

文章编号:1007-5321(2017)03-0001-18

DOI:10.13190/j.jbupt.2017.03.001

车联网认证机制和信任模型

刘宴兵, 宋秀丽, 肖永刚

(重庆邮电大学 网络信息安全技术重庆市重点工程实验室, 重庆 400065)

摘要: 车联网通过人-车-路-后台实时互联感知实现交通智慧管理、决策和控制,其安全认证机制和信任模型是当前研究的重点和难点. 为了解决车联网安全面临的主要问题——单一的认证机制和信任模型无法满足车联网复杂多通信场景下安全的差异化保障,综述了面向多通信场景的车联网认证方法论和信任模型的相关研究现状和成果;勾画、概括了新方向,通过深入研究认证机制的内在机理,构建按安全需求划分的认证机制和理论框架,并设计相关协议,实现了不同场景下的安全性、时效性和隐私性的个性化认证服务;设计了基于车辆节点消息和行为的动态信任模型,提供了强实时性和高精确性的信任评估,为能主动感知恶意节点提供了方法支撑;考虑未来车联网极有可能运行于量子通信环境,推演了量子门限匿名认证和量子信任演化决策机理的研究方向;最后对相关研究技术进行了安全性评估和未来发展展望.

关键词: 车联网;多通信场景;认证机制;信任模型

中图分类号: TN929.5; TP391.44; U495

文献标志码: A

Authentication Mechanism and Trust Model for Internet of Vehicles Paradigm

LIU Yan-bing, SONG Xiu-li, XIAO Yong-gang

(Chongqing Key Laboratory of Network Information Security Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

Abstract: The internet of vehicles paradigm aims to achieve efficient management, decision-making and control of intelligent transportation through real-time perception among humans, vehicles, roadside units and trusted center. Currently, the authentication mechanism and trust model have become one of the research focus difficulties of internet of vehicles security. The main problem is that the authentication mechanism and trust model only consider one single aspect of security performance, which cannot satisfy the diversified security demands of multi-communication scenarios. In order to address this problem, the article proposes an authentication methodology and a trust model oriented to internet of vehicles multi-communication scenarios. The basic idea of research work involves three aspects. Firstly, the research status and achievements of the methodology and trust model under multi-communication scenarios was summarized. Secondly, the outline of new research directions was drawn, the intrinsic characters of authentication was studied, the authentication mechanism as well as the theoretical framework based on gradient security demands was constructed, and the related protocols to achieve diversified authentication services for different scenarios from the view of security, timeliness and privacy was designed. Thirdly, message-based and behavior-based dynamic trust model was given to provide strong real-time and high accurate

收稿日期: 2017-04-27

基金项目: 国家自然科学基金项目(61309032,61272400)

作者简介: 刘宴兵(1971—),男,教授,博士生导师, E-mail: liuyb@cqupt.edu.cn.

trust evaluation, which can offer technical support for malicious nodes detecting, Finally, the internet of vehicles paradigm is likely to run in the quantum communication environment in the future, the threshold quantum anonymous authentication and the research direction of quantum trust evolution decision mechanism. The authors also evaluate the security for related research techniques and look ahead the future development.

Key words: internet of vehicles; multi-communication scenarios; authentication mechanism; trust model

0 引言

车联网以移动的车辆为信息感知对象,通过人-车-路-后台实时互联感知实现交通智能管理、信息服务、智能决策和车辆智能控制等一体化,为交通行业提供更安全、高效、节能、环保、舒适的出行方式和多样化的智能服务模式。车联网的实现依赖于各种传感技术、无线通信技术、控制技术和互联网技术等,且具有通信网络拓扑结构自主、变化频繁以及通信场景多样化等特点,使车联网中的车辆节点比传统的网络节点面临更多、更复杂的网络攻击,给系统的安全防护和主动防御带来了新的挑战。一方面,认证机制和信任模型已经在传统网络中得到广泛的应用^[1],也是支撑新兴车载网络应用和提供安全服务保证的坚实演化基础;另一方面,由于车联网多通信场景的特殊性及其应用的多样性,当前车联网安全认证和信任机制的研究尚未形成完整体系,亟需对面向多通信场景的车联网认证机制和信任模型展开系统理论的研究,从而为车联网安全措施部署与应用实践奠定方法支撑和理论基础。

目前,国家对车联网中安全体系基础设施的建设已经提出了指导方针。《国民经济和社会发展的第十三个五年规划纲要》提出“强化信息安全保障……着力构建量子通信和泛在安全物联网……加快构建高速、移动、安全、泛在的新一代信息基础设施,推进信息技术广泛应用”。“中国制造 2025”的规划指南中指出“以加快建立具有全球竞争优势、安全可控的信息产业生态体系为主线,强化科技创新能力、产业基础能力和安全保障能力,突破关键瓶颈……”作为信息产业发展的指南。2016 年,国家已经将“LTE-V 无线传输技术标准化及样机研发验证”列入“新一代宽带无线移动通信网”国家科技重大专项课题,在助推 LTE-V 标准形成的同时,也极大地加速了车联网产业化发展进程。同时,在中国科学院最近发布的《科技发展新常态与面向 2020 年的战略选择》研究报告中,“量子通信将可能率先

取得重大突破”也被列为中国在未来 5 ~ 10 a 内可能产生的 19 个重大科技突破之首。车联网的未来部署应该考虑到与量子通信技术的结合。目前,车联网在经典和未来量子通信环境下主要涉及 5 个方面的交互通信场景:车—车、车—路侧单元(RSU, road-side unit)、车—可信中心(TC, trusted center)、车—车厂和 RSU-TC,如图 1 所示。

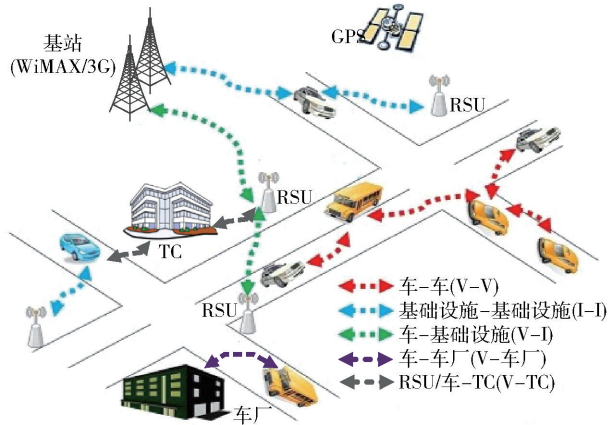


图 1 车联网环境通信场景示意图

而现有的相关认证机制和信任模型的单一性无法完全覆盖整个车联网需要对场景按照实际需求进行划分的环境;同时,在不同的场景下设计差异性的认证和信任服务,实现安全性、时效性和隐私性方面的量效均衡也是车联网安全研究的迫切需求。此外,有机结合认证机制和信任模型,从安全防护和主动防御方面维护高效安全的车联网环境,需要考虑认证机制和信任模型的通信环境从当前通信向量子通信演化。

目前相关认证和信任技术在车联网中的运用存在以下 3 方面的问题。

1) 相关认证技术和结构的单一性

车辆作为车联网中的移动感知节点,根据其在网络中的行为可将场景分为安全的网络接入(车—TC、车—车厂)和实时的通信交互(车—车、车—RSU)。前者在车—TC 场景下将身份认证作为基础

的安全能力控制访问权限,并为后续的协同通信场景提供安全环境,因此,要求身份认证方法在时间延迟容忍的前提下保证安全性;在车—车场景下,车辆与车厂进行数据通信报告车辆信息,从而获得如远程协助解锁、在线电子部件或系统故障诊断排除与程序升级、车型技术资料与咨询等服务,该场景下隐藏的漏洞将严重威胁车辆本身的安全和车主的人身安全,因此,需要认证方法强调更强的安全性。后者从节点间瞬时通信场景展开研究,由于节点之间身份不确定性和会话临时性(李静林等^[2]指出,平均每条消息的传输时间为1~10 s,在100 km/h时速下,车—车、车—RSU通信链路能稳定保持15 s以上的概率只有57%),需要保护车辆隐私和信息安全的同时,注重提高认证的时效性。基于以上分析,如何构建适应多场景的认证机制将是一个有意义的、值得探索的设计思路。

2) 信任计算的弱实时性和低精确性

车联网的通信特性对面向应用的信任模型提出了时间约束和精度要求,信任度的价值与其计算的时间和精度密切相关,如果没有在规定时间内完成计算或者没有达到需要的精度,对信任的度量将失去价值。目前常用违章驾驶记录对信任度进行评估,但在现有管理制度和技术条件下,从某车辆发生违章事故开始到该违章记录可被查询存在较长的时间差,无法及时反映车辆的驾驶行为。车联网中的车辆以1~10 Hz的频率广播自身的行驶状态信息,为信任模型的计算提供了大量的实时数据,有助于得到具备实时性与精确性的车辆信任度,进而做出正确的信任决策。

3) 缺乏对未来量子通信环境的考虑

未来,随着量子通信技术的产业化和广域量子通信网络的实现,车联网极可能运行于量子通信环境之中。量子通信是利用量子相干叠加、量子纠缠效应进行信息传递的一种新型通信技术,由量子论和信息论相结合而产生。相比于当前通信技术,量子通信具有时效性高、抗干扰性能好、保密性能好、隐蔽性能好、信噪比低等特点和优势。而且,量子通信与传播媒介无关,传输不会被任何障碍阻隔,量子隐形传态通信能穿越大气层。因此,量子通信应用广泛,既可在太空中通信,又可在海底通信,还可在光纤等介质中通信。由于绝对安全的特性,量子通信在通信、保密、金融等领域有着巨大的需求,正在经历着从基础研究向应用技术转化的进程。研究车

联网在当前通信和量子通信环境下的认证机制和信任模型具有重要的实践意义和应用前景。

通过以上分析可以发现,强调某个单一侧面的认证机制和信任模型已经难以适应车联网环境中不同通信场景对安全性、隐私保护和时效性的差异性需求。因此,需要改进或重新定义车联网面向多场景的认证机制和信任模型,并且能够从当前通信环境向未来量子通信环境过渡。笔者主要从认证机制需要从单一场景向多场景考虑演化、信任计算向强实时性和高精确性演化和车联网从当前通信环境向量子通信环境演化3个角度综述相关研究成果和概括最新演化研究方向,同时,对相关研究的未来发展进行展望。

1 国内外研究现状及发展动态

1.1 车联网的认证机制

现有的车联网认证机制大多只适用于单一的通信场景,主要包括针对车辆节点身份合法性的身份认证、针对某一具体身份的静态和动态属性的认证以及针对各实体之间传递消息的认证,缺乏对多通信场景的综合考虑。

身份认证方面,现有研究成果的身份认证主要由基于嵌入式安全模块的移动终端可信增强架构和基于身份的加密机制组成。前者,车辆节点作为移动终端,通过集成安全模块构建可信增强架构,辅助完成身份认证授权功能。目前主要的车载安全模块包括可信平台模块^[3]和防篡改装置^[4],其优点是将专业的密码安全引擎、安全算法等基础安全能力组件化,通过硬件提高计算速度。但是,其不足之处主要是构建代价高,且不同厂家构造的安全模块标准不一,安全性难以统一。后者验证的本质是考虑终端是否掌握正确的口令或密钥^[5],可以避免公钥基础设施(PKI, public key infrastructure)对证书的依赖和复杂的证书管理开销,减少为无线通信带宽带来的负担。在构建认证协议的过程中,较多基于双线性映射理论构造加解密或签名验证方法,通过双线性映射理论应用过程中的难解问题确保安全性,并结合Zhu等^[6]提出的消息认证码(MAC, message authentication code)实现认证,或者通过连接、异或等符号根据数学推导理论构造认证交互的协议^[7],通过减小计算量避免过多的时间开销。但是,该方法会造成在构建和管理密钥时的额外开销。现有的轻量认证技术比较如表1所示。

表 1 基于 PKI 和非 PKI 身份认证比较

优缺点	基于 PKI 的身份认证	非 PKI 认证
单一认证	优点:安全保障和管控节点的能力强	优点:低计算开销和无证书管理开销
	缺点:证书更新频繁,管理开销大	缺点:存在密钥托管的问题
组认证	优点:减少证书管理的开销	优点:降低密钥管理开销和计算开销
	缺点:组长是整个通信组的攻击弱点和安全瓶颈,难以预防组内攻击	缺点:组长是整个通信组的攻击弱点和安全瓶颈,难以预防组内攻击

属性认证方面,属性认证是一种比身份认证更细粒度的认证方法,车联网中主要通过基于属性的加密实现对车辆的属性认证^[8],是基于身份加密机制^[9]的延伸. Waters^[10]将密文策略基于属性的加密应用于车联网的认证及访问控制策略中^[11-12],其基本思想是将访问结构部署在密文中,根据用户的属性集合生成用户私钥,当车—RSU 和车—车的临时会话需要认证车辆的属性时,系统根据接收方的具体属性构造访问树,将访问树和密文一起发送给接收方,接收方的属性集合满足访问树才能成功解密消息,其他用户则不能解密密文,使加密者在控制用户的接入上具有主动性,实现了对车辆属性的有效验证. 加密策略是属性加密的关键部分, Huang 和 Ruj 等^[13-14]采用由多层次的与门和或门组成的策略树来描述加密策略,属性匹配机构在进行判决时将车辆的属性与访问树的节点相对应,只有属性集合满足访问树的结构时,才授权车辆访问. 但是此策略在解密时需要进行大量运算,加重了节点的负担. 析取范式 (DNF, disjunctive normal form) 在布尔逻辑中是有限个简单合取式构成的, Rao 等^[15]将其应用于车联网认证和访问控制策略中,其优点是将多层次的访问树优化为 DNF,任意一个传统的访问树都能化成一个根节点为 OR,所有父亲节点为 AND 形式的 DNF 树,提高认证策略的灵活性和可扩展性,并减小解密开销,有效地提高信息的访问效率.

消息认证方面,现有的研究成果中主要包括基于匿名证书的消息认证、基于群签名的消息认证和基于身份公钥密码的消息认证. Zhou 等^[16]提出了基于匿名证书的认证协议,该协议为车辆预先分配多个匿名证书,通信时随机选取一个证书用于签署发送的消息,签署后撤销该证书,对外提供匿名性以

保护消息发送者的身份隐私. 但是该协议需要车辆预装载大量的匿名证书,增加了车载单元 (OBU, on board unit) 的存储压力,且权威机构通过证书追踪车辆身份也具有很高的难度. 基于群签名的消息认证中,通过群签名,群组中的每个合法成员可以代表整个群组进行匿名签名,验证者只能通过签名得知该车是否来源于该群体,而不能得知车辆的具体身份. 群签名认证隐藏了发送者身份,模糊了身份与签名的关联性,被研究者广泛采用^[17]. 但是该类认证协议的缺点在于延迟较大,降低了消息认证的效率,且认证效率受车辆数目的影响,实用性较差. Bayat 等^[18]提出了基于身份公钥密码算法的认证协议,此协议避免了在车辆上存储证书且能同时认证多个消息,提高了消息验证的效率,但无法有效抵抗重放攻击和假扮攻击^[19]. 此外,一些数学思想也被引入该类消息认证中,如双线性映射^[20-21]、椭圆曲线密码^[22]等,但这些认证协议对 RSU 的计算能力要求高,运算效率相对低,不满足车辆通信的瞬时性要求. 另外,消息发送者请求 RSU 对消息进行认证的同时,还存在隐私保护的需求,传统的 MAC 已不能解决这个问题. 为此, Van 等^[23]提出了保护隐私的 MAC,但该协议复杂的计算过程进一步加大了 RSU 的计算压力,无法适用于车联网的瞬时通信环境.

1.2 车联网信任模型

车辆节点的未来行为具有不确定性^[24],但可以根据车辆节点历史行为数据预测其行为趋势. Tan 等^[25]提出了车联网信任模型的概念,该模型通过甄别可信车辆和非可信车辆为驾驶决策提供支持,由此促进安全驾驶、提高交通效率. Yao 等^[26]提出了以车辆节点为中心的动态信任模型,为不同类型的应用与不同类型的节点赋予不同的权重来计算车辆的信任值;同时也提出了以数据为中心的信任模型,由实体的可信度、事件与实体的相关度、空间远近与时间远近计算其加权信任度. Cho 等^[27]研究容迟网络中基于起源的信任模型,该模型规定信任评估要知道消息的详细情况,即来自源节点的消息到达目的节点之前被转发的情况,增加了信任计算的时延. 吴启武等^[28]利用信任分类与动态管理的方法,使用 Beta 分布描述当前节点的信任情况,以 GeoDTN + Nav 路由协议为应用框架,提出了一种新的基于贝叶斯理论的车联网安全路由信任模型. 夏怒等^[29]提出了一种面向域间路由系统的信任模型 TMIRS,

在该模型中,车辆节点在每个评估周期对其邻居自治域的历史路由通告行为进行直接评估,同时收集被评估自治域的其他邻居自治域对其的直接评估,最后综合多方来源的直接评估结果计算被评估自治域的信任度.蒋黎明等^[30]结合 D-S 证据理论和图论方法提出了一种新的证据信任度量模型,解决了现有证据信任模型中普遍存在的在信任聚合过程中缺少对信任链之间依赖关系的有效处理等引起的模型性能下降问题. Vicsek^[31]使用了信任传递的概念,将信任值从一个节点传递到下一个节点,但节点的推荐信任度是不同的,具有较高本地信任值的节点所推荐的关于其他节点的信任值更值得信任.

上述文献为车联网信任模型设计提供了重要的参考,但缺乏将车辆运动状态这一重要信息作为评估指标的信任模型,且部分或局部忽略了信任度计算过程中实时性和精确性的问题.此外,信任度的计算偏重于考虑单一场景,仅设计与该场景相适应的信任评估和聚合算法,缺乏综合考虑不同应用场景下车辆的信任计算问题.群体运动是由大量自主驱动代理组成的群体展现出的运动规律性,它包含隔离、对齐和聚合 3 个特征^[32-33],对于建立考虑车辆运动状态的信任模型有着重要的参考价值,因此,笔者拟采用群体运动模型作为运动特征评估算法的依据,建立车联网中面向多应用场景的信任模型.

1.3 量子认证和信任机制

在量子通信领域,出现了一些关于量子认证机制的研究成果.根据酉变换和量子单向函数的特性,Shi 等^[34]提出了一个量子不可否认的认证协议,该协议仅仅对指定的接收者能认证成功. Hao 等^[35]提出了一个基于 ping-pong 技术的量子身份认证机制,该机制能验证用户身份的合法性,当再次认证时,需更新初始认证密钥. Chen 等^[36]提出了一个基于 EPR 纠缠对的量子身份认证机制,该机制使用量子力学原理实现零知识证明的身份识别功能.董颖娣等^[37]借助测量设备量子密钥分发协议的安全性,提出了基于测量设备无关协议的量子身份认证协议,该协议使用共享密钥加密认证密钥,并发送到第三方进行贝尔态测量验证身份的合法性.纵观量子认证机制,至今还没有出现量子匿名认证的相关成果,仅仅在当前通信领域,一些学者开展了直接匿名认证机制的研究工作.为了保护可信平台模块持有者的身份隐私,将直接匿名认证作为匿名用户使认证者确信其被可信机构所认可的一种机制^[38]. Brickell

等^[39-40]直接通过匿名认证加强签名者身份的隐私性,但该认证无法追踪到恶意节点的身份信息并撤销. Chen 等^[41]使用了链接算法来保证进行重复签名的用户的不可抵赖性,是使用门限验证网络中不同节点的前提. Calandriello 等^[42]指出车辆可以自动生成匿名证书,有效地降低了证书机构存储和搜索证书的代价.

相比量子认证,针对量子信任决策的成果相对比较少. Li 等^[43]研究了在量子囚徒困境中关于信任对自适应合作演化的影响,根据邻居节点收益的多少参与者动态调节信任值. Yukalov 等^[44]提出了一个量子信息处理设备的通用理论,该理论能应用到人类决策创建、自动多模寄存器组装等领域. Ashtiani 等^[45]提出了一个基于量子决策理论的计算信任值的公式,通过该公式接口单元,针对各种上下文不同的非确定和风险,能将信任者的情感和主观爱好进行量化.在当前通信领域,关于信任决策机制的研究成果大量涌现.陈菲菲等^[46]利用机器学习方法研究了动态信任评估模型,算法采用基于规则的机器学习方法,具有从大量输入数据中自学习以获取评估规则的能力.林闯等^[47]提出了可信网络中一种基于行为信任预测的博弈控制机制,论述了如何利用贝叶斯网络对用户的行为信任进行预测.李小勇等^[48]提出了基于多维决策属性的信任关系量化模型,引入直接信任、风险函数、反馈信任、激励函数和实体活跃度等多个决策属性,从多个角度推理和评估信任关系的复杂性和不确定性.沈士根等^[49]引入与节点信任度绑定的激励机制,建立无线传感器网络节点信任博弈模型以反映信任建立过程中表现出的有限理性和每次博弈过程的收益.在信任模型中,存在自私用户为最大化自身利益而故意策略性谎报推荐信息的问题.魏志强等^[50]提出了一种基于 VCG (Vickrey-Clarke- Groves) 机制的防护策略信任机制,用以获得用户的真实推荐.

1.4 相关研究存在的问题

虽然现有的认证和信任技术对研究车联网的认证机制和信任模型具有重要的参考价值,但仍需要考虑车联网节点通信场景的多样化特点,从多个角度来设计、实现和攻击防御,并将其从当前通信环境向未来量子通信环境演化拓展.总结现有的车联网认证机制和信任模型后发现存在以下不足.

1) 认证机制方面

① 身份认证协议考虑因素的局限性. 现有身

图2 多场景认证和信任模型结构

2.1 面向多通信场景的认证机制

从车联网中各通信场景对安全性、隐私性和时效性的不同需求入手,应建立一种集成身份、属性和消息的认证机制,为通信节点提供差异性认证服务.将身份认证作为车辆节点接入网络时的基础认证服务(车—TC),基于双线性映射理论构造满足高安全性需求的认证会话密钥,通过优化通信负载、减少交互流程构造低通信时延的认证协议,使 TC 完成对车辆节点合法身份的验证和授权,并研究认证方法从身份向生物识别的拓展,以满足车—车厂通信场景下对认证服务的更强安全需求.在通信交互场景中(车—车和车—RSU),为保证认证机制的时效性与隐私性,研究应立足从面向实体和面向消息2个角度分别实现认证.其一,以通信节点为研究主体,对车辆进行细粒度的属性认证,优化认证策略,构建基于属性加密的认证方法,保证车—车和车—RSU 认证的可扩展性;其二,以车—车通信消息为研究主体,构造轻量级的消息认证方法,快速验证消息签名,保证消息的完整性和不可抵赖性,达到保护节点间通信安全的目的.

2.1.1 节点身份认证协议

根据车联网中不同角色通信实体间的信任关系,研究表明可将车辆节点身份接入认证的管理设计成基于分层信任的目录树结构,如图3所示.其中,TC 作为一个可信任中心包括多个子信任中心 TC_i ,每个子信任中心 TC_i 管辖一定数量街区的 RSU, TC_i 被管辖范围内的所有 RSU_{i-j} 信任.基于此种信任结构,车辆节点接入某个 TC_i 所执行的接入身份认证协议的性能和安全性将影响后续车—车、车—RSU 通信质量.

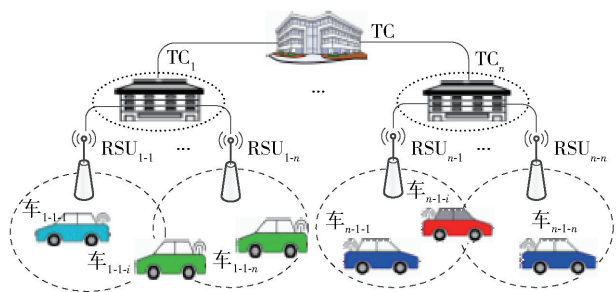


图3 车联网中节点信任关系示意图

如图4所示,通过研究基于双线性映射理论的全局参数管理和认证会话密钥计算、分离认证的预处理部分和认证核心交互过程,减少接入认证切换时的参数设置开销以及认证会话过程中的处理开

销,并考虑普遍的网络攻击因素设计安全的身份认证协议.

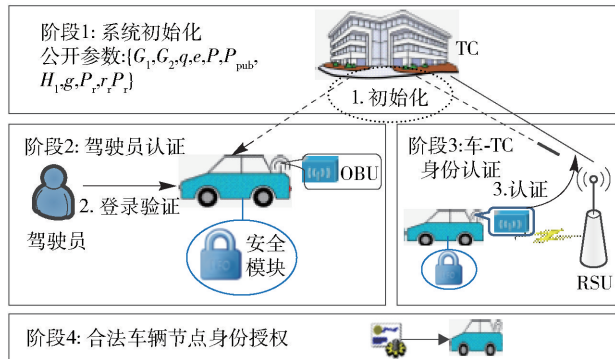


图4 身份认证流程架构

1) RSU 初始化:TC 通过有线安全传输协议为 RSU 设置公私钥对 $\{P_r = H_1(ID_r), S_r = sH_1(ID_r)\}$, RSU 随机选取整数 $r_r \in Z_q^*$, 并且广播参数 $r_r P_r$.

2) 车辆节点初始化:TC 根据驾驶者提供的身份信息 $ID_i \in \{0,1\}^*$ (如电话、邮箱)、登录密码和车辆节点信息 $INFO_i$ 设置共享秘密 $x_i \in Z_q^*$, 并建立两者间的联系 $R_i = H(ID_i \parallel PW_i) \oplus x_i$, 计算全局唯一身份标识 $IM_i = H_1(ID_i \parallel x_i \parallel TS_{reg}) \in G_1$, 为车辆节点设置参数 $\{IM_i, sIM_i, H(\cdot), E(\cdot), R_i, Z_i\}$.

根据上述预置的参数,驾驶员通过人机交互接口输入证据信息验证其身份的合法性.上述措施均为接入认证前车联网系统的初始化操作.基于车载网络中节点间的通信方式及数据流向,构造时间容忍情况下强调安全性的认证协议,包括以下协议.

① 车辆节点自构造安全参数:临时匿名身份 $AID_i = H(IM_i \parallel TS_i)$, $(IM_i \parallel TS_i) \in \{0,1\}^*$ 、时间戳 $A_i = E_K\{ID_i \parallel IM_i \parallel TS_i\}$, 并向 RSU 发起认证请求消息 $m_1 = \{AID_i, A_i, TS_i, r_i P, P_{pub}\}$.

② RSU 初步验证接收消息的时效性,并计算解密密钥: $SK_{r-i} = g(k_r) = g(H_1(e(r_r S_r, r_i P))) = SK_{i-r} = g(k_i) = H_1(e(r_r P_r, P_{pub}))$, 解密 A_i 获得 $\{ID_{TC}, ID_i\}$ 并向 TC 转发认证请求.

③ TC 通过与 RSU 共享的密钥信息 K 计算 $MAC^* = H(ID_r \parallel A_i \parallel TS_i \parallel k)$ 是否与 MAC 相等,来验证接收消息的完整性和一致性,并验证车辆节点 $\{ID, IM, AID\}$ 的合法性,最后完成对具有合法身份节点的授权,并结束认证会话.

④ RSU 广播合法车辆的身份,使该局域车载网络范围内的其他节点知晓具有合法身份的车辆节点.

通过车—TC 的身份接入认证后,车辆节点具有获取娱乐、资讯、地图等联网运行服务,并且为后续

车—车、车—RSU 协同通信场景提供基础安全环境。相关认证过程如图5所示。

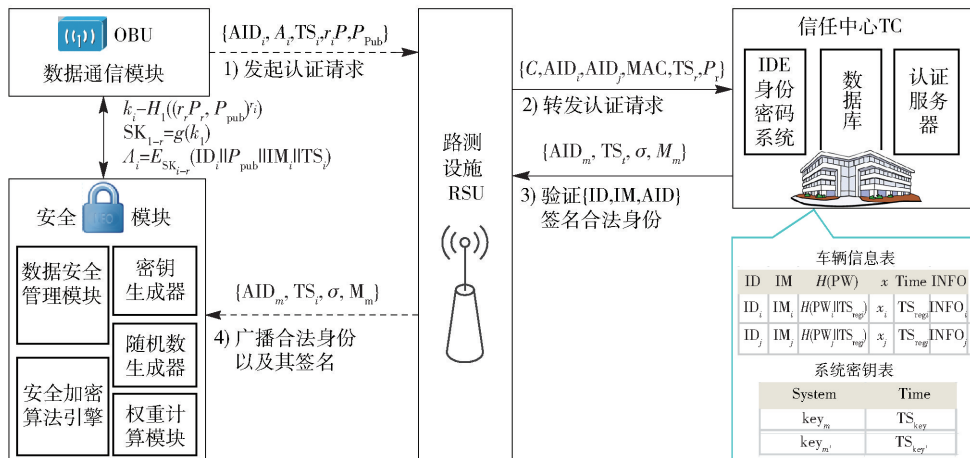


图5 身份认证协议会话流程

2.1.2 细粒度的属性认证策略

通过分析车联网的通信特点,发现车—车、车—RSU 通信大多具有自主性和临时性,要求认证策略具有可扩展性,并保证通信的隐私性。为了实现对车联网中车—车和车—RSU 临时性会话中的细粒度认证,需要构造一种可扩展的属性认证策略,保证节点间的安全通信。新的方向将更加注重研究具有隐私保护性和一对多加密特性的属性认证策略,其基本思想是通过设计车辆的认证策略和构造基于属性的加密算法实现对车辆的属性认证。同时,为了解决认证策略不可扩展和消息解密消耗大的问题,设计基于 DNF 的属性加密认证策略,实现对车辆的细粒度认证以及车—车和车—RSU 安全的消息共享。

具体而言,该属性认证策略包含以下2个部分。

1) 构建访问策略

基于所建立的通信模型构造访问策略,包括车联网中属性的定义和选取、访问策略的描述2部分。下面将车联网中的属性从2个维度进行描述。一个维度是以车联网中的实体划分,将属性分为车辆属性(对车辆节点的各种特性进行描述)、环境属性(对系统的环境进行描述,对通信环境实时感知)、资源属性(对网络中的通信资源安全级别进行描述)、操作属性(对车辆节点的操作权限进行描述);另一个维度是以属性的变换周期划分,分为固定属性和动态属性,保证车辆属性的实时性。

如图6所示,对于访问策略的描述,为优化访问树,使表达更加清晰,减小节点计算开销,研究采用

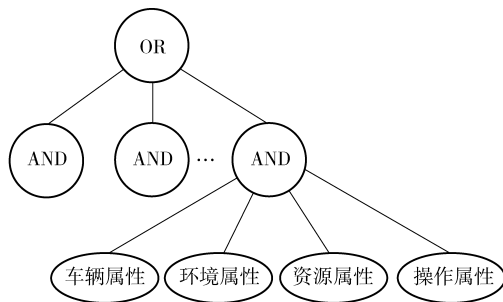


图6 访问策略描述示意图

DNF 构建访问结构。基于 DNF 策略,将待验证的属性加入访问结构中,从而生成匿名通信的认证策略。

2) 基于属性加密的认证策略构造

构造车联网中基于属性的认证策略,其研究思路和步骤如下。

① 系统的初始化:基于双线性映射理论的思想,以系统的安全参数作为认证策略的输入,输出系统公钥 $PK = (p, G_1, G_2, e, g, e(g, g)^\alpha)$ 和主密钥 $MK = g^\alpha$ 。

② 密钥生成:密钥的生成以车辆的属性为依据,通过输入主密钥 MK 和属性集 $Attr$ 生成与用户属性集相关的私钥 SK^s 。

③ 加密阶段:动态属性密钥 SK^d 当 RSU 或网内车辆需要验证未知车辆的属性时,根据认证需求生成访问策略 S ,用拉格朗日插值为 S 中每个 DNF 合取式选取一个多项式,利用系统公钥 PK ,对输入的消息明文 M 进行加密,构造 $CT = (W, C, \tilde{C}, C_w, \{C_m\})$ 并发送给待认证的车辆节点。

④ 解密阶段:车辆接收到认证方发送来的 CT, 将自身属性集合 Attr 与 CT 中访问结构 S 进行匹配, 如果 Attr 满足 S, 则利用 SK^s 和 SK^d 构造解密组件 K_m 、 $e(g, g)^{\omega}$ 和 $M' = e(K_m, \tilde{C}) / e(C_w, C_m)$, 并生成一个时间戳 T, 计算 $Q = H(M' \parallel T)$ 并发送给认证方。

⑤ 认证阶段:认证方接收 Q 时生成时间戳 T' , 并验证 $T' - T \leq \Delta T$, ΔT 为有效的认证时间范围, 验证 $M' = C / e(g, g)^{\omega} = M$, $Q = H(M \parallel T)$, 如果匹配, 则验证成功; 否则连接终止。

具体过程如图 7 所示。

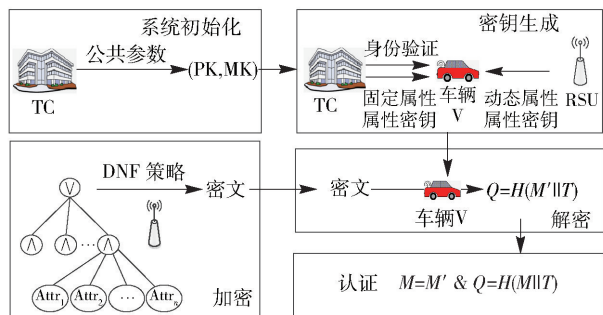


图7 车辆属性认证策略流程

2.1.3 轻量级的消息认证方法

车联网环境下的认证体系中, 由于车联网实时性的要求, 需要快速、高效的认证方法, 以较低的复杂度和空间开销完成车辆间的消息认证。低复杂度能够降低 RSU 计算能力的要求, 低空间开销可以有效地适应 RSU 相对不足的存储能力。笔者研究概括出基于 Diffie-Hellman 密钥协商机制和聚合消息认证码的消息认证方法。针对以上研究内容, 拟按照以下途径展开工作。

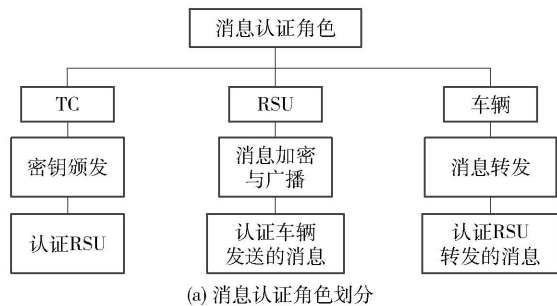
1) 通信角色划分

车联网环境下通信角色划分的思路: 从功能性、通信资源的访问权限以及可信性等方面对车联网环境中的通信组件进行层次划分, 给出不同通信角色在消息认证实施过程中的层次关系以及交互方式, 为消息认证的构建提供基础分析, 如图 8 所示。

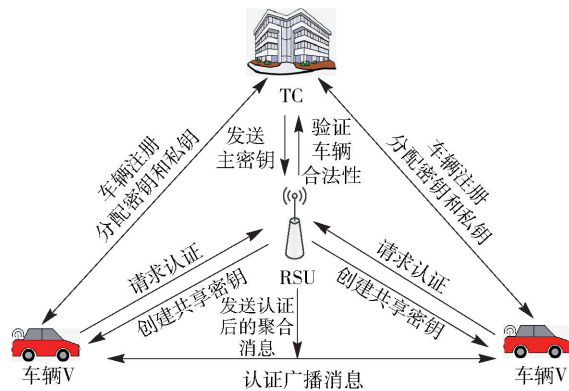
2) 通信消息认证

针对车联网环境中角色多与高动态性的特点, 拟通过聚合消息认证码实现车辆间通信消息的认证, 其方法如下。

① 建立共享密钥: 当 RSU R_j 接收到车辆 V_i 首次发送的消息 $\{ID_{V_i}, g^a, T_s\}$ 时, R_j 使用其私钥 SK_{R_j} 解密消息, 获得车辆的身份 ID_{V_i} 、元素 g^a 以及时间



(a) 消息认证角色划分



(b) 消息认证基本原理

图8 消息认证基本原理及角色划分示意图

戳 T_s , 然后用其公钥 PK_{V_i} 认证 V_i , 若 V_i 通过认证, 则 R_j 为车辆 V_i 签发假名身份 AID_i 。通过 AID_i, R_j 可以了解到是哪辆车在发送消息, 并能映射到共享密钥 K_{ij} 。同理, V_i 接收到 R_j 发送的消息 $\{AID_i, g^b, T_s\}$ 之后用其私钥解密, 并实现对 R_j 的认证, 如果认证成功, V_i 用私钥 SK_{V_i} 签名 $\{g^b, T_s\}$ 并发送给 R_j 。当双方认证均通过时, 使用 Diffie-Hellman 密钥协商机制生成车辆与 RSU 之间的共享密钥 $g^{ab} \rightarrow K_{ij}$ 。车与 RSU 相互认证的过程如下:

$$\begin{aligned} V_i &\rightarrow R_j: \{ID_{V_i}, g^a, T_s\}_{PK_{R_j}}, \{g^a, T_s\}_{SK_{R_i}} \\ R_j &\rightarrow V_i: \{AID_i, g^b, T_s\}_{PK_{V_i}}, \{g^a, g^b, T_s\}_{SK_{R_j}} \\ V_i &\rightarrow R_j: \{g^b, T_s\}_{SK_{V_i}} \end{aligned}$$

② 生成认证签名: 在共享密钥的基础上, 车与车之间的消息认证主要采用聚合认证码完成对消息的认证。车辆 V_i 使用与 R_j 的共享密钥 K_{ij} 加密消息 $\{m, AID_i, T_s\}$, 获得加密后的消息 $C_i = \{m, AID_i, T_s\}_{K_{ij}}$ 。之后将加密后的消息 C_i 及消息时间戳 T_s 发送给 R_j , 若 T_s 新鲜, 则计算 $MAC_{K_{ij}}(C_i) \rightarrow tag_i$; 否则拒绝本次消息认证服务, 并丢弃该消息。如果消息需要通过多跳转发, 为防止转发车辆篡改消息, 使用聚合认证码对消息进行签名。例如, 当转发节点 V_i 接到消息后, 计算其签名 $MAC_{K_{ij}}(C_i) \rightarrow tag$, 并与 V_i 的聚

合认证签名 tag_i 做异或运算,将签名更换为 $\text{tag}_i = \text{tag}_i \oplus \text{tag}$,再将 $\{AID_i, C_i, \text{tag}_i\}$ 转发给下一跳节点。

③ 消息验证:在车联网环境下,车辆间发送消息可能需要通过多跳通信路由转发,而 RSU 与每一个转发节点都有一个共享密钥 K_{ij} 。因此,当 R_j 收到

车辆经过 l 辆车转发而来的消息 $\{C_i, AID_i, \text{tag}_i\}$ 时,计算 $\text{tag}' = \bigoplus_{i=1}^l \text{MAC}_{K_{ij}}(C_i)$,将 tag' 与 tag_i 的值进行对比,如果相同则通过认证;否则不通过,由此可以验证 R_j 接收到消息的完整性,具体的聚合标签认证流程如图9所示。

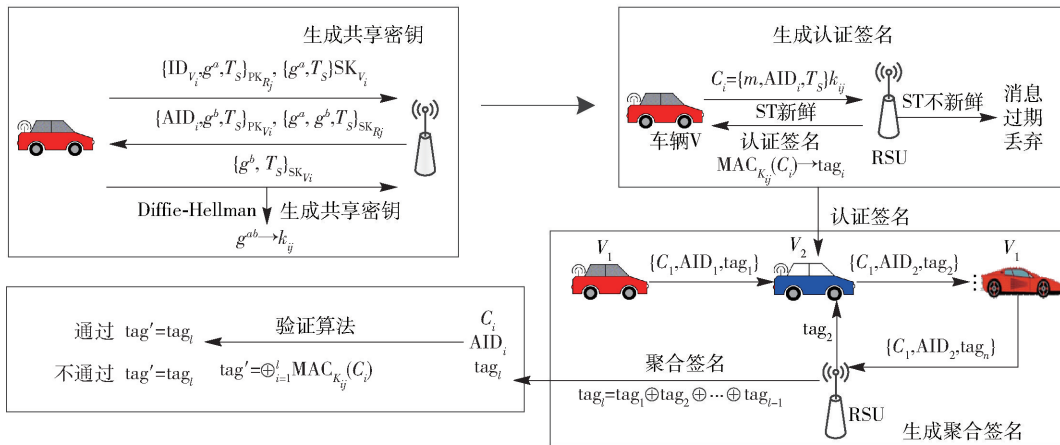


图9 聚合签名认证流程

2.2 面向多应用场景车联网信任模型

研究发现,以车联网在多应用场景下对信任计算实时性和精确性的需求为切入点,构建面向多应

用场景的信任模型,按照信息收集、信任评估、信任聚合和信任决策的步骤展开研究工作,实现对车辆的多维度信任度量将更加有效。

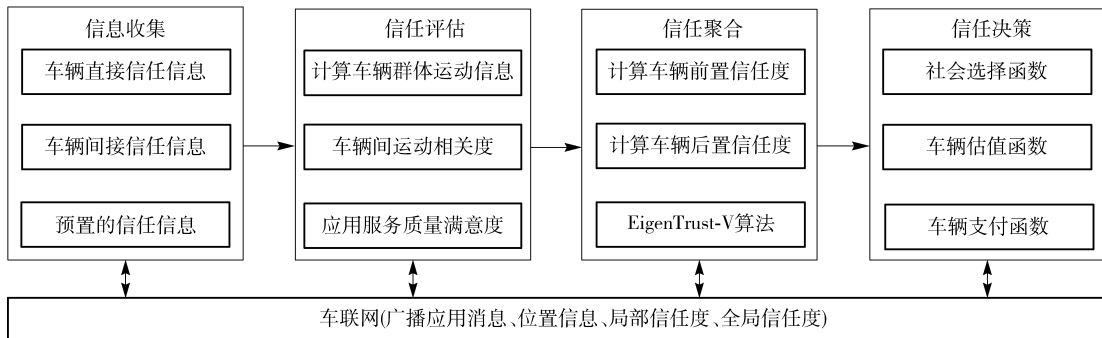


图10 车联网信任模型功能模块

如图10所示.通过分析节点通信行为和节点运动行为,对车辆的消息信任和行为信任进行实时评估.在节点通信行为方面,通过分析车辆的历史交互记录,对车辆的直接信任度和间接信任度进行聚合,得到全局信任度,作为网络恶意节点检测的依据.在节点运动行为方面,通过对车辆的驾驶行为进行建模,设计基于车辆运动信息的行为信任模型,以及相关的信任评估和信任聚合算法,评估车辆的驾驶行为,主动预防违规驾驶造成的交通事故,确保交通安全。

2.2.1 信息收集方法

面向多应用场景的车联网信任模型需要持续地

收集大量信息,为信任评估和信任聚合提供数据.为了达到实时性和精确性的要求,将集成收集直接信任信息、间接信任信息和预设的信任信息等功能模块.在消息信任应用场景下,直接信任信息为车载应用之间的直接交互记录,间接信任信息为其他车辆之间的交互记录,预设的信任信息指系统指定的可信节点.在行为信任应用场景下,直接信任信息为车辆计算得到的信誉记录,间接信任信息为车辆接收到的其他车辆的信誉记录,预设的信任信息可由系统指定。

2.2.2 信任评估算法

信任评估算法将以收集到的车辆应用交互信息

和行驶轨迹信息为数据源,根据应用服务质量满意度和车辆行为群体相关度对信任进行量化。同时,由于实时性和精确性的要求,信任评估的计算方式要降低时空复杂度,以提高计算速度和吞吐量。因此,研究工作概括出面向本地应用交互次数和相邻车辆运动状态的信任评估算法。

在消息信任应用场景下,车辆节点 V_i 对车辆节点 V_j 应用服务质量的信任评估 c_{ij} 由满意交互次数 $\text{sat}(i, j)$ 与不满意交互次数 $\text{unsat}(i, j)$ 综合决定,即 $c_{ij} = \text{sat}(i, j) - \text{unsat}(i, j)$ 。在行为信任应用场景下,面向交通行驶安全的信任评估将根据群体运动模型进行计算。信任评估算法的输入为相邻车辆相遇获得的驾驶记录,输出为对应每次相遇的信誉记录。通过相邻车辆的行驶轨迹,判断是否满足群体运动模型的特征,做出车辆驾驶行为是否可信的判断。通过提供实时的、高精度的车辆行为信息,达到保障驾驶安全和提高交通效率的目的。

行为信任评估算法的步骤如下:

① 基于运动轨迹,计算车辆的群体运动信息,包括车辆自身的速度和加速度、相邻车辆的速度和加速度等。根据群体运动规律,车辆的速度满足 $v_i(t+1) = \langle v_j(t) \rangle$ 。其中, $v_i(t+1)$ 表示车辆 V_i 在 $t+1$ 时刻的速度,其值与半径 r 范围内所有相邻车辆 V_j 在 t 时刻速度的平均值 $\langle v_j(t) \rangle$ 一致。同样的,加速度也有类似的规律: $a_i(t+1) = \langle a_j(t) \rangle$,即车辆 V_i 在 $t+1$ 时刻的加速度 $a_i(t+1)$ 与半径 r 范围内所有相邻车辆 V_j 在 t 时刻加速度的平均值 $\langle a_j(t) \rangle$ 一致。

② 定义车辆与周围相邻车辆的相关度。

车辆在时刻 t 与相邻车辆的速度大小的相关度 $c_{ij}^{\text{abs}}(t)$ 为

$$c_{ij}^{\text{abs}}(t) = |v_i(t)| - |\langle v_j(t) \rangle| \quad (1a)$$

其中: $v_i(t)$ 为车辆 V_i 在时刻 t 的速度, $v_j(t)$ 为相邻车辆在时刻 t 的速度。车辆 V_i 在时刻 t 与相邻车辆的方向相关度 $c_{ij}^{\text{dir}}(t)$ 为

$$c_{ij}^{\text{dir}}(t) = v_i(t) \langle v_j(t) \rangle \quad (1b)$$

类似地,可以得到有关加速度大小和车辆行驶方向的相关度。

③ 定义相关度与信任值之间的映射关系。

相关工作将通过分析 $c_{ij}^{\text{abs}}(t)$ 和 $c_{ij}^{\text{dir}}(t)$ 的函数特征给出信任值 0 或 1。先将 $c_{ij}^{\text{abs}}(t)$ 的平均值定义为 $\text{avg}_{ij}^{\text{abs}}$, $c_{ij}^{\text{dir}}(t)$ 的平均值定义为 $\text{avg}_{ij}^{\text{dir}}$,再将平均值与指定阈值比较可以得出信任值,高于阈值则信任值

为 1,低于阈值则信任值为 0。

类似地,可以得到有关加速度相关度与信任值之间的映射关系。

2.2.3 信任聚合算法

在消息信任应用场景下,基于 EigenTrust 算法设计面向车联网领域的 EigenTrust-V 算法。在 EigenTrust 算法中,每个节点存储和计算所有节点的全局信任度,通过节点间局部信任值和全局信任度的查询与广播,采取不断迭代的方式,让全局信任度收敛到误差范围以内。文中结合车联网的自组网络拓扑特点,全局信任度的计算公式为

$$t_i^{(k+1)} = \sum_{j=1}^n c_{ji} t_j^{(k)} \quad (2)$$

其中: $t_i^{(k+1)}$ 为节点 V_i 在第 $k+1$ 次迭代时的全局信任度, c_{ji} 为 V_j 对节点 V_i 的局部信任度。式(2)将车联网中所有节点对节点 V_i 的局部信任度以全局信任度为权值进行加权求和,得到节点 V_i 的全局信任度。

研究表明,根据车联网环境需要 EigenTrust-V 算法将在以下 2 个方面进一步改进。

1) EigenTrust 算法考虑向网络中所有节点交换局部和全局信任度,但是在车联网环境中,只有少数的节点处于活动状态,即式(2)中许多分量为 0,为了提高计算速度,节省系统资源, EigenTrust-V 算法设置了参与运算的节点数。

2) EigenTrust 算法通过分布式散列表来确定管理节点,但是在车联网中,由于本身就存在可信性而且可用的 RSU 节点, EigenTrust-V 算法直接将 RSU 设置为管理节点和可信任节点,从而提高信任计算的效率。

在行为信任应用场景下,信任聚合算法的输入为信誉记录,即车辆相遇不断生成的直接或间接经验,这些记录具有实时性。车辆每次相遇相当于进行了贝叶斯方法中的一次随机实验,输出为每个车辆的信任记录。算法处理的过程如下:

① 定义信誉记录的数据结构。车辆之间的每次交互事件产生如下的信誉记录:

$r(\text{trustor}, \text{trustee}, \text{postion}, \text{timestamp}, \text{reputation_value})$ 。其中, trustor 表示给出信任值的车辆, trustee 表示受评估的车辆, position 表示事件发生的位置, timestamp 表示事件发生的时间, reputation_value 表示信任评估算法计算得到的信任值。

② 建立信任度假说和前置信任度。假设 $\theta \in [0, 1]$, θ 表示车辆的信任度, θ 的概率由参数决定。

将任意2个车辆之间的每次交互当成一次随机实验,车辆之间的交互可以看作伯努利实验.根据贝叶斯方法,假设 θ 服从Beta分布,则前置信任度为

$$P(\theta|\alpha, \beta) = \frac{\theta^{\alpha-1}(1-\theta)^{\beta-1}}{B(\alpha, \beta)} \quad (3a)$$

其中 α 和 β 是决定概率密度函数的参数,由历史数据归纳而得. α 为车辆信任值等于1的次数, β 为信任值等于0的次数.历史数据越多,得到的 θ 的分布越准确.由式(3b)(3c)可以得到 θ 的均值 μ 和标准差 σ .

$$\mu = \frac{\alpha}{\alpha + \beta} \quad (3b)$$

$$\sigma = \sqrt{\alpha\beta / \{(\alpha + \beta)^2(\alpha + \beta + 1)\}} \quad (3c)$$

③ 计算后置信任度.随着数据不断的累积,每个车辆的信任值得到不断的修正.在历史数据的基础上,新的数据 (n, N) 对信任度进行更新, n 为新数据中车辆信任值为1的个数, N 为所有随机实验的次数,更新的后置信任度为

$$P(\theta|\alpha, \beta, n, N) = \frac{P(n, N|\theta)P(\theta|\alpha, \beta)}{P(n, N)} \quad (4)$$

随着越来越多的车辆相遇记录在车联网中累积,新的证据不断产生,信任聚合算法可以对车辆信任度做出实时而精确的描述.

2.2.4 信任决策方法

面向多应用场景的车联网信任模型不仅要实时而精确地提供信任值,还要能激励个体在进行信任决策时做出对自身和整个车联网都有利的行为,达到提高应用通信安全和保障车辆行为安全的目的.因此,下面将研究基于博弈理论的信任决策方法及其影响.

传统的信任决策方法根据个体的信任度为其授予或撤销一定的权限,实现对个体的奖励或惩罚,缺乏从系统的角度描述个体决策合理性的研究.笔者概括出使用VCG激励相容机制实现车联网信任模型的优化决策,从博弈论的角度研究如何构造一个信任决策机制,实现推荐者的个体效用与整体车联网效率的一致性,设计的社会选择函数和支付函数应该满足下列要求.

1) 社会选择函数为

$$a = f(w_1, \dots, w_n) \in \arg \max_{a \in A} \sum_i w_i(a) \quad (5a)$$

其中: a 为车联网整体状态; A 为车联网整体状态的集合; w_1, \dots, w_n 为单个车辆的决策; f 为社会选择函数,表示车辆个体决策导致的车联网状态;估值函数

$w_i(a)$ 表示车辆 V_i 当车联网状态为 a 时获得的好处.社会选择函数使车联网通信效率和交通安全达到最大化.

2) 支付函数为

$$p_i(w_1, \dots, w_n) = \max_{b \in A} \sum_{j \neq i} w_j(b) - \sum_{j \neq i} w_j(a) \quad (5b)$$

其中 $p_i(w_1, \dots, w_n)$ 表示单个车辆决策为 w_1, \dots, w_n 时车辆 V_i 的支付函数,即车辆 V_i 的损失. W_1, \dots, W_n 分别对应单个车辆的决策集,对所有车辆的决策 $w_i \in W_i, \dots, w_n \in W_n$,车辆支付函数规定每个车辆必须支付当它参与和不参与时,其他车辆的社会财富之差,即车辆加入或不加入车联网对车联网状态的影响.

这种决策机制可以激励车辆的决策行为,使其符合社会群体选择的结果,促进所有车辆达到稳定的Nash均衡,同时整个车联网的安全性能也会随车辆个体行为的协作而提升.

2.3 量子通信环境下的车联网认证机制和信任模型

笔者拟将车联网的认证机制和信任模型从当前通信环境推演拓展到量子通信环境,主要研究量子门限匿名认证机制和量子信任决策机制.量子门限匿名认证机制拟使用纠缠交换和量子酉变换的同态特性完成对任意车辆节点的合法性认证;通过门限机制实现对任意 t 个合法车辆节点的联合追踪,识别欺骗车辆节点真实身份.量子信任决策机制将车辆节点的属性作为量子概率幅进行量子并行计算,建立节点与节点之间、节点与攻击者之间的演化博弈量子变换矩阵,体现车辆节点行为的有限理性和选择信任策略的模仿性,使用量子搜索算法寻找车辆节点信任演化稳定策略.

针对研究量子门限匿名认证机制和量子信任决策演化这2种机制的具体研究技术路线如下.

2.3.1 量子门限匿名认证机制

拟建立量子门限匿名认证机制,该机制能对任意车辆节点的合法性进行认证,而不暴露车辆节点的身份.通过门限机制实现任意 t 个合法节点可联合追踪被认证车辆节点的身份,达到匿名的门限追踪恶意节点的效果,从而保障车联网中用户的隐私安全.量子门限匿名认证机制的初步设计步骤如下.

1) 份额的分发和身份注册

在系统初始化参数设置的阶段,考虑一个可信

任中心 TC,一个部署在道路两旁或十字路口的路边单元 RSU,一个由 n 个车辆节点单元 OBU 组成的集合 $O = \{OBU_1, OBU_2, \dots, OBU_n\}$. 可信任中心 TC 负责管理所有的 RSU 和 OBU,RSU 负责管理 n 个车辆节点单元,可信任中心 TC 和 RSU 都是可信任度高的实体.

车辆节点单元的注册过程如图 11 所示. 在图 11 中,可信任中心 TC 首先将一个秘密信息 S 分成 n 个份额 $y_i (i = 1, 2, \dots, n)$, 给每个车辆节点单元 OBU_i 分发一个秘密份额,第 i 个车载节点单元 OBU_i 拥有第 i 个秘密份额 $y_i (1 \leq i \leq n)$;然后 TC 使用一个 Hash 函数计算秘密信息 S 的 Hash 值 $H(S)$,并将这个 Hash 值 $H(S)$ 发送给 RSU. n 个车辆节点单元中的每个节点单元将自己的身份信息 $ID_i (i = 1, 2, \dots, n)$ 发送给 RSU,作为初始注册信息.

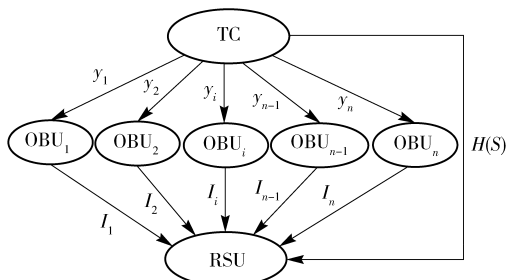


图 11 份额分发和身份注册过程

2) 匿名身份认证

① n 个纠缠对中 n 个粒子的分发过程如图 12 所示. RSU 运行纠缠粒子生成算法构造 n 个纠缠粒子对 $|\psi_i\rangle_{12} (i = 1, 2, \dots, n)$, 每个粒子是一个 q 维量子态. RSU 将每个纠缠粒子对中的其中一个粒子分发给一个 OBU,另外一个粒子自己保留.

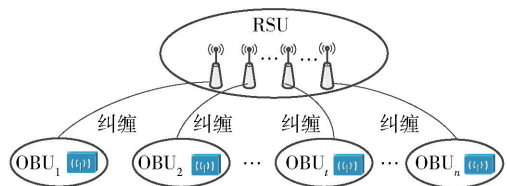


图 12 纠缠粒子的分发过程

② t 个车辆节点单元量子酉变换 $U(\cdot)$ 过程. 假定 n 个车辆节点的集合 $O = \{OBU_1, OBU_2, \dots, OBU_n\}$, 其中由 t 个车辆节点单元组成门限匿名追踪子集合 $\gamma = \{OBU_1, OBU_2, \dots, OBU_t\}$. 每个车辆节点单元 $OBU_j (j = 1, 2, \dots, t)$ 对自己手中的粒子进行量子酉变换 $U(\cdot)$, 其中, 在 $U(\cdot)$ 中输入 OBU_i 的秘密份额 y_i 和身份信息 ID_i .

③ $2t$ 个粒子纠缠交换认证过程. 纠缠交换之后,RSU 中的 t 个粒子的纠缠态中包含 $OBU_j (j = 1, 2, \dots, t)$ 的秘密份额 y_i 和身份信息 ID_i 同态运算值. RSU 将计算出 Hash 值 $H(S')$, 与 TC 传输给它的 Hash 值 $H(S)$ 进行比对,如果相等,认证通过. 量子酉变换 $U(\cdot)$ 之后, t 个车辆节点单元 $OBU_j (j = 1, 2, \dots, t)$ 取出手中的 $|\psi_j\rangle_2 (j = 1, 2, \dots, t)$ 粒子进行联合测量,RSU 手中对应的 t 个粒子 $|\psi_j\rangle_1 (j = 1, 2, \dots, t)$ 将坍塌到纠缠态,如图 13 所示,展示了 $2t$ 个粒子纠缠交换之后的状态.

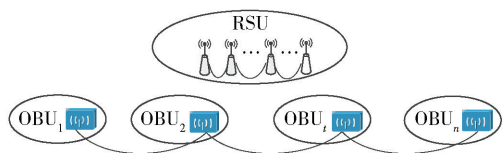


图 13 $2t$ 个粒子纠缠交换之后的状态

3) 被认证者的身份追踪

在已知 t 个秘密份额 $y_r (r = 1, 2, \dots, t)$ 的情况下,对于任意 t 个节点单元组成门限匿名追踪子集合 $\gamma = \{OBU_1, OBU_2, \dots, OBU_t\}$, 由拉格朗日插值公式可恢复出 S :

$$S = f(0) \equiv \sum_{r=1}^t y_r \prod_{\substack{j=1 \\ j \neq r}}^t (-x_j/x_r - x_j) \bmod p$$

在该公式中,在上述的认证过程中,如果 Hash 值的比对不相等,说明其中一个或者多个 OBU 提供了假的秘密份额或身份信息. 此时,RSU 请求 TC 合作找出欺骗者,能追踪出 OBU 的真实身份. 该过程依赖于 TC 和 RSU 都是可信的合作实体.

2.3.2 量子信任决策演化机制

新的研究内容应主要针对车联网信任模型中的信任决策,设计量子信任决策演化机制,在车联网节点中建立理性的信任决策. 车辆节点不是一开始就能找到最优策略,它们会在博弈过程中不断调整,通过模仿与试错寻找较好的动作策略. 量子信任决策演化机制的拟初步设计步骤如下.

1) 构建车辆节点理性博弈模型

车联网节点信任建立过程中表现出有限的理性行为,它们会在博弈过程中不断调整自己的动作策略. 车联网中任意 2 个具有有限理性的车辆节点间的一次消息或行为交互是一次博弈. 定义车辆节点博弈包括 4 个基本要素.

① 博弈的参与者:车联网中的所有车辆节点.

② 车辆节点的策略空间:车辆节点的信任评

级,如可信或不可信。

③ 博弈的次序:博弈中各博弈方的车辆行为顺序将极大地影响博弈的结果。相同的博弈方和策略空间同时决策行动和先后决策行动的结果完全不同。

④ 博弈方的收益:当博弈方的策略实施结束后,车联网节点之间每次博弈的收益,指获取资源或获得奖励等。

在定义的车联网中博弈基本要素的基础上,构建的车辆节点理性博弈模型由一个四元数组 $G(P, N, S, U)$ 的博弈组成。其中, P 表示由 n 个车辆节点组成的一个车联网, N 表示由车辆节点构成的个体集合 $\{N_1, N_2, \dots, N_n\}$, S 表示可供车辆节点选择的策略集合 $\{s_1, s_2, \dots, s_n\}$, U 表示 2 个车辆节点在博弈一次后得到的收益形成的支付矩阵。

2) 设计量子多属性信任决策演化机制及多属性信任决策算法

考虑一个具有 n 个节点的车联网,将这 n 个节点之间的信任关系形成的车联网表示成一个 $n \times n$ 的矩阵 A 。可供车辆节点选择的信任策略 $s_i \in \{0, 1\}$, 1 表示信任, 0 表示不信任。矩阵 A 中元素 $a_{ij} = 1$ 表示节点 i 到节点 j 之间有一条弧,用量子形式来表示 A 中的元素为 $a_{ij} = \alpha_{ij}|0\rangle + \beta_{ij}|1\rangle$ 。其中, α_{ij} 是 0 的概率为 $|\alpha_{ij}|^2$, β_{ij} 是 1 的概率为 $|\beta_{ij}|^2$, 且 $|\alpha_{ij}|^2 + |\beta_{ij}|^2 = 1$ 。

某个具体的车辆节点 N_i , 该节点的属性集为 $NB_i = \{b_{i1}, b_{i2}, \dots, b_{im}\}$ 时,该节点的量子态信任决策演化过程如图 14 所示。

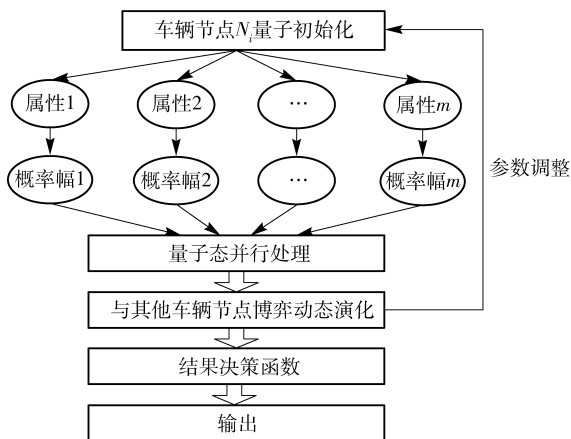


图 14 量子信任决策演化流程

将车辆节点 N_i 的属性做量子并行计算,建立与其他节点或攻击者的演化博弈算子,使用量子搜索

算法找出最优解,将博弈均衡点所获得的聚合信任值输入结果决策函数,输出决策结果。

3 相关技术安全性评估分析和展望

3.1 针对相关技术的安全性评估

针对多通信场景(车—TC、车—车厂、车—RSU、车—车)对认证和信任服务在安全性方面的差异性需求,从可抵抗的网络攻击,如中间人攻击、合谋攻击、隐私泄露、重放攻击、篡改攻击、口令猜测、恶意车辆节点检测等,分析前面勾画概括出的认证机制和信任模型的安全性。

3.1.1 当前通信环境下的安全性分析

设计的身份认证协议在会话内容中预先基于双线性映射理论构造临时加密安全参数 Λ_i 作为挑战码,属性认证协议则通过为车辆节点分配固定属性集和动态属性集设计认证策略,基于双线性映射理论和拉格朗日插值共同构造属性密钥和加密算法,攻击者构造临时会话密钥 $SK = g(H_1(e(r_r P_r, P_{pub})r^i))$ 和解密组件 $e(g, g)^{\alpha_s} = e(SK_w, \tilde{C})/e(C_w, C_m)$ 将面临基于计算 Diffie-Hellman 问题假设的计算困难性问题,从而有效避免车辆认证过程中的中间人攻击与合谋攻击。在车辆节点每次开启认证会话前,便随机动态构造匿名身份 AID_i , 在认证协议交互过程中,不涉及口令的使用,所携的交互内容均标识随机数 r_i 和当前时间戳 t_i 确保消息的唯一性和新鲜性,并结合具有抗碰撞攻击、雪崩效应以及计算单向性特点的 Hash 函数构造聚合消息认证码 tag_i , 从而避免认证过程中的隐私泄露,以及攻击者的口令猜测攻击、重放攻击和篡改攻击。此外,信任模型通过车辆的历史通信行为和运动行为计算车辆信任度,并将最新产生的行为记录快速地纳入计算过程中,从而不断地更新信任度 θ 的条件概率 $P(\theta|\alpha, \beta, n, N)$, 以达到实时性和精确性的要求。因此,信任模型能够实时地检测到具有异常行为的潜在恶意节点。在信任决策过程中建立了基于博弈理论的激励机制,促使单个车辆的决策符合车联网的群体选择,因此信任模型能够鼓励优秀节点并且抑制恶意节点。为了阻止恶意消息的传播,可以限制消息产生的频率以及计算信任度时来自不同车辆的历史记录的比例。为了防止短期滥用信任系统,可以调整时间窗口,并适当增加短期信誉记录的权重。笔者通过设计认证体系和信任模型,满足车联网的多种通信场景对安全性的个性化需求。

3.1.2 量子通信环境下的安全性分析

将车联网的认证机制和信任模型从当前通信环境拓展到量子通信环境,除了考虑经典随机预言模型的安全性外,进一步需要将构建的量子匿名门限认证和量子信任决策演化机制置于量子世界的随机预言模型(由美国斯坦福大学的 Boneh 研究团队构建)中,以证明它们在该模型下量子敌手查询的可证明安全性。笔者拟构建的量子匿名门限认证和信任决策演化机制除了自身的可证明安全性外,还能保证车联网系统如下的隐私安全。

在量子匿名门限认证机制中,首先,该机制能追踪恶意的车辆节点。TC、RSU 都是诚实的实体,当 OBU 给出不诚实的反馈信息产生纠纷时,由 TC 和 RSU 合作可以获取恶意 OBU 的身份信息,撤销该节点,从而保障车联网中用户的合法性。其次,该机制能抵抗中间节点发送虚假信息。假设攻击者在有限时间内只能捕获门限值以下单个或少量的车辆节点,在车联网中广播虚假的交通事件。但没有足够的车辆节点采集发布这一数据,导致中间节点认为它是少数节点发送的无效信息而不予转发,从而提高了中间节点抵抗虚假信息的能力。

在量子信任决策演化机制中,首先,该机制能减少车辆节点不诚实的反馈。由于使用演化博弈,车联网节点信任建立过程中表现出的有限理性决定了节点会在博弈过程中不断模仿与试错并寻找较好的动作策略。车联网信任博弈的均衡是不断调整和改进的过程,能减少车联网节点不诚实的虚假信息反馈。其次,该机制能减少车辆节点误导推荐信任。在车辆节点群组中多属性相互共享与交叉,当一个车辆节点提供交互经验信息时,其他车辆节点根据共享的该车辆节点的属性,可选择性判断信息的真假,减少误导推荐的发生。

3.2 技术挑战与未来展望

1) 面向多通信场景的认证机制

车联网环境下的认证机制是基于车辆、RSU 与 TC 等通信实体共同搭建的,在设计认证机制时需要考虑各单元的计算能力与通信方式,同时还需结合网络拓扑高动态性、车辆节点高移动性与节点通信瞬时性的特点。因此,如何满足各认证场景(车—TC、车—车厂、车—RSU、车—车)对安全性、隐私性和时效性的差异性需求,设计适用于不同场景的认证协议和方法实现对通信节点的差别认证是具有挑战性的难题。同时,该问题也是未来开展研究工作

的前提和基础。为有效地解决这个关键问题,进一步需要从以下 2 个方面开展研究工作。

其一,强调安全性的认证协议。复杂的认证协议所带来的时间开销将影响车辆节点接入网络时的认证速度,造成获取网络服务的延迟。未来将注重研究数学理论在认证过程中的应用,通过降低数据处理复杂度、减少认证会话中的交互过程和优化通信负载实现时间延迟容忍内的认证,构造强安全性的认证密钥以及签名验证算法,抵抗节点在认证会话中的假冒、篡改、伪造等攻击,为通信交互场景下的认证营造基础的安全环境。

其二,强调隐私性与时效性的认证策略。车联网环境中车—车、车—RSU 通信的临时性和自主性对此类场景下的认证提出了时效性与隐私性的要求,此外,通信场景中的实体与消息的认证需求也存在一定差异。因此,未来应该进一步从面向实体和面向消息 2 个层面,分别展开车辆属性认证方法和节点间通信消息认证方法的研究。车辆属性认证方法主要依靠基于属性的加密算法和相关技术,实现车—车和车—RSU 通信中一对多的动态认证,并通过优化认证策略和加密算法提升认证的扩展性和性能;节点间通信消息认证主要研究消息签名算法和消息验证方法,研究多跳转发消息的快速认证,进一步解决消息认证过程中用户隐私保护的问题。

2) 面向多应用场景的车联网信任模型

构建面向多应用场景的具备强实时性和高精确性的信任模型是增强车联网通信安全和保障交通安全的关键,相关的信任评估和信任聚合算法是构成信任模型的基础。在车联网环境下,车辆节点具有交互时间短、通信范围有限等特点。因此,为建立快速而准确的信任评估方法,需要分析和研究自组织网络条件下的信任聚合算法,需对信任度的管理节点、预设的信任节点以及参与计算的节点之间的协同度展开进一步研究。

车辆节点的行为属性具有实时和动态的特征,需要设计和实现具有强实时性、适应车联网行为信任场景的信任评估算法。相关研究工作将以车辆的实时运动状态信息为输入,利用群体运动模型研究车辆运动规律,设计能够精确地反映车辆行为内在特征的信任评估算法。此外,由于车联网通信环境的特殊性,如何降低算法的时空复杂度也是未来研究关注的问题。

车联网行为信任模型的基本要求是动态地反映

信任度的变化,实时而精确地表征车辆的当前信任度。如果将2个车辆之间的每次交互当成一次经验,则产生一个局部信任值。因此,未来研究工作应该利用全局信任度聚合算法分析车联网信任度的生成和变化规律,采用贝叶斯方法,由不断生成的局部信息在一定的时间窗口内聚合、更新全局信任度,随着经验的不断累积,车辆全局信任度也会更加精确。

3) 量子通信环境下的车联网认证和信任机制

将车联网的认证和信任机制拓展到量子通信环境中,与当前通信环境下的车联网认证和信任机制有着较大的区别,需要考虑量子态的叠加性、纠缠性、不可克隆性、量子的波粒二象性和测量坍塌性等基本特性。当数据量相当大时,需要相当多的相互合作的量子存储器来存储和计算这些量子态数据。因此,如何将经典的 (t, n) 门限匿名追踪算法用量子态表示和计算以及如何用量子演化矩阵来表示经典的演化博弈动力学方程是需要解决的关键问题,也是具有挑战性的难题。为有效地解决这些关键问题,应该进一步从以下2个方面开展研究工作。

其一,门限匿名认证的量子态表示。基于量子的基本特性,在量子行为向经典转变的过程中不存在清晰的界线或者临界的大小,而且模糊的边界自身也会随着测量的方式而变化。量子信息表示和计算需要具有一些不同于经典信息表示和计算的特性。进一步将重点研究秘密份额的分发和车辆身份注册、 (t, n) 门限身份认证、匿名追踪恶意车辆节点这些过程的量子态表示和计算问题。同时,拉格朗日插值多项式的量子态表示和计算是将要深入研究的重要问题。

其二,信任博弈的量子演化计算。量子通信环境下的信任模型与当前通信环境下的类似,也需要动态适应车辆行为和环境的实时变化,需要从多维属性的角度来做出信任决策。进一步将重点研究量子信任决策机制中车辆节点多个属性的量子并行计算,当多个节点之间存在交叉属性的情况下,多属性量子态的叠加表示和纠缠交换。同时,在节点与节点之间、节点与攻击者之间的信任博弈量子演化计算是将要深入研究的重要问题。

4 结束语

对无线、控制和计算机等技术的依赖,使车联网易遭受更复杂的网络攻击,如远程入侵、控制和轨迹追踪等,亟需有效的认证机制管理非法用户的访问。

当前车联网安全面临的主要问题是,复杂的通信环境使单一的认证机制无法满足不同场景对安全和服务质量的差异性需求。目前相关研究基本上还处于初期的探索阶段,要最终形成成熟的应用技术,还可能需要更具创新性的研究,或者大量细致的完善工作。在国内对车联网及其应用研究日渐重视的背景下,适时启动一些诸如面向复杂通信场景的安全认证机制和信任模型等关键支撑技术的研究课题是必要而且迫切的。笔者系统介绍了多通信场景下的车联网认证机制及信任模型相关技术挑战,结合技术需求总结提炼解决相关问题的研究新方向新内容,并对技术未来发展进行了研究展望。

参考文献:

- [1] Peng Huaxi. An identity-based authentication model for multi-domain[J]. Chinese Journal of Computers, 2006, 29(8): 1271-1281.
- [2] Li Jinglin, Liu Zhihan, Yang Fangchun. Internet of vehicles: the framework and key technology[J]. Journal of Beijing University of Posts and Telecommunications, 2014, 37(6): 95-100.
- [3] Suresh J S, Jongkun L. A TPM-based architecture to secure VANET[J]. Indian Journal of Science and Technology, 2015, 8(15): 215-234.
- [4] Sumra I A, Hasbullah H B, Bin J L, et al. Comparative study of security hardware modules (EDR, TPD and TPM) in VANET[C]//3th National Information Technology Symposium. Riyadh: Nits, 2011: 6-9.
- [5] He Debiao, Sherali Zeadally, Xu Baowen, et al. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(12): 2681-2691.
- [6] Zhu Hui, Pan Wenhui, Liu Beishui, et al. A lightweight anonymous authentication scheme for VANET based on bilinear pairing[C]//4th International Conference on Intelligent Networking and Collaborative Systems (INCoS). Bucharest: IEEE, 2012: 222-228.
- [7] Chuang M C, Lee J F. TEAM: trust-extended authentication mechanism for vehicular ad hoc networks[C]//International Conference on Consumer Electronics, Communications and Networks. Xianning: IEEE, 2011: 1758-1761.
- [8] Li Qiang, Feng Dengguo, Zhang Liwu. Enhanced attribute-based authenticated key agreement protocol in the standard model[J]. Chinese Journal of Computers,

- 2013, 36(10): 2156-2167.
- [9] Goyal V, Pandey O, Sahai A. Attribute-based encryption for fine-grained access control of encrypted data[C]//Proceedings of the 13th ACM Conference on Computer and Communications Security. Alexandria: ACM, 2006: 89-98.
- [10] Waters B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization [C]//Public Key Cryptography - PKC 2011. [S. l.]: Springer Berlin Heidelberg, 2011: 53-70.
- [11] Yeh L Y, Chen Yencheng, Huang Jiunlong. ABACS: an attribute-based access control system for emergency services over vehicular ad hoc networks[J]. IEEE Journal on Selected Areas in Communications, 2011, 29(3): 630-643.
- [12] Yeh L Y, Huang Jiunlong. PBS: a portable billing scheme with fine-grained access control for service-oriented vehicular networks[J]. IEEE Transactions on Mobile Computing, 2014, 13(11): 2606-2619.
- [13] Huang Dijiang, Verma M. ASPE: attribute-based secure policy enforcement in vehicular ad hoc networks [J]. Ad Hoc Networks, 2009, 7(8): 1526-1535.
- [14] Ruj S, Nayak A, Stojmenovic I. Improved access control mechanism in vehicular ad hoc networks[C]//Ad-hoc, Mobile, and Wireless Networks. [S. l.]: Springer Berlin Heidelberg, 2011: 191-205.
- [15] Rao Y S, Dutta R. Efficient attribute based access control mechanism for vehicular ad hoc network[C]//International Conference on Network and System Security. Springer Berlin Heidelberg: Springer, 2013: 26-39.
- [16] Zhou Jian, Zhou Xianwei. Anonymous shared certificate entity authentication protocol [J]. Wireless Personal Communications, 2013, 72(4): 2761-2772.
- [17] Mamun M S I, Miyaji A, Takada H. A multi-purpose group signature for vehicular network security[C]//International Conference on Network-Based Information Systems. Salerno: IEEE, 2014: 511-516.
- [18] Bayat M, Barmshoory M, Rahimi M. A secure authentication scheme for VANETs with batch verification[J]. Wireless Networks, 2015, 21(5): 1-11.
- [19] Shim, Kyung Ah. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks[J]. IEEE Transactions on Vehicular Technology, 2012, 61(4): 1874-1883.
- [20] Lee C C, Lai Yanming. Toward a secure batch verification with group testing for VANET[J]. Wireless networks, 2013, 19(6): 1441-1449.
- [21] Zhang Jianhong, Xu Min, Liu Liying. On the security of a secure batch verification with group testing for VANET [J]. International Journal of Network Security, 2014, 16(5): 351-358.
- [22] Li Jinguo, Lin Yaping. Secure anonymous authentication scheme based on elliptic curve and zero-knowledge proof in VANET[J]. Journal on Communications, 2013, 34(5): 52-61.
- [23] Van Danghai, Thuc N D. A privacy preserving message authentication code[C]//International Conference on It Convergence and Security. Kuala Lumpur: IEEE, 2015: 1-4.
- [24] Wei Zhexiong, Tang Helen, Yu F. Richard, et al. Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning[J]. IEEE Transactions on Vehicular Technology, 2014, 63(9): 4647-4658.
- [25] Tan Shuaishuai, Li Xiaoping, Dong Qingkuan. Trust based routing mechanism for securing OSLR-based MANET[J]. Ad Hoc Networks, 2015, 30(3): 84-98.
- [26] Yao Xuanxia, Zhang Xinlei, Ning Huansheng, et al. Using trust model to ensure reliable data acquisition in VANETs[J]. Ad Hoc Networks, 2016, 55(4): 107-118.
- [27] Cho Jin-Hee, Chen Ing-Ray, et al. PROVEST: a provenance-based trust model for delay tolerant networks [J]. IEEE Transactions on Dependable and Secure Computing, 2012, 14(6): 99-114.
- [28] Wu Qiwu, Liu Qingzi. Trusted model of secure routing for VANET based on bayesian theory[J]. Journal of Sichuan University (Engineering Science Edition), 2015, 47(2): 129-135.
- [29] Xia Nu, Li Wei, Lu You, Jiang Jian, Shan Feng, Luo Junzhou. A trust model for the inter-domain routing system[J]. Journal of Computer Research and Development, 2016, 53(4): 845-860.
- [30] Jiang Liming, Zhang Kun, Xu Jian, Zhang Hong. A new evidential trust model based on graph theory for open computing systems[J]. Journal of Computer Research and Development, 2013, 50(5): 921-931.
- [31] Vicsek T. A question of scale[J]. Nature, 2001, 411(6836): 421-431.
- [32] Vicsek T, Zafeiris A. Collective motion[J]. Physics Reports, 2012, 517(3-4): 71-140.
- [33] Vicsek T. Universal patterns of collective motion from minimal models of flocking [C]//Proceedings - 2nd IEEE International Conference on Self-Adaptive and

- Self-Organizing Systems, SASO 2008. Venice: IEEE, 2008: 3-11.
- [34] Shi Weimin, Zhou Yihua, Yang Yuguang. Quantum deniable authentication protocol[J]. Quantum Information Processing, 2014, 13(7): 1-10.
- [35] Hao Yuan, Liu Yimin, Pan Guozhu, et al. Quantum identity authentication based on ping-pong technique without entanglements[J]. Quantum Information Processing, 2014, 13(11): 2535-2549.
- [36] Chen Yongzhi, Wen Xiaojun. Quantum identity authentication with zero knowledge[J]. Chinese Journal of Quantum Electronics, 2015, 32(2): 156-160.
- [37] Dong Yingdi, Peng Jinye, Zhang Xiaobo, Zhang Zhenlong. Quantum identity authentication scheme based on measurement-device-independent quantum key distribution protocol[J]. Journal on Communications, 2016, 37(2): 151-156.
- [38] Brickell Ernie, Camenisch J, Chen Liqun. Direct anonymous attestation[C]//ACM Conference on Computer and Communications Security ACM. Washington: ACM, 2004: 132-145.
- [39] Brickell Ernie, Chen Liqun, Li Jiangtao. Simplified security notions of direct anonymous attestation and a concrete scheme from pairings[J]. International Journal of Information Security, 2009, 8(5): 315-330.
- [40] Brickell Ernie, Li Jiangtao. Enhanced privacy id: a direct anonymous attestation scheme with enhanced revocation capabilities[C]//ACM Workshop on Privacy in the Electronic Society (WPES 2007), Alexandria: ACM, 2007: 21-30.
- [41] Chen Liqun, Ng S L, Wang Guilin. Threshold anonymous announcement in VANETs[J]. IEEE Journal on Selected Areas in Communications, 2011, 29(3): 605-615.
- [42] Calandriello G, Papadimitratos P, Hubaux J P, et al. On the performance of secure vehicular communication systems[J]. IEEE Transactions on Dependable & Secure Computing, 2012, 8(6): 898-912.
- [43] Li Qiang, Chen Minyou, Perc M, et al. Effects of adaptive degrees of trust on coevolution of quantum strategies on scale-free networks[J]. Scientific Reports, 2013, 3(42): 2949-2956.
- [44] Yukalov V I, Sornette D. Quantum decision theory as quantum theory of measurement[J]. Physics Letters A, 2009, 372(46): 6867-6871.
- [45] Ashtiani M, Azgomi M A. A formulation of computational trust based on quantum decision theory[J]. Information Systems Frontiers, 2016, 18(4): 735-764.
- [46] Chen Feifei, Gui Xiaolin. Research on dynamic trust-level evaluation mechanism based on machine learning[J]. Journal of Computer Research and Development, 2007, 44(2): 223-229.
- [47] Lin Chuang, Wang Yuanzhuo, Yang Yang, Qu Yang. Research on network dependability analysis methods based on stochastic petri net[J]. Acta Electronica sinica, 2006, 34(2): 322-332.
- [48] Li Xiaoyong, Gui Xiaolin. Trust quantitative model with multiple decision factors in trusted network[J]. Chinese Journal of Computers, 2009, 32(3): 405-416.
- [49] Shen Shigen, Ma Xuan, Jiang Hua, Li Wei, Cao Qiyang. Evolutionary game theory based trust strategy model and dynamics analysis in wireless sensor networks[J]. Control and Decision, 2012, 27(8): 1133-1138.
- [50] Wei Zhiqiang, Zhou Wei, Ren Xiangjun, et al. A strategy-proof trust based decision mechanism for pervasive computing environments[J]. Chinese Journal of Computers, 2012, 35(5): 871-882.