基于信誉积分的路况信息共享中共谋攻击节点检测方法

玄世昌，汤浩，杨武
（哈尔滨工程大学信息安全研究中心，黑龙江 哈尔滨 150001）

摘 要：针对车联网中共谋节点可能协同发布虚假路况信息，导致路况信息共享过程中消息真实性无法保证的问题，提出了一种基于信誉积分的路况信息共享中共谋攻击节点检测方法。在路况信息聚合过程中，设计了恶意信息检测算法，能够检测到共谋节点发布的虚假消息，保证系统中传递消息的真实准确。安全性评估和实验表明，相比于现有方案，该方法对共谋节点的检测效率更高，共谋节点数量占比适应场景更广泛。

关键词：车联网；路况信息共享；区块链；共谋攻击
中图分类号：TP39
文献标识码：A
DOI: 10.11959/j.issn.1000−436x.2021051

Method for detecting collusion attack node in road condition information sharing based on reputation point

XUAN Shichang, TANG Hao, YANG Wu
Information Security Research Center of Harbin Engineering University, Harbin 150001, China

Abstract: Aiming at the problem that on occasion of the release of false road condition information by collusion nodes in the Internet of vehicles collaboratively, message authenticity could not be guaranteed in the process of road condition information sharing, a method for detecting collusion attack nodes in road condition information sharing based on reputation points was proposed. In the process of road condition information aggregation, a malicious information detection algorithm was designed to detect false messages issued by colluding nodes, which could ensure the authenticity and accuracy of messages delivered in the system. Experimental results show that the proposed method has higher detection efficiency for collusion nodes and adaption to a proportion of collusion nodes through security evaluation and experiments in comparison with the existing schemes.

Keywords: Internet of vehicles, road condition information sharing, blockchain, collusion attack

1 引言

随着智慧城市的兴起和交通压力的增长，融合了移动边缘计算技术和车辆自组织网络（VANET, vehicular ad-hoc network）的车联网（IoV, Internet of vehicles）受到了学术界的广泛关注。目前，城市中已经部署了许多车联网服务。例如，实时交通信息服务可以为用户更好地规划出行路线，避免交通堵塞；天气信息共享服务可以为用户规划出行时间。这些服务都需要依靠道路中的车辆共享数据作为基础支撑。

因为共享的数据（如位置信息等）可能存在隐私泄露的风险，所以在车联网中通常对用户的信息进行假名转换和管理。但是，这种方法也为网络中可能存在的恶意节点提供了掩护，导致网络中容易出现共谋攻击。攻击者在网络中部署大量恶意的节

收稿日期：2020−09−16；修回日期：2021−02−05
通信作者：杨武，yangwu@hrbeu.edu.cn
基金项目：国家自然科学基金资助项目（No.61802086, No.U20B2048）；中央高校基本科研业务费专项资金资助项目（No.3072020CF0601）
Foundation Items: The National Natural Science Foundation of China (No.61802086, No.U20B2048), The Fundamental Research Funds for the Central Universities (No.3072020CF0601)

点进行共谋攻击。这些恶意节点不仅可以依靠真实的身份信息伪装为可信节点，还可以通过互相掩护共享虚假的路况信息。这些恶意节点通常具有更高的性能，往往会成为网络中的洪泛节点，并被更多的节点加入快速节点池中，从而进一步增加了参与共享过程的可能性。显然，如果存在多个恶意节点，将很难保证实时路况信息共享的正确性。

车载自组织网络在信息安全和隐私保护方面需要满足以下 5 个要求。1) 认证：每个身份都必须得到保证和验证，此外，每个有效的消息都必须得到保证。2) 完整性和正确性：在传输过程中，必须保证数据不被修改或丢弃，发送方的地理数据必须准确，避免接收方被误导。3) 不可否认性：发送方不能否认数据的操作。4) 隐私性：真实身份不能通过数据直接链接，具有一定的匿名性。5) 效率：在上述条件下，必须达到一定的处理能力。

区块链技术在 2008 年首次被提出[1]。区块链可以被视为一个公共分类账，所有提交的交易都存储在一个区块链中。区块链技术具有分散性、安全性、匿名性和可审计性等关键特征。该技术能以较低的成本实现车联网的安全、隐私保护和信任建立等服务，并能够有效地解决路况信息共享时产生的共谋攻击问题。

本文首先介绍了区块链和车联网的概念；其次，总结了研究人员将区块链技术应用到车联网场景中的工作进展；再次，设计了一种基于信誉积分的路况信息共享中共谋攻击节点检测方法；最后从理论分析和实验验证两方面对该方法进行了分析。

2　相关工作

2.1　区块链技术

近年来，加密货币引起了工业界和学术界的广泛关注。比特币通常被认为是第一种加密货币。区块链技术是比特币的核心机制。区块链技术由于其在加密货币中的应用而被认可，但是区块链技术的可应用领域不局限在加密货币中。由于区块链技术允许在没有任何银行或中介机构的情况下完成支付，因此可以用于各种金融服务，如数字资产、汇款和在线支付等[2]。此外，区块链技术正在成为下一代互联网系统中最受关注的技术之一，例如智能合约[3]、公共服务[4]、物联网（IoT, Internet of things）[5]和声誉系统[6]。

区块链技术具有以下关键特征。

1) 分散性。在传统的集中交易系统中，每一笔交易都需要通过中央受信机构（如中央银行）进行验证。这必然导致中央服务器的成本和性能瓶颈。不同的是，区块链网络中的交易可以在任何 2 个对等点（P2P, peer-to-peer）之间进行，而不需要中央机构的认证。所以，区块链技术可以显著降低服务器成本（包括开发成本和运营成本），缓解中心服务器的性能瓶颈。

2) 安全性。区块链网络中传播的每一笔交易都需要确认并记录到网络中每一个节点所存储的数据块中，因此，几乎不可能被篡改。此外，每个广播块将由其他节点验证并检查，所以任何伪造都很容易被发现。

3) 匿名性。每个用户都可以使用自己生成的地址参与区块链网络的交互。用户可以通过生成多个地址来避免身份暴露。但是，由于固有的限制，区块链无法提供完美的隐私保护。

4) 可审计性。由于区块链上的每一笔交易都在验证后记录到区块中，用户可以通过访问分布式网络中任何节点的区块链数据来验证和跟踪以前的交易记录。例如，在比特币中，每一笔交易都可以迭代追踪到之前的全部交易。这提高了区块链中数据的可追踪性和透明度。

2.2　路况信息共享

车联网的理想目标是实现人车物环境的深度融合，降低社会成本，提高运输效率和城市服务水平。

近年来，物联网、云计算和大数据技术的发展，催生了大量的服务和应用程序。其中的数据资源已成为最有价值的资源。在车联网应用中，车辆、用户的大规模交通数据共享方法，已经成为备受关注的研究热点。

车联网的数据可以分为 3 种类型：车辆数据、用户数据和环境数据。

1) 车辆数据。车辆数据包括车辆使用数据（车速、里程、行驶路段/时间/方向/频次、单次行驶/拥堵/畅行时长等）、性能数据（发动机转速、油耗、百米加速等）、工况数据（蓄电池/电机/发动机状态、主缸压力、ABS 状态、EBD 状态、ESP 状态、牵引力控制系统状态、告警信息等）。

2) 用户数据。用户数据包括用户操控数据（加速、制动、驻车、远近光/雾灯/位置灯、方向盘转

角/转速等）、用户画像数据（地址、行程分析、常用路线、不良行为分析、活动范围等）。

3) 环境数据。环境数据包括天气、路况、道路类型/限速/拥堵等情况。

有了这些详细的数据，车辆可以知道车主的用车习惯以及车况状态，其中包括车辆的运行状态、行为轨迹等信息。这将有助于政府相关部门对交通进行调度和车企有针对性地对产品、技术和服务等进行改良升级。

2.3 区块链在路况信息共享中的应用

将区块链技术应用到车联网中，可以安全、可信地记录车辆的全部数据，从而解决车辆数据诚信问题。

区块链可接入汽修汽配、车辆管理、汽车制造商、汽车租赁、保险等众多机构。智能合约能够实现交易的自动执行。车辆与车辆之间、车辆与人之间、车辆与服务商之间等使用区块链技术来保护分享的数据，从而提高驾驶的安全性和服务商管理的效率。由于区块链分布式存储的数据具有不可篡改性，使用车辆唯一识别码（VIN, vehicle identification number）作为唯一账号接入区块链网络时，车辆的违章、故障、交通事故等信息可以被永久记录，实现证据的固化，从而解决车辆数据诚信问题。用户可将车联网设备行车期间的车内外数据分享给第三方，使诚信数据产生价值，让用户获利。

目前，已经展开了一些将区块链技术应用到路况信息共享中的研究工作。

2.3.1 使用区块链技术激励用户参与共享路况信息

在路况信息共享场景中，吸引大量优质用户参与进来是比较困难的。

Yang 等[7]提出了一种基于区块链的车辆网络分散信任管理方案。在该方案中，每辆车首先根据接收到的消息为其相邻的车辆生成一个评级，然后将评级结果上传到所连接的路边单元（RSU, road side unit）。根据车辆的评级结果，每个 RSU 计算其所涉及车辆的信任值，并将这些数据打包成一个块。工作量证明（PoW, proof of work）和权益证明（PoS, proof of stake）作为协商一致的机制用于将块添加到区块链中。每个车辆都可以很容易地从 RSU 获得其他车辆的信任值，从而能够评估接收到其他车辆共享消息的可信度。

Li 等[8]提出了一种基于区块链的激励车辆公告网络 CreditCoin。该网络通过声誉点数（即金币）来激励车辆分享与道路相关的信息。

在共享路况信息的过程中，只有一套完善的激励策略是不够的，还需要关注共享路况信息网络环境中的安全因素。

2.3.2 使用区块链技术解决共享路况信息中的安全性问题

车辆之间共享道路相关信息（如事故、交通拥堵等路况信息），可以提高交通效率。然而，由于网络中车辆的高机动性和交通条件动态性等特殊限制，车辆之间往往不能充分信任。由于恶意车辆共享的不准确信息会对交通安全和效率产生不良影响。因此，在非可信环境下，有必要设计一种有效的车辆网络信任管理机制。随着智能车辆的快速部署，使用完全可信的集中实体管理大量车辆是不切实际的。在这种情况下，分散系统对于信任管理更有效。区块链的分散化、透明性和不变性使其成为分散化信任管理系统的理想选择。

Lu 等[9]提出了一种面向车联网的基于区块链的信任管理系统（BARS, blockchain-based nonymous reputation system），并提出了一种信誉评分机制，根据区块历史上的消息来确定车辆的可信度；Malik 等[10]提出了一种使用区块链的车联网认证和撤销框架。这些系统设计保护了车辆的隐私，但没有解决通信安全问题。Singh 等[11]提出了一种基于区块链的加密信任点，用于车辆之间的安全数据共享。类似地，Sherstha 等[12]讨论了为车联网提供的基于区块链的消息发布服务。尽管这 2 种解决方案都提供了良好的车辆通信安全性，但它们都没有解决相关的隐私问题。Zhang 等[13]的方案强调了车联网产生的数据量，以及移动边缘计算在抵消基于区块链的车联网的资源消耗方面的重要性，该方案有助于减少区块链的计算开销，但移动边缘计算的引入并没有使其真正去中心化。

此外，Singh 等[14]提出了一种基于奖励的车辆通信机制 TrustBit，并使用区块链与唯一加密 ID 的安全通信和奖励系统。Zhang 等[15]介绍了一种基于区块链的车联网数据共享和存储安全平台，但是该平台会产生额外的开销。Khelifi 等[16]提出了区块链在车联网中用于安全数据网络缓存的方法。Lei 等[17]讨论了一种使用区块链技术的异构智能交通系统的动态密钥管理方案。

尽管上述系统为车辆通信提供了良好的安全性，但它们未能保护车辆的隐私。如果产生隐私泄

露，可能会使人处于潜在的风险中。为了解决车辆在共享路况信息中存在的共谋攻击，Feng 等[18]提出了交通信息交换中抗内外合谋攻击（TFAA, traffic messages exchange against inside and outside collusive attack）方案。TFAA 方案试图解决共享路况信息过程中由信任漏洞带来的共谋攻击，并通过实验验证了 TFAA 方案的准确性和有效性。但是从文献[18]的设计机制可以看出，TFAA 方案在恶意节点数量占比超过 50%的情况下并不适用。

路况信息共享过程中，真实性是基础。然而，由共谋攻击带来的路况信息真实性问题的研究工作目前还处于起步阶段。现有的解决方法因为机制的局限，不能适用于共谋节点数量占比较多的情况。针对以上问题，本文提出了一种基于信誉积分的路况信息共享中共谋攻击节点的检测方法。

3　共谋节点检测方案

在一个典型的路况信息共享方案中，首先由道路上行驶的车辆将其行驶数据上传到 RSU；其次由 RSU 通过聚合多台车辆的行驶数据得到当前道路的路况信息，并将当前道路的路况信息广播到区块链网络中。在这个过程中，可能存在一部分恶意节点。这些节点具有真实身份，它们可以合谋将一个假的路况信息上传到区块链中。区块链中的路况信息可以被用来估测道路的拥堵。因此，虚假的路况信息会给需要依赖路况信息做分析的服务造成很大影响，并对道路上的司机造成误导，甚至给道路造成安全隐患。本文针对车联网共享路况信息存在恶意节点的场景，设计了一种有效的抗共谋攻击的方法（MDCA-RP, method of detecting collusion attack node based on reputation point）。

3.1　系统模型

一个典型的车联网共享路况信息的场景由注册服务器、共识节点（CN, consensus node）、RSU 和车辆组成，如图 1 所示。

1) 注册服务器。注册服务器为车辆提供在网络中所需要的一个或者多个虚拟的身份信息。服务器在完成假名注册后，会在区块链网络中广播假名地址。

2) 共识节点。共识节点将发送到网络中的路况信息打包并生成一个新的区块，再经过共识算法验证该区块的合法性后将区块上链。每个共识节点只负责一个区域的共识。

3) RSU。RSU 是车辆参与共享路况信息过程中的媒介，负责每条道路实时信息的聚合与上传工作。在进行路况信息聚合的过程中，RSU 需要进行恶意节点识别。

4) 车辆。在整个车联网共享路况信息的过程中，车辆是终端实体。

在 MDCA-RP 中，需要进入网络的车辆要先到注册服务器中进行用户信息注册。注册阶段注册服务器会为车辆生成一定数量的假名信息。注册服务器会将这些假名信息返回给车辆进行存储，同时也会将这些假名信息中的地址信息公布到区块链网络中。

车辆有了假名信息后就可以参与路况信息聚合。车辆在道路中将采集的实时信息共享给 RSU。RSU 在对实时信息进行聚合的阶段，会对实时信息和车辆的信誉积分进行分析，其中，信誉积分需要 RSU 从区块链中进行获取，从而对车辆节点进行恶

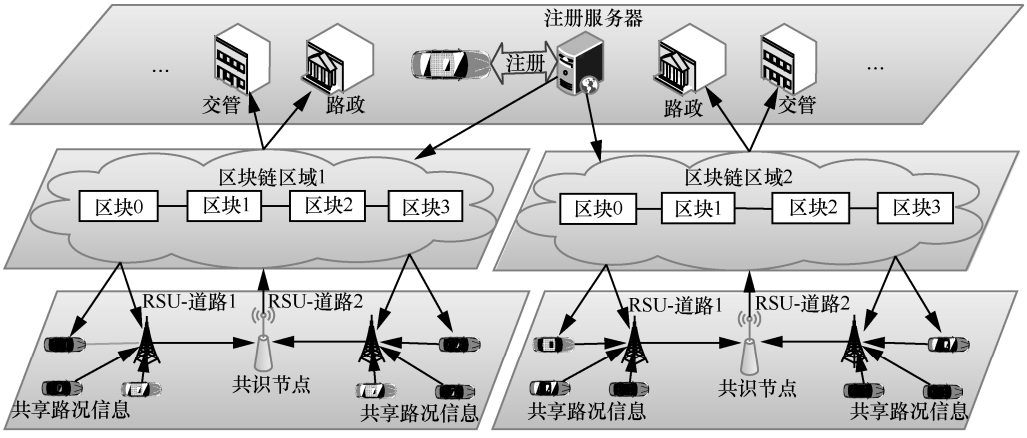


图 1　一个典型的车联网共享路况信息的场景

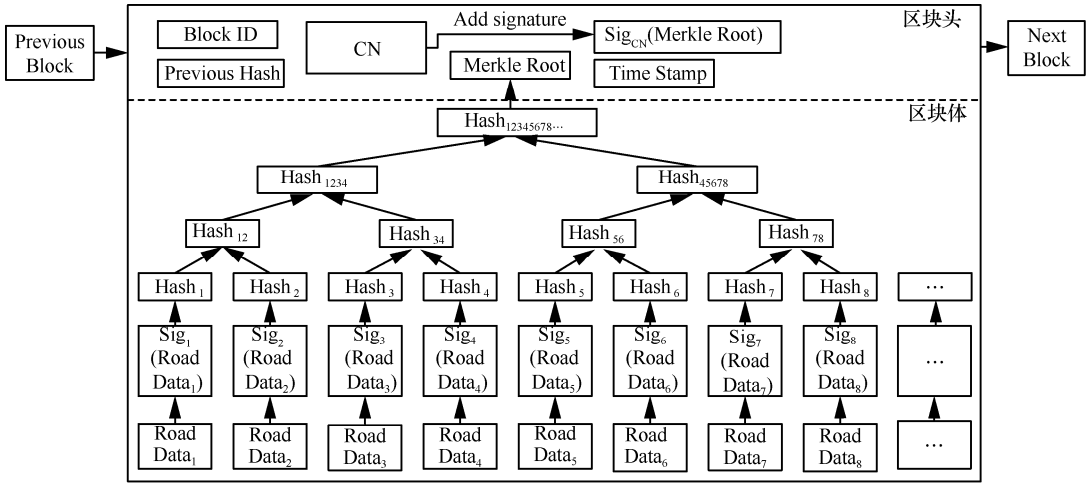


图 2　MDCA-RP 的区块结构

意检测。RSU 聚合路况信息后，将数据打包发布到网络中。网络中的共识节点就会对这条数据包进行验证，然后将一个区块时间间隔内 RSU 打包的数据打包成一个区块发布到网络中。最后，由网络中其他共识节点对这个区块进行验证，验证通过后此区块将会加入区块链。公布到区块链网络中的路况信息可以被车辆、交管、路政等需要路况信息的实体查询。

在 MDCA-RP 的设计中，考虑到产生数据的量非常庞大，按照不同区域进行划分，每个区域拥有单独的区块链网络。车辆作为收集路况信息最底层、规模最庞大的实体，是最容易进行恶意攻击的实体。传统的车辆网络中，如果大量的虚拟车辆节点协商好对系统进行攻击，那么系统是没有什么反抗能力的。所以，如何有效地防止大量节点合谋进行攻击是 MDCA-RP 主要关心的问题。

3.2　区块结构

MDCA-RP 的区块结构由区块头和区块体组成，具体如图 2 所示。

在区块头部分，MDCA-RP 设计的区块结构与传统的车载区块链网络不同。除了区块 ID（Block ID）、前一个区块的哈希值（Previous Hash）、默克尔树根（Merkle Root）、时间戳（Time Stamp）外，MDCA-RP 引入了几个新的关键字。

CN，即区块链网络中的共识节点。区块链网络中的每个共识节点负责将一个区域内路况信息的数据封装成区块。在共识节点封装区块时，应该把该节点的 ID 同时封装到区块头中。

SigCN (Merkle Root)，CN 对默克尔树根的签名。网络中其他的共识节点可以通过验证这个签名快速地完成区块有效性的验证。区块体部分主要用于记录区块网络中发生的事件。这里 MDCA-RP 主要关注网络中的 2 种事件：服务器为车辆注册假名的事件和路况信息共享的事件。

区块体中道路信息的结构如图 3 所示，每条道路上的 RSU 打包路况信息由以下关键字组成。

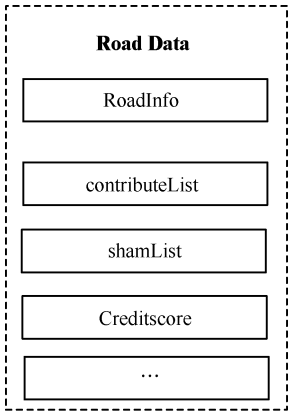


图 3　区块体中道路信息的结构

RoadInfo，一条道路上的 RSU 对这一阶段内道路中的车辆共享的路况信息聚合的结果。这条关键字后面的信息上传到网络中，可以被其他的车辆、交通运输、交警和路政等部门和个人用来参考和分析。

contributeList，参与共享路况信息做出贡献节点的列表。该字段用于记录本次路况信息聚合过程中做出贡献的车辆的数量。

shamList，发布虚假路况信息节点的列表。该字段用于记录本次路况信息聚合过程中发布虚假

信息的恶意节点的数量。

Creditscore，一个 RSU 产生一条路况信息的信誉积分。信誉积分用于激励车辆进行路况信息共享。RSU 一个时间段内聚合一次路况信息产生的信誉积分是一定的，并根据车辆贡献值进行分配。

MDCA-RP 主要有 3 个操作流程，分别是服务器为车辆注册生成假名的过程、车辆与 RSU 建立连接的初始化过程和 RSU 对共享的路况信息进行聚合的过程。

3.3　车辆注册阶段

注册服务器为车辆注册生成假名的操作流程如图 4 所示。在车辆注册阶段，服务器收到车辆发送的消息 <ID,Num>，其中 ID 为车辆发送来的身份信息，Num 为车辆想要注册的假名数量。注册服务器会返回一个 result 结构体数组，其中包含了假名的公钥和私钥。

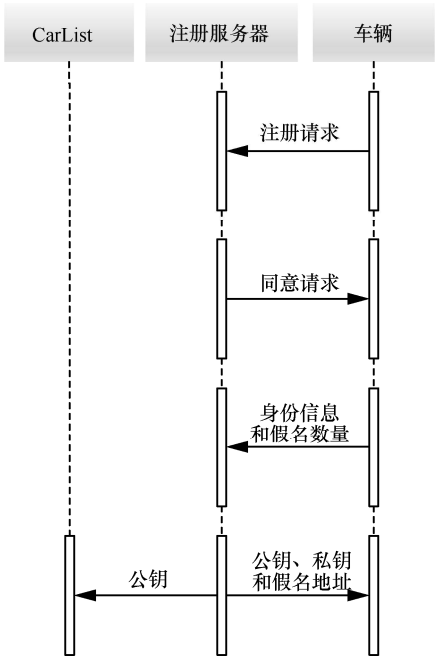


图 4　注册服务器为车辆注册生成假名的操作流程

首先，车辆参与路况信息前需要向服务器发送注册假名的请求。其次，注册服务器同意车辆的请求后，车辆需要发送用户身份信息和注册的假名数量。最后，服务器返回假名的公钥、私钥和假名地址给用户，同时将这些信息打包成区块发布到区块链中的车辆列表（CarList）中存储。

图 4 注册假名流程中，注册服务器采用椭圆曲线数字签名算法生成公私密钥对。设椭圆曲线公钥密码系统参数为 SP，则有

$$\mathrm{SP}=(F_q,E,G,P,q,a,b,h) \tag{1}$$

其中，F_q 是有限域；E 是 F_q 上的椭圆曲线；G 是 E 上的 q 阶生成元（q 为一大素数），称为基点；P 为椭圆曲线 E 上的点；a、b 是椭圆曲线 E 的系数；h 是一个单向安全的哈希函数。

根据系统参数 SP，用户 a 随机选择 n 个整数 $(K_{a1},K_{a2},\cdots,K_{an})\in[1,q-1]$ 作为其私钥 $(\mathrm{pri}K_{a1},\mathrm{pri}K_{a2},\cdots,\mathrm{pri}K_{an})$，由式(2)计算公钥为 $(\mathrm{pub}K_{a1},\mathrm{pub}K_{a2},\cdots,\mathrm{pub}K_{an})$。

$$K=kG \tag{2}$$

其中，K 为计算得到的公钥，k 为用户私钥，G 为 E 上的 q 阶生成元。

3.4　初始化阶段

RSU 与车辆之间建立连接的初始化阶段操作流程如图 5 所示。在初始化阶段，RSU 会监听连入的车辆。通过检测车辆的行为特征，RSU 能够鉴别是否存在共谋节点和虚假节点。

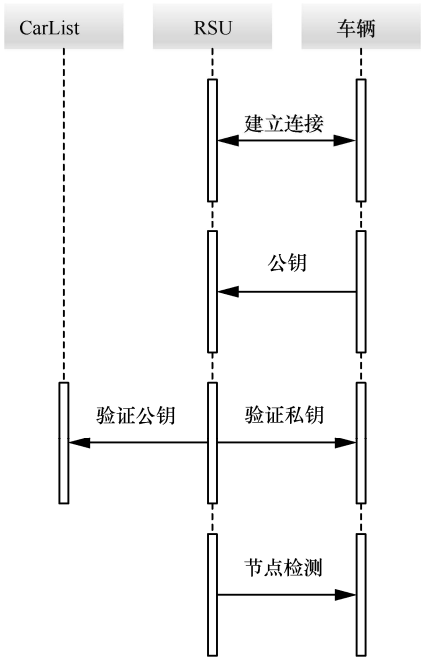


图 5　RSU 与车辆之间建立连接的初始化阶段操作流程

在初始化阶段为 RSU 设计了基于行为特征的节点检测算法。当车辆生成数据时，RSU 检查它是否合法。如果车辆在已注册列表中，则向其发送身份询问。如果它对询问产生了积极的响应，验证正确并且行为合法，那么车辆和本地区块链之间就成功地建立了联系。

基于行为特征的节点检测算法的具体步骤

如下。

步骤 1 车辆与 RSU 建立连接时，向 RSU 发送$\left\langle \text{pub}K, R_{\text{pre}}, T_{\text{pre}} \right\rangle$，其中 pub$K$ 是车辆的公钥；R_{pre}是车辆上次共享路况的 RSU，T_{pre}是车辆上次共享路况的时间。

步骤 2 RSU 在 CarList 中查询用户的公钥 pub$K$ 是否真实存在。如果是，则执行步骤 3；否则直接结束。

步骤 3 RSU 根据 T_{pre} 查询在 $T_{\text{pre}} \pm \min$ BlockPeriod 是否存在区块，其中，minBlockPeriod 是最小区块时间间隔。如果存在区块，则返回 BlockID 并执行步骤 4；否则将 pub$K$ 加入 unTrustList 并结束，其中，unTrustList 表示不可信的车辆列表。

步骤 4 RSU 根据 BlockID 寻到对应区块，并查询其中是否保存了车辆的公钥 pub$K$。如果是，则执行步骤 5；否则将 pub$K$ 加入 unTrustList 中。

步骤 5 RSU 判断 pub$K$ 在区块 BlockID 中存在于 TrustList 还是 HalfList 中。如果存在于 TrustList 中，则将 pub$K$ 加入 TrustList 中；如果存在于 HalfList 中，则将 pub$K$ 加入 HalfList 中。

3.5 路况信息聚合阶段

RSU 聚合车辆上传数据的操作过程如图 6 所示。在路况信息聚合阶段，RSU 根据车辆的信誉值计算权值。通过每个车辆的权值比重聚合路况信息，然后筛选出对路况信息做出贡献的车辆和发布虚假消息的车辆。

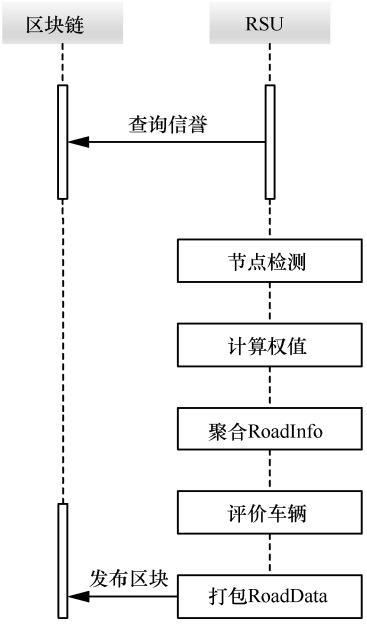


图 6 RSU 聚合车辆上传数据的操作过程

在 RSU 进行数据聚合之前，需要在节点检测的基础上查询车辆的信誉积分。如果该节点的信誉积分高于低采纳阈值 Trustlow，即为信任节点；如果该节点的信誉积分低于低采纳阈值 Trustlow，即为低采纳节点；如果该节点的信誉积分低于失信阈值 Trustdeline，即为失信节点。信任节点、低采纳节点和失信节点分别存在 TrustList、HalfList、unTrustList 中。

在路况信息聚合阶段，一个 RSU 负责处理的一条道路中的 n 个车辆发送到 RSU 的消息，记为 $\text{txV}_1,\text{txV}_2,\cdots,\text{txV}_n$。其中，txV 是车辆打包生成的数据结构，且包括 m 个实时信息字段 $\text{mes}_1, \text{mes}_2,\cdots,\text{mes}_m$，并且满足 $\text{mes}_i \in [1, \text{value}_i]$，$1 \leqslant i \leqslant m$。为了聚合每个路况信息字段的最终数据，$n$ 个车辆的 $\text{mes}_1,\text{mes}_2,\cdots,\text{mes}_m$ 建立如式(3)所示的 0-1 模型。

$$\mathbf{mes}_{1\cdots m}=\begin{bmatrix} m_{11} & m_{12} & \cdots & m_{1k} \\ m_{21} & m_{22} & \cdots & m_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \cdots & m_{nk} \end{bmatrix} \tag{3}$$

其中，$\mathbf{mes}_{1\cdots m}$表示 $\text{mes}_1,\text{mes}_2,\cdots,\text{mes}_m$ 中的每条消息。对于 mes 来说，当第 i 个车辆取值为 j 时，则将 m_{ij} 赋值为 1，否则为 0，如式(4)所示。

$$m_{ij}=\begin{cases} 0, \text{空值} \\ 1, \text{取值} \end{cases} \tag{4}$$

其中，$i \in [1,n], j \in [1, \text{val}_i]$ 路况信息聚合过程是在 $\text{mes}_i \in [1, \text{val}_i], i \in [1,m]$ 找出权值 weight 最大的取值作为最终 mes_i 的值。权值 weight 的计算式为

$$\text{weight}_i=\begin{cases} \text{trust}, \text{TrustList} \\ \dfrac{\text{trust}}{c}, \text{HalfList} \\ 0, \text{unTrustList} \end{cases} \tag{5}$$

其中，c 为半可信调整系数且大于 1，$i \in [1,n]$。

因此，可以通过车辆的信誉值计算得到 n 个车辆的数据聚合权值 $(\text{weight}, i \in [1,n])$。经过式(6)计算可以得到 $1\cdots m$ 个字段实时信息的 $1\cdots \text{val}_i$ 取值的权值分布，如式(7)所示。

$$\text{mes}_{ij}=\sum_{k=1}^{n} m_{kj}\text{weight}_k \tag{6}$$

$$\mathbf{mes}_{ij}=\begin{bmatrix} \text{mes}_{11} & \text{mes}_{12} & \cdots & \text{mes}_{1\text{val}_1} \\ \text{mes}_{21} & \text{mes}_{22} & \cdots & \text{mes}_{2\text{val}_2} \\ \vdots & \vdots & \ddots & \vdots \\ \text{mes}_{m1} & \text{mes}_{m2} & \cdots & \text{mes}_{m\text{val}_m} \end{bmatrix} \tag{7}$$

其中，$i\in[1,m], j\in[1,\mathrm{val}_i], k\in[1,n]$。

根据 $1\cdots m$ 个字段实时信息的 $1\cdots \mathrm{val}_i$ 取值权值分布，利用式(8)对每个字段取权值最大的实时信息取值。最后 RSU 将包含 m 条关键字的实时信息聚合成为 $\mathrm{RoadInfo}\langle \mathrm{mes}_1,\mathrm{mes}_2,\cdots,\mathrm{mes}_m\rangle$。

$$\mathrm{mes}_i=\max\_\mathrm{loc}(\mathrm{mes}_{ij}), j\in[1,\mathrm{val}_i] \tag{8}$$

其中，max_loc 函数返回 mes_{ij} 最大值对应的位置 j。

RSU 聚合路况信息后，要对做出贡献的车辆和发布虚假消息的车辆进行统计，分别记录在 RoadData 的 contributeList 和 shamList 中。对于 m 条数量的路况信息关键字，如果车辆共享真实信息达到 φ 个（φ 由式(9)给出），则认为该车辆为网络中的实时路况信息共享工作做出了贡献；否则认为该车辆是发布虚假消息的恶意车辆。

$$\varphi=m\sigma \tag{9}$$

其中，$\sigma\in(0,1)$ 是自定义的检测参数。

RSU 根据式(10)计算 n 个车辆共享真实路况信息的数量 $\beta_i, i\in[1,n]$。

$$\beta_i=\sum_{j=1}^{m}\begin{cases}0, \mathrm{mes}_j\neq \mathrm{txV.mes}_j\\ 1, \mathrm{mes}_j=\mathrm{txV.mes}_j\end{cases} \tag{10}$$

RSU 会根据 β_i 对车辆 i 进行评价，如果 $\beta_i\geqslant\varphi$，则将车辆 i 加入 contributeList；否则将车辆 i 加入 shamList。

最后，RSU 将聚合的 RoadInfo 和 contributeList、shamList 打包生成 RoadData。contributeList、shamList 为系统奖惩车辆和后续对车辆的恶意行为检测提供支持。其中，系统根据 contributeListh 和 shamList 决定车辆 i 的奖惩。车辆 i 的信誉更新方式由式(11)给出。其中，mul 为惩罚参数。

$$\mathrm{Trust}_i=\begin{cases}\mathrm{Trust}_i+\dfrac{\mathrm{Credistscore}}{\mathrm{ContributeList.num}}, V_i\ \mathrm{in\ contributeList}\\ \mathrm{Trust}_i-\dfrac{\mathrm{Credistscore}\times\mathrm{mul}}{\mathrm{shamList.num}}, V_i\ \mathrm{in\ shamList}\end{cases} \tag{11}$$

4　安全性分析和实验验证

4.1　安全性分析

在路况信息共享的过程中，网络中存在的恶意节点发送虚假的路况信息，会导致道路中的车辆、交通运输、交警和路政等部门产生错误的结果，给道路安全带来安全隐患。MDCA-RP 能够针对恶意节点在网络中的不同数量、不同行为做出相应的对策。

首先，对真实的网络环境中做出如下假设。

1) 道路中的 RSU 具有足够算力，可以作为矿工节点。

2) 道路中车辆与 RSU 之间是开放的网络。

3) 车辆之间不进行直接通信，所有共享都与区块链网络进行交互。

其次，假设与一个 RSU 建立连接的诚实车辆数量为 n_{h}，这条道路中存在的恶意节点的数量为 n_{m}。由式(12)可以定义恶意节点与诚实节点的比率 ε。本文将危险情况分为 2 种：$\varepsilon<1$ 和 $\varepsilon\geqslant1$。

$$\varepsilon=\frac{n_{\mathrm{m}}}{n_{\mathrm{h}}} \tag{12}$$

1) $\varepsilon<1$。这种情况下，恶意节点的数量是少数的。当这些恶意节点发布虚假路况信息给 RSU 后，RSU 可以通过加权的方式聚合路况信息。由于这些节点的数量少，即使是加权计算，它们的权值也比真实的节点小。进而，恶意节点发送的虚假路况信息会被 RSU 所忽略，保证了聚合的路况信息的安全性。

2) $\varepsilon\geqslant1$。这种情况下，有人操纵大量恶意节点进行合谋，向网络中发布大量虚假路况信息。针对这种情况，MDCA-RP 的方法是根据节点的行为特征筛查出合谋的恶意节点。在真实的网络环境中，要同时控制大量真实的车辆进行合谋攻击是非常难的，可能的方法就是通过虚拟一些网络节点进行合谋攻击。但是这种伪造的虚拟节点经过 MDCA-RP 的验证就会被发现。

TFAA 方案采用车辆间通信共享数据，而 MDCA-RP 采用车辆直接将数据共享给 RSU 进行聚合的方法，MDCA-RP 和 TFAA 的比较如表 1 所示。由表 1 可以看出，由于方案设计机制的原因，TFAA 方案中车辆会对恶意节点共享的恶意信息产生响应做出错误的决策，而 MDCA-RP 中的车辆则不会产生响应。根据 TFAA 的实验结果可以看出，其网络中车辆对恶意节点的响应与共享周期呈线性关系。然而，MDCA-RP 由于路况信息直接由 RSU 进行聚合，然后上传到网络中，不经过车辆间互评的阶段。因此，MDCA-RP 网络中的车辆对恶意节点发布的虚假路况信息是不能进行评价和响应的。MDCA-RP 在网络中的车辆对于虚假信息的响应方面是优于 TFAA 方案的。

表 1 MDCA-RP 和 TFAA 的比较

方案	车辆相互评价	$\varepsilon \geqslant 1$ 时识别恶意节点能力	路况信息准确率
MDCA-RP	无	较强	较高
TFAA	有	无	一般

综上所述，不论网络中节点的数量如何，MDCA-RP 都可以检测出恶意节点，进而过滤掉虚假的路况信息，保证最终聚合路况信息的真实性和共享路况信息过程的安全。

4.2 实验验证

下面，通过实验来验证 MDCA-RP 的安全性以及消息的准确性。具体将从恶意节点信誉积分变化和恶意节点数量对路况信息结果的准确率的影响2个方面与 TFAA 进行对比。

实验过程中使用如表 2 所示的数据格式作为车辆共享的数据。其中 m_1、m_2、m_3、m_4、m_5 代表 5 种不同类型的车辆实时信息，其取值范围各有不同。设定 <0,2,1,3,30> 为真实消息，<0,0,0,0,0> 和 <1,2,3,3,5>为 2 组虚假消息。

表 2 车辆共享数据格式

字段	含义
id	公钥，车辆的区块链地址
to	RSU 的区块链地址
body	车辆实时信息< m_1,m_2,m_3,m_4,m_5>
txindex	本车交易数量编号
issue_Time	注册账户的时间戳
expiry_Time	注销账户的时间戳

不同恶意节点数量对路况信息准确率的影响实验中，设定真实节点的数量是 50 个，虚假节点的数量是 0~100 个。

恶意节点信誉积分变化实验中，模拟恶意节点在网络中进行 20 个周期的路况信息共享。其中，设定 50 台车辆（40 台正常车辆，10 台共谋车辆）从恶意节点中随机选取 4 个节点（a、b、c、d）与 TFAA 方案进行对比，即 4 个节点不规律地发布 2 组虚假消息。不同恶意节点数量对路况信息准确率的影响如图 7 所示。

从图 7 中可以看出，MDCA-RP 整体路况信息的准确率基本都能达到 90%。当恶意节点数量在50%左右时，其准确率开始降低到 95%以下，这时的准确率容易出现波动，会漏掉几个恶意节点的路况信息；当恶意节点占比超过 50%后，将采用优先分析车辆的行为特征。TFAA 只对恶意节点占比从10%到 50%的情况做了实验分析。从图 7 中可以看出，网络中存在的恶意节点越多，TFAA 处理的准确率越低，并且 TFAA 不能处理的恶意节点数量占多数情况。

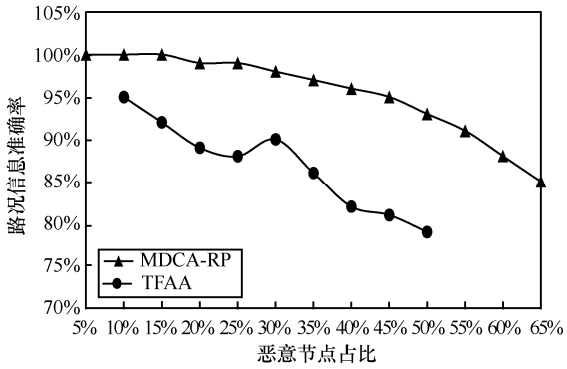


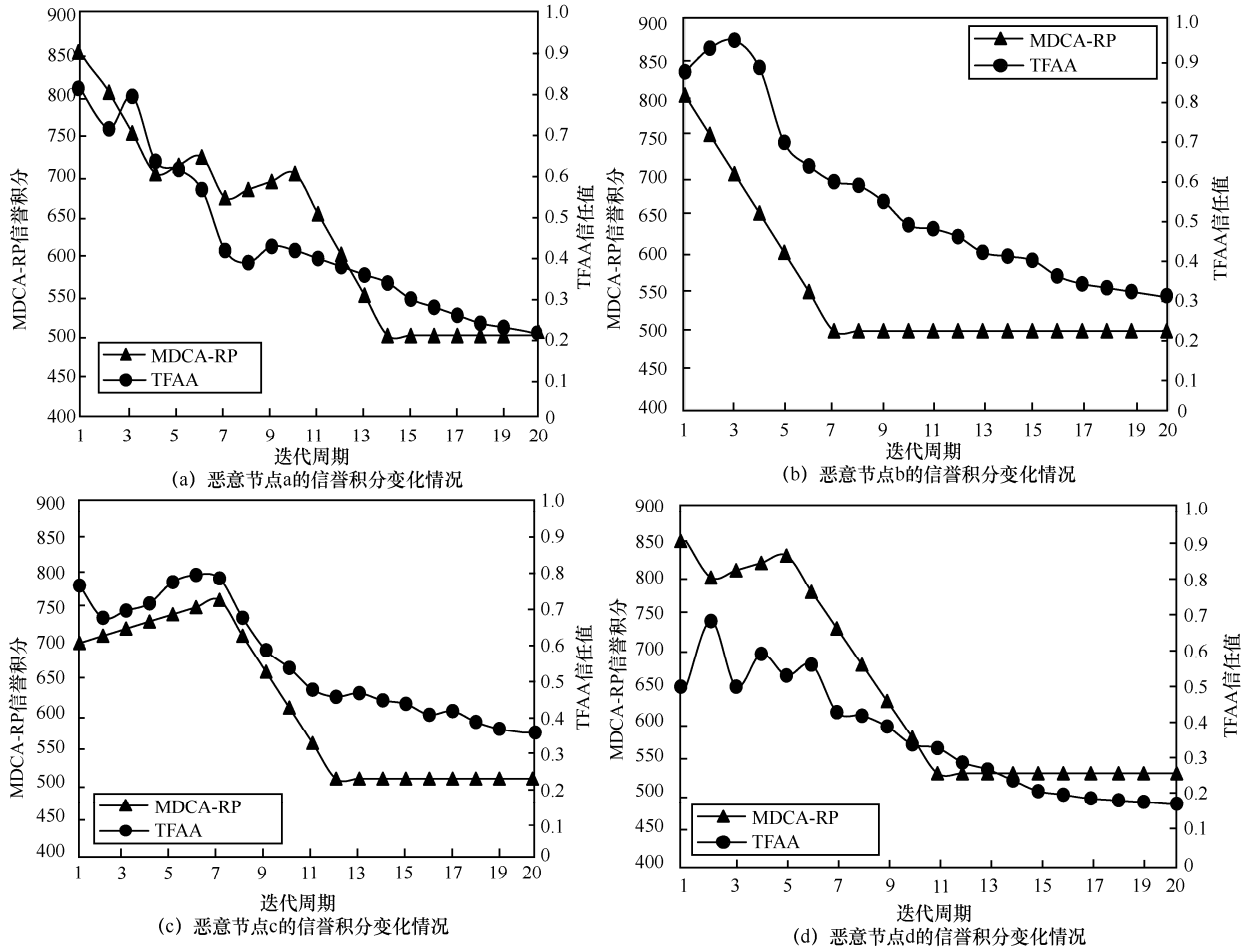
图 7 不同恶意节点数量对路况信息准确率的影响

恶意节点信誉积分对比如图 8 所示。从图 8 中可以看出，MDCA-RP 对恶意节点发布虚假消息时，信誉积分下降得很快，对系统做贡献时信誉积分增长得却很慢，这样可以使恶意节点的信誉积分很快就降低到失信阈值之下。当阈值为 550 时，节点的信誉积分降低到 500 以下就不再降低了，系统也不会采纳这个信誉积分的路况信息。

经过实验验证，MDCA-RP 与 TFAA 方案相比，对于数量较少的恶意节点发动攻击的情况，MDCA-RP 能够快速地降低恶意节点的信誉积分，让其发挥不了作用；对于 TFAA 不能处理的大量恶意节点合谋进行攻击情况，MDCA-RP 能够通过分析恶意节点的行为特征将其筛查出来。最终证明，MDCA-RP 能够更好地应对路况信息共享过程中的共谋攻击。

5 结束语

本文针对车联网中共谋节点协同发布虚假路况信息，导致路况信息共享过程中消息真实性无法保证的问题，通过研究信誉管理的机制，结合信誉积分模型和节点特征检测算法，提出了基于信誉积分的路况信息共享中共谋攻击节点检测方法。通过与现有工作的安全性对比分析，以及车辆节点信誉积分变化情况和路况信息准确率的对比实验，验证了本文所提方法的有效性，并且显著提高了检测高占比共谋节点的能力。



（a）恶意节点a的信誉积分变化情况　（b）恶意节点b的信誉积分变化情况

（c）恶意节点c的信誉积分变化情况　（d）恶意节点d的信誉积分变化情况

图 8　恶意节点信誉积分对比

在未来的研究中，可将深度学习用于恶意节点的行为特征检测中，进一步提高检测能力。

参考文献：

[1] NAKAMOTO S. Bitcoin: a peer to peer electronic cash system[EB]. (2008-10-31)[2020-07-10].

[2] FOROGLOU G, TSILIDOU A L. Further applications of the blockchain[C]//12th Student Conference on Managerial Science and Technology. [S.n.:s.l.], 2015: 1-8.

[3] KOSBA A, MILLER A, SHI E, et al. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts[C]//2016 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2016: 839-858.

[4] AKINS B W, CHAPMAN J L, GORDON J M. A whole new world: income tax considerations of the bitcoin economy[J]. Pittsburgh Tax Review, 2015, 12(1): 24-56.

[5] ZHANG Y, WEN J T. An IoT electric business model based on the protocol of bitcoin[C]//2015 18th International Conference on Intelligence in Next Generation Networks. Piscataway: IEEE Press, 2015: 184-191.

[6] SHARPLES M, DOMINGUE J. The blockchain and kudos: a distributed system for educational record, reputation and reward[C]//European Conference on Technology Enhanced Learning. Berlin: Springer, 2016: 490-496.

[7] YANG Z, YANG K, LEI L, et al. Blockchain-based decentralized trust management in vehicular networks[J]. IEEE Internet of Things Journal, 2019, 6(2): 1495-1505.

[8] LI L, LIU J Q, CHENG L C, et al. CreditCoin: a privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2018, 19(7): 2204-2220.

[9] LU Z J, WANG Q, QU G, et al. BARS: a blockchain-based anonymous reputation system for trust management in VANETs[C]//2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering. Piscataway: IEEE Press, 2018: 98-103.

[10] MALIK N, NANDA P, ARORA A, et al. Blockchain based secured

identity authentication and expeditious revocation framework for vehicular networks[C]// 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering. Piscataway: IEEE Press, 2018: 674-679.

[11] SINGH M, KIM S. Crypto trust point (CTP) for secure data sharing among intelligent vehicles[C]//2018 International Conference on Electronics, Information, and Communication. Piscataway: IEEE Press, 2018: 1-4.

[12] SHRESTHA R, BAJRACHARYA R, NAM S Y. Blockchain-based message dissemination in VANET[C]//2018 IEEE 3rd International Conference on Computing, Communication and Security. Piscataway: IEEE Press, 2018: 161-166.

[13] ZHANG X D, LI R, CUI B. A security architecture of VANET based on blockchain and mobile edge computing[C]//2018 1st IEEE International Conference on Hot Information-Centric Networking. Piscataway: IEEE Press, 2018: 258-259.

[14] SINGH M, KIM S. Trust bit: reward-based intelligent vehicle commination using blockchain paper[C]//2018 IEEE 4th World Forum on Internet of Things. Piscataway: IEEE Press, 2018: 62-67.

[15] ZHANG X H, CHEN X F. Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network[J]. IEEE Access, 2019, 7: 58241-58254.

[16] KHELIFI H, LUO S L, NOUR B, et al. Reputation-based blockchain for secure NDN caching in vehicular networks[C]//2018 IEEE Conference on Standards for Communications and Networking. Piscataway: IEEE Press, 2018: 1-6.

[17] LEI A, CRUICKSHANK H, CAO Y, et al. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems[J]. IEEE Internet of Things Journal, 2017, 4(6): 1832-1843.

[18] FENG J Y, LIU N, CAO J, et al. Securing traffic-related messages exchange against inside-and-outside collusive attack in vehicular networks[J]. IEEE Internet of Things Journal, 2019, 6(6): 9979-9992.

[作者简介]

玄世昌（1984− ），男，黑龙江讷河人，博士，哈尔滨工程大学副教授、硕士生导师，主要研究方向为网络与信息安全、区块链技术等。

汤浩（1996− ），男，黑龙江密山人，哈尔滨工程大学硕士生，主要研究方向为网络安全、区块链技术等。

杨武（1974− ），男，辽宁宽甸人，博士，哈尔滨工程大学教授、博士生导师，主要研究方向为信息安全、数据挖掘、互联网安全。