车联网中安全认证技术的分析与研究

王曼竹[1]，李梓琦[1,2]，陈翌飞[1]，洪高凤[1]，苏伟[1]
（1. 北京交通大学电子信息工程学院，北京 100044；2. 北京工业大学城市建设学部城市交通学院，北京 100124）

摘　要：目前，车联网安全认证技术并不能很好地抵御车联网环境下的各种攻击，且在平衡安全和性能方面也存在缺陷。在深入分析车联网研究现状和安全威胁的基础上，提出了基于层次化的车辆—车辆（V2V, vehicle-to-vehicle）安全认证方案，并进一步提出了基于多个可信第三方的 L 型安全认证方案。所提方案更适合用于车联网环境，旨在保障汽车通信过程的信息安全，防止通信数据被不法分子窃取和篡改等。

关键词：车联网；安全认证；V2V 安全认证方案；L 型安全认证方案
中图分类号：TN929.5
文献标识码：A
doi: 10.11959/j.issn.2096−3750.2021.00212

Research and implementation of safety authentication technology in Internet of vehicles

WANG Manzhu[1], LI Ziqi[1,2], CHEN Yifei[1], HONG Gaofeng[1], SU Wei[1]
1. School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China
2. College of Metropolitan Transportation, Beijing University of Technology, Beijing 100124, China

Abstract: Nowadays, safety certification technology for Internet of vehicles (IoV) cannot well defend the various attacks, and there are also many shortcomings when considering the balance between safety and performance. Based on the in-depth analysis of the research status and security threats for IoV, a hierarchical vehicle-to-vehicle (V2V) safety authentication scheme was proposed. Furthermore, an L-type safety authentication scheme which based on more than one trusted third parties was proposed. Aimed at ensuring the information safety of the communication process and preventing the communication data from being stolen, the schemes were more suitable to IoV.

Key words: IoV, security certification, V2V safety authentication scheme, L-type safety authentication scheme

1　引言

随着物联网技术的发展和人们对无人驾驶领域的不断探索，车联网（IoV, Internet of vehicles）已成为当前热点话题之一。车联网即 V2X（vehicle to everything）系统，是车辆—车辆（V2V, vehicle-to-vehicle）、车辆—基础设施（V2I, vehicle-to-infrastructure）、车辆—网络（V2N, vehicle-to-network）和车辆—行人（V2P, vehicle-to-pedestrian）通信的统称。车联网主要由车载单元（OBU, on board unit）和路侧单元（RSU, road side unit）两部分组成，两者都具有较强大的运算性能。OBU 是装载在车辆上的无线计算单元；RSU 是安装在城市道路两边的通信及计算机设备，其功能是与 OBU 共同完成实时的高速通信，并通过有线设备连接在骨干网络上。在许多交通场景中，V2V 和 V2I 这 2 种模型经常组合使用，主要采用专用短程通信（DSRC, dedicated short range communication）技术。DSRC 是一种可以实现双向无线传输的高效通信技术，通过 V2V 和 V2X 的连接，可以在小范围内实时、准确且可靠地传输图像、语音和数据[1]。

近年来，车联网在世界各国呈现快速发展态势。2018 年美国 5G 白皮书《面向 5G 的蜂窝式 V2X

收稿日期：2020−09−13；**修回日期：**2020−11−24
通信作者：苏伟，wsu@bjtu.edu.cn

通信》指出，随着电子技术、传感技术和计算机技术的飞速发展，车辆 V2X 通信正在逐步成为现实[2]。中国通信学会的《车联网安全技术与标准发展态势前沿报告（2019）》[3]对车联网安全技术在我国以及全球的发展态势做出了分析，报告认为车联网产业已上升至国家战略高度。为了顺应“互联网+智能交通”的发展，我国车联网技术也正在与“北斗 + 5G”等自主关键技术进行创新融合[4]。同时，针对车联网技术的快速发展，各国也相继出台了各类标准和政策，如 2006 年，美国发布了 IEEE 1609.2 标准，专注于 V2V 安全应用和单跳 V2I 通信；欧洲电信标准协会开发了 V2X 的欧洲规范；新加坡、日本等国家也在开发 V2X 智能交通系统规范[5]。

车联网在未来交通中有至关重要的作用，如何保障车联网的安全性非常关键。中国通信学会的《车联网安全技术与标准发展态势前沿报告（2019）》指出，我国车联网未来可能出现的集中式管理架构和分布式管理架构都需要保证极高的安全性。目前，当车辆通过 DSRC 或 5G 接收来自 RSU 或者基站的控制信息时，对信息的认证工作还不够完善。非法入侵者极有可能影响车辆的智能驾驶，产生安全问题。针对此问题，国内外学者从不同角度提出了安全认证方案。Vijayakumar 等[6-7]提出了双重认证和密钥管理技术，用于在车联网中安全传输数据；Boneh 等[8]利用椭圆曲线上的双线性建立了高效的基于身份标识号（ID, identity document）的加密方案；Lu 等[9]提出了一个基于身份的在线/离线签名认证框架；谭杰等[10]在离散对数的知识签名技术理论基础上提出了基于知识签名的快速身份认证协议；陈葳葳等[11]利用区块链技术的防篡改和分布式特性，基于公钥基础设施（PKI, public key infrastructure）体制提出了基于区块链的快速匿名身份认证方案。然而，上述安全认证方案存在各自的问题。如集中式的经典 PKI 证书管理方案虽能实现匿名认证，但车辆数量增加后会产生较长的处理时延；基于知识签名的快速身份认证协议能使载有 OBU 的车辆通过 RSU 快速加入车联网，但同一区域 OBU 数量激增会影响 RSU 对 OBU 的准确认证，甚至使系统瘫痪，在提高认证速率的同时没有考虑安全性；基于区块链的快速匿名身份认证方案能有效利用区块链技术的防篡改、分布式特性实现高效的安全认证，但其安全性过度依赖存入同一区块链的车辆身份信息，没有考虑未来不同品牌车辆可能会有不同的区块链，没有加入更多的可信第三方。上述问题使现有安全认证技术不能更好地适用于车联网环境。

本文对车联网环境中存在的安全威胁进行分析，着眼于信息安全与隐私保障策略，提出了基于层次化的 V2V 安全认证方案，并进一步提出了基于多可信第三方的 L 型安全认证方案。基于层次化的安全认证模型是一种更高效的认证体系，有可信第三方参与的双向安全认证可以更好地保障车辆通信安全；L 型安全认证方案则拥有多个可信第三方，进一步提升了安全性。

2　车联网安全威胁及认证方案设计原则

2.1　车联网安全威胁

近年来，车联网安全事件频发，且安全威胁逐步升级。攻击者采用不正当手段对网络架构进行攻击，恶意破坏系统的正常运行。车联网受到的攻击一般分为如下 3 个方面[12]。

1) 从攻击者的角度进行划分，可以将其分为内部攻击和外部攻击。内部攻击者攻击网络批准的节点，如注册车辆；外部攻击者通常没有合法身份，其通过伪装或窃听攻击网络。

2) 从攻击方式进行划分，可以将其分为主动攻击和被动攻击。主动攻击是指攻击者将恶意数据分组注入网络从而影响系统的正常通信和操作；被动攻击指攻击者一般不影响网络的正常通信，通过监听或窃取消息获取车辆用户信息。

3) 从攻击目的进行划分，可以将其分为理性攻击和恶意攻击。理性攻击是指攻击者攻击是为了自身便利，如散布错误道路信息误导其他车辆而方便自身驾驶；恶意攻击是指攻击者攻击是为了影响交通系统整体正常运转，产生了较大的安全风险。

攻击者对车联网进行上述攻击时，可能使用的方法共有 8 种：①消息伪造攻击，攻击者传播虚假消息影响车辆，如向汽车发送假的交通堵塞消息，迫使汽车转移路线；②消息重播攻击，攻击者重放以前由合法用户发送的有效消息；③消息修改攻击，攻击者改变由合法用户发送的消息；④模仿攻击，攻击者以其他车辆或 RSU 的名义发送消息；⑤RSU 抢占/复制攻击，攻击者攻击 RSU，并使用被攻击的 RSU 发起虚假信息（如广播虚假的路况信息）进行恶意攻击；⑥拒绝服务（DoS, denial of

service）攻击，攻击者通过注入无关的干扰或虚假消息，耗尽通信信道的容量或消耗车辆、RSU的计算资源，破坏系统通信；⑦移动跟踪攻击，由于 V2X 是基于无线的通信方式，因此攻击者可以轻松地窃听所传输的信息，一旦攻击者积累了足够数量的信息，就可以分析出车辆的行进轨迹或移动方式；⑧女巫攻击，攻击者在网络中以多重身份同时出现，破坏网络拓扑并消耗系统资源。

2.2 车联网安全认证方案设计原则

随着车联网安全威胁事件的频发，车联网安全保护备受重视。为在车联网中实现车与车之间的安全通信，在设计车联网安全认证方案时必须遵循 2 个原则：一是满足通信过程的安全需求，二是适应车联网的通信环境。

通信过程的安全需求主要包括如下 6 个方面。

1) 消息的认证性与完整性：在通信过程中，消息的接收者需要能够确定消息发送者是否为可靠实体，并且消息是否被其他人篡改过[13]。

2) 身份隐私保护：任何车辆、路边单元或攻击者都无法从消息中识别出消息发送者的真实身份[14]。

3) 可追溯：当攻击者尝试在网络上发布虚假数据或恶意消息时，执法人员可以从拦截的消息中跟踪得到消息发送者的身份，并采取相应的措施。

4) 不可链接：攻击者无法从任何 2 个或更多消息中得知它们是否由同一车辆发送，即这些消息具有不可相关性。

5) 不可否认：当执法部门追溯消息时，消息发送者无法对其已经发出的消息进行否认。

6) 抵御攻击：车联网中的身份验证和通信必须能够抵御网络中的各种攻击，确保安全性与可靠性。

车联网的通信环境主要包括如下 3 个方面。

1) 可承载大规模车辆用户的通信。

2) 可适应复杂的通信环境。

3) 尽可能实现轻量级。

3 基于层次化结构的 V2V 安全认证方案

3.1 层次化管理结构

为应对车联网通信环境中的安全威胁，在通信过程中，需要明确通信双方的合法身份，并对通信过程进行加密。由于车辆本身不具备进行大量数据计算及数据存储的能力，车辆的身份需要由本地授权（LA, local authority）进行认证。常见的证书管理方案是集中式方案，当车联网中用户数量增加时，具有非常明显的缺点。首先，随着用户数量的增加，LA 处将收到大量的验证请求，并需要存储大量车辆身份数据。LA 不仅需要对请求进行及时处理，还需要对身份证书进行撤销与更新。这将给其性能带来非常大的考验。可以想象，当车辆数量达到其性能瓶颈时，处理时延将大大延长，无法满足车联网系统对实时性的要求。另外，由于地理位置的限制，当车辆与 LA 的距离达到一定程度时，通信模型的物理层实现将造成很大的成本。

为了解决上述问题，本文提出一种具有层次化结构的 V2V 安全认证方案，即建立 3 层结构的管理模型，3 层结构模型示意图如图 1 所示。该模型引入认证中心（CA, certificate authority）对 LA 进行管理。

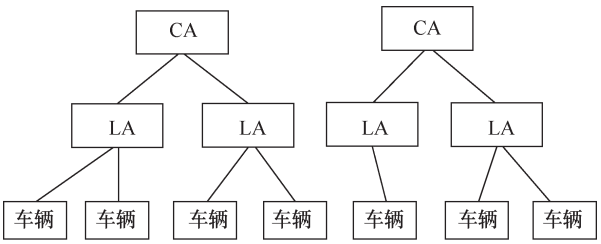


图 1 3 层结构模型示意图

对各部分结构进行详细介绍，具体如下。

1) 中心认证。CA 是 LA 的上一级，负责对 LA 的身份进行保存和管理。每个 CA 对其所负责的 LA 颁发具有时效性的身份证书，并对其进行定期更新。此外，CA 还对 LA 下属车辆划分进行管理，并保证 LA 正常工作。LA 需要向 CA 提供自身工作速率及接入的车辆数量，但不需要提供具体的车辆信息。CA 应具备对 LA 负责车辆数量控制的能力。CA 通过对 LA 处理请求的速率判断其工作状态，若 LA 的工作速率低于某一门限值，CA 将控制该 LA 随机断开 M 辆车的连接，若工作速率仍低于该门限值，则再断开 M 辆车的连接，直至工作速率高于门限值或剩余车辆数量小于 M。当判断剩余车辆数量小于 M 时，可判定该 LA 损坏。

2) 本地认证。对车辆的管理由本地认证中心 LA 直接实现，LA 的管理职责为对车辆请求进行处理和颁发车辆身份证书。认证中心 CA 为 LA 授权这些权利，并且为提升可靠性，LA 与 CA 主要通

过有线链路进行连接。该车辆身份证书也应满足 CA 的限制条件：如果用户不在为它颁布证书的 LA 所属的 CA 区域内使用该证书，此证书无效，是不合法的；如果用户所属的 LA 保持在同一 CA 域内，则身份证书不需要重新申请，可直接使用；如果超出该 CA 域，则需要向下一个 CA 域的某一 LA 重新申请身份证书；当 CA 令 LA 放弃部分车辆时，LA 的响应方式为撤销该部分车辆的身份证书，保障了车辆在高速行驶的过程中不需要频繁地申请新的身份证书。

3) 车辆用户。装载在车辆上的 OBU 是该模块的核心部分，用户之间进行通信和共享信息时，主要是通过自己拥有的 OBU 进行的。由于身份证书的有效时间有限，每隔一定的时间，用户需要向 LA 提起申请，请求其及时更新证书。在有效时长内，证书可在同一 CA 域内持续使用。若更换 CA 域或身份证书超出有效时长，车辆需要重新申请身份证书。若该车辆被对应 LA 放弃，所拥有的身份证书也就会失效，当再次有通信需求时，将重新申请身份证书。

对 CA、LA 及车辆编号的管理，可参考互联网协议（IP, Internet protocol）地址划分。CA 可类比为网络号，LA 类比为子网，而车辆可类比为主机号。在考虑高移动性对认证环节的影响时，可以参考通信网络模型对链路流量的规划和管理，通过对成本函数和目标函数建模确定最佳解决方案。即在保障认证速度的前提下，确定 CA 负责的 LA 个数及 LA 所管理的区域半径的最低成本方案，在此不详细展开。

3.2　V2V 通信的实现过程

车辆间通信的实现过程可分为 3 个部分：车辆注册证书、车辆通信、撤销车辆证书。处于车联网中的车辆为证明其合法身份，首先需要向可信第三方 LA 发送请求，请求其颁发身份证书。在两车通信之前，需要确定通信双方的合法身份。此外，为提升系统安全性，车辆的合法身份证书并不是永久的，而是有时效性的。若身份证书过期，LA 将对其身份证书进行撤销。

1) 车辆注册证书

车联网系统中的车辆为获得合法身份，需要向 LA 发送注册证书请求，并需要定期向 LA 申请更新证书。车辆向 LA 发出申请证书请求后，LA 就会发送给车辆一个 ID 及该 ID 的生存时间 T 作为在此系统内的身份信息，并获得一对公、私钥。LA 将上述合法车辆的身份信息及生存时间进行分组存储，并定期为合法车辆更新身份证书。

2) 车辆通信

车辆 V1 与车辆 V2 建立连接的流程如图 2 所示。

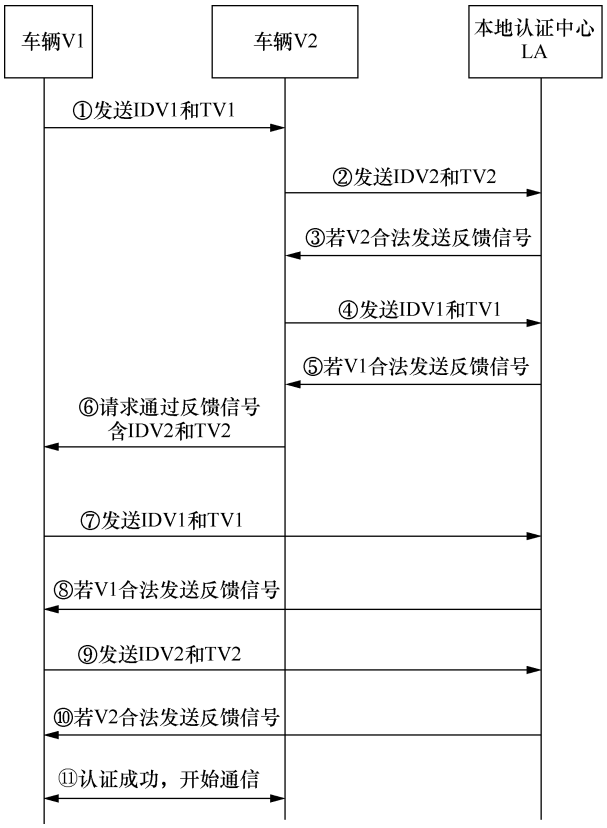


图 2　车辆建立连接流程

若车辆 V1 尝试与车辆 V2 进行通信。V1 首先将自身的 IDV1 及该标识号的生存时间 TV1 发给 V2，等待 V2 对其身份进行验证。

当 V2 接收到 V1 的连接请求、IDV1 及 TV1 后，将向 LA 发起验证请求。发送 V2 自身的 IDV2 及生存时间 TV2 给 LA。LA 在收到 V2 的请求后，首先需要对 V2 的身份进行验证。若 V2 身份合法，向 V2 发出请求通过反馈信号。当 V2 收到反馈后，与 LA 建立通信，将需要检验的 IDV1、TV1 发送给 LA。LA 对 V1 的身份进行验证，若合法，则向 V2 发送合法反馈信号。在 V1 与 V2、LA 传递消息的过程中，都需要对消息进行加密。

当 V2 检验 V1 身份合法后，向 V1 发送请求通过反馈信号，并将 V2 自身的 IDV2 及 TV2 发送给 V1。当 V1 收到 V2 的身份信息后，向 LA 发起验证请求，步骤同上。若经验证，V2 的身份合法，

则 V1 与 V2 建立通信连接，进行通信。

从上述过程可以看出，车辆可以向任意其他车辆发送通信请求，在发送请求时，不需要对车辆身份进行验证，在对方同意请求后对车辆身份信息进行验证。双方的身份在整个建立通信的流程中各进行了两次安全认证，对身份信息的验证过程是在 LA 处进行的，车辆处不需要存储大量数据。

V1 与 V2 通信的过程基于 RSA 算法。若 V1 向 V2 发送明文 X。首先 V1 用自己的私钥 SK1 对要发送的内容进行签名，获得 $D_{SK1}(X)$ [15]。再利用 V2 的公钥对 $D_{SK1}(X)$ 进行加密，获得密文 $E_{PK2}(D_{SK1}(X))$。将加密所获得的密文在无线信道中进行传输。V2 接收到密文后，首先通过 V2 的私钥 SK2 对其进行解密，获得 $D_{SK1}(X)$。随后再通过 V1 的公钥 PK1 对其进行核实签名过程。通过上述的认证过程，可以同时对保密通信和数字签名进行实现。由于 SK2 仅为 V2 拥有，即使窃取消息，也无法对其正确解密。由于 SK1 仅为 V1 所有，若非 V1 发送，V2 便无法获得正确明文。车辆通信过程如图 3 所示，图 3 为 V1 向 V2 发送明文 X 的流程。

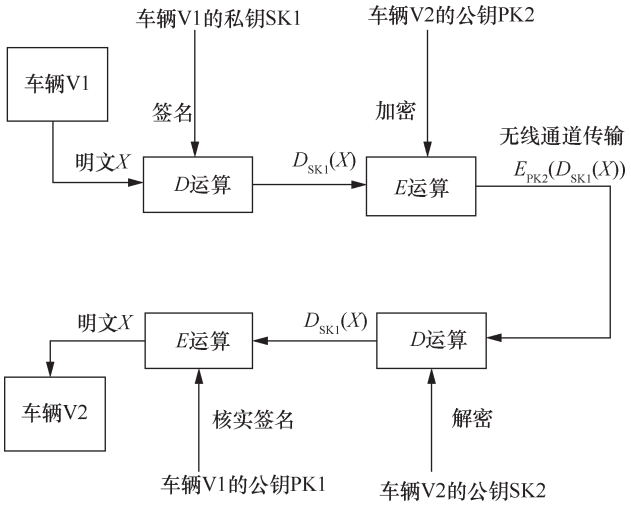


图 3　车辆通信过程

通过上述过程，能确保通信过程不被窃取、侦听，通信对方身份合法，并非伪造，为通信过程的安全性及可靠性提供了保障。

3) 撤除车辆证书

若发生以下两种情况，LA 对车辆身份证书进行撤销。

如果车辆的身份证书过期，那么 LA 就撤销它的身份，此时，该车辆不再是系统的合法用户。如果该车辆想要再次享有在该系统通信的权利时，需要重新向 LA 发送申请证书请求，要求颁发新的证书。

LA 一旦发现有用户使用虚假身份试图与其他用户通信并窃取信息等非法行为时，将立即撤销其身份证书，取消其合法身份。

4　基于多个可信第三方的 L 型安全认证方案

根据对未来车联网发展趋势的判断，一方面，当车联网被广泛应用时，车联网的基站建设可能会分配给各家汽车公司。由汽车公司在车辆生产的同时完成车辆注册入网，分配并定期更新公/私钥，因此，不同品牌的车辆将拥有不同的可信第三方。另一方面，随着汽车数量的不断增加，管理部门记录的数据量将变得更加庞大，更需采用高效的方式完成大规模的管理任务。因此，若要实现安全认证方案在 V2X 下的普遍适用，需提出一种新的可信第三方管理方案。

文献[16]提出了一种具有两个可信第三方的安全认证模型，该模型提出 L 型安全认证的思想，实现多个可信第三方参与的安全认证方式。本节将把该模型应用到车联网安全方案中，并进行分析。

L 型认证技术解决了目前无多个可信第三方参与身份有效性验证的问题，也减轻了分配公/私钥的复杂任务。车辆管理部门、通信管理部门只需要建立起基站之间的相互信任即可。当 L 型认证技术中每一个可信任第三方的布局密度与层次化结构中 LA 的最佳布局密度相同时，车辆在车联网环境中的高移动性对 L 型安全认证方案将不会造成额外的影响。同时，通过加强对基站安全性的维护，可以在缩减任务规模的情况下，更好地解决车联网的安全性问题。

4.1　车辆与可信第三方的要求

1) 车辆与可信方都必须有存储单元、收/发单元和处理单元。

2) 处理单元负责产生随机数、验证身份信息、数据检验等。随机数用于参与数据检验，经公/私钥加密、解密后的数据是否与该车辆发送的随机数一致。

3) 存储单元负责记录身份有效性验证消息、身份验证结果。

4) 收/发单元负责接收和发送通信与身份验证

过程中的所有信息。

4.2　L 型系统安全认证方案身份验证过程

L 型系统安全认证方案身份验证过程包含车辆 A、车辆 B、第一可信第三方 TTP_A、第二可信第三方 TTP_B，具体验证过程如下。

1) 车辆 A、车辆 B 发送各自的身份信息 I_A、I_B 及产生的随机数 R_A、R_B。TTP_A 收到车辆 A 发送的消息 2 后，根据车辆 A 的身份信息 I_A 验证车辆 A 的身份，获取车辆 A 的身份验证结果 Res_A。并向 TTP_B 发送消息 3，包括 I_B、R_A、TTP_A 产生的随机数 RTP_A。

2) 当 TTP_B 收到 TTP_A 发送的消息 3 后，根据车辆 B 的身份信息 I_B 验证车辆 B 的身份，获取车辆 B 的身份验证结果 Res_B。并向 TTP_A 发送消息 4，包含车辆 B 的身份验证结果 Res_B、TTP_B 对 R_A 和 Res_B 的第一签名、TTP_B 对 RTP_A 的第二签名。

3) 当 TTP_A 收到 TTP_B 发送的消息 4 后，验证 TTP_B 的第二签名（RTP_A）$_B$，当验证通过后，检查包含在消息 4 中的第二签名对象中的随机数 RTP_A 与在消息 3 中发送给 TTP_B 的 RTP_A 是否一致。向车辆 A 发送消息 5，包含 TTP_A 对 Res_A、Res_B、TTP_B 的第一签名以及对 Res_A、R_B 的第二签名。

4) 当车辆 A 收到来自 TTP_A 的消息 5 后，首先验证第一签名（R_A,Res_B）$_B$，验证通过后，检查从消息 5 中得到的随机数 R_A 是否与自身在消息 2 中发送给 TTP_A 的 R_A 一致。

5) 在 4)中，若检查包含在消息 5 中的 R_A 与其在消息 2 中发送给 TTP_A 的随机数 R_A 一致，车辆 A 将根据验证结果 Res_B 判断车辆 B 身份的有效性，并向车辆 B 发送包括对 TTP_A 的签名的消息 6。

6) 当车辆 B 收到消息 6 后，首先验证 TTP_A 的签名（R_A,ResB）$_A$，验证通过后，检查从消息 6 中得到的 R_B 是否与其在消息 1 中发送给车辆 A 的随机数 R_B，若一致，车辆 B 根据验证结果 Res_A 判断车辆 A 身份的有效性。L 型认证系统示意图如图 4 所示。

对验证过程进行详细分析。

身份验证过程 2)中，可信第三方 TTP_B 收到 TTP_A 发送的消息 3 后，根据 I_B 验证车辆 B 的身份，具体包括：如果 I_B 是车辆 B 的区分符，则 TTP_B 提取车辆 B 的公钥 P_B，此时 Res_B 包括 P_B；如果 I_B 是车辆 B 的证书 $Cert_B$，则 TTP_B 检查 $Cert_B$ 的有效性，此时 Res_B 中包括 $Cert_B$ 的有效性状态；如果车辆 B 的公钥或证书的有效性不能被 TTP_B 获得，此时 Res_B 中包括表示验证失败的内容。

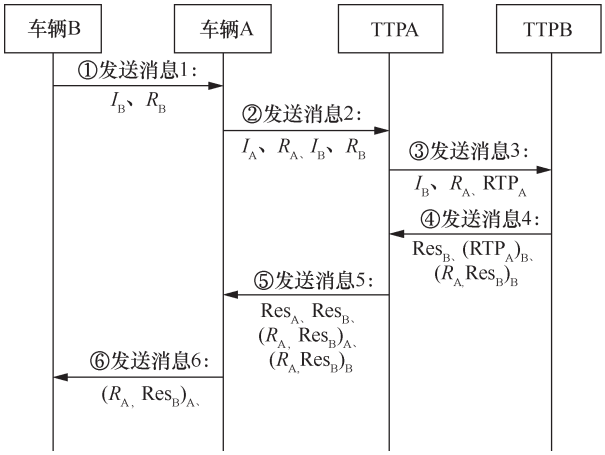


图 4　L 型认证系统示意图

身份验证过程 3)中，TTP_A 从消息 4 中得到 RTP_A 的具体方式是：如果 TTP_A 验证 TTP_B 的第二签名时能够从第二签名中恢复 RTP_A，则 TTP_A 在验证 TTP_B 的第二签名通过后从该签名中直接恢复 RTP_A；如果 TTP_A 验证 TTP_B 的第二签名时不能恢复 RTP_A，则消息 4 中还进一步包括 RTP_A 字段，TTP_A 从消息 4 中直接获取 RTP_A。

身份验证过程 4)和身份验证过程 5)中，车辆 A 从消息 5 中得到 R_A 的具体方式是：如果车辆 A 验证 TTP_B 的第一签名时能够从第一签名中恢复 R_A，则车辆 A 在验证 TTP_B 的第一签名通过后从该签名中直接恢复 R_A；如果车辆 A 验证 TTP_B 的第一签名时不能恢复 R_A，则消息 5 中还进一步包括 R_A 字段，车辆 A 从消息 5 中直接获取 R_A。

身份验证过程 6)中，车辆 B 从消息 6 中得到 R_B 的具体方式是：如果车辆 B 验证 TTP_A 的签名时能够从该签名中恢复 R_B，则车辆 B 在验证 TTP_A 的签名通过后从该签名中直接恢复 R_B；如果车辆 B 验证 TTP_A 的签名时不能恢复 R_B，则消息 6 中还进一步包括 R_B 字段，车辆 B 从消息 6 中直接获取 R_B。

上述认证过程由 TTP_A 进行车辆 A 的身份有效性验证，由 TTP_B 进行车辆 B 的身份有效性验证，实现了不同的可信第三方对其管理车辆进行身份有效性验证，为未来不同品牌的车辆拥有不同的可信第三方的情况提供了一种安全的认证方案。

5 方案性能分析

在车联网中，由于车辆往往在快速行驶，认证方案在保证安全性的同时，要尽可能实现更快的计算速度。因此，本节从安全性能、计算开销、通信开销 3 个方面对方案进行了评估。

5.1 安全性能

下面针对第 2 节提出的安全需求，分析两个方案的安全性能。

在层次化认证方案中，通过合法身份证书验证通信双方身份的合法性。在通信过程中，需要通过解密算法，用车辆 V2 正确的私钥对信息进行解密，再用车辆 V1 正确的公钥核实签名，才可以正确地获得消息，这可以保证消息合法且未被篡改。假如攻击者在该过程中截获了消息，也无法对消息进行正确解密。车辆用户每隔一段时间需要对身份证书及公/私钥进行更换，可以保证消息的不可链接性。由于车辆用户对每条消息都进行了签名，一旦验证成功，车辆就无法否认自己是消息发送者。在 L 型认证方案中，由 TTP_A 进行车辆 A 的身份有效性验证，由 TTP_B 进行车辆 B 的身份有效性验证，车辆 A 和车辆 B 需要从签名中正确恢复 R_A 和 R_B。在认证的过程中，可信第三方需要对公钥和证书的有效性进行验证，若公钥或证书的有效性不能被可信第三方获得，消息中将包括表示验证失败的内容。在该过程中使用随机产生的随机数，因此，两条消息之间没有任何关系，攻击者不能从截获的两条或多条消息中获得有效信息。通过上述步骤，两种方案可以保证消息的认证性与完整性、可追溯、不可链接、不可否认、抵御攻击等安全需求。

5.2 计算开销

本节对两种方案的计算开销进行分析。

对于第 3 节提到的基于层次化结构的 V2V 安全认证方案，流程中所涉及的计算过程主要为：校验身份证书过程、加密运算过程、签名运算过程。考虑主要计算步骤，设校验身份证书所需要的时间为 T_m。由第 3 节的分析可知，车辆通信阶段所需要的计算开销为 $4T_m$。设 D 运算时间为 T_D，E 运算时间为 T_E。则该过程的总计算开销为 $4T_m+2T_D+2T_E$。若任意 m 个车辆建立两两通信过程，则总计算开销为 $m(m-1)/2\times(4T_m+2T_D+2T_E)$。

对于 L 型安全认证模型，可假设认证过程的加密算法、校验身份证书过程与第 3 节所述相同。设验证随机数过程的计算开销为 t。由第 4.2 节可知：TTP_A 收到车辆 A 发送的消息 2 后，根据车辆 A 的身份信息 I_A 验证车辆 A 的身份，所产生的计算开销为 T_D 或 T_m，因此，此处近似取 T_D 与 T_m 的平均值为（T_D+T_m）/2；TTP_B 收到 TTP_A 发送的消息 3 后，根据车辆 B 的身份信息 I_B 验证车辆 B 的身份，产生的计算开销为 T_D 或 T_m，因此，此处近似取 T_D 与 T_m 的平均值为（T_D+T_m）/2；TTP_A 收到 TTP_B 发送的消息 4 后，验证第二签名所产生的计算开销为 T_E；验证通过后，验证随机数所产生的计算开销为 t。后续验证步骤所产生的计算开销同理。由此可得，若全部验证过程通过，所产生的总计算开销为 $T_D+T_m+T_E+t+T_E+t+T_E+t=T_D+T_m+3T_E+3t$。若任意 m 个车辆建立两两通信过程，计算开销为 $m(m-1)/2\times(T_D+T_m+3T_E+3t)$。

表 1 计算开销比较

方案	计算开销
层次化结构安全认证方案	$m(m-1)/2\times(4T_m+2T_D+2T_E)$
L 型安全认证方案	$m(m-1)/2\times(T_D+T_m+3T_E+3t)$

参考在 2.2 GHz 主频的 Core i5 处理器、4 GB 内存和 Windows 8 操作系统环境下测试的部分运算时间[17]。在多次测试中，T_m 约为 7 ms，T_D 约为 1 ms，T_E 约为 2 ms，t 约为 0.08 ms。计算开销变化曲线如图 5 所示，图 5 给出了 2 种认证方案的计算开销与车辆数量之间的关系。

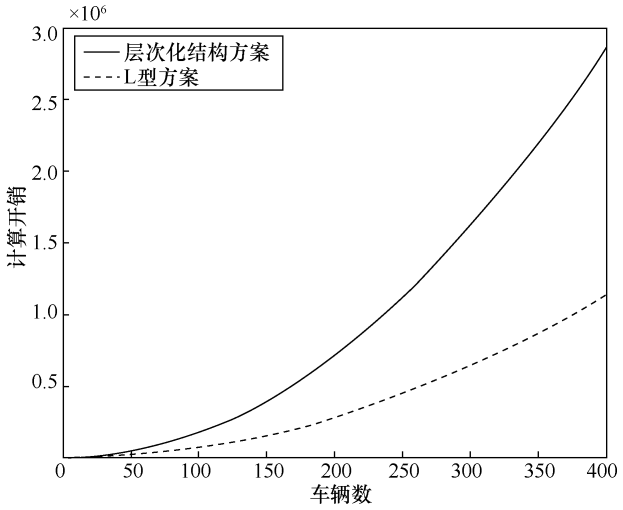


图 5 计算开销变化曲线

由图 5 可知，对于车辆数量相同的情况，L 型安全认证模型虽然引入了多个可信第三方，但其仍保持较快的计算速度。

5.3　通信开销

本节对两种方案的通信开销进行分析，只考虑车辆进行安全认证过程中参数的传输代价，包括身份信息、签名、证书等。

对于层次化结构的 V2V 安全认证方案，假设 IDV1、IDV2 的大小为 8 byte，生存时间 TV1、TV2 的大小为 4 byte，反馈信号的大小为 2 byte，传输过程中加密算法产生的开销为 50 byte。依据第 3.2 节，该方案的认证过程产生的通信开销为 8+4+8+4+2+8+4+2+2+2×(8+4+2)+50=120 byte。

对于 L 型安全认证方案，假设车辆身份信息 I_A、I_B 为 8 byte，验证结果 Res_A、Res_B 为 2 byte，随机数为 4 byte，签名所产生的开销为 50 byte。依据第 4.2 节，该方案的认证过程产生的通信开销为 8+4+8+4+4+2+2+50=82 byte。

由此可知，相较于层次化结构的 V2V 安全认证方案，在相同条件下，L 型安全认证方案的通信开销较小。通信开销比较如表 2 所示。

表 2　通信开销比较

方案	消息组成	通信开销
层次化结构安全认证方案	{IDV1, IDV2, TV1, TV2, 反馈信号}	120 byte
L 型安全认证方案	$\{I_B, R_B, I_A, R_A, Res_A, Res_B, RTP_A\}$	82 byte

6　结束语

车联网作为具有广阔发展前景的一种移动自组织网络，保障通信过程的安全性及可靠性是至关重要的。在通信过程中，需要对通信双方的身份进行认证，并对传输过程进行加密。通过可信第三方对身份进行认证，车辆可任意选择通信对象，在与其建立连接前要确定对方的合法身份，并基于非对称密码体系进行保密通信。由于车辆位置分布较广泛，对可信第三方的管理可基于层次化结构。考虑日益增长的车联网用户数量，若进一步提升安全性，可将唯一可信第三方更改为双可信第三方，通过对 L 型安全认证方案的应用来保障通信过程的安全。

参考文献：

[1] QU F Z, WU Z H, WANG F Y, et al. A security and privacy review of VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2015, 16(6): 2985-2996.

[2] 5G Americas white paper: cellar V2X communications towards 5G[R]. 2018.

[3] 中国通信学会. 车联网安全技术与标准发展态势前沿报告[R]. 2019.
China Institute of Communications. Report on the trend of Internet of vehicles security technology and standards[R]. 2019.

[4] 高柯夫, 孙宏彬, 王楠, 等. “互联网+”智能交通发展战略研究[J]. 中国工程科学, 2020, 22(4): 101-105.
GAO K F, SUN H B, WANG N, et al. Development strategy of Internet plus intelligent transportation[J]. Strategic Study of CAE, 2020, 22(4): 101-105.

[5] 陈山枝. 打造“5G+车联网”中国模式[J]. 中国工业和信息化, 2020(11): 44-49.
CHEN S Z. Building the “5G+IoV” in China model[J]. China Industry & Information Technology, 2020(11): 44-49.

[6] VIJAYAKUMAR P, AZEES M, KANNAN A, et al. Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(4): 1015-1028.

[7] VIJAYAKUMAR P, AZEES M, CHANG V, et al. Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks[J]. Cluster Computing, 2017, 20(3): 2439-2450.

[8] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[C]//Proceedings of Advances in Cryptology — CRYPTO 2001. Heidelberg: Springer Press, 2001: 213-229.

[9] LU H, LI J, GUIZANI M. A novel ID-based authentication framework with adaptive privacy preservation for VANETs[C]//Proceedings of 2012 Computing, Communications and Applications Conference. Piscataway: IEEE Press, 2012: 345-350.

[10] 谭杰, 郑明辉. 车联网中基于知识签名的快速身份认证协议研究[J]. 中南民族大学学报(自然科学版), 2020, 39(4): 420-424.
TAN J, ZHENG M H. Research on fast identity authentication protocol based on knowledge signature in VANET[J]. Journal of South-Central University for Nationalities (Natural Science Edition), 2020, 39(4): 420-424.

[11] 陈葳葳, 曹利, 邵长虹. 基于区块链技术的车联网高效匿名认证方案[J]. 计算机应用, 2020, 40(10): 2992-2999.
CHEN W W, CAO L, SHAO C H. Blockchain based efficient anonymous authentication scheme for IoV[J]. Journal of Computer Applications, 2020, 40(10): 2992-2999.

[12] SHAHID M A, JAEKEL A, EZEIFE C, et al. Review of potential security attacks in VANET[C]//Proceedings of 2018 Majan International Conference (MIC). Piscataway: IEEE Press, 2018: 1-4.

[13] 吴黎兵, 谢永, 张宇波. 面向车联网高效安全的消息认证方案[J]. 通信学报, 2016, 37(11): 1-10.
WU L B, XIE Y, ZHANG Y B. Efficient and secure message authentication scheme for VANET[J]. Journal on Communications, 2016, 37(11): 1-10.

[14] 李铭煜. 车联网 V2X 间数据安全通信的研究与设计[D]. 北京: 北京交通大学, 2018.
LI M Y. Research and design of secure data communication between V2X in IoV[D]. Beijing: Beijing Jiaotong University, 2018.

[15] 谢希仁. 计算机网络[M]. 北京: 电子工业出版社, 2013.
XIE X R. Computer networking[M]. Beijing: Publishing House of Electronics Industry, 2013.

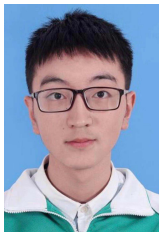
[16] 张变玲, 杜志强, 李琴, 等. 一种实体身份有效性验证方法及其装置: CN106572066B[P]. 2019.

ZHANG B L, DU Z Q, LI Q, et al. Method and device for validating entity identity: CN106572066B[P]. 2015.

[17] 周雨彤. 车联网寻径系统信息安全与隐私保障策略的研究[D]. 北京: 北京交通大学,2019.
ZHOU Y T. Research on information security and privacy guarantee strategy of IoV path-finding system[D]. Beijing: Beijing Jiaotong University, 2019.

[作者简介]

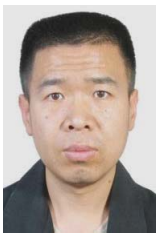
王曼竹（1999– ），女，北京交通大学电子信息工程学院在读，主要研究方向为通信工程。



李梓琦（1998– ），男，北京交通大学电子信息工程学院和北京工业大学城市建设学部城市交通学院双培生，主要研究方向为轨道交通信号与控制。

陈翌飞（1999– ），男，北京交通大学电子信息工程学院在读，主要研究方向为通信工程。

洪高风（1995– ），男，北京交通大学电子信息工程学院博士生，主要研究方向为5G 车联网以及边缘云计算。



苏伟（1978– ），男，北京交通大学教授，主要研究方向为新一代信息网络关键理论与技术。