

车载自组织网匿名接入认证机制研究综述

高天寒, 李艳强

(东北大学软件学院, 辽宁 沈阳 110167)

摘要: 车载自组织网络具有良好的发展前景, 但同时面临严重的安全问题, 其中接入认证及隐私保护是确保 VANET 安全的基础。对现有 VANET 匿名接入认证方案进行了分类综述, 对比分析各方案的优点和缺点, 如匿名证书和数字签名, 最后, 指出该领域未来的研究重点和方向。

关键词: 车载自组网; 接入认证; 隐私保护; 匿名证书; 数字签名

中图分类号: T393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00089

Survey on anonymous authentication mechanisms of VANET

GAO Tian-han, LI Yan-qiang

(School of Software, Northeastern University, Shenyang 110167, China)

Abstract: VANET has an attractive prospect, it faces serious security issues but at the same time. Access authentication and privacy protection will play important roles to address the issues. A detailed survey on the literature anonymous authentication mechanisms of VANET in terms of their implementation approaches were presented such as anonymous credential and digital signature. The advantages and disadvantages of each mechanism were elaborated and the novel research directions were also given with the help of analysis.

Key words: VANET, access authentication, privacy protection, anonymous credential, digital signature

1 引言

车载自组织网络 (VANET, vehicular ad hoc network) 是一种利用无线局域网技术, 以车辆和路边单元作为网络节点, 为车与车 (V2V)、车与路边单元 (V2R) 之间提供通信服务而创建的移动网络。VANET 是无线 Mesh 网络的一种应用, 无线 Mesh 网络融合了无线局域网和自组织网络 (ad hoc) 的优势, 是一种大容量、高速

率、覆盖范围广的网络。同时无线 Mesh 网络的分层拓扑结构能够提供可靠传输, 具备可扩展性好、前期投资低等特性, 是无线宽带接入的理想解决方案。

在信息化飞速发展的时代, VANET 为实现城市智能交通系统提供了技术支持。在未来的车载网络中, 车辆节点可以从其他车辆节点或路边单元得到道路前方的交通情况, 以选择更为通畅的出行路线, 还可以向周围车辆或路边

收稿日期: 2016-05-13; 修回日期: 2016-06-25。通信作者: 高天寒, gaoth@mail.neu.edu.cn

基金项目: 国家自然科学基金资助项目 (No.61300196, No.61402095); 中央高校基本科研业务费专项基金资助项目 (No.N120404010, No.N130817002)

Foundation Items: The National Natural Science Foundation of China (No.61300196, No.61402095), China Fundamental Research Funds for the Central Universities (No. N120404010, No. N130817002)

单元发布交通事故的消息，以便其他车辆节点做好应对措施。特殊的车辆（如急救车辆）可以向周围车辆节点或者路边单元发送消息，甚至通过车载网发布消息改变红绿灯的状态以争取更多的时间。VANET 正成为工业界和学术界关注的焦点。

VANET 作为应用于车辆上的移动网络具有其独特的优势。

1) 车辆的承载空间可以确保其无线通信设备的良好性能，同时还具有强大的计算能力和存储能力。

2) VANET 的节点运动相对其他移动自组织网络更有规律。车辆同向行驶时，网络拓扑相对比较稳定；车辆反向行驶时，网络拓扑变化快、链路寿命短。结合节点的行驶方向、车速和道路信息可以预测链路状态。

但是 VANET 面临以下安全问题和挑战。

1) 身份认证：车辆节点在进入路边单元通信范围或其他节点的通信范围后，车辆节点和路边单元、车辆节点之间需要进行相互认证，以确保通信可靠性。

2) 隐私保护：车辆节点的真实身份对于车主来说非常重要，如果真实身份遭到泄露，恶意分子可以根据节点的身份进行跟踪、攻击，甚至危害到车主的生命。

3) 可追踪性：一旦某车辆节点产生责任纠纷或者恶意发送虚假消息，系统应能够揭露车辆节点的真实身份，防止节点利用匿名身份逃脱责任。

4) 无关联性：其他节点无法根据接收到的信息来分析出某个节点的行踪。

5) 恶意节点的识别和撤销：识别并撤销恶意节点是 VANET 中的关键问题，当一些节点发生故障、传感器被操纵、密钥被提取并用于伪造消息，以及有其他恶意行为的时候，系统要能够识别并撤销这些恶意节点，排除潜在的安全威胁。

同时，VANET 也面临诸如重放、窃听、篡改、假冒、拒绝服务等传统网络攻击。应对上述安全威胁和挑战将为 VANET 的快速发展和普及扫清障碍。

在主动攻击与被动攻击并存的情况下，接入

安全成为确保 VANET 安全的关键。同时，用户接入 VANET 的消息中通常包含大量敏感信息，上述信息一旦泄露会对用户隐私造成破坏，且相关信息的非法关联将为用户带来更为严重的损失。隐私保护逐渐成为保证 VANET 接入安全的重要环节，对 VANET 匿名接入认证技术的需求愈发迫切。

本文对现有 VANET 匿名接入认证方案进行分类综述，对比分析各方案的优势和缺点。最后，指出该领域未来的研究重点和方向。

2 相关知识

2.1 网络模型

如图 1 所示，VANET 一般由 3 部分组成：第三方信任机构 (TA, trust authority)、路边单元 (RSU, road side unit)、车载单元 (OBU, on board unit)。

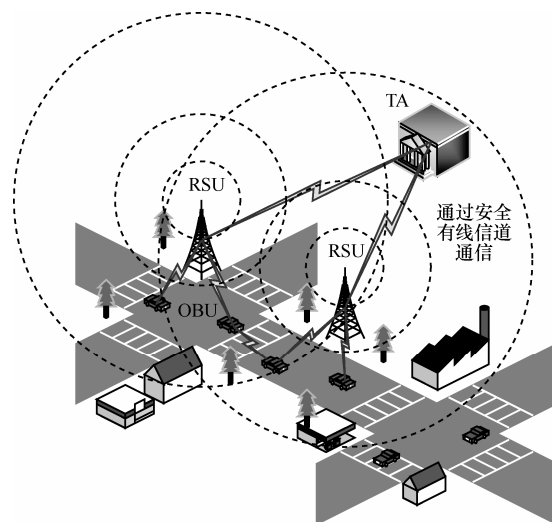


图 1 VANET 网络架构

1) TA 是公认的第三方信任机构，用于车辆和路边基础设施的注册，产生公共参数，分发密钥等。只有 TA 能够揭露节点的真实身份。

2) RSU 是建立在路边的基础设施，用于为车辆节点提供网络接入服务。

3) OBU 是装载在车辆上的通信单元，通常集成嵌入式系统、防篡改安全模块、全球导航定位系统等。

V2V 和 V2R 之间通信使用短距离无线通信 (SDRC) 协议，RSU 和 OBU 的通信范围为 300 m。TA 和 RSU 之间通过有线网络连接，通常具有很

高的安全性和足够的带宽。

2.2 密码学知识

1) 双线性对

双线性对是一个双线性映射: $e: G_1 \times G_2 \rightarrow G_T$, 其中, G_1 、 G_2 是 2 个素数阶 q 的加法循环群, G_T 是一个乘法循环群, 双线性对具有下面的性质。

① 双线性: 对任意的 $P \in G_1$, $Q \in G_2$ 和 $a, b \in \mathbb{Z}_q$, 有 $e(aP, bQ) = e(P, Q)^{ab}$ 。

② 非退化性: 一定存在某个 $P \in G_1$, $Q \in G_2$, 满足 $e(P, Q) \in G_T$ 。

③ 可计算性: 存在有效算法计算双线性对的值。

2) 基于身份的加密机制

基于身份的加密机制 (IBE) 由 4 个算法组成: 参数生成 (Setup)、密钥提取 (Extract)、加密 (Encrypt)、解密 (Decrypt)。

① Setup: 输入一个安全参数 k 并返回系统参数 $params$ 和主密钥。该系统参数包括一个有限明文空间 M 和一个有限密文空间 C 。系统参数将被公开, 而主密钥由私钥生成器 (PKG) 保留。

② Extract: 以主密钥、任意 $ID \in \{0,1\}^*$ 作为输入, 并返回一个用户 ID 所对应的私钥 d 。

③ Encrypt: 以 $params$ 、 ID 、 $m \in M$ 作为输入, 返回密文 $c \in C$ 。

④ Decrypt: 以密文 $c \in C$ 、私钥 d 及 $params$ 作为输入, 返回明文 $m \in M$ 。

3) 基于身份的签名机制

基于身份的签名机制 (IBS) 由 4 个算法组成: 参数生成、密钥生成、签名、验证。

① Setup: 输入 k bit 的安全参数, 输出主公/私钥对 (mpk, msk) 。

② Extract: 输入 msk 和身份 $ID \in \{0,1\}^*$, 生成身份为 ID 的用户私钥 usk , 并将 usk 安全地发送给该用户。

③ Sign: 输入 usk 和消息 m , 返回对消息 m 的签名 σ 。

④ Verify: 输入 mpk 、 ID 、 m 和 σ , 如果 σ 对 ID 和 m 是有效的, 则返回 1; 否则, 返回 0。

3 研究方案综述

首先, VANET 接入认证方案不单只提供认证

的功能, 还会涉及其他安全问题: 认证、信息加密、隐私保护、追踪性和无关联性及恶意节点的撤销。当然, 不同 VANET 的接入认证方案所达成的目标和解决方法也不尽相同, 相应方案的工作效率也会有所差异。例如, 有些方案解决了认证问题却忽略了无关联性。总之, VANET 接入认证方案和核心目标是要在保障安全和隐私的前提下, 尽量提高认证效率。本节根据方案构建底层技术的异同, 对 VANET 匿名接入认证进行分类综述。

3.1 基于匿名证书的认证方案

文献[1]中提出一种匿名认证协议, 用匿名证书来代替真实身份, 车辆节点间的认证需要检验匿名证书。方案中车辆节点在每个认证阶段使用不同的公私密钥对防止关联追踪, 车辆节点需要预装载大量匿名证书, 加大了存储开销。另外, 不断更换密钥对会造成密钥分配、密钥协商和密钥存储等方面的额外开销。

文献[2]提出一种高效的隐私保护协议 (ECPP), 解决了车辆节点需要预装载大量匿名证书的问题。OBU 向 RSU 请求发布一个临时匿名证书, 并通过两轮交互获得匿名证书, 过程如图 2 所示。如果车辆节点要保护位置隐私, 则需要频繁更换匿名证书, 从而造成 OBU 与 RSU 进行频繁的交互, 影响系统效率。此外, 本方案并不提供无关联性和追踪性保障。

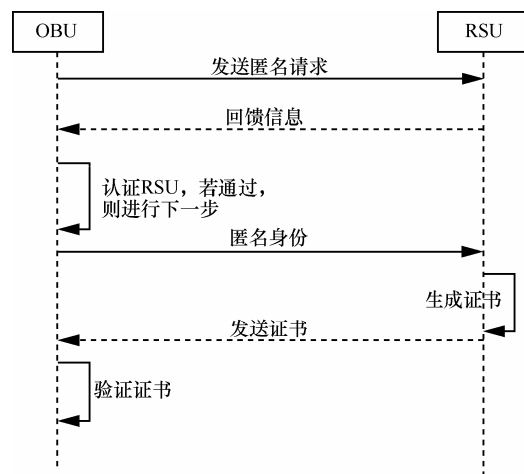


图2 ECPP 匿名证书生成过程

文献[3]针对文献[2]方案的缺陷提出一种采用临时匿名证书的匿名认证协议。RSU 给 OBU

发布多重匿名证书,减少 OBU 与 RSU 交叉认证开销。另外,采用基于身份的密钥产生机制消除了 RSU 对 OBU 在认证多重匿名证书时的有效性检验,但是 OBU 需要频繁与 RSU 交互,且认证算法过于复杂,影响方案效率。

3.2 基于群组的认证方案

面向群的签名方案大致有 2 种:群签名和环签名。群签名中,群需要预先确定且有群管理者,可以对给出的签名进行撤销;环签名不能直接提供匿名性的撤销功能。群签名方案在文献[4]中第一次提出,一个群体中的任意一个成员可以以匿名的方式代表整个群体对消息进行签名。文献[5,6]明确群签名方案可以提供匿名性,签名过程的真实签名者无法通过群信息来鉴别,而且同一个群里的 2 个不同签名具有不可关联性。由于群管理者拥有群成员的身份信息,因此,可以保证不可抵赖性,防止签名的伪造,具有可追溯性。

在 VANET 认证方案中,使用基于群签名的方案可以有效实现车辆节点的匿名性、不可抵赖性和可追溯性,防止用户隐私泄露,可以适应 VANET 中车辆节点的高移动性和短消息传输等特点。

群管理者(GM, group manager)是一个新的实体,具有设置参数、生成群公钥、追溯责任并撤销匿名的职能,相较于 TA, GM 能够由车辆节点担当,而不一定是一个完全可信的第三方。文献[7]使用车辆群组来减轻目标车辆的追踪。

在文献[8,9]中,群中成员使用自己的个人私钥签名信息,并附加群公钥信息,签名可以被群公钥验证,因此验证者可以获知发送者的成员身份,但无法知道具体的身份信息,因为所有的成员都具有同一个假名。群签方案的另一个优势是不需要频繁地改变群内生成的假名,因为 GM 可以对群内某个违法车辆的匿名性进行单独撤销,以实现动态的群组管理。当发现某个车辆节点的行为不端时,GM 能够生成一个新的群公钥并为每个群成员分配对应私钥。当 OBU 请求一个私钥证书时,GM 会首先检查请求者是否在撤销名单内,对于名单内的 OBU 会被排除在群外,不会为它分配更新的私钥。如果不端车辆出现过多,也会导致频繁更换假名的问题出现,进而增大系

统开销,导致效率很低。

在文献[10]方案中,当车辆节点使用一个原来的假名加入群组时,它需要等待一个随机的时间间隔来改变自己的假名,这样可以使新旧假名间实现不可关联。GM 可以通过签名追溯到个体签名者,保证不可抵赖性。一种能保证连续移动车辆之间通信认证的群签名方案在文献[5]中被提出,方案中加入了假名的使用,可以有效地保证匿名性,同时也确保通信的不可抵赖性、不可复制性、可追溯性。方案对群组的构成实现了层次的划分,按照 TA、STA、RTA 等由上至下逐步提高信任等级。

Lin 在文献[11]中提出 GSIS 方案,使用一个额外的基于身份的签名方案,消息由没有隐私需求的节点发送(如 RSU),以此来保证带宽。方案实现了对节点的高匿名性保证,而且不需要额外扩展、健壮的网络环境,可以节省大量网络开销,且经过网络仿真可知其通信时延相对较低。但在车辆数目急剧增长的情况下,会增加传输过程中的分组丢失率。

3.3 基于身份的认证方案

基于身份的密码学是公钥密码学的一种崭新形式。IBC 的最大优势在于简化了传统基于证书的公钥体制繁重的密钥管理过程^[12]。大多数 IBC 方案基于双线性对实现的,Zhao 等在文献[13]中详细给出了众多关于 IBC 方案的讨论结果。

基于 IBC 的 VANET 认证方案与基于公钥密码方案主要的不同就是节点以自己的身份作为公钥,且认证过程中不需要额外生成公钥和证书,在匿名证书的基础上进行改进,采用基于身份的机制设计认证方案。文献[14,15]提出了一种基于身份的自适应隐私保护认证框架,车辆节点的匿名身份由节点利用 TA 的公钥加密产生,每接入到一个 RSU 都可以申请更换匿名身份,保证了无关联性。OBU 与 RSU 之间的认证使用 IBS 签名方案,OBU 之间认证使用基于身份的在线和离线签名认证机制,提高了节点间相互认证的效率。但是方案中的恶意节点撤销依赖 TA 管理公钥列表,造成很大的管理开销。

文献[16,17]提出一种基于身份的认证方案,可以批量认证消息,提高认证效率。RSU 可以把

多个节点发送的消息合并成一个信息块, 然后利用双线性对一次性验证该消息块。方案存在的缺陷是, 如果合并信息块存在一条验证不通过的消息, 相应节点需不断重发消息, 造成 RSU 通信范围内的认证瘫痪。

基于身份的认证方案中私钥由 PKG 产生, 一般过程如下。

- 1) 产生主密钥和公开系统参数, 并公开系统参数。
- 2) 节点请求私钥, 向 PKG 提供节点的身份 ID。
- 3) PKG 根据节点的身份 ID 计算出私钥, 并发送给节点。

一旦 PKG 遭到攻击就会使整个网络不安全, 暴露出密钥托管的问题。

文献[18]提出一种解决密钥托管问题的方案。如图 3 所示, 把传统的由一个 PKG 生成私钥, 改为由独立的一组 PKG (DPKG) 来共同生成私钥。

1) 建立阶段

- ① 公告板生成系统参数。
- ② DPKG 产生一个主私钥 msk 。
- ③ 公告板生成一个主密钥。

2) 密钥提取阶段

- ① 节点向 DPKG 发送密钥请求。
- ② DPKG 发送 $N-msk$ 给节点。
- ③ 节点根据 $N-msk$ 和系统参数生成私钥。

但是这种方案也有不足之处, 在密钥提取阶段, 节点要想成功生成私钥就必须能够接收到所有的 msk , 可能存在单点失败风险。

以上基于身份的认证方案大都是基于双线性对实现的, 双线性对运算开销较大。文献[19]提出一种基于身份的高效自适应隐私保护认证方案, 此方案放弃利用双线性映射的数学难题, 而是以椭圆曲线上的 DL (discrete logarithm) 难题和 CDH (computational diffie hellman) 难题为基础构建认证过程, 有效地提高了运算效率, 降低了运算开销。

3.4 其他认证方案

除了以上几类认证方案, 还有一些其他形式的认证方案。文献[20]采用智能卡的方式存储 TA 发布的私钥以及证书, 每个 OBU 都有能唯一确认身份的 OBU ID 及证书。RSU 只需要验证 OBU 的证书及 OBU ID, 然后与验证通过的 OBU 进行群组通信, 此方案能有效保证条件隐私和认证效率, 但群组通信容易产生通信瓶颈, 一旦 RSU 遭到攻击, 则可能威胁整个网络的安全。

文献[21]方案利用 BF-IBE 机制进行信息加密并利用 BLS 机制进行签名。车辆节点注册时由 TA 给 OBU 发布票证, OBU 凭此票证与 RSU 完成接入认证, 请求匿名令牌, 此方案提高了认证效率, 解决了 OBU 与 RSU 频繁交互的问题, 匿名身份由节点自己产生, 降低 TA 和 RSU 的计算开销。但是匿名令牌由 RSU 为车辆节点颁发, 如果有多个 RSU 遭到攻击则容易暴露车辆节点的位置信息, 不能保证无关联性。另外, 此方案很难实现节点的撤销。

文献[22]方案利用变色龙散列函数, 产生一

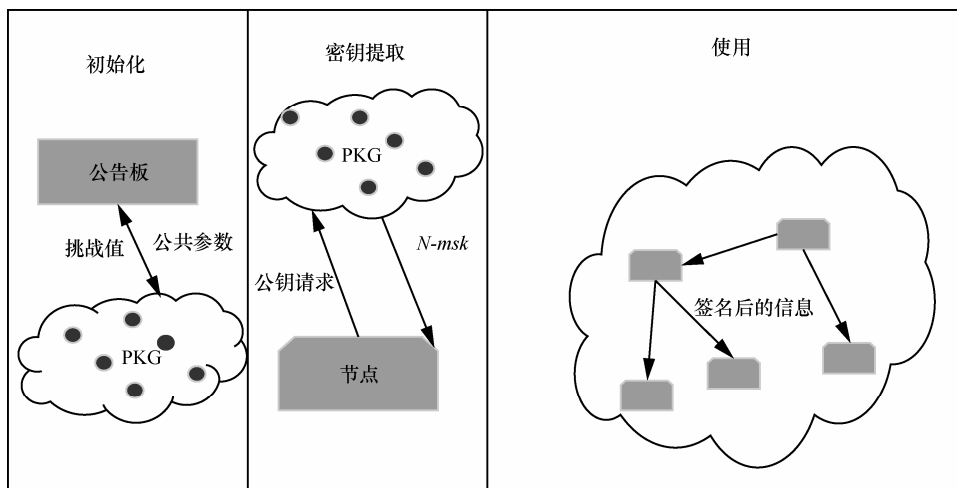


图3 密钥托管问题解决方案

表1 认证方案的对比分析

认证方案	认证	身份隐私	假名的产生	追踪性	无关联性	恶意节点的撤销
基于匿名证书	对节点的匿名证书进行有效性检验	利用匿名证书保护身份隐私	由TA或者RSU向节点颁发匿名证书	TA可根据节点的匿名证书,得到节点的真实身份	一般不提供无关联性保障,但一些方案利用RSU与TA的合作更换匿名证书确保无关联性	TA管理撤销列表,TA干涉RSU停止向恶意节点颁发证书
基于身份	对利用匿名公钥产生的数字签名进行有效性检验	利用节点产生的匿名身份达到身份隐私目的	利用TA为节点颁发的私钥以及TA的公钥产生匿名身份	TA用私钥解密匿名凭证,即可得到节点的真实身份	节点的匿名身份可以不断改变	TA存储映射,不需要合作
基于群组	对利用群公钥产生的签名进行有效性检验	利用群签的特性达到身份隐私保护目的	群公钥和个体私钥由GM产生,GM可以是车辆、RSU或者认证机构	GM配合TA揭示节点的真实身份	由于无法判断签名是哪个节点产生的,因此无法根据节点发送的消息关联某个节点	GM决定群内个体签名者的密钥,不需要合作实体
其他	验证散列值、唯一的标识列码等	由TA计算的匿名身份或者匿名公钥保护身份隐私	由TA根据安全散列函数计算的散列值,或者节点计算的匿名公钥	TA能够用散列值运算得到节点的身份;或者只有TA能解密唯一序列码	更换假名	具体方法根据方案不同而有所差异,如文献[19]没有提供节点撤销的功能

个唯一标识其身份的变色龙散列值,节点向周围广播参数,其他节点通过这些参数形成一个散列值以认证该节点。此方案安全特性好,每个节点可以产生多个变色龙散列值以充当匿名,具有很好的扩展性,但恶意节点的检测及撤销比较困难。

3.5 分析对比

表1从认证、身份隐私、假名产生、追踪性、无关联性、恶意节点的撤销等方面,对本文涉及的VANET匿名接入认证方案进行对比分析,从而能够更加直观地观察不同类型方案的主要差异。

4 结束语

在VANET接入认证领域内,安全性和效率是2个重要的目标,且用户的隐私保护问题已经成为接入认证的必要需求,其中包括身份隐私和位置隐私。本文对当前主流的VANET匿名接入认证方案进行了综合和对比分析,不同类型的方案有不同的使用场景。

在未来针对VANET匿名接入认证的研究中,高效的恶意节点撤销方案是重要研究方向;此外如何在保证隐私和安全性的基础上提高认证效率,如在认证时减少节点间的交互,以及从改善传统的网络架构入手来设计更高效的匿名认证机制等也将成为研究重点。

参考文献:

[1] RAYA M, HUBAUX J P. Securing vehicular ad hoc networks[J]. Journal of Computer Security, 2007, 15(1): 39-68.

[2] LU R, LIN X, ZHU H, et al. Ecpp: efficient conditional privacy preservation protocol for secure vehicular communications[C]//The 27th IEEE Conference on Computer Communications. c2007.

[3] JUNG C D, SUR C, PARK Y, et al. A robust and efficient anonymous authentication protocol in VANET[J]. Journal of Communications & Networks, 2009, 11(6): 607-614.

[4] CHAUM D, VAN HEIJST E. Group signatures[C]//Advances in Cryptology-Eurocrypt'91. c1991: 257-265.

[5] CHAURASIA B K, VERMA S, BHASKER S M. Message broadcast in VANET using group signature[C]//The 4th Wireless Communication and Sensor Networks. c2008: 131-136.

[6] CAMENISCH J, STADLER M. Efficient group signature schemes for large groups[C]//Advances in Cryptology-CRYPTO'97.c1997: 410-424.

[7] CHEN X, ZHANG F, KONIDALA D M, et al. A new ID-based group signature scheme from bilinear pairings[C]//The International Workshop on Information Security Applications. c2003: 585-592.

[8] BRESSON E, STERN J, SZYDLO M. Threshold ring signatures and applications to ad hoc groups[C]//Advances in Cryptology. c2002: 465-480.

[9] CHOW S S M, HUI L C K, YIU S M. Identity based threshold ring signature[C]//ICISC. c2004: 1-15.

[10] SAMPIGETHAYA K, LI M, HUANG L, et al. AMOEBA: robust location privacy scheme for VANET[J]. IEEE Journal on Selected Areas in Communications, 2007, 25(8): 1569-1589.

[11] LIN X, SUN X, HO P H, et al. GSIS: a secure and privacy-preserving protocol for vehicular communications[J]. IEEE Transactions on Vehicular Technology, 2007, 56(6): 3442-3456.

[12] 田野, 张玉军, 李忠诚. 使用对技术的基于身份密码学研究综述[J]. 计算机研究与发展, 2006, 43(10): 1810-1819.

TIAN Y, ZHANG Y J, LI Z C. Using the technology of identity based on cryptography research review[J]. Journal of Computer Research and Development, 2006, 43(10): 1810-1819.

[13] ZHAO S, AGGARWAL A, FROST R, et al. A survey of applications of identity-based cryptography in mobile ad hoc networks[J]. IEEE Communications. Surveys Tutorials, 2011, 14(2): 380-400.

[14] LU H, LI J, GUIZANI M. A novel ID-based authentication frame-

- work with adaptive privacy preservation for VANETs[C]// Computing, Communications and Applications Conference (ComComAp), 2012. IEEE, c2012: 345-350.
- [15] LI J, LU H, GUIZANI M. ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANET[J]. Parallel & Distributed Systems IEEE Transactions on, 2015, 26(4): 938-948.
- [16] SUN J, ZHANG C, ZHANG Y, et al. An identity-based security system for user privacy in vehicular ad hoc networks[J]. IEEE Transactions on Parallel & Distributed Systems, 2010, 21(9): 1227-1239.
- [17] BAYAT M, BARMSHOORY M. A secure authentication scheme for VANETs with batch verification [J]. Wireless Netw, 2015, 21: 1733-1743.
- [18] BALDINI G, MAHIEU V, FOVINO I N, et al. Identity-based security systems for vehicular ad hoc networks[C]//International Conference on Connected Vehicles and Expo. c2013: 672-678.
- [19] HE D, ZEADALLY S, XU B, et al. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks[J]. IEEE Transactions on Information Forensics & Security, 2015, 10(12): 1.
- [20] PARUCHURI V, DURRESI A. PAAVE: protocol for anonymous authentication in vehicular networks using smart cards[C]//IEEE Global Telecommunications Conference. IEEE, c2010: 1-5.
- [21] HUANG D, MISRA S, VERMA M, et al. PACP: an efficient pseudonymous authentication-based conditional privacy protocol for VANET[J]. IEEE Transactions on Intelligent Transportation Systems, 2011, 12(3): 736 -746.
- [22] CHEN C Y, HSU T C, WU T, et al. Anonymous authentication and key-agreement schemes in vehicular ad hoc networks[J]. Journal of Internet Technology, 2014, 15(6): 893-902.

作者简介:



高天寒 (1978-), 男, 辽宁沈阳人, 东北大学副教授、博士生导师, 主要研究方向为移动计算、网络安全。



李艳强 (1992-), 男, 河北邢台人, 东北大学硕士生, 主要研究方向为网络安全。