中使用了笔名机制，节点根据笔名建立邻居位置表并转发数据包，敌手窃听到的数据包(包括 Beacon 信标 $<HELLO, PName, Loc, T_S, group\text{-}sig(PName, Loc, T_S)>$ 和普通数据包 $<Loc\_d, PName, trapdoor, DATA>$)中只包含节点的笔名，隐藏了其真实身份，从而保证节点在更新邻居位置表和转发数据包的过程中不暴露真实身份，隐私得到了保护。

(2)恶意节点篡改和伪造 Beacon 信标，破坏路由：1)由于节点间发送的 Beacon 信标中带有群签名，收到信标的节点能

(下转第 170 页)