doi:10.19562/j.chinasae.qcgc.2024.02.012

车载自组网络下基于量子随机数的高效组密钥分发方案*

石 琴[1,2],单 榴[1,2],程 腾[1,2],刘 强[1,2],王川宿[3],张 星[3]
(1. 合肥工业大学汽车与交通工程学院,合肥 230009; 2. 安徽省智慧交通车路协同工程研究中心,合肥 230000;
3. 奇瑞汽车股份有限公司,芜湖 241000)

[摘要] 针对车载自组网络近场通信中密钥分发通信开销大、安全性低的问题,本文提出了一种基于量子随机数的高效量子组密钥分发方案。在该方案中:(1)通过车端和云端的量子随机数共同生成车辆的匿名凭证,并采用零知识证明方式实现车辆与路端的身份互认,保护了车辆隐私;(2)通过一种两段式的组密钥,即路端和云端的两个关键参数实现了组密钥的更新。组密钥在保证前向安全和后向安全的前提下,信令开销减少了一半,大大缩短了组密钥下发时间。最后,通过安全性和性能分析证明了该方案的安全性。

关键词:车载自组网络;匿名认证;组密钥;信息安全

Efficient Group Key Distribution Scheme Based on Quantum Random Numbers in VANETs

Shi Qin[1,2], Shan Liu[1,2], Cheng Teng[1,2], Liu Qiang[1,2], Wang Chuansu[3] & Zhang Xing[3]
1. *School of Automotive and Transportation Engineering, Hefei University of Technology, Hefei* 230009;
2. *Intelligent Transportation Vehicle-Road Collaborative Engineering Research Center of Anhui Province, Hefei* 230000;
3. *Chery Automobile Co., Ltd., Wuhu* 241000

[**Abstract**] To address the problem of high communication overhead and low security of key distribution in the near-field communication of VANETs, an efficient quantum group key distribution scheme based on quantum random numbers is proposed in this paper. In this scheme, Firstly, the anonymous credentials of the vehicle are jointly generated by quantum random numbers at the vehicle side and the cloud side, and zero-knowledge proof is used to achieve mutual identity recognition between the vehicle and the road side, which protects the privacy of the vehicle. Then, a two-stage group key achieves the update of the group key, i.e. two key parameters at the roadside and the cloud side. The group key reduces the signaling overhead by half and greatly shortens the group key issuance time while ensuring forward and backward security. Finally, the security of the scheme is demonstrated by security analysis and performance analysis.

Keywords: VANETs; anonymous authentication; group key; information security

前言

车载自组网络技术(VANET)作为智能交通系统的重要组成部分被认为是解决交通拥堵问题的有效手段之一[1-2]。在车联网场景下,车辆与车辆之间以及车辆与路端之间会交换包括车辆的位置、速度、行驶轨迹等隐私数据[3-4]。然而,由于其特殊的网络

* 安徽省自然科学基金(2208085MF171)、中央高校基本科研业务费专项资金(JZ2023YQTD0073)和国家自然科学基金(82171012)资助。
原稿收到日期为 2023 年 06 月 24 日,修改稿收到日期为 2023 年 07 月 30 日。
通信作者:程腾,副教授,博士,E-mail:cht616@hfut.edu.cn。

结构,车载自组网络极易受到安全攻击[5-6]。随着VANET的广泛应用,车载自组网络中隐私保护和身份认证问题变得尤为重要。为保证通信的完整性和保密性,数据需要进行加密。

由于车载自组网络的网络拓扑结构极易发生变化,为了保证前向安全和后向安全,密钥需要及时更新。考虑到车载自组网络中通信对象的计算能力较弱,传统基于大数因子分解的公私钥加密方式难以适用[7-8]。相比之下,基于离散对数问题的椭圆曲线算法[9-11]在计算上有很大提高,但随着量子计算的出现,基于公私钥的加密方式的安全性也难以保证[12]。

为保证通信双方的身份合法性,须进行身份认证。然而,传统基于PKI数字证书的身份认证方式存在隐私泄露的风险,且可拓展性差、管理维护成本高,并存在CA安全性等问题[13-15]。基于匿名凭证的身份认证方法可以克服隐私泄露和被追踪的风险,但普通匿名凭证生成依赖于自身产生的伪随机数,存在安全隐患[16-17]。此外,传统方案中认为路端设备大多安全[18],但长期处于室外,存在物理破解可能性。因此,为在保护通信隐私和用户隐私的前提下实现可靠的身份认证,需要对身份认证信息进行真正的匿名处理。

目前密钥分发方式主要存在两种,集中式密钥分发方案与分布式密钥分发方案。分布式密钥分发方式指一次性会话由所有参与者决定,目前分布式的组密钥分发存在基于逻辑树的更新策略,例如Jiao等[19]提出了一种简单高效的逻辑密钥树节点编码方法,并给出了其更新算法,为在LKH的树结构中实现新的加解密方案提供了基础。而基于逻辑树的节点编码方式,也出现了许多其他变种的更新方案,如Yildiz等[20]在文中提到了使用Factorial tree,并详细介绍了Factorial tree相较于binary tree key hierarchy的优点,即Factorial tree降低了密钥储存成本和密钥更新消息的数量。Shawky等[21]提出用区块链代替云端,实现组密钥的分发,路端需要对每一辆车形成一份智能合约,每次组成员更新时,路端都需要对智能合约进行更新。这种分布式的密钥分发虽然不需要可信服务器的参与,解决了用户分布比较广时密钥的分配问题。但是同样,当网络规模很大时,每个用户所要保存的主密钥的数量也就越多。而集中式密钥分发方案比大多数分布式密钥分发方案更有效,每一个用户不需要保存大量的密钥,只需要有一个和密钥分发服务器(KDC)之间共享的密钥就可以了,剩下的事情由KDC安排。Kamil等[22]在LTE-V2X的场景下,提出了一套基于无证书身份认证的组密钥分发策略,但是在他的方案中,只考虑了车端身份的合法性,并没有将路端设备的合法性考虑在内。Tan等[18]提出的方案也实现了匿名与隐私保护,同时创新地将矩阵应用于数据的加解密,但是作者并没有提到组密钥是如何更新的。集中式密钥分发方案存在一个缺陷,即当网络的规模很大时,KDC要保存大量的密钥,各个用户和KDC之间的通信量也会很大,造成了KDC的负担过重的问题。

为解决上述VANET通信中涉及的隐私和安全问题,本文中提出了一种适用于车载自组网络下基于量子随机数的高效组密钥生成方案。在该方案中,通过基于车端与云端的量子随机数产生车辆的匿名凭证,车路之间的身份认证通过云端以零知识证明的方式实现车辆与路端的身份互认。并提出了一种两段式的组密钥生成方案,通过第一个组通信密钥参数(GSP_c)和第二个组通信密钥参数(GSP_r)实现了组密钥的更新、安全性和实时性。文中结合车辆之间近场通信的方式,兼顾通信效率和安全措施的需要,在传统集中式密钥分发方案的基础上实现了对组密钥进行更新。

1　系统模型

在所提出的V2X场景中,车路云的架构如图1所示。云端与每一个RSU之间建立点对点连接通信,车路、车车之间采用PC5通信。云端由KDC、身份认证服务器(AUSF)和车载信息服务供货商(TSP)构成。KDC负责生成、分发和管理V2X场景中使用的量子密钥。AUSF负责车、路的身份认证,并为车

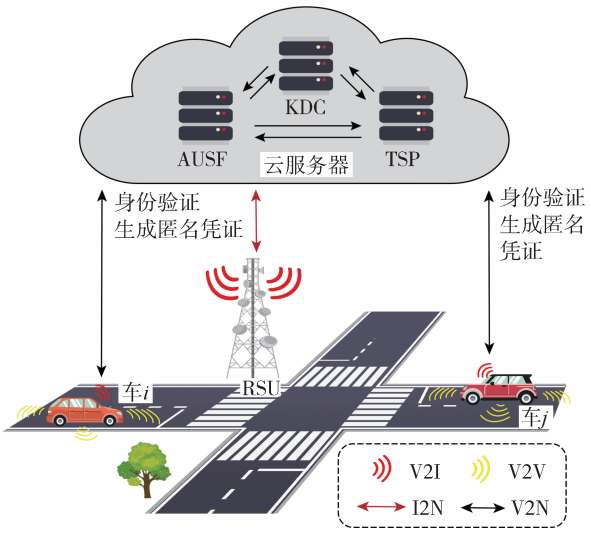


图1　车路云架构图

辆和RSU颁发匿名凭证,同时为路端设备提供零知识证明。TSP负责提供车辆相关服务,如车辆定位、导航等。在V2X场景中,车端、路端及云端均已预先充注一批量子会话密钥以及量子完整性验证密钥等待使用,车路、路云、车云之间互不信任,双方在真正通信前彼此之间均须进行身份互认。

2 具体方案

本文所提出的方案包括以下5个阶段:注册阶段、初始化阶段、组通信前密钥下发阶段、组通信阶段以及组成员变化时组密钥更新阶段。本方案中使用的主要数学符号如表1所示,方案流程图如图2所示。

表1 数学符号定义

符号	定义
VIN_i	车辆识别码
H()	单向哈希函数
T_{si}	时间戳
$E_{key}()$	用密钥加密
$D_{key}()$	用密钥解密
ANC_i	匿名身份凭证
$\{\}_{i=0}^{n}$	下标从0开始,依次累加到n
AddReq	宏定义
$PFSK_v$、$PFSK_r$	车端、路端预充注量子会话密钥
$PFIK_v$、$PFIK_r$	车端、路端预充注完整性验证密钥
$PFSK_{tagv}$、$PFSK_{tagr}$	车端、路端预充注量子会话密钥标识
$PFIK_{tagv}$、$PFIK_{tagr}$	车端、路端预充注完整性验证密钥标识

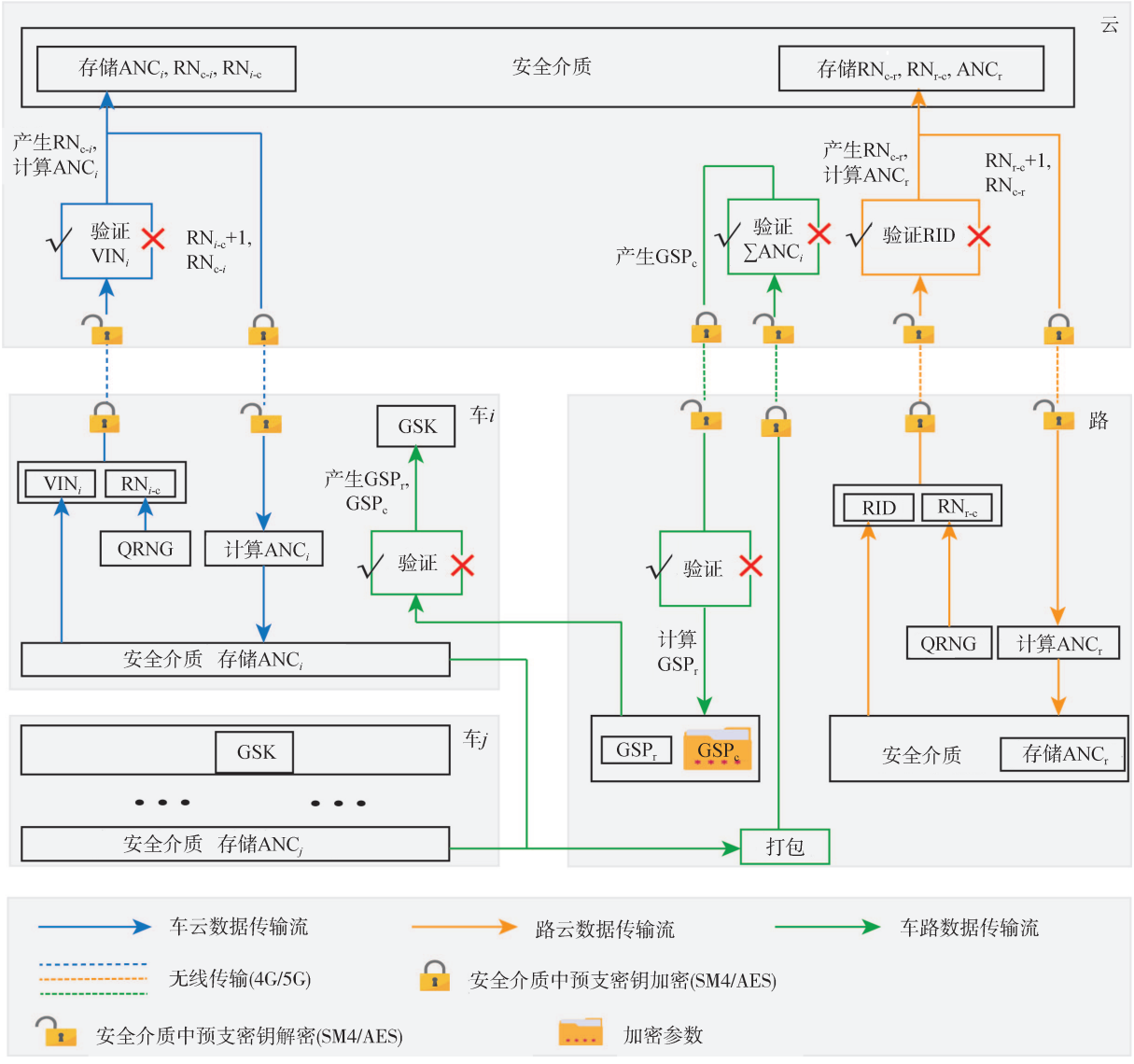


图2 方案流程图

2.1　注册

注册阶段主要完成车辆与路端设备的量子会话密钥与量子完整性校验密钥的预充注,以及车端唯一标识与路端唯一标识的云端入库操作。注册阶段完成后,云端存有路端设备的唯一标识RID、车端唯一标识VIN、车端与路端预充注的量子会话密钥以及量子完整性校验密钥。由于车端与路端预充注的密钥有限,使用过后就会丢弃,因此当车端或路端设备的密钥数量低于预设值时,就需要向云端申请量子会话密钥与量子完整性校验密钥进行补充。

2.2　初始化

车辆身份的唯一标识(车辆的VIN码)是由量子随机数发生器产生的一串随机数,在初始化阶段,需要进行车端与云端的身份互认,以及路端与云端的身份互认,并产生各自的匿名凭证存储在云端。初始化流程如图3所示。

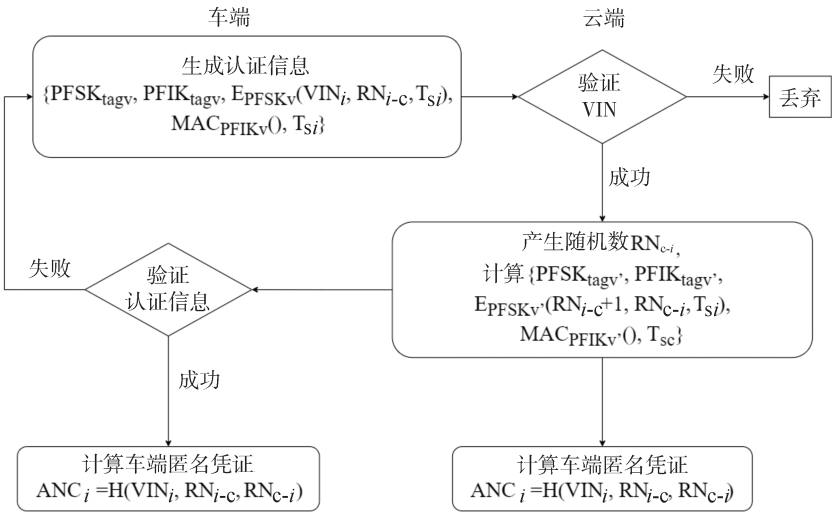


图3　初始化流程图

步骤1:车辆i的量子随机数发生器产生一个真随机数RN_{i-c},加上自己身份的唯一标识VIN_i码和当前时间戳后,使用车端预充注的量子会话密钥进行加密,得到加密后的消息$E_{PFSKv}(VIN_i, RN_{i-c}, T_{si})$,同时使用另一个预充注的量子完整性验证密钥对加密后的消息计算消息验证码(MAC),对消息进行拼接,拼接后,将消息发送给云端。

步骤2:云端的AUSF收到车辆的身份认证请求后,首先检查时间戳以判断消息的有效性,即检查$T_c-T_{sc}\leqslant T_\Delta$是否成立,如果时间差过大,则对收到的消息不做进一步处理。云端的AUSF根据接收的消息里面的$PFSK_{tagv}$与$PFIK_{tagv}$在云端的安全介质内找到对应的$PFSK_v$、$PFIK_v$以及对应密钥的拥有者VIN_i,然后对收到的消息计算MAC以验证消息的完整性,如果消息完整,则使用$PFSK_v$对消息进行解密。得到车辆的唯一标识VIN_i码与车端产生的随机数RN_{i-c},AUSF对解密后得到的VIN_i码与在数据库中查询到的VIN_i进行比较:如果两者相等,则云端的认证服务器产生一随机数并计算VIN_i、RN_{i-c}、RN_{c-i}的哈希值作为车端i的匿名凭证ANC_i,云端存储ANC_i、RN_{i-c}、RN_{c-i}。

步骤3:云端对RN_{i-c}进行加一操作,并加上自己产生的随机数RN_{c-i},和当前时间戳拼接后,使用云端预充注的一个车端量子会话密钥进行加密,得到加密后的消息$E_{PFSKv'}(RN_{i-c}+1, RN_{c-i}, T_{si})$,同时使用云端预充注的车端量子完整性验证密钥对加密后的消息计算MAC,对消息进行拼接,将拼接后的消息发送给车辆i。

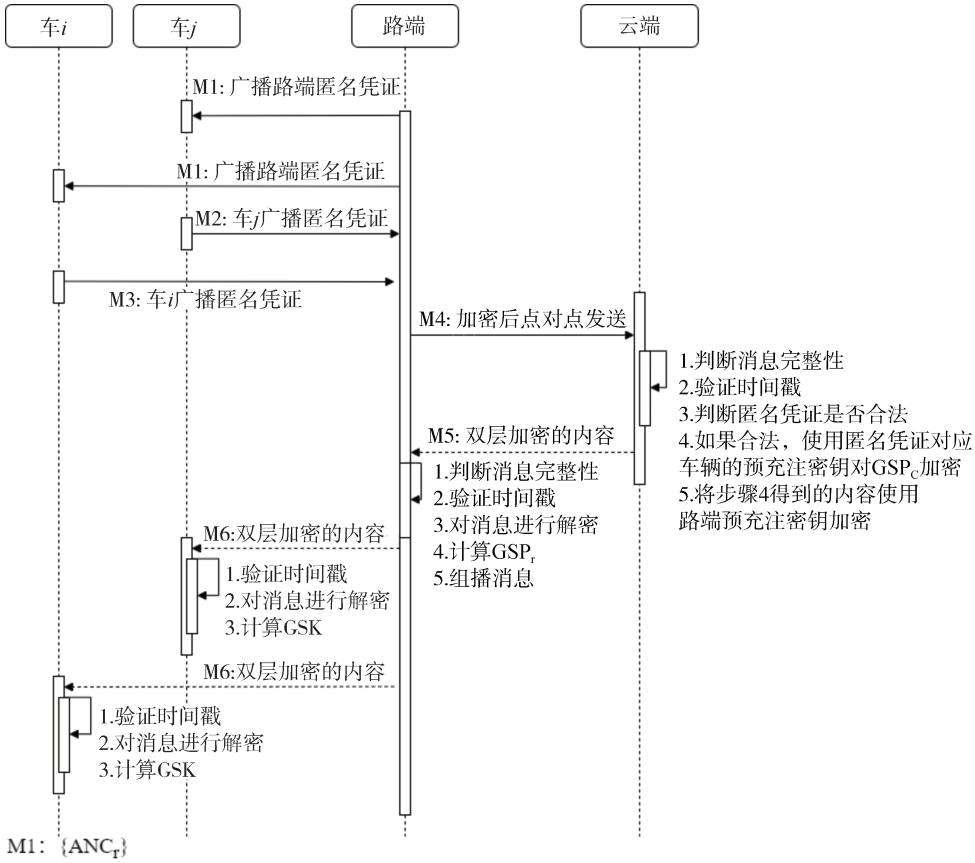
步骤4:车端收到云端返还的消息后,检查$T_i-T_{si}\leqslant T_\Delta$是否成立来检查$T_{si}$的新鲜度,如果时间戳与本地时间相差过大,则对消息不做进一步处理。车辆i根据收到的消息里面的$PFSK_{tagv'}$与$PFIK_{tagv'}$在车端的安全介质内找到对应的$PFSK_v$和$PFIK_v$,对收到的消息计算MAC值,以验证消息的完整性,若消息完整,则使用$PFSK_v'$对消息进行解密,得到云端返回的$RN_{i-c}+1$与云端产生的随机数RN_{c-i}。

步骤5:车端根据$\{VIN_i, RN_{i-c}, RN_{c-i}\}$计算得到自己的匿名凭证$ANC_i$,并储存在车端。车辆与路端进行通信时凭借匿名凭证进行互验,每辆车在与路端进行组通信前都需要进行身份认证,并完成匿名凭证的计算。

路端的身份认证流程与车端的身份认证流程相似,在此不做赘述,具体流程可参考初始化阶段车端的身份认证流程。

2.3 组通信前密钥下发

车路之间均采用PC5广播通信。每辆车i及每个RSU在初始化阶段后,均已完成与云端的身份认证,并通过计算得到了各自的匿名凭证ANC_i及ANC_r。云端在初始化过程后也得到了车端与路端的匿名凭证。车辆与路端交互得到组密钥的流程如图4所示。



M1: $\{ANC_r\}$

M2: $\{AddReq, ANC_j, H(RN_{c\text{-}j})\}$

M3: $\{AddReq, ANC_i, H(RN_{c\text{-}i})\}$

M4: $\{ANC_r, PFSK_{tagr}, PFIK_{tagr}, E_{PFSKr}(RID, \{AddReq, ANC, H(RN_{c\text{-}i})\}_{i=0}^{n}, T_{sr}), MAC_{PFIKr}(), T_{sr}\}$

M5: $\{ANC_r, PFSK_{tagr'}, PFIK_{tagr'}, E_{PFSKr'}(RID, \{ANC_i, PFSK_{tagv}, E_{PFSKv}(RN_{i\text{-}c}, GSP_c)\}_{i=0}^{n}, T_{Si}), MAC_{PFIKr'}(), T_{sc}\}$

M6: $\{GSP_r, \{ANC_i, PFSK_{tagv}, E_{PFSKv}(RN_{i\text{-}c}, GSP_c)\}_{i=0}^{n}\}$

图4 组密钥分发流程图

步骤1:路端在自己的广播范围内广播自己的ANC_r。

步骤2:当车辆驶入路端通信范围,通过PC5广播接收路端设备的匿名凭证。车端想要使用组通信服务时,需要向路端提出申请,车端向路端广播消息M3。

步骤3:路端对车端广播的匿名凭证进行聚合成组$\{AddReq, ANC, H(RN_{c-i})\}_{i=0}n$。

步骤4:路端连同当前路端设备的路端唯一标识与当前时间戳T_{sr}使用量子会话密钥进行加密,得到加密后的消息$E_{PFSKr}(RID, \{AddReq, ANC, H(RN_{c-i})\}_{i=0}n, T_{sr})$,路端使用路端安全介质内的预充注量子完整性校验密钥计算消息验证码$MAC_{PFIKr}()$,并在消息的头部添加当前路端设备的匿名凭证与所使用的$PFSK_{tagr}$与$PFIK_{tagr}$等必要信息,将M4转发给云端,对请求组通信服务的车端验证身份。

步骤5:云端接收路端对车端的身份认证请求,首先检查时间戳T_{sr}的新鲜度,在有效期内,云端

AUSF再根据消息里面的$PFSK_{tagr}$与$PFIK_{tagr}$在云端的安全介质内找到对应的$PFSK_r$、$PFIK_r$,以及对应密钥的拥有者ANC_r。对收到的消息计算MAC验证消息的完整性,若消息完整,则使用$PFSK_r$对消息进行解密。解密后得到路端设备的唯一标识码RID,以及待验证车辆的验证信息,AUSF对解密得到的RID与在数据库中根据ANC_r查询到的RID进行比对:如果两者相等,则表明该路端合法,云端进行步骤6。

步骤6:云端的认证服务器对待验证的车辆信息进行认证。根据车辆的ANC_i,云端找到生成匿名凭证的参数VIN_i、RN_{c-i}和RN_{i-c}。云端对查询到的RN_{c-i}进行哈希计算,与$\{AddReq, ANC_i, H(RN_{c-i})\}$中的哈希值$H(RN_{c-i})$进行比对。若两者相同,则车端身份验证成功。但此时车端对路端的身份仍不信任。

步骤7:云端对路端发送的车端的匿名身份验证完成后,云端根据车辆i的ANC_i找到生成匿名凭证的关键参数RN_{i-c}以及车端的一个$PFSK_v$。云端量子随机数发生器产生一个组通信密钥参数GSP_c,并储存在云端,以便后续车辆加入时快速查询。对RN_{i-c}、GSP_c进行加密后得到$E_{PFSKv}(RN_{i-c}, GSP_c)$。云端将验证通过后的所有车的组密钥关键参数$GSP_c$加密打包,使用PFIKr′计算MAC值后,在头部添加ANC_r、$PFSK_{tagr'}$、$PFIK_{tagr'}$,尾部添加当前时间戳T_{sc},拼接得到消息M5并将其转发给路端。

步骤8:路端根据收到的消息里面的ANC_r判断接收方身份是否与自己的匿名凭证相同,以确认是否是自己的消息。然后路端通过查明$T_r-T_{sc}\leqslant T_\Delta$是否成立来检查$T_{sc}$的新鲜度,验证时间戳有效后,路端根据消息体里的$PFSK_{tagr'}$与$PFIK_{tagr'}$在路端的安全介质内找到对应的$PFSK_{r'}$以及$PFIK_{r'}$。路端使用$PFIK_{r'}$对收到的消息计算MAC以验证消息的完整性,若消息完整,再使用$PFSK_{r'}$对消息进行解密。解密后路端得到一个RID,并将自己的RID与解密后的RID进行比对以验证身份。身份核验成功后计算所有通过云端认证的车辆的匿名凭证哈希值作为组密钥参数GSP_r,即$GSP_r=H(\{ANC_i\}_{i=0}n)$。

步骤9:路端将组密钥参数GSP_r与解密得到的消息进行拼接后得到M6,并通过PC5协议广播给车辆。

步骤10:车辆收到广播的消息后取得路端计算的组会话密钥参数GSP_r,然后根据自己的匿名凭证,找到属于自己的消息$\{ANC_i, PFSK_{tagv}, E_{PFSKv}(RN_{i-c}, GSP_c)\}$,并根据$PFSK_{tagv}$找到对应的$PFSK_v$对消息进行解密,得到自己随机数$RN_{i-c}$,以及云端产生的组会话密钥参数$GSP_c$。车辆$i$对解密得到的随机数与自己在初始化阶段产生的随机数进行比对,核验路端身份是否合法,若合法,则接受GSP_c。

2.4　组通信

身份合法的车辆已经获得了生成组通信加密密钥的两个关键参数GSP_r与GSP_c。车组车辆根据这两个参数计算得到组通信的对称密钥GSK,以此进行通信,其中$GSK=H(GSP_r, GSP_c)$。

2.5　组成员变化时组密钥更新

由于路端设备固定,而在一个路端广播通信范围内,车辆会持续动态更新,即会持续有新的车辆加入或离开。文中将路端广播通信范围内的车辆看成一个组,一个路端设备管理的组面临的车辆的更新可分为以下两种情况。

2.5.1　新成员加入

当新的车辆已完成初始化阶段,并准备加入当前路端设备想要获得组通信服务时,为防止新加入的车辆获得当前路端范围内车辆组通信广播的消息,需要对组通信加密的密钥进行更新。对于新加入的车辆j,车端、路端、云端须执行以下步骤。

步骤1:新加入的车辆j执行基于组通信前密钥下发阶段的步骤2。

步骤2:路端对新加入的车辆,向云端申请组成员增加请求。路端将新加入车辆的信息加密后发送给云端:类似于基于组通信前密钥下发阶段的步骤4。云端接收到的消息体为:$\{ANC_r, PFSK_{tagr}, PFIK_{tagr}, E_{PFSKv}(RID, AddReq, ANC_j, H(RN_{c-j}), T_{sj}), MAC_{PFIKv}(), T_{sr}\}$。与基于组通信前密钥下发阶段步骤4不同的是加密的消息体中只有新加入车辆j的认证信息。

步骤3:云端对新加入的车辆进行身份验证,如果车辆身份合法,则将该车辆加入当前路端的组内。并基于组通信前密钥下发阶段,云端查询当前车组通信的组密钥关键参数GSP_c,加密后计算MAC值,发送给路端。路端接收到的消息体为:$\{ANC_r, PFSK_{tagr'}, PFIK_{tagr'}, E_{PFSKr'}(RID, \{ANC_i, PFSK_{tagv}, E_{PFSKv}(RN_{i-c}, GSP_c)\}_{i=0}n, T_{si}), MAC_{PFIKr'}(), T_{sc}\}$。

步骤4:路端执行基于组通信前密钥下发阶段的步骤8,将新加入的车辆j加入当前路端的组,并重新计算GSP_r。路端将重新计算的组密钥参数GSP_r与从云端解密得到的内容$\{ANC_i, PFSK_{tagv}, E_{PFSKv}(RN_{i-c}, GSP_c)\}_{i=0}n$进行拼接,得到消息体$\{GSP_r, \{ANC_i, PFSK_{tagv}, E_{PFSKv}(RN_{i-c}, GSP_c)\}_{i=0}n\}$,并通过

PC5协议广播给车辆。

步骤5:对于新加入的车辆执行基于组通信前密钥下发阶段的步骤10。对于一直处于当前组内的车辆,则只对GSP_r进行更新。

步骤6:所有车辆执行组通信阶段的步骤,完成组密钥的更新。

2.5.2 组成员离开

步骤1:准备离开的车辆j向路端申请离开请求$\{DelReq, ANC_j, H(RN_{c-j})\}$。

步骤2:路端对准备离开当前组的车辆,验证当前组里是否存在车辆向云端申请组成员减少的请求。有则路端将离开车辆的信息加密后发送给云端:类似于组通信前密钥下发阶段的步骤3,得到$\{ANC_r, PFSK_{tagr}, PFIK_{tagr}, E_{PFSKv}(RID, DelReq, ANC_j, H(RN_{c-j}), T_{sr}), MAC_{PFIKr}(), T_{sr}\}$。与组通信前密钥下发阶段不同的是加密的消息体中只有新加入车辆j的认证信息。

步骤3:云端对准备离开的车辆进行身份认证,如果车辆身份合法,则将该车辆从当前路端的组内删除,重新产生新的GSP_c,并将执行结果告知路端。路端接收的消息体为:$\{ANC_r, PFSK_{tagr'}, PFIK_{tagr'}, E_{PFSKr'}(RID, \{ANC_i, PFSK_{tagv}, E_{PFSKv}(RN_{i-c}, GSP_c)\}_{i=0}n, T_{si}), MAC_{PFIKr'}(), T_{sc}\}$。

步骤4:路端执行基于组通信前密钥下发阶段的步骤8,将离开的车辆j从当前路端的组删除,并重新计算GSP_r。然后将组密钥参数GSP_r与解密得到的消息进行拼接,得到$\{GSP_r, \{ANC_i, PFSK_{tagv}, E_{PFSKv}(RN_{i-c}, GSP_c)\}_{i=0}n\}$,并通过PC5协议广播给车辆。

步骤5:当前组成员的所有车辆执行组通信阶段的步骤,完成组密钥的更新。

3 安全性分析

3.1 形式化安全性分析

采用Scyther对方案模型进行建模、分析和验证,以检测协议中可能存在的安全漏洞和缺陷,在对协议进行建模时需要对协议的安全属性进行声明,以描述协议应该满足的安全属性。这些属性描述了协议执行过程中安全相关的行为,例如身份认证、密钥交换、消息完整性、机密性等。通过声明和验证这些安全属性,可以检测协议实现中可能存在的漏洞和攻击,并帮助确保协议的正确性和安全性[23]。本文涉及到的安全属性如下:

Secret属性用于指定协议或系统中的机密(secret)信息。这些机密信息可能是协议中的加密密钥、密码等等,需要得到保护且只能在授权的条件下访问或使用。

Alive是一个用于验证协议或系统是否具有活性(liveness)属性的属性。如果一个系统或协议具有活性属性,那么在某个时间点上,它应该能够执行某些操作或产生某些响应。在Scyther中,Alive属性用于检查一个协议是否满足这种活性属性。

Weakagree是一种协议安全属性,指两个或多个实体在协议的某个点上是否达成一致(agreement)。在Scyther中,Weakagree属性用于检查协议中的实体是否能够达成共识,而不需要它们的决策完全相同。

Niagree是另一种协议安全属性,指两个或多个实体在协议的某个点上是否不能达成一致(disagreement)。在Scyther中,Niagree属性用于检查协议中的实体是否不能达成共识。

在本方案的建模中,共有3个角色,车端V、路端R与云端S,车端V与云端S生成匿名凭证的流程验证结果以及车端V与路端R的组密钥分发流程的验证结果如图5所示。从中可以看出3种角色都可以实现机密(Secert)、一致(Niagree)、存活(Alive)、弱一致(Weakagree)。这意味着实现了相互认证。综上所述,形式验证的结果表明所提出的方案是安全的。

3.2 非形式化安全性分析

在密码学中,须考虑前向安全性和后向安全性。前向安全是在当前密钥被攻击者窃取后,无法计算出之前的会话密钥,前向安全保护之前的通信不会受密钥在未来窃取伪造的威胁,保证上一时段密钥的安全。后向安全性是指在当前密钥被攻击者窃取后,无法计算出之后即将生成的密钥,攻击者不可伪造和推算下一时段的密钥信息,保证了下一时段的成员密钥安全[24-25]。

(1)前向安全性:在本方案中,使用了两段式密钥的方式,当一个车辆加入当前路端范围,须执行上述的初始化阶段与基于组的认证流程。在这个过程中,云端告知了新加入的车辆组密钥参数GSP_c,同时路端通过组播的方式告知了新加入车辆与组内原有成员组密钥参数GSP_r,对于新加入的车辆,由于不知道未加入组前的GSP_r',因此无法计算得到之前的组密钥GSK,实现了前向安全。

(2)后向安全性:当当前组内某车辆准备离开当前路端范围时,向路端发送请求,路端告知云端,云

Scyther results : verify

Claim				Status	Comments
MyProtocol	Vi	MyProtocol,Vi1	Secret RNsi	Ok	No attacks within bounds.
		MyProtocol,Vi2	Secret RNis	Ok	No attacks within bounds.
		MyProtocol,Vi3	Alive	Ok	No attacks within bounds.
		MyProtocol,Vi4	Weakagree	Ok	No attacks within bounds.
		MyProtocol,Vi5	Niagree	Ok	No attacks within bounds.
	R	MyProtocol,R1	Secret RNsr	Ok	No attacks within bounds.
		MyProtocol,R2	Secret RNrs	Ok	No attacks within bounds.
		MyProtocol,R3	Alive	Ok	No attacks within bounds.
		MyProtocol,R4	Weakagree	Ok	No attacks within bounds.
		MyProtocol,R5	Niagree	Ok	No attacks within bounds.
	S	MyProtocol,S1	Secret RNsi	Ok	No attacks within bounds.
		MyProtocol,S2	Secret RNis	Ok	No attacks within bounds.
		MyProtocol,S3	Secret RNsr	Ok	No attacks within bounds.
		MyProtocol,S4	Secret RNrs	Ok	No attacks within bounds.
		MyProtocol,S5	Secret GSK	Ok	No attacks within bounds.
		MyProtocol,S6	Alive	Ok	No attacks within bounds.
		MyProtocol,S7	Weakagree	Ok	No attacks within bounds.
		MyProtocol,S8	Niagree	Ok	No attacks within bounds.

Done.

图5　Scyther安全性验证结果图

端将对当前路端组内剩下车辆的组密钥参数GSP_c进行更新,使用车辆内预充注的密钥对GSP_c进行加密,并将加密的结果使用路端设备内预充注的密钥进行加密发送给路端。路端也将重新计算组密钥参数GSP_r,将结果组播给组内剩下车辆。得益于对称加密与单向哈希函数的快速,完美实现了后向安全,同时保障了及时性。

4　性能分析

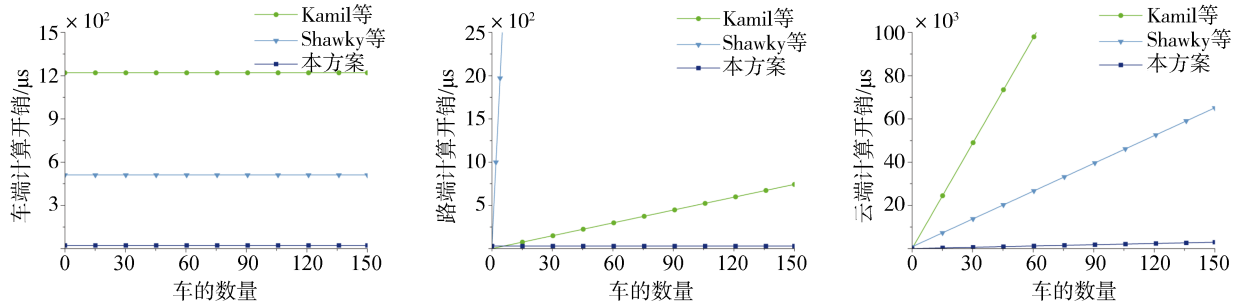
将本方案与目前存在的集中式与分布式组密钥分发方案进行了对比,并列举出其身份验证方法与主要加解密方式。对比结果如表2所示。

表2　不同方案对比

方案	类型	身份验证方法	加密/解密方法
Kamil[22]	集中式	无证书	ECC
Shawky[21]	分布式	匿名认证	ECC
本方案	集中式	匿名认证	量子

Shawky等[21]与Kamil等[22]都使用了基于ECC的椭圆曲线算法作为主要加密方式,但Shawky等使用区块链代替云端完成了组密钥的分发。

为定量地与其他方案对比,假设了一个车路云协同实验场景:当前场景共有n辆汽车,一个路端设备。计算车辆与路端和云端建立身份认证后并完成组密钥分发这个阶段所有交通参与者的通信开销,并对各个方案使用的方法进行对比,结果如图6~图8所示。



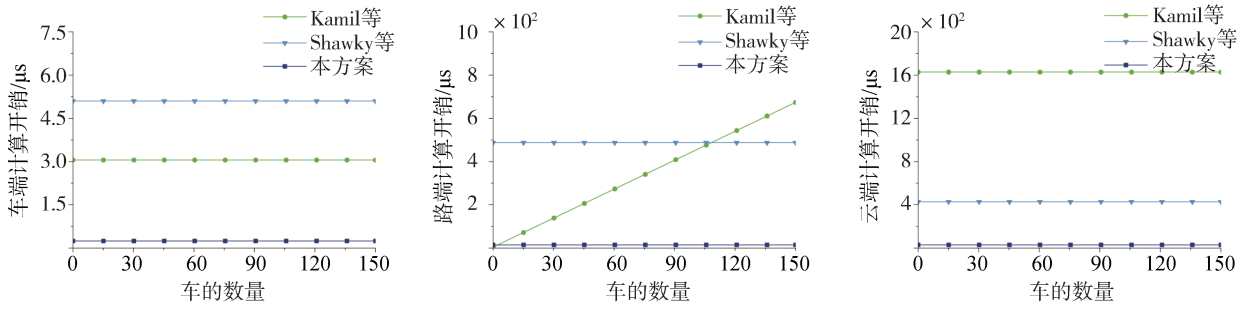
(a) 车端的计算开销　(b) 路端的计算开销　(c) 云端的计算开销

图6　无车进出时车路云的计算开销

对于车辆密钥的预充注,是产线的一次性操作,对预充注流程的时间消耗难以进行定量计算。此外,在现有条件下,一次充注的密钥数量可以实现较长时间的使用,无须频繁充注。因此,在考虑计算开销和信令开销时,并未将这些方面的开销纳入其中。

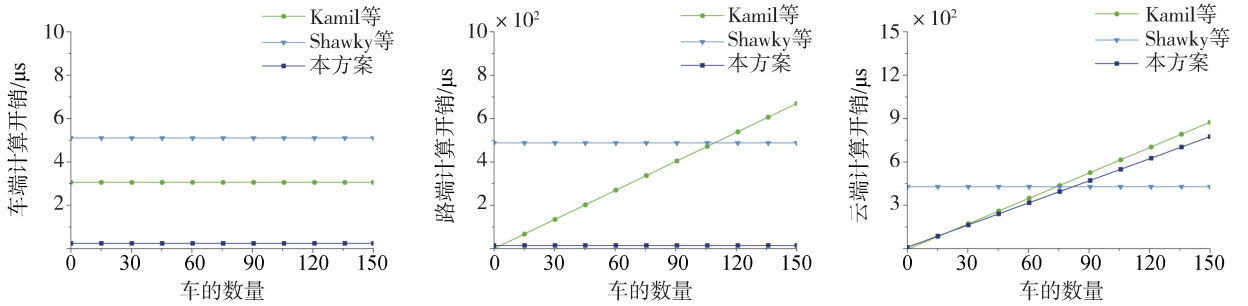
在网络通信中,建立一个连接所耗费的资源远大于内容存储耗费的资源,因此文中没有像传统方案一样计算参与者需要的字节数,而是比较建立连接的数量。表3为组密钥分发过程中车路云三者之间的流程与建立的总连接数。

在CPU型号为i5-7300hq、内存8 GB的设备上计算表4中操作的时间,由于每种计算的时间很短,因此通过循环100 000次,并取平均值,得到每次计



(a) 车端的计算开销 (b) 路端的计算开销 (c) 云端的计算开销

图7 新车加入时车路云的计算开销



(a) 车端的计算开销 (b) 路端的计算开销 (c) 云端的计算开销

图8 有车辆离开时车路云的计算开销

表3 信令开销

方案	过程	信令开销
Kamil[22]	Vehicle $\xrightarrow{n}$ RAN $\xrightarrow{1}$ Server $\xrightarrow{2}$ RAN $\xrightarrow{n+1}$ Vehicle Server $\xrightarrow{1}$ Vehicle	2n+5
Shawky[21]	Vehicle $\xrightarrow{n}$ RSU $\xrightarrow{1}$ Blockchain $\xrightarrow{n}$ Vehicle	2n+1
本方案	Vehicle $\xrightarrow{n}$ RAN $\xrightarrow{1}$ Server $\xrightarrow{1}$ RAN $\xrightarrow{1}$ Vehicle	n+3

表4 加密操作执行时间 μs

类别	定义	时长
T_h	单向哈希	0.245 6
T_{hmac}	MAC值	2.016
T_{sign}	ECC私钥签名	23.48
T_{veri}	ECC公钥验证	72.39
T_{mul}	ECC标量乘法	405.1
T_{add}	ECC点加运算	1.406
T_{sm}	SM4对称密钥加解密	5.100

算所需时间。假定所有方案使用的哈希算法为SHA-256,MAC算法为HMAC,使用相同的ECC椭圆曲线加解密算法,对称加密算法为SM4。具体时间开销如表5所示。测试所使用的代码已上传到https://gitee.com/liuqiang112358/timetest。

为保障前向安全性与后向安全性,在同一个路端范围内的车辆发生变化时,须及时进行组密钥更新。通常可分为新成员加入与成员撤销两个过程。表6和表7为车辆在执行组密钥更新时须执行的操作时间。其中新加入的车辆所需要的时间包括身份认证所需要的时间。

综上所述,可以得到车路云三者在不同状态下执行组密钥更新所需要的计算开销,如图6~图8所示。可以看到本文方案在多车组密钥分发阶段与组密钥更新阶段有着更大的优势,相比较于区块链的方式,信令开销减少一半。

表5 各种方案的计算费用比较(注册+组密钥分发总流程)

方案	车	路	服务器或第三方
Kamil[22]	$5T_h+3T_{add}+3T_{mul}$	$(3T_h+3T_{add})n$	$3T_{add}+T_h+(4T_h+4T_{mul}+T_{add})n$
Shawky[21]	$2T_{sm}+T_{mul}+T_{veri}+T_{sign}$	$(n+1)T_{sm}+n(T_{mul}+T_{veri})+T_{sign}$	$(n+2)T_{mul}+(n+1)T_{sign}$
本方案	$3T_{sm}+3T_{hamc}+2T_h$	$4T_{sm}+4T_{hamc}+2T_h$	$(3n+4)T_{sm}+(2n+4)T_{hamc}+(n+1)T_h$

表6　组密钥更新计算开销(加入)

方案	新加入车辆	原来车组车辆	路	云
Kamil[22]	$5T_h+3T_{add}+3T_{mul}$	T_h+2T_{add}	$(n+1)(T_h+3T_{add})$	$5T_{add}+4T_h+4T_{mul}$
Shawky[21]	$2T_{sm}+T_{mul}+T_{veri}+T_{sign}$	T_{sm}	$2T_{sm}+T_{mul}+T_{veri}$	$T_{mul}+T_{sign}$
本方案	$3T_{sm}+3T_{hamc}+2T_h$	T_h	$2T_{sm}+2T_{hmac}+T_h$	$4T_{sm}+4T_h+4T_{hmac}$

表7　组密钥更新计算开销(离开)

方案	原来车组车辆	路	云
Kamil[22]	T_h+2T_{add}	$n(T_h+3T_{add})$	$(n-1)(4T_{add}+T_h)$
Shawky[21]	T_{as}	$2T_{sm}+T_{mul}+T_{veri}$	$T_{mul}+T_{sign}$
本方案	T_h	$2T_{sm}+2T_{hmac}+T_h$	$(n+1)T_{sm}+2T_h+2T_{hmac}$

5　结论

根据车路云三者所处的环境,结合车端与云端的量子随机数发生器设计了一套匿名认证方案。同时根据车路云三者之间的通信方式,设计了一种新型的组密钥更新方式,实现了身份认证过程中车辆的隐私保护。通过两段式的组密钥生成方案实现组密钥的更新,通过云端产生的GSP_c组密钥参数保证组密钥安全性,通过路端产生的GSP_r组密钥参数实现了分发的高效率和实时性。当组成员更新频繁时,可以有效减少云端数据处理的压力。在这个过程中保证全过程的一次一密。整体上来说降低了组密钥通信开支,同时保证了通信的前向安全与后向安全。

参考文献

[1] HAN Y, SONG W, ZHOU Z, et al. eCLAS: an efficient pairing-free certificateless aggregate signature for secure VANET communication [J]. IEEE Systems Journal, 2022, 16 (1): 1637-1648.

[2] QI J Y, GAO T H, DENG X Y, et al. A pseudonym-based certificateless privacy-preserving authentication scheme for VANETs [J]. Vehicular Communications, 2022, 38.

[3] YANG Q, ZHU X Q, WANG X L, et al. A novel authentication and key agreement scheme for internet of vehicles [J]. Future Generation Computer Systems, 2023, 145: 415-428.

[4] GHANE S, JOLFEI A, KULK L, et al. Preserving privacy in the internet of connected vehicles [J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 22 (8): 5018-5027.

[5] AZAM S, BIBI M, RIAZ R, et al. Collaborative learning based sybil attack detection in vehicular AD-HOC networks (VANETS) [J]. Sensors, 2022, 22 (18).

[6] WANG X J, NIE L S, NING Z L, et al. Deep learning-based network traffic prediction for secure backbone networks in internet of vehicles [J]. ACM Transactions on Internet Technology, 2022, 22 (4): 1-20.

[7] FUEYO M, HERRANZ J. On the efficiency of revocation in RSA-based anonymous systems [J]. IEEE Transactions on Information Forensics and Security, 2016, 11 (8): 1771-1779.

[8] MOHAMED T M, AHMED I Z, SADEK R A. Efficient VANET safety message delivery and authenticity with privacy preservation [J]. PeerJ Computer Science, 2021, 7.

[9] ALI I, CHEN Y, ULLAH N, et al. An efficient and provably secure ECC-based conditional privacy-preserving authentication for vehicle-to-vehicle communication in VANETs [J]. IEEE Transactions on Vehicular Technology, 2021, 70(2): 1278-1291.

[10] GUO R, XU L, LI X, et al. An efficient certificateless ring signcryption scheme with conditional privacy-preserving in VANETs [J]. Journal of Systems Architecture, 2022, 129.

[11] GOUDARZI S, SOLEYMANI S A, ANISI M H, et al. A privacy-preserving authentication scheme based on Elliptic Curve Cryptography and using Quotient Filter in fog-enabled VANET [J]. Ad Hoc Networks, 2022, 128.

[12] BERNSTEIN D J, LANGE T. Post-quantum cryptography [J]. Nature, 2017, 549: 188 - 194.

[13] ZHANG L, KANG B, DAI F F, et al. Hybrid and hierarchical aggregation-verification scheme for VANET [J]. IEEE Transactions on Vehicular Technology, 2022, 71 (10): 11189-11200.

[14] WASEF A, LU R, LIN X, et al. Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks] [J]. IEEE Wireless Communications, 2010, 17 (5): 22-28.

[15] SALEM A H, ABDEL-HAMID A, EL-NASR M A. The case for dynamic key distribution for PKI-based VANETs [J]. International Journal of Computer Networks & Communications (IJCNC), 2016, 6 (1): 61-78.

[16] XI N, LI W H, JING L, et al. ZAMA: a ZKP-based anonymous mutual authentication scheme for the IoV [J]. IEEE Internet of Things Journal, 2022, 9 (22): 22903-22913.

[17] LI J, LI Y, CAO C, et al. Conditional anonymous authentication with abuse-resistant tracing and distributed trust for internet of vehicles [J]. IEEE Internet of Things Journal, 2021, 9 (11): 8749-8762.

[18] TAN H W, ZHENG W Y, GUAN Y G, et al. A privacy-preserving attribute-based authenticated key management scheme for accountable vehicular communications [J]. IEEE Transactions on Vehicular Technology, 2023, 72 (3): 3622-3635.

[19] JIAO R H, OUYANG H, LIN Y, et al. A computation-efficient group key distribution protocol based on a new secret sharing scheme [J]. Information, 2019, 10 (5): 175.

(下转第355页)

[10] NGUYEN A, GUERRA T, SENTOUH C, et al. Unknown input observers for simultaneous estimation of vehicle dynamics and driver torque: theoretical design and hardware experiments[J]. IEEE/ASME Transactions on Mechatronics, 2019, 24(6): 2508-2518.

[11] DOUMIATI M, VICTORINO A C, CHARARA A, et al. Onboard real-time estimation of vehicle lateral tire-road forces and sideslip angle[J]. IEEE/ASME Transactions on Mechatronics, 2011, 16(4): 601-614.

[12] LI X, XU N, LI Q, et al. A fusion methodology for sideslip angle estimation on the basis of kinematics-based and model-based approaches[J]. Proceedings of the Institution of Mechanical Engineers, Part D: Journal of Automobile Engineering, 2019, 234(7): 1930-1943.

[13] LIAO Y, BORRELLI F. An adaptive approach to real-time estimation of vehicle sideslip, road bank angles, and sensor bias[J]. IEEE Transactions on Vehicular Technology, 2019, 68(8): 7443-7454.

[14] CHENG S, LI L, CHEN J. Fusion algorithm design based on adaptive SCKF and integral correction for side-slip angle observation[J]. IEEE Transactions on Industrial Electronics, 2018, 65(7): 5754-5763.

[15] JIANG G, LIU L, GUO C, et al. A novel fusion algorithm for estimation of the side-slip angle and the roll angle of a vehicle with optimized key parameters[J]. Proceedings of the Institution of Mechanical Engineers, Part D: Journal of Automobile Engineering, 2016, 231(2): 161-174.

[16] CHELI F, SABBIONI E, PESCE M, et al. A methodology for vehicle sideslip angle identification: comparison with experimental data[J]. Vehicle System Dynamics, 2007, 45(6): 549-563.

[17] VILLANO E, LENZO B, SAKHNEVYCH A. Cross-combined UKF for vehicle sideslip angle estimation with a modified dugoff tire model: design and experimental results[J]. Meccanica, 2021, 56(11): 2653-2668.

[18] PIYABONGKARN D N, RAJAMANI R, GROGG J A, et al. Development and experimental evaluation of a slip angle estimator for vehicle stability control[J]. IEEE Transactions on Control Systems Technology, 2009, 17(1): 78-88.

[19] HONG S, LEE C, BORRELLI F, et al. A novel approach for vehicle inertial parameter identification using a dual Kalman filter[J]. IEEE Transactions on Intelligent Transportation Systems, 2015, 16(1): 151-161.

[20] SONG R, FANG Y. Vehicle state estimation for INS/GPS aided by sensors fusion and SCKF-based algorithm[J]. Mechanical Systems and Signal Processing, 2021, 150: 107315.

[21] LIU W, XIA X, XIONG L, et al. Automated vehicle sideslip angle estimation considering signal measurement characteristic[J]. IEEE Sensors Journal, 2021, 21(19): 21675-21687.

[22] JOHNSON J, JOHNSON D, BOUDRA P, et al. Filters using Bessel-type polynomials[J]. IEEE Transactions on Circuits and Systems, 1976, 23(2): 96-99.

[23] FANG H, HAILE M A, WANG Y. Robust extended Kalman filtering for systems with measurement outliers[J]. IEEE Transactions on Control Systems Technology, 2022, 30(2): 795-802.

[24] CHEN J, HU S, YE Y, et al. A cascaded scheme for high-performance estimation of vehicle states[J]. Proceedings of the Institution of Mechanical Engineers, Part D: Journal of Automobile Engineering, 2021, 235(8): 2101-2113.

[25] BERNTORP K, CAIRANO S D. Tire-stiffness and vehicle-state estimation based on noise-adaptive particle filtering[J]. IEEE Transactions on Control Systems Technology, 2019, 27(3): 1100-1114.

(上接第309页)

[20] YILDIZ H, CENK M, ONUR E. PLGAKD: a PUF-based lightweight group authentication and key distribution protocol[J]. IEEE Internet of Things Journal, 2020, 8(7): 5682-5696.

[21] SHAWKY M A, JABBAR A, USMAN M, et al. Efficient blockchain-based group key distribution for secure authentication in VANETs[J]. IEEE Networking Letters, 2023, 74.

[22] KAMIL I A, OGUNDOYIN S O. A lightweight certificateless authentication scheme and group key agreement with dynamic updating mechanism for LTE-V-based internet of vehicles in smart cities[J]. Journal of Information Security and Applications, 2021, 63: 102994.

[23] CREMERS C. Scyther: semantics and verification of security protocols[J]. Technische Universittndhoven, 2006.

[24] 薛庆水,卢子谶,杨谨瑜.基于Shamir的动态强前向安全签名方案[J].计算机应用研究, 2023, 40(5):1522-1527, 1534.
XUE Q S, LU Z X, YANG J Y. Dynamic strong forward secure signature scheme based on shamir[J]. Application Research of Computers, 2023, 40(5): 1522-1527, 1534.

[25] 向新银.格上基于身份的前向安全签名方案[J].计算机工程, 2015, 41(9):155-158.
XIANG X Y. Identity-based forward secure signature scheme from lattices[J]. Computer Engineering, 2015, 41(9): 155-158.