计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200800024

车联网互信认证与安全通信综述

王春东　罗婉薇　莫秀良　杨文军
天津理工大学计算机科学与工程学院　天津 300384

摘　要　随着车联网的多场景应用和5G通信的高速发展,保证高速车辆之间的互信认证和安全通信变得日益重要。当前车联网访问场景中的身份认证与车联网的通信安全已成为最重要的两道防线。首先介绍了现有车联网互信认证和安全通信的研究背景,指出了安全互信认证和安全通信所使用的原理与技术,包括椭圆曲线加密、哈希函数、数字签名、区块链等。然后,对协议进行分类,包括匿名接入安全互信认证协议、群组接入安全互信协议、跨域认证安全互信协议等。由于无线信道的广播特性,车辆之间的信息交换节点可能被窃听,伪造或重播,因此探讨了基于区块链的车联网安全通信、基于5G的轻量型车联网安全通信,分析了现有车联网互信认证和安全通信存在的问题和安全威胁。最后,探讨了5G通信给车联网安全认证和通信方面带来的影响,以及融合5G技术进一步发展车联网的互信认证和安全通信,同时对车联网和5G技术结合研究的未来关键趋势也做出了一定的预测和展望。

关键词:车联网;互信认证;安全通信;区块链;5G技术
中图法分类号　TP393

Survey on Mutual Trust Authentication and Secure Communication of Internet of Vehicles

WANG Chun-dong,LUO Wan-wei,MO Xiu-liang and YANG Wen-jun
School of Computer Science and Engineering,Tianjin University of Technology,Tianjin 300384,China

Abstract　With the rapid development of multi-scenario applications of the Internet of Vehicles and 5G communications,ensuring mutual trust authentication and secure communication between high-speed vehicles has become increasingly important. The identity authentication in the current Internet of Vehicles access scenario and the security in the process of communicating with Internet of Vehicles have become the two most important lines of defense. First,this paper introduces the research background of existing mutual trust authentication and secure communication in Internet of Vehicles,and points out the principles and technologies used in secure mutual trust authentication and secure communication,including elliptic curve encryption,Hash function,digital signature,blockchain,etc. Then,it classifies protocols,including anonymous access security mutual trust authentication protocol,group access security mutual trust protocol,cross-domain authentication security mutual trust protocol,etc. Due to the broadcast characteristics of the wireless channel,the information exchanged between vehicle nodes may be eavesdropped,forged or replayed. Therefore,the security communication of Internet of Vehicles based on blockchain and 5G-based light-weight car networking security communication are discussed. Then,it analyzes the existing problems and security threats in the mutual trust authentication and secure communication of the existing car networking. Finally,the impact of 5G communication on the safety certification and communication of the Internet of Vehicles is discussed,and the integration of 5G technology will further develop the mutual trust authentication and secure communication of the Internet of Vehicles in the future. At the same time,it also makes certain predictions and prospects for the future key trends of the combined research of the Internet of Vehicles and 5G technology.

Keywords　Internet of vehicles,Mutual trust authentication,Secure communication,Blockchain,5G Technology

1　引言

随着汽车工业的发展,汽车保有量快速增长,如何在各种交通工具之间采用某种科技手段来进行协调,以减少交通事故和缓解交通堵塞,已经成为当下无法回避的一个课题。在当前的环境下,车辆与高速发展的网络相结合,产生了车载自组织网络(Vehicle Ad-hoc Network,VANET)。车联网通过搭载传感器等设备实现车与万物(Vehicle-to-everything,V2X)的智能信息交互。V2X按照交互对象的不同分为车辆与车辆(V2V)、车辆与设施(V2I)、车辆与行人(V2P)、车辆与互联网(V2N)。V2X采用专用短程通信技术DSRC或基于蜂窝通信的V2X技术C-V2X进行通信,能够提高交通的安

到稿日期:2020-08-03　返修日期:2020-09-27　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:天津市科学技术委员会基金资助项(15JCYBJC15600);通用技术基础研究基金(U1536122)
This work was supported by the Foundation of Tianjin Science and Technology Committee(15JCYBJC15600) and Fundamental Research Fund for General Technology(U1536122).
通信作者:王春东(michael3769@163.com)

全性。然而这两种主流无线通信方式在车辆操作中仍然存在安全隐患。如腾讯科恩实验室以远程无物理接触的方式直接拿到了特斯拉控制行车系统的车电网络(CAN 总线)的权限[1];百度通过破解进入车载 T-Box 的 Wi-Fi 和移动通信网络[2],成功实现了车辆的远程控制。

车联网动态的网络拓扑变化迅速,使得互联网传统安全机制无法应用于车联网中。高速切换节点时,任何伪造节点与恶意攻击都可能导致系统故障,从而危害安全。互信认证协议为了保证数据安全,在车辆入网时从证书中心获取数字证书,在发送数据之前使用数字签名算法为数据生成签名,并采用证书分化和撤销的方式来进行身份认证。初期的互信认证协议[3-12]效率低下,不能有效抵抗重放攻击,且不具备可追踪性,只适用于简单的 VANET。VANET 的消息数量庞大,具有很强的时效性,为了保证车辆之间通信的可靠性、信息认证的完整性和隐私性,以及消息的不可否认和可追踪性,高效率的认证方案显得愈加重要。同时 V2X 通信必须达到真实性、可授权、可用性、数据机密性、数据完整性等基本安全要求以抵抗各种攻击。因此需要进一步提高与完善车联网中现有的互信认证与安全通信技术。

车联网采用 CAN 总线、LIN 总线、移动蜂窝通信、蓝牙技术、Wi-Fi 等成熟的通信技术。车联网系统中主要包括 5 个通信场景:车内通信、车-车通信、车-人通信、车-路通信和车-云通信[13]。本文的安全通信以车-车通信为背景。在开放的无线信道中实现安全的互信认证是车联网安全的一个重要内容。

2 基本原理

2.1 椭圆曲线加密

椭圆曲线是非对称加密的一种场景应用,即只可正向求值,不可逆向反推。椭圆曲线密码学[14](Elliptic Curve Cryptography,ECC)由 Neal Koblitz 和 Victor Miller 首先提出。ECC 基于离散对数的原理,164 位的 ECC 密钥的安全级相当于 RSA 1024 位密钥的保密强度[15]。由于 ECC 处理速度更快,存储空间和传输带宽占用较少,我国第二代居民身份证使用的就是 256 位的 ECC 密码。

椭圆曲线数字签名算法[16](Elliptic Curve Digital Signature Algorithm,ECDSA)是 ECC 和 DSA 的结合,比特强度高于其他公钥体制,能够避免网络中的隐私信息受到威胁。图 1 是 ECC 算法的流程图,其原理如式(1)所示:

$$C_1-KC_2=M+rK-K(G)=M+rK-r(KG)=M \quad (1)$$

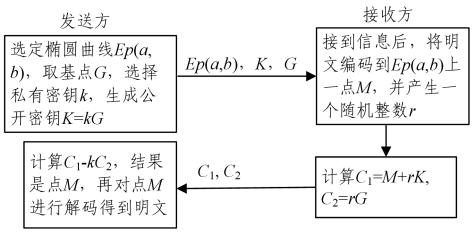

图 1 ECC 算法流程图

Fig. 1 ECC algorithm flow chart

2.2 哈希函数

将任意长度的消息 M 转化成一段固定长度的 Hash 值 $H(M)$,按照该思想建立的表为哈希表,M 和 $H(M)$的对应关系为哈希函数 F[17](Hash Function)。哈希函数基于单向的思想,不可根据 $H(M)$得到 M,因此可用于验证数据的完整性和鉴别数据是否遭到篡改。F 是多对一映射,不同的关键字可能得到同一散列地址。当不同的关键字值对应到同一个存储位置时,按冲突方法处理。哈希表的建立过程如图 2 所示,哈希表如图 3 所示。通过原始信息可以计算出哈希值,反之则无法推测出原始信息,保证了消息不被泄露。

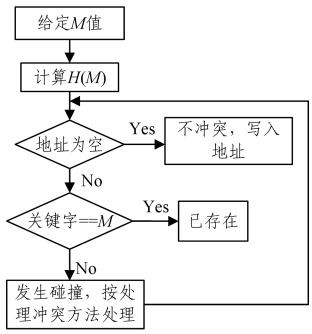

图 2 创建哈希表

Fig. 2 Creating a hash table

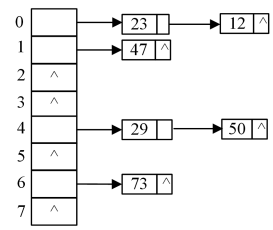

图 3 哈希表

Fig. 3 Hash table

2.3 数字签名

数字签名[18]是通过哈希函数和公钥算法实现的,能够实现对消息完整性以及发送方身份的验证,保证了信息来源的可靠性。发送方 A 首先使用 B 的公钥 kB 对明文 m 进行加密,得到 $kB(m)$;再对 m 进行 hash 运算,得到 $hash(m)$。同时发送方 A 使用自己的私钥 ka 对 $hash(m)$进行签名,得到 $ka(hash(m))$。A 将 $kB(m)$与签名信息 $ka(hash(m))$一起传递给接收方 B。接收方 B 使用 A 的公钥 kA 对数字签名验签得到 $hash(m)$,并使用私钥 kb 对 $kB(m)$进行解密得到明文 m。如果通信双方的 $hash(m)$一致,则说明明文 m 是可靠的。图 4 给出公钥签名算法模型。

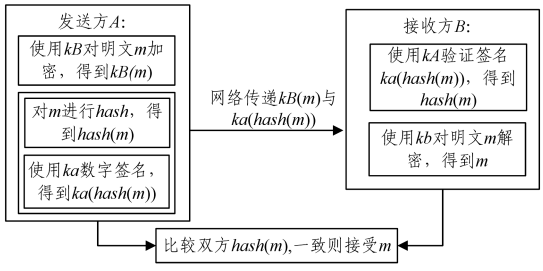

图 4 公钥签名算法模型

Fig. 4 Public key signature algorithm model

2.4 联盟区块链

区块链技术[19]实际上是一个共享数据库。区块链的基本处理单元是数据块,每个块与前一个块相连,不依赖于某一

个中心节点，而是分布式存储，并且每个节点都拥有完整的拷贝，因此交易不可伪造。区块链分为公有链、私有链和联盟链。联盟链是在共识的过程当中受制于预选节点的区块链，即有若干个机构共同参与管理的区块链，每个机构运行多个节点，节点内的数据只允许在机构内进行读写和发送交易，并且共同记录交易数据。

联盟区块链[20]具有去中心化、数据可靠、安全可信等特点，并且需要通过对方授权的密钥才能看到其他参与者的数据。与公有链的完全去中心化的不可控以及自由加入和退出相比，其具有极高的安全性与灵活性。

3 协议分类

根据车联网系统中安全认证协议适用的应用场景不同，将协议分为匿名接入安全互信认证协议、群组接入安全互信认证协议和跨域接入安全互信认证协议。

3.1 符号

互信认证协议使用的符号与对应描述如表 1 所列。

表 1 符号对照表

Table 1 Symbol comparison table

符号	描述
OBU	车载单元
MME	移动管理实体
eNodeB	基站节点
HSS	本地用户服务器
RSU	路侧单元
TPD	防干扰设备
VE	车载设备
MTC	机器类型通信
TA	受信任的授权机构

3.2 匿名接入认证

3.2.1 认证思路

在车载 LTE/LTE-A 网络中实现匿名接入认证的思路是用伪身份 DID 来代替车辆真实身份[21-25]。首先，车载单元 OBU 访问网络获得系统参数并进行初始化，然后通过 HSS 或者认证中心 AuC 连接到 EPC 注册。车辆 OBU 的真实身份 ID 由哈希函数 h 和随机数 a 保护生成伪身份 DID。由于离散对数计算的复杂度，攻击者不能获得随机数 a，同时由于随机数的存在，OBU 发送的访问请求消息可避免 OBU 位置信息泄露，因此可以实现匿名接入认证。

3.2.2 认证目的

基于匿名的该类协议目的包括：1）匿名接入。车辆节点注册时检验匿名证书，可以实现身份的保密性。2）隐私保护。车辆 OBU 和新的基站 RSU 频繁交互，更换匿名证书，保证消息的完整性和可靠性。3）抵抗各种恶意攻击[26-33]。

3.2.3 安全性与有效性

He 等[34]提出一种基于 LTE 网络的匿名认证方案 CPPA。该方案支持相互身份验证和隐私保护，解决了 VANET 中的安全和隐私问题，并且不使用双线性对，降低了 VANET 中信息处理的计算复杂性。Xu 等[35]提出一种基于 LET-A 的车联网匿名漫游认证方案。该方案基于椭圆曲线公钥密码体制实现匿名接入，能够实现车辆 OBU 的匿名，攻击者不能从 OBU 和目标 eNodeB 之间发送的信息中获得 OBU 当前位置信息，保证了协议的安全性。Rahnama 等[36]提出一种新的 IoV 认证协议，在 OBU 节点匿名注册上使用生物识别模板代替密码，提高了安全性，并降低了密码计算复杂性带来的开销，提高了有效性。Lin 等[37]提出一种基于身份的签名方案 GSIS，消息由没有隐私需求的节点发送，在保证匿名性的同时，一旦发生任何争端事件，权威机构可透露消息发送者的真实身份 ID，为每辆车提供必需的可追溯性，因此其安全性和隐私性也能得到保证。

3.3 群组接入认证

3.3.1 认证思路

在基于 LTE/LTE-A 的网络中同时对大量的车载单元 VE 进行互信认证时，为了减少车载 VEs 与服务器之间的通信次数，可以使用群组接入认证以避免大规模的网络拥塞。群组可以定义不同级别的隐私等级。根据接入场景的不同，可以选择不同等级的隐私级别保护，等级越高，隐私级别越高，如表 2 所列。

表 2 不同级别的隐私等级

Table 2 Different levels of privacy levels

	等级 1	等级 2	等级 3	等级 4	等级 5
匿名性	是	是	是	是	是
不可链接性	否	是	是	是	是
可追溯性	否	否	是	是	是
不可陷害性	否	否	否	是	是
不可抵赖性	否	否	否	否	是

群组接入认证使用数字签名生成群签名方案[38-42]，真实签名者无法通过群消息来鉴定，且群签名之间具有不可关联性，可以实现表 2 中的不可链接性和不可抵赖性。车载 VE 的身份 ID 是它唯一的标识符，HSS 使用椭圆曲线加密为 VE 计算一组不可链接的伪标识。当访问网络时，VE 在认证过程中可以不断改变其假名 ID，因此群组中任何一个成员均可以匿名的方式代表整个群体进行签名。在群组认证阶段，当一组 VE 同时访问网络时，根据每个 VE 的通信能力、存储量等选择组长。组长之间进行双向认证，确认双方身份后，每个 VE 生成一个会话密钥，以确保 MME 通信期间的安全性，并且不需要再次向 MME 请求签名，减少了通信量。同时，在群组接入认证中，群管理者（Group Manager，GM）作为可信管理员具有设置参数、跟踪 VE 真实 ID 以及追溯责任并撤销匿名的职能，以实现可追溯性。

3.3.2 认证目的

群组接入认证的目的包括：1）群组认证和密钥协商。所有的车辆节点以群组的方式接入基站，认证成功后能够在车辆节点和 MME 之间建立安全通道。2）隐私保护。根据隐私保护的不同等级，实现对应的安全保护要求。3）攻击抵抗。能够抵抗重放攻击、中间人攻击等各种攻击。

3.3.3 安全性与有效性

Rajabzadeh 等[43]提出了一种签名技术以避免车辆节点的快速接入接出所造成的拥塞，即群签名技术。一个群体中的任意一个成员均可以匿名的方式代表整个群体对消息进行签名，群消息隐藏真实签名者，可以保证不可抵赖性且签名无法伪造，确保了安全性。Lin 等[44]提出一种基于群签名的短期证书匿名认证方案，使用密钥隔离的假名自授权 KPSD 模

型，在短时间内生成短时密钥，但是由于车辆频繁更换群组导致开销较大。文献[45]提出一种应用在 VANET-蜂窝集成网络中的安全群组管理框架 SEGM，其通过使用贡献性组密钥协议，支持组的动态维护，因此具有高效的通信能力，并且可以防止恶意的窃听者与针对组设置的各种攻击，保证了安全性与有效性。文献[46]提出基于群组接入的安全互信认证方案 GAPL，该方案中 VE 组长把成员的全部签名聚合成一个签名以确保消息的可靠性；同时每个 VE 在注册时会生成相应的伪身份，由于随机数的存在，攻击者不能逆推出对应的真实身份，从而保证了身份的不可链接性，确保了用户的隐私不被泄露，解决了当大量车载设备接入基站时引发的信道拥塞和安全认证问题。

3.4 跨域接入认证

3.4.1 认证思路

在复杂车联网环境中，为了确保不同位置的车辆用户可以访问任意服务器的资源，不同信任域[47-50]的车辆节点需要通过跨域接入认证与其他信任域的资源进行交互。跨域接入认证就是利用先前域中的信任信息快速建立当前域中的信任关系。跨域接入认证使用弱中心化的联盟链[51-53]架构，通过设置不同类型链上用户等级权限，使用链上存证和链下认证相结合的方式，利用域间数据同步机制来有效减少通信交互次数。首先，车辆通过可信机构 TA 授权获得证书以及私钥和公钥信息进行线下注册。移动车辆接入车联网某个路侧单元 RSU 的管辖范围。接着车辆 VE 和 RSU 进行首次认证。车辆 VE 通过可信机构 TA 在区块链上公布证书周期、路侧单元公钥身份等信息，并与目前区域内的 RSU 比对，进而认证 RSU 的状态是否合法。然后 VE 使用匿名化的假名信息与 RSU 进行交互验证，验证假名、公钥和签名信息都符合后，RSU 将车载 VE 的假名和公钥信息进行序列化背书，并在系统备份。当车载 VE 进入新的管辖域，再次与新的路侧 RSU 进行认证时，VE 只需提供背书序列的假名信息呈递至 RSU，RSU 提交至可信机构 TA，TA 在链上查询链码即可返回结果，从而与 RSU 实现跨域认证。

3.4.2 认证目的

跨域接入认证的目的包括：1)有效的跨域共享。弱中心化的联盟链架构可有效解决多域下不同系统之间数据缺乏可靠性、容易出现单点故障的问题。2)降低开销。使用链上存证和链下认证相结合的方式，域间数据同步机制能够有效减少通信交互次数和开销。3)安全保护。区块链的特性与域中信任关系的建立能够保证消息的完整性、不可篡改性和隐私性。

3.4.3 安全性与有效性

由于车联网中存在频繁出入、跨域的高效移动节点，需要建立可靠的跨域认证来保护车辆的隐私安全。文献[54]提出针对 LTE-V 网络跨域通信场景的高效跨域认证方案，利用密钥共享和聚合代理签名大大减少了车辆与网络之间的信号交换量。该方案在车载设备密度较大的 LET-V 网络中有较低的信号过载，在保证安全性与有效性的情况下有较高的车辆密度优势。然而在 VANET 中，如果车辆位于非同源区域，远程身份认证服务器无法在没有归属域身份认证服务器帮助的情况下对车辆进行身份验证，从而导致更长的通信延迟。Jiang 等[55]提出一种区块链证书颁发机构(BCCA)信任模型和系统架构，与之前的跨域认证方案相比，其利用不易篡改的区块链机制和哈希算法，减少了公钥算法的签名和验证次数，提高了认证效率与安全性。Wang 等[56]提出利用联盟区块链技术构建一个以根证书颁发机构为验证节点的分散网络模型 BlockCAM。授权证书的哈希值存储在每个块中，验证过程中仅需比较用户提供的证书计算出的哈希值与区块链中存储的哈希值是否一致，因此身份验证过程省略了密钥加解密开销，效率高于现有的公钥基础结构(PKI)跨域身份验证方案[57-66]，可以提高 VANET 中跨域接入认证的效率，并且不会损害车辆的安全性。

4 安全通信分类

4.1 区块链安全通信

4.1.1 安全通信思路

现有传统 LTE 网络下的集中式与分布式架构在车联网安全通信下仍存在不足。随着区块链技术的发展[67-69]，以及共识机制、智能合约、非对称加密的提出，节点之间无须相互信任。区块链技术可运用于车联网安全通信中，利用区块链的可追踪、不可篡改以及分布式的存储特性保证通信数据的安全性。首先使用路侧单元采集车辆的通信行为数据。采集过程由智能合约执行，路侧单元被授权生成和验证新区块。然后将车联网信息资源的访问控制逻辑编写成智能合约部署到区块链。智能合约由全节点执行，结果通过共识机制得到。

4.1.2 目的

根据基于区块链的安全通信机制的分布式系统，车辆节点之间不需要相互信任，也无须第三方验证，因此可以提高目前通信的效率，降低成本，以及保证数据的可靠存储。

4.1.3 模块

区块链系统可将车辆节点的操作作为数据存储。由于 RSU 通过蜂窝网络[70-71]互连，将 RSU 作为区块链的全节点，存储完整的区块链数据并进行“挖矿”[72-73]。车载单元具备的计算资源及存储资源有限，将车载单元作为区块链的轻量级节点，存储区块链的区块头且不参与挖矿，不会造成额外的开销。文献[74]提出基于区块链的车联网安全通信框架。该方案分为以下几个模块：1)区块链网络模块存储节点的公钥信息、历史通信行为数据，并为智能合约提供部署和运行平台；2)访问控制模块会对车联网中不同节点的风险进行预测，由此来控制它们的访问权限。区块链车联网安全通信框架如图 5 所示。

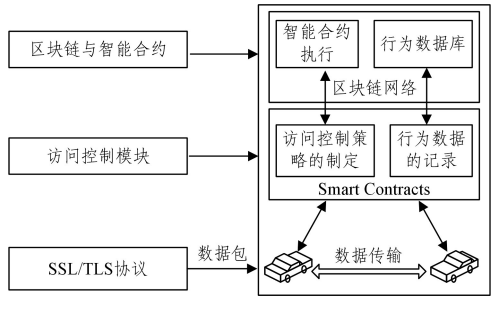

图 5 区块链车联网安全通信框架

Fig. 5 Security communication framework of blockchain Internet of vehicles

SSL/TLS[75]协议模块用于车联网节点之间的数据传输过程，首先该协议协商出会话密钥以及加密算法，然后节点之间通过密钥对数据进行加密传输。部署策略如图 6 和图 7 所示。

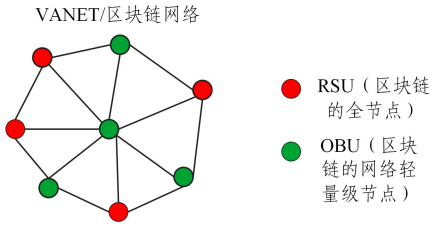

图 6 VANET/区块链网络

Fig. 6 VANET/blockchain network

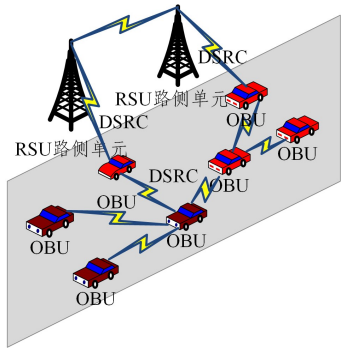

图 7 区块链车联网场景图

Fig. 7 Scene diagram of blockchain Internet of vehicles

4.1.4 安全性与有效性

在基于区块链的车联网分布式架构中，攻击者无法通过入侵单个 PDP 来篡改节点的访问权限，除非它控制了超过 51%的网络节点，因此该架构提高了车联网中分布式访问控制的安全性。同时区块链网络存储了节点的公钥信息和历史通信行为数据，为智能合约提供部署和运行平台，相比集中架构更加有效。

4.2 5G 轻量级安全通信

4.2.1 安全通信思路

5G 智能车联网场景[76]由车载单元 OBU、路侧单元 RSU、人、5G 网络与卫星网络组成，为终端用户提供智能服务，如图 8 所示。

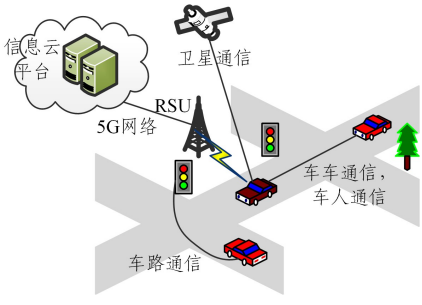

图 8 5G 车联网场景图

Fig. 8 Scene diagram of 5G Internet of vehicles

5G 网络对车辆异构性的安全通信有着更高的要求。5G 智能车联网安全框架分为 3 层：智能安全感知层、智能安全网络层和智能安全应用层，如图 9 所示。

图 9 5G 智能安全车联网框架图

Fig. 9 Framework of 5G smart and secure Internet of vehicles

在 5G 的智能安全网络层中高速传输数据时，必须确保敏感数据的机密性。文献[77]设计了一个轻量级的安全保护机制，在 mMTC，uRLLC 应用场景下提出了一种将随机信号与无线信道相结合的密钥生成方法，解决了无线信道随机性有限和移动受限时密钥生成率低的问题。当信道特性变化缓慢时，合法的发送端和接收端从接收信号空间提取密钥，通过控制发送信号的方差来改善接收信号的随机性，从而使密钥的更新与时间的方差无关。因此无线信道安全机制能够快速更新密钥，减少网络信令开销和缩短延迟，满足了轻量级的安全通信要求。

4.2.2 目的

5G 网络的传输速率是 4G 网络的数倍，车联网接入 5G 网络以后，在海量车载单元接入接出的同时要保证敏感数据的完整性、机密性和低延迟，以维持车联网中的轻量级安全机制。

4.2.3 安全性与有效性

为了设计轻量级的安全保护机制，文献[78]提出一种用于客户端-服务器体系结构的可搜索加密方案。该方案利用模块化的可逆性质，有助于其在安全的反向索引表上进行搜索，可确保更高级别的安全性。无线信道中的物理参数常用于密钥生成，但是由于无线信道中的噪声容易产生量化误差，降低了授权用户之间的密钥一致性（KAR）。为了实现高 KAR，Wang 等[79]提出一种基于分组和移位的鲁棒量化方案，其中所有可用参数都用于密钥生成。该方案将随机信号和无线信道相结合，解决了密钥生成率低的问题，提高了效率。文献[80]提出一种基于 MIMO 的接收信号空间的密钥生成模型。合法的发送方和接收方从接收信号空间提取密钥，并控制发送信号的方差来改善接收信号的随机性，从而使密钥的更新与无线信道的时间方差无关，并以最佳的功率分配方法来最大化密钥率。该方法在确保快速更新密钥的同时，保护了数据的隐私性和完整性，因此具有安全性与高效性。

5 分析

5.1 隐私保护

车辆具有高速移动的特性，车辆的各种信息需要被保护以防止泄露。隐私保护主要包括以下 3 个方面。

（1）位置隐私。车辆的位置状态信息在车联网中起标识作用，但又不可泄露，地位特殊。车联网中的车辆会周期性地通过路侧单元向其他节点发送自己的位置信息，容易被监听和追踪。

(2)数据隐私。在车辆行驶过程中,用户每一次操作都会被记录和保存下来。这些用户隐私数据被采集,然后传入车联网云端,在数据传输过程中,信息具有机密性,不能被泄露。

(3)身份隐私。车联网云端存储着大量的车主信息,如果攻击者攻击服务器和云服务系统,并且获取了这些信息,就会伪造身份发起 Sybil 攻击,即控制多个虚假身份进行攻击,后果将会十分严重。

5.2 问题

不同的认证方案对应不同的通信应用场景,根据车辆在车联网中动态移动的特性,我们综合了各种文献,给出互信认证与安全通信面对的主要问题。

(1)成本较高。车联网中路侧单元是无线通信的接入点,车-路侧单元的通信协作需要大量的资金投入,如基础设施更新维护所需的人力、物力等。路侧单元需要全年不断的人员维护以及能源供应,才能保持通信长期稳定可靠。

(2)通信标准不统一。目前对于车联网,各国的通信标准和技术不一致。多种不同的网络通信协议导致的主要问题有通信效率低、计算性能得不到保障、传输时延高,导致无法保证可靠的网络连接和数据传输。

(3)隐私和信息安全保护。无线通信会引起数据传输过程中的各种问题,如重放、假冒和监听等。

因此在车联网中,研究如何进行车辆的互信认证和安全通信非常重要。

5.3 典型攻击

目前,车联网中存在许多安全威胁,各种类型的攻击会导致车联网信息资源在共享过程中数据的机密性和可用性降低[18],以下是车联网中的典型攻击[81-87]:

(1)女巫攻击(Sybil Attack)。恶意节点伪造多个非法身份窃取信息。在车联网中,每个节点都有固定的唯一 ID,攻击节点通过使用其他合法节点的 ID 来发起访问,窃取信息。

(2)信息篡改攻击。攻击节点篡改收到的信息,并将篡改后的错误信息发送给其他节点。

(3)重放攻击。攻击节点窃取合法节点的认证凭证,再将它重新发送给认证节点,破坏认证的正确性,以达到欺骗的目的。

(4)拒绝服务攻击(Denial of Service,DoS)[21]。DoS 攻击通过在车载网络中充斥无用的信息来阻塞信道,降低网络的效率,从而导致合法车辆的节点无法正常请求资源信息。

(5)中间人攻击(Man In The Middle Attack,MITM)。MITM 攻击可以恶意控制两个或多个节点之间的通信信道,并且可以拦截、嗅探、篡改或替换目标受害节点的数据。而受害节点被隐瞒,从而认为通信信道是安全的。

6 未来趋势与展望

6.1 趋势

车联网安全防护体系由两大部分组成:一是将车联网设备与车辆内部网络连接,即车载网络;二是将车联网设备连接到互联网,与外界信息进行交换,即车辆互联网。由于车联网具有网络拓扑高速变化的特性,需要建立高实时性和低延迟性的多场景认证技术和通信技术。

6.1.1 多场景认证

由于车联网的主动安全、行车效率、车载娱乐等多场景业务需求越来越广泛,这些丰富的应用场景[88]导致车辆容易被远程控制。可以看出,针对车联网安全的攻击也不断变化。因此保证安全的多场景认证技术面临着诸多问题,安全危胁贯穿整个网络架构,还有待进一步解决。

6.1.2 通信技术

5G 技术[89]的应用使车联网的通信[90]时延更低、数据传输速率更快[91]以及网络覆盖范围更广。但是 5G 增加了车联网网络拓扑的不稳定性,从而引发了更多安全问题。在 5G 车联网中,为了保护用户信息在经过基站及路侧单元时不被盗取,通信的认证依旧是研究的焦点。当前使用最多的互信认证技术主要有椭圆曲线密码、身份认证以及数字签名技术。在 5G 通信中,可以结合 SDN 分层的网络结构进一步实现互信认证。

6.2 5G 安全研究展望

本文主要探讨了车联网的互信认证方面与通信技术方面,而车联网的信息安全不仅限于身份认证和通信数据传输方面。车联网中的通信技术标准并不唯一,且异构网络具有多样性[92],这些都给目前车联网的隐私和安全保护带来了挑战。

5G 技术带来的不只是通信速度的提升,还增加了信道流量,从而使得车联网需要更好的流量分载算法。5G 通信网络中每个节点的资源、数据传输率在提升用户体验的同时不可避免地会带来干扰。Nam[93]提出一种基于 5G 移动通信的干扰处理技术,其在对干扰信号进行解码和处理的同时能增加有效信息的接收率。

结束语 车联网应用越来越普遍,网络安全形势日趋严峻。本文主要讨论了目前车联网接入场景中的身份认证问题与车联网通信过程中的安全问题。对于安全互信认证所面临的身份匿名保护和多节点隐私问题,本文在实时通信交互场景下节点间进行信息共享读取和安全认证交易方面,介绍了部分解决方案。车联网的匿名接入安全互信认证、群组接入安全互信认证、跨域通信安全互信认证在满足安全属性的前提下都拥有较好的通信和计算性能,在车辆切换场景中有较好的应用效果。

车联网通信的安全可靠性是推动车联网发展的重要条件之一。本文针对车联网通信安全问题,介绍了基于区块链的车联网安全通信框架、基于 5G 的轻量型车联网安全通信框架,在有效保证数据传输过程中信息完整性以及机密性的前提下,降低通信时延,减少计算资源的消耗,并对车联网未来研究的重点趋势进行了预测和展望。当前车联网和 5G 应用相结合,能够更好地建立统一的安全体系,但同时 5G 车联网也将面临更大的挑战,未来需要进一步的研究。

参 考 文 献

[1] MI C. For the first time in the world, Tencent Keen Lab successfully hacked Tesla[EB/OL]. https://www.ithome.com/html/auto/259086.htm.

[2] Baidu successfully cracked the T-BOX system, car networking

security reached a new level [EB/OL]. http://www.elecfans.com/qichedianzi/20161130453520.html.

[3] SANKAR M, DAYA S G, BISWAS G P. An efficient and batch verifiable conditional privacy-preserving authentication scheme for VANETs using lattice[J]. Springer Vienna, 2019, 101(12): 1763-1788.

[4] HONG Z, WEN J Y, CUI J, et al. Efficient Conditional Privacy-Preserving and Authentication Scheme for Secure Service Provision in VANET[J]. Tsinghua Science and Technology, 2016, 21(6): 620-629.

[5] XIE Y, XU F, LI D, et al. Efficient Message Authentication Scheme with Conditional Privacy-Preserving and Signature Aggregation for Vehicular Cloud Network[J]. Wireless Communications and Mobile Computing, 2018, 2018: 1-12.

[6] YONG X, LI B W, JIAN S, et al. EIAS-CP: new efficient identity-based authentication scheme with conditional privacy-preserving for VANETs [J]. Telecommunication Systems, 2017, 65(2): 229-240.

[7] WU L B, FAN J, XIE Y, et al. Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks[J]. International Journal of Distributed Sensor Networks, 2017, 13(3): 334-350.

[8] XIE Y, WU L B, ZHANG Y B, et al. Efficient and Secure Authentication Scheme with Conditional Privacy-Preserving for VANETs[J]. Chinese Journal of Electronics, 2016, 25(5): 950-956.

[9] LIU H, LI H, MA Z. Efficient and Secure Authentication Protocol for VANET[C]// International Conference on Computational Intelligence & Security. IEEE, 2010.

[10] RAJPUT U, ABBAS F, WANG J, et al. CACPPA: A Cloud-Assisted Conditional Privacy Preserving Authentication Protocol for VANET [C] // IEEE/ACM International Symposium on Cluster. ACM, 2016.

[11] LO N W, TSAI J L. An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks Without Pairings[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(5): 1319-1328.

[12] BUTCHER A, LUCKETT R, VERDON J, et al. Local Magnitude Discrepancies for Near-Event Receivers: Implications for the U. K. Traffic-Light Scheme[J]. Bulletin of the Seismological Society of America, 2017, 107(2): 532-541.

[13] KAIWARTYA O, ABDULLAH A H, CAO Y, et al. Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects[J]. IEEE Access, 2017, 4(pp): 5356-5373.

[14] LI D W, WANG Z Y, ZHAO J G. Security analysis of elliptic curve cryptosystem [J]. Computer Technology and Development, 2012, 22(4): 227-230, 234.

[15] AGNEW G B, MULLIN R C, VANSTONE S A. An implementation of elliptic curve cryptosystems over F/sub 2/155 [J]. IEEE Journal on Selected Areas in Communications, 2002, 11(5): 804-813.

[16] JOHNSON D, MENEZES A, VANSTONE S. The Elliptic Curve Digital Signature Algorithm (ECDSA) [J]. International Journal of Information Security, 2001, 1(1): 36-63.

[17] WEI P C, ZHANG W, LIAO X F, et al. Construction of hash function with secret key based on double chaotic system [J]. Journal of Communications, 2006, 27(9): 27-33.

[18] HAMANN E, KREYSS J, VASUDEVAN N. Digital signature: US7096365 B1[P]. 2006-08-22.

[19] CHRISTIDIS K, DEVETSIKIOTIS M. Blockchains and Smart Contracts for the Internet of Things[J]. IEEE Access, 2016, 4: 2292-2303.

[20] WANG A P, FAN J G, GUO Y L. Application of Blockchain in Energy Interconnection[J]. Electric Power Information & Communication Technology, 2016, 14(9): 1-6.

[21] ZHAO Z G. An Efficient Anonymous Authentication Scheme for Wireless Body Area Networks Using Elliptic Curve Cryptosystem[J]. Journal of Medical Systems, 2014, 38(2): 13.

[22] LI X, LIU T, OBAIDAT M S, et al. A Lightweight Privacy-Preserving Authentication Protocol for VANETs[J]. IEEE Systems Journal, 2020, PP(99): 1-11.

[23] JIANG Y, GE S, SHEN X. AAAS: An Anonymous Authentication Scheme Based on Group Signature in VANETs[J]. IEEE Access, 2020, PP(99): 1-1.

[24] CHENG S, MINGYUE Z, WEIPING P. Efficient pairing-based batch anonymous authentication scheme for VANET[J]. The Journal of China Universities of Posts and Telecommunications, 2018, 25(1): 89-98.

[25] PRADWEAP R V, HANSDAH R C. A Novel RSU-Aided Hybrid Architecture for Anonymous Authentication (RAHAA) in VANET[C]// Proc. of the International Conference on Information Systems Security. 2013.

[26] ROSELINMARY S, MAHESHWARI M, THAMARAISELVAN M. Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA)[C]// 2013 International Conference on Information Communication and Embedded Systems (ICICES). IEEE, 2013.

[27] HAN S, BAN D, PARK W, et al. Localization of Sybil Nodes with Electro-Acoustic Positioning in VANETs[C]// 2017 IEEE Global Communications Conference(GLOBECOM 2017). IEEE, 2017.

[28] ALKAHTANI M S. Survey on security attacks in Vehicular Ad hoc Networks (VANETs)[C]// International Conference on Signal Processing & Communication Systems. IEEE, 2013.

[29] MA Z, ZHANG J, GUO Y, et al. An Efficient Decentralized Key Management Mechanism for VANET With Blockchain [J]. IEEE Transactions on Vehicular Technology, 2020, 69(6): 5836-5849.

[30] SHEHADA D, YEUN C Y, ZEMERLY M J, et al. A secure mobile agent protocol for vehicular communication systems[C]// International Conference on Innovations in Information Technology. IEEE, 2015.

[31] MOKHTAR B, AZAB M. Survey on Security Issues in Vehicular Ad Hoc Networks [J]. Alexandria Engineering Journal, 2015, 54(4): 1115-1126.

[32] SAMARA G, ALSALIHY W, SURESS R. Security issues and challenges of Vehicular Ad Hoc Networks (VANET)[C]// International Conference on New Trends in Information Science & Service Science. IEEE, 2010.

[33] ADHIKARY K, BHUSHAN S. Recent techniques used for preventing DOS attacks in VANETs[C]// International Conference on Computing. 2017.

[34] 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): 2681-2691.

[35] XU C, HUANG X, MA M, et al. An Anonymous Handover Authentication Scheme Based on LTE-A for Vehicular Networks [J]. Wireless Communications & Mobile Computing, 2018, 2018: 1-15.

[36] RAHNAMA A, BEHESHTI-ATASHGAH M, EGHLIDOS T, et al. A Lightweight Anonymous Authentication Protocol For IoT Wireless Sensor Networks[C]// 2019 16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC). 2019.

[37] 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.

[38] ZHU X, JIANG S, WANG L, et al. Privacy-preserving authentication based on group signature for VANETs[C]// 2013 IEEE Globecom Workshops (GC Wkshps). IEEE, 2013.

[39] XU J, DANG L. An efficient RFID anonymous batch authentication protocol based on group signature[J]. Discrete & Continuous Dynamical Systems, 2019, 12(4/5): 1489-1500.

[40] WAGHMODE R, GONSALVES R, AMBAWADE D. Security enhancement in group based authentication for VANET[C]// IEEE International Conference on Recent Trends in Electronics. IEEE, 2016.

[41] CIRNE P, ZUQUETE A, SARGENTO S. TROPHY: Trustworthy VANET routing with group authentication keys[J]. Ad Hoc Networks, 2018, 71(3): 45-67.

[42] BONG J S, SUH Y H, JANG U J, et al. RSU-independent Message Authentication Scheme using CRT-based Group Key in VANET[J]. Journal of KIISE, 2019, 46(3): 277-284.

[43] RAJABZADEH A M, SALMASIZA-DEH M, SUSILO W, et al. A Secure and Efficient Authentication Technique for Vehicular Ad-Hoc Networks[J]. IEEE Transactions on Vehicular Technology, 2018, 67(6): 5409-5423.

[44] LIN X, LU R. Pseudonym-Changing Strategy for Location Privacy[M]// Vehicular Ad Hoc Network Security and Privacy, 2015: 71-90.

[45] LAI C, ZHENG D, ZHAO Q, et al. SEGM: A secure group management framework in integrated VANET-cellular networks [J]. Vehicular Communications, 2018, 11(JAN.): 33-45.

[46] XU C, LIU H, PAN Z, et al. A group authentication and privacy-preserving level for vehicular networks based on fuzzy system [J]. Journal of Intelligent and Fuzzy Systems, 2020(2): 1-16.

[47] LUO C Y, HUO S W I, XING H Z. Identity-based cross-domain authentication scheme in pervasive environment[J]. Journal of Communications, 2011(9): 115-119, 126.

[48] ZHOU Y W, YANG B, WU Z Q, et al. Identity-based cross-domain direct anonymous authentication mechanism[J]. Science in China: Information Science, 2014, 44(9): 1102-1120.

[49] JIANG L, WU Z Q, WANG H Y, et al. Cross-domain Authentication Mechanism of DAA Based on Dynamic Trust Value[J]. Computer Engineering, 2010, 36(11): 156-158.

[50] CHEN Y, DONG G, BAI J, et al. Trust Enhancement Scheme for Cross Domain Authentication of PKI System[C]// 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). 2019.

[51] ZHOU Z C, LI L X, LI Z H. et al. Efficient cross-domain authentication scheme based on blockchain technology[J]. Journal of Computer Applications, 2018, 38(2): 316-320, 326.

[52] ALI G, AHMAD N, CAO Y, et al. xDBAuth: Blockchain Based Cross Domain Authentication and Authorization Framework for Internet of Things[J]. IEEE Access, 2020, 8: 58800-58816.

[53] MISCIONE G, ZIOLKOWSKI R, ZAVOLOKINA L, et al. Tribal Governance: The Business of Blockchain Authentication[C]// Hawaii International Conference on System Sciences (HICSS). 2018.

[54] XU C, HUANG X, MA M, et al. A Secure and Efficient Message Authentication Scheme for Vehicular Networks based on LTE-V[J]. KSII Transactions on Internet and Information Systems, 2018, 12(6).

[55] JIANG W, LI H, XU G, et al. PTAS: Privacy-preserving Thin-client Authentication Scheme in Blockchain-based PKI[J]. Future Generation Computer Systems, 2019, 96(7): 185-195.

[56] WANG W, HU N, LIU X. BlockCAM: A Blockchain-Based Cross-Domain Authentication Model[C]// 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC). IEEE, 2018.

[57] LIN J Q, JING J W, ZHANG Q L, et al. Summary of recent research on PKI technology[J]. Journal of Cryptography, 2015, 2(6): 487-496.

[58] MILLAN G L, PEREZ M G, PEREZ G M, et al. PKI-based trust management in inter-domain scenarios[J]. Computers & Security, 2010, 29(2): 278-290.

[59] GUAN Z Y, CHEN Y J, LI D W, et al. A cross-domain authentication scheme for Internet of Vehicles based on blockchain[J]. Cyberspace Security, 2020, 11(9): 62-69.

[60] DONG G, CHEN Y, FAN J, et al. Anonymous cross-domain authentication scheme for medical PKI system[C]// ACM Turing Celebration Conference - China. ACM, 2019.

[61] ZHAO G, BA Z, WANG X, et al. Constructing authentication web in cloud computing[J]. Security & Communication Networks, 2016, 9(15): 2843-2860.

[62] CHEN Y, DONG G, BAI J, et al. Trust Enhancement Scheme for Cross Domain Authentication of PKI System[C]// 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). 2019.

[63] TAN H, XUAN S, CHUNG I. HCDA: Efficient Pairing-Free Homographic Key Management for Dynamic Cross-Domain Authentication in VANETs[J]. Symmetry, 2020, 12(6): 1003.

[64] YAO Y, WANG X W, JIANG D D, et al. A cross-heterogeneous domain authentication model based on PKI technology [J]. Journal of Northeastern University (Natural Science Edition), 2011, 32(5): 638-641.

[65] ASGHAR M, DOSS R R M, PAN L. A Scalable and Efficient PKI Based Authentication Protocol for VANETs[C]// 2018

28th International Telecommunication Networks and Applications Conference (ITNAC). 2018.

[66] TANGADE S, MANVI S S, LORENZ P . Decentralized and Scalable Privacy-Preserving Authentication Scheme in VANETs [J]. IEEE Transactions on Vehicular Technology, 2018(99):1.

[67] KOSBA A, MILLER A, SHI E, et al. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts [C]// Security & Privacy. IEEE, 2016.

[68] WANG W, HOANG D T, HU P, et al. A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks[J]. IEEE Access, 2019(99):1-1.

[69] CHRISTIDIS K, DEVETSIKIOTIS M . Blockchains and Smart Contracts for the Internet of Things[J]. IEEE Access, 2016, 4: 2292-2303.

[70] GHAYET E M Z, TABBANE N, LABIOD H, et al. A Fuzzy Multi-Metric QoS-Balancing Gateway Selection Algorithm in a Clustered VANET to LTE Advanced Hybrid Cellular Network [J]. Vehicular Technology IEEE Transactions on, 2015, 64(2): 804-817.

[71] HE X, ZHANG H, LUO T, et al. Network capacity analysis for cellular based cognitive radio VANET in urban grid scenario [J]. Journal of Communications & Information Networks, 2017, 2(5): 1-11.

[72] LI H, PEI L, LIAO D, et al. Blockchain Meets VANET: An Architecture for Identity and Location Privacy Protection in VANET [J]. Peer to Peer Networking & Applications, 2019, 12(1): 1178-1193.

[73] LIU X, HUANG H, XIAO F, et al. A Blockchain-Based Trust Management With Conditional Privacy-Preserving Announcement Scheme for VANETs[J]. IEEE Internet of Things Journal, 2020, 7(5): 4101-4112.

[74] LI B H. Research on Secure Commu-nication Technology of Internet of Vehicles Based on Blockchain [D]. Chongqing: Chongqing University of Posts and Telecommunications, 2019.

[75] ALI ALKAZIMI, EDUARDO B. FERNANDEZ . Heartbleed: a misuse pattern for the OpenSSL implementation of the SSL/TLS protocol[C]// Proceedings of the 23rd Conference on Pattern Languages of Programs. Monticello, Illinois: The Hillside Group, 2016: 1-8.

[76] FENG D G, XU J, LAN X. Research on 5G Mobile Communication Network Security[J]. Journal of Software, 2018, 29(6): 303-315.

[77] YAN X C, MAO Y X, ZHAO H X. Security requirements and security protection countermeasures in typical 5G application scenarios[J]. ZTE Technology, 2019, 25(4): 6-13.

[78] SHAHZAIB T, SUSHMITA R, YOGACHANDRAN R, et al. A New Secure and Lightweight Searchable Encryption Scheme over Encrypted Cloud Data[J]. IEEE Trans on Emerging Topics in Computing, 2019, 7(4): 530-544.

[79] WENJIE W, HONGYAN J, XIANGGEN X, et al. A wireless secret key generation method based on Chinese remainder theorem in FDD systems[J]. ece China. Information ences, 2012, 55(7): 1605-1616.

[80] LOU Y M, JIN L, ZHONG Z, et al. Key generation scheme based on MIMO receiving signal space[J]. Science in China: Information Science, 2017, 47(3): 362-373.

[81] HAN S, BAN D, PARK W, et al. Localization of Sybil Nodes with Electro-Acoustic Positioning in VANETs[C]// 2017 IEEE Global Communications Conference (GLOBECOM 2017). IEEE, 2017.

[82] ALKAHTANI M S. Survey on security attacks in Vehicular Ad hoc Networks (VANETs) [C] // International Conference on Signal Processing & Communication Systems. IEEE, 2013.

[83] LAOUITI A, QAYYUM A, MOHAMAD SAAD M N . Attacks on Security Goals (Confidentiality, Integrity, Availability) in VANET: A Survey[M]// Advances in Intelligent Systems and Computing, 2015: 51-61.

[84] SHEHADA D, YEUN C Y, ZEMERLY M J, et al. Secure Mobile Agent Protocol for Vehicular Communication Systems in Smart Cities[J]. Information Innovation Technology in Smart Cities, 2018: 251-271.

[85] MOKHTAR B, AZAB M . Survey on Security Issues in Vehicular Ad Hoc Networks [J]. Alexandria Engineering Journal, 2015, 54(4): 1115-1126.

[86] SAMARA G, ALSALIHY W, SURESS R . Security issues and challenges of Vehicular Ad Hoc Networks (VANET) [C]// International Conference on New Trends in Information Science & Service Science. IEEE, 2010.

[87] ADHIKARY K, BHUSHAN S . Recent techniques used for preventing DOS attacks in VANETs[C]// International Conference on Computing. 2017.

[88] LI L C. Research on Resource Scheduling Method of Mobile Edge Computing in the Internet of Vehicles Scenario[D]. Wuhan: Huazhong University of Science and Technology, 2018.

[89] PARKVALL S, DAHLMAN E, FURUSKAR A, et al. NR: The New 5G Radio Access Technology[J]. IEEE Communications Standards Magazine, 2018, 1(4): 24-30.

[90] SHI H, BAI X, REN C, et al. Development of Internet of Vehicle's Information System based on Cloud[J]. Journal of Software, 2014, 9(7): 15-21.

[91] WANG X, NING Z, HU X, et al. A City-Wide Real-Time Traffic Management System: Enabling Crowdsensing in Social Internet of Vehicles[J]. IEEE Communications Magazine, 2018, 56(9): 19-25.

[92] MARICA A, CLAUDIA C, ANTONELLA M. Priority-Based Content Delivery in the Internet of Vehicles through Named Data Networking[J]. Journal of Sensor & Actuator Networks, 2016, 5(4): 17.

[93] NAM W, BAI D, LEE J, et al. Advanced interference management for 5G cellular networks[J]. IEEE Communications Magazine, 2014, 52(5): 52-60.

WANG Chun-dong, born in 1969, Ph.D, professor, is a senior member of China Computer Federation. His main research interests include network information security, mobile intelligent terminal security, public opinion analysis and control, Internet of Things security and security situation awareness.