车联网中可证安全的分布式匿名高效边缘认证协议

张海波[①②] 兰 凯[*①②] 黄宏武[①②] 王汝言[①②] 邹 灿[③]

[①](重庆邮电大学通信与信息工程学院 重庆 400065)

[②](先进网络与智能互联技术重庆市高校重点实验室 重庆 400065)

[③](三六零数字安全科技集团有限公司 北京 100015)

摘 要：针对当前车联网(IoV)中的分布式认证协议直接依赖于半可信路边单元(RSU)的问题，该文提出一种新的分布式认证模型。该模型中的RSU通过3阶段广播自发建立边缘认证区，利用区域内的RSU同步保存车辆的认证记录，RSU可以通过校验节点同步保存的认证记录来防止恶意RSU的异常认证行为。然后，利用切比雪夫混沌映射设计了IoV中的分布式匿名认证协议，通过车辆发送消息不直接携带身份信息的方式来避免假名机制所带来的存储负担。最后，利用随机预言机对协议安全性进行了证明。仿真结果表明所提方案具有更低的认证时延和通信成本。

关键词：车联网；分布式认证；混沌映射；随机预言机

中图分类号：TN915 **文献标识码**：A **文章编号**：1009-5896(2023)08-2902-09

DOI: 10.11999/JEIT220846

Provably Secure Distributed Efficient Edge Authentication Protocol with Anonymity in Internet of Vehicles

ZHANG Haibo[①②] LAN Kai[①②] HUANG Hongwu[①②]

WANG Ruyan[①②] ZOU Can[③]

[①](*School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing* 400065, *China*)

[②](*Advanced Network and Intelligent Connection Technology Key Laboratory of Chongqing Education Commission of China, Chongqing* 400065, *China*)

[③](360 *Digital Security Technology Group Co., Ltd, Beijing* 100015, *China*)

Abstract: Considering the problem that the current distributed authentication protocols in the Internet of Vehicles (IoV) directly depend on semi-trusted Road Side Units (RSU), a new distributed authentication model is proposed. The RSUs in this model establish automatically the edge authentication area through a three-stage broadcast, and these RSUs in the area save synchronously the vehicle certification records. RSU can prevent abnormal authentication behavior of malicious RSU by verifying the authentication records saved synchronously by nodes. Then, a distributed anonymous authentication protocol in IoV is designed by using Chebyshev chaotic mapping, to avoid the storage burden caused by the pseudonym mechanism, the vehicle sends messages without directly carrying identity information. Finally, the security of the protocol is proved by using random oracle. The simulation results show that the proposed scheme has lower authentication delay and communication cost.

Key words: Internet of Vehicles (IoV); Distributed authentication; Chaotic mapping; Random oracle

收稿日期：2022-06-27；改回日期：2022-11-10；网络出版：2022-11-11

*通信作者： 兰凯 2396128830@qq.com

基金项目：国家自然科学基金(61901071, 61801065)，长江学者和创新团队发展计划基金(IRT16R72)，重庆市留创计划创新类资助项目(cx2020059)

Foundation Items: The National Natural Science Foundation of China (61901071, 61801065), The Program for Changjiang Scholars and Innovative Research Team in University (IRT16R72), Chongqing Innovation and Entrepreneurship Program for the Returned Overseas Chinese Scholars (cx2020059)

1　引言

近些年，车联网(Internet of Vehicles, IoV)中的隐私与安全问题[1]成为众多学者的研究热点，保证合法的车载单元(On Broad Units, OBU)安全高效地接入IoV是解决该问题的关键手段。因此，接入认证协议的设计至关重要，目前IoV中的认证协议可以分为集中式认证和分布式认证两类。

关于集中式认证已有许多研究[2–5]。Ying等人[2]针对IoV中身份认证的效率性，提出基于智能卡的轻量级认证协议，实现车辆身份不可链接性的同时有效提升了认证效率。Chen等人[3]指出Ying等人方案无法抵御离线身份猜测攻击和位置欺骗攻击并在其基础上提出了改进协议，提高了协议安全性。Cui等人[4]提出基于混沌映射的全会话密钥协议，利用雾头实现OBU与可信中心(Trusted Authority, TA)之间的认证。Wei等人[5]提出基于树的相互认证协议，通过树形结构的设定保障安全的同时减少了认证开销。然而上述方案均依赖于TA，这会带来更高额能量损耗与认证时延，且当其发生数据泄露时将造成较大安全威胁。

为了避免集中式认证的诸多问题，文献[6–13]利用边缘节点路边单元(Road Side Units, RSU)实现用户的分布式认证。Chuang等人[6]针对IoV拓扑结构高速动态变化的特点提出了分布式轻量级认证方案，该方案以传递信任关系的方式提高认证性能且仅需牺牲很少的存储空间。Yao等人[7]针对传统认证方案忽略了用户隐私性的问题，提出了一种分布式车辆雾服务的匿名认证机制，该机制具有灵活的跨数据中心认证能力，能够抵御数据篡改攻击。刘雪艳等人[8]提出了非线性对无证书匿名认证方案，有效解决了认证中的复杂证书管理与密钥托管等问题。Li等人[9]针对恶意车辆匿名追溯中的追踪器滥用跟踪的问题，提出了一种防止滥用跟踪的匿名身份验证方案，该方案以分布式的方式设定追踪密钥，任何单一实体均无权限直接进行追溯。Vijayakumar等人[10]提出了一种高效分布式匿名认证方案，方案中以TA为车辆生成假名的方式保障匿名性，但大量假名的管理与维护浪费了较多存储资源。Tsai等人[11]综合考虑移动设备计算能力有限、消息传输易遭受外部攻击和用户隐私易泄露3个方面的问题，提出了高效的分布式移动云计算服务认证方案，方案中的移动用户仅使用一个私钥就可以访问来自多个服务商的多个云计算服务。Irshad等人[12]指出Tsai方案易受到服务器欺骗攻击、去同步攻击和拒绝服务攻击，并在其基础上提出了基于双线性对的改进模型，该模型可增强接入认证的健壮性。Jia等人[13]为了进一步改善Irshad方案的性能，提出了不可追踪的匿名认证方案，该方案具有较好的安全性和较低的计算成本与通信成本。

然而，上述文献均忽略了边缘节点本身的可信程度。在IoV中，边缘节点RSU容易受到各种外部攻击，这使得其信任等级不如TA，因此，如何在半可信的RSU上实现可信的认证是实现IoV分布式认证的一个重要问题。本文通过RSU之间的3阶段广播实现了IoV的自动分区和边缘认证区域的建立，并利用TA完成了对区域合法性的检验；通过计算切比雪夫混沌映射实现了RSU与OBU的快速匿名认证，且该匿名性以车辆不直接发送身份相关信息的方式避免了传统假名机制所带来的存储负担问题；通过分布式RSU节点存储的RSU对OBU的认证记录保证RSU无法做出错误的认证行为；通过安全性证明与分析确保了所提协议满足相关安全属性，最终实现了高效率和高可靠性的IoV分布式认证。

2　场景模型

RSU根据范围内本地车辆的数量自发建立边缘认证区，当车辆在边缘认证区进行身份认证时，由区域内的RSU负责对车辆身份进行认证。整个IoV区域将被划分成很多个边缘认证区域，场景模型如图1所示。这里的本地车辆指移动范围有限或活动区域比较固定的车辆，除本地车辆外还存在少数移动范围大、移动区域不固定的流动车辆，这部分车辆仍然利用中心服务器进行认证。

RSU：既是车辆认证的载体又是保存车辆认证记录的副本节点，是IoV中的关键环节，分布于IoV的各个区域。OBU：车辆的通信单元，可以与RSU或其他车辆交换信息。

3　安全认证原理

3.1　RSU注册公钥

存在双线性映射$e: G_1 \times G_2 \to G_T$，其中$G_1, G_2$为双线性群，$\varphi$为$G_2$到$G_1$的同构映射。密钥生成中

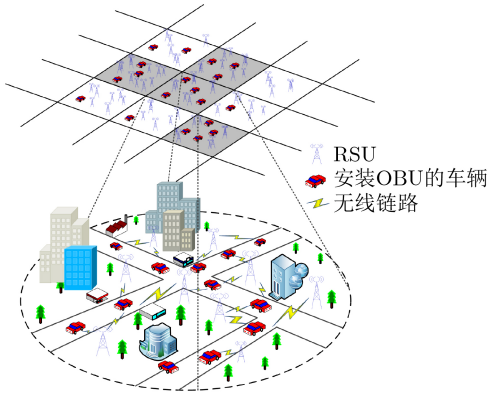

图 1 场景模型

心(Key Generation Center, KGC)生成G_1, G_2和φ，随机选择x_2, $y_2 \in G_2$，并计算$x_1=\varphi(x_2), y_1=\varphi(y_2)$，将参数$(G_1, G_2, x_1, x_2, y_1, y_2)$发送给RSU和TA。RSU生成随机数$\mathrm{sk}_i$作为私钥，计算公钥$\mathrm{pk}_i = {y_1}^{\mathrm{sk}_i}$，然后发送$<\mathrm{RSU_{ID}}, \mathrm{pk}_i, t_1>$给KGC，本文中的$\{t_i | i \in N^*\}$均表示时间戳，KGC生成数字证书$\mathrm{cert}_i$(该证书中包含RSU的ID、公钥以及数字签名，主要用于对RSU公钥合法性的检验)，并发送给对应的RSU。

3.2 OBU注册ID

OBU通过安全通道将要注册的用户名ID_{V_i}和验证密码pw_{V_i}发送给TA。TA收到消息后生成随机数r_t，计算$h(\mathrm{ID}_{V_i}||\mathrm{pw}_{V_i})$和$h(h(T_{\mathrm{sk_{TA}}})||r_t)$，其中$h$为哈希函数，$\mathrm{sk_{TA}}$为TA的私钥，$T$为切比雪夫混沌映射且$T_{\mathrm{sk_{TA}}}=T_{\mathrm{sk_{TA}}}(x) \bmod p$，$x, p$为TA设置的公共参数。然后TA计算$\vartheta = h(h(\mathrm{ID}_{V_i}||\mathrm{pw}_{V_i})||\mathrm{date}) \cdot h(h(T_{\mathrm{sk_{TA}}})||r_t))$，这里的date为注册时间，保存$<\mathrm{ID}_{V_i}, \vartheta>$到表$\Gamma$，并发送$<\mathrm{ID}_{V_i}, h(h(T_{\mathrm{sk_{TA}}})||r_t)>$给车辆。

3.3 边缘认证区的构建

通过RSU对车辆身份实现安全快速认证，需要构建以RSU为节点的边缘认证区域。该过程可分为两个阶段，RSU在阶段1依据范围内本地车辆数量进行自动分区，在阶段2完成认证区有效ID的申请。

3.3.1 构建认证区阶段1

由于车辆轨迹和每个RSU记录的本地车辆均存在耦合，因此RSU需要对边缘区域节点和本地车辆达成一致。本文利用3次广播实现了对RSU和本地车辆的两次筛选，利用第3次广播选择$\mathrm{RSU_{num}}$向TA提交认证区的构建请求。3次广播的通信流程如图2所示。具体过程如下：

步骤1 当RSU_n的本地车辆列表的长度L_n超过$l_{\min}$时，RSU_n计算$(\alpha\zeta+\beta\tau)\sum_{i=1}^{L_n} f_{V_i} \geq \kappa$(其中$\zeta, \tau$分别为预设的边缘认证能量和时延收益值，$\alpha, \beta$为两者对应的调节系数，$\kappa$为额定收益值)，如果成立则计算$C^0=\{h(\mathrm{ID}_{V_i}||f_{V_i}))|i \in N^*\}$(其中$\mathrm{ID}_{V_i}$和$f_{V_i}$对应$\mathrm{RSU}_n$保存的车辆$V_i$的信息)，并广播消息$m_1 = <\mathrm{ID_{RSU}}_n, C^0, t_0, \mathrm{req}_1>$，这里的req及后文的res均表示消息类型。

步骤2 所有其他$\mathrm{RSU}_{j_1}(1 \leq j_1 \leq \max, j_1 \neq n)$验证时间戳和消息类型，如果均正确则计算$C^{j_1}=\{h(\mathrm{ID}_{V_i}^{j_1}||f_{V_i}^{j_1}))|i \in N^*\}$，这里$\mathrm{ID}_{V_i}^{j_1}$和$f_{V_i}^{j_1}$为$\mathrm{RSU}_{j_1}$的车辆列表信息。然后计算$(\mathrm{len}(C^{j_1} \wedge C)/\mathrm{len}(C)) \geq \rho$，其中$\mathrm{len}(C)$返回集合$C$的长度，$\rho$为系统的预设值，若成立则广播应答消息$m_{j_1} = <\mathrm{ID_{RSU}}_{j_1}, C^{j_1}, t_{j_1}, \mathrm{res}_1>$。

步骤3 RSU_{j_2}在T时间内监听所有其他RSU_{j_1}广播的应答消息m_{j_1}，T以时间戳t_{j_1}为起点，并不断计算$(\mathrm{len}(C^{j_1} \wedge C^{j_2})/\mathrm{len}(C^0)) \geq \rho$，其中$C^{j_2}=\{h(\mathrm{ID}_{V_i}^{j_2}||f_{V_i}^{j_2}))|i \in N^*\}$是$\mathrm{RSU}_{j_2}$在步骤2中已计算过的集合，$C^{j_1}$为应答消息$m_{j_1}$中的集合，$T$时间后计算$(m_{\mathrm{res}_1}+1/M) > 0.5$，其中$m_{\mathrm{res}_1}$为成立的消息数量，$M$为收到的所有应答消息的数量。若成立则计算所有车辆集合的最大交集$C^{V_i}=\sum_{j_2=1}^{L} \wedge C^{j_2}$，从而确定本地车辆列表，然后计算该列表的哈希摘要$\mathrm{dig}_{j_2}=h(h(\sum_{i=1}^{\mathrm{len}(C^{V_i})} \oplus(\mathrm{ID}_{V_i}||f_{V_i})))$并广播应答消息$m_{j_3} = <\mathrm{ID_{RSU}}_{j_2}, \mathrm{dig}_{j_2}, t_{j_2}, \mathrm{res}_2>$。

步骤4 当RSU_{j_3}收到所有其他RSU的第2个应答消息后，生成一个随机数s_{j_3}并广播消息$<\mathrm{ID_{RSU}}_{j_3}, s_{j_3}, t_{j_3}, \mathrm{res}_3>$。

步骤5 RSU收到所有包含随机数的消息后，计算$\mathrm{num}=((\sum_{j_3=1}^{L} s_{j_3}) \bmod L)+1$，其中$L$为经过步骤2和步骤3筛选后剩下的RSU的数量。RSU对已收到消息中的$\mathrm{ID_{RSU}}_{j_3}$进行排序，选择第num个RSU与TA完成阶段2的认证区有效ID的申请过程。

3.3.2 构建认证区阶段2

在此阶段$\mathrm{RSU_{num}}$向TA提交认证区ID的申请，流程如图3所示。TA首先对消息中的签名进行群验证，然后确定认证区域的RSU节点和本地车辆，最后生成认证区ID_B和初始群会话密钥k_0。

步骤1 $\mathrm{RSU_{num}}$广播消息$<\mathrm{ID}_{R_{\mathrm{num}}}, t_5, \mathrm{req}_2>$，其他RSU收到消息后计算$\mathrm{sign}_n = e(x_1, y_2)^{\mathrm{sk}_n}$并向$\mathrm{RSU_{num}}$发送$<\mathrm{ID}_{R_n}, \mathrm{sign}_n, t_6, \mathrm{res}_4>$。

步骤2 $\mathrm{RSU_{num}}$收到所有应答消息后计算$\mathrm{sign}=\prod_{n=1}^{L} \mathrm{sign}_n$，然后向TA发送请求消息$<C_{\mathrm{cert}_n}, \mathrm{sign}, t_7, \mathrm{req}_3>$，其中$C_{\mathrm{cert}_n}$为包含所有RSU数字证书的集合。

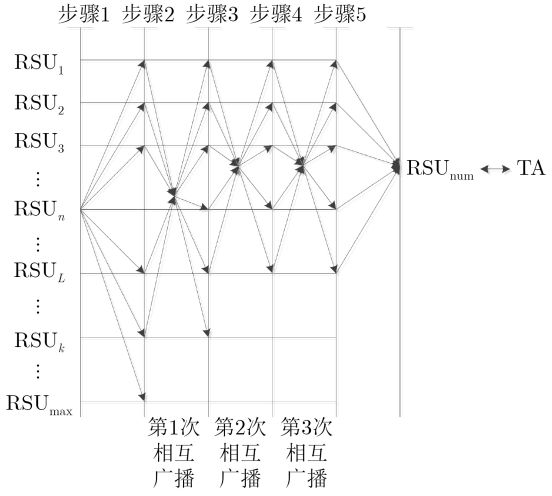

图 2 RSU之间的3次相互广播

步骤3　TA检查消息中的数字证书、时间戳和消息类型，然后验证$\text{len}(C_{\text{cert}_n}) > l^r_{\min}$，均无误则计算$\text{sign}^* = e(\prod_{n=1}^{L} \text{pk}_n, x_2)$，检验$\text{sign}^*? = \text{sign}$，如果相等则向$\text{RSU}_{\text{num}}$发送$<< \text{cert}_{\text{TA}}, t_8, \text{res}_5 >_{\text{sk}_{\text{TA}}}, \text{pk}_{\text{TA}} >$。

步骤4　RSU_{num}收到消息后，首先检查TA的签名，若验证无误则计算$C_R = \sum_{n=1}^{L} \wedge(C_{R_n})$，这里的$C_{R_n}$表示本地车辆集合，然后附上所有的频率信息构成集合$C_{V:F} = \{ \text{ID}_{V_1} : f_{V_1}, \text{ID}_{V_2} : f_{V_2}, \cdots, \text{ID}_{V_j} : f_{V_j} \}$。向TA发送消息$< \text{ID}_{R_{\text{num}}}, C_{V:F}, t_9, \text{req}_4 >$。

步骤5　TA收到消息后，检查时间戳和消息类型。然后验证$\text{len}(C_{V:F}) > l^v_{\min}$是否成立，成立则将$C_{V:F}$代入$(\alpha\zeta + \beta\tau) \sum_{i=1}^{L_n} f_i \geq \kappa$进行检验。若上述检验均成立，则在表$\Gamma$的$C_{V:F}$中查找所有$V_i$对应的$\vartheta$，然后计算$C_\eta = \{ (\text{ID}_{V_1} : \vartheta_{V_1}), (\text{ID}_{V_2} : \vartheta_{V_2}), \cdots, (\text{ID}_{V_j} : \vartheta_{V_j}) \}$，并生成认证域的编号$\text{ID}_B$和初始群会话密钥$k_0$，最后通过安全通道向$\text{RSU}_{\text{num}}$发送消息$< C_\eta, \text{ID}_B, k_0, t_{10}, \text{res}_6 >$。

步骤6　RSU_{num}收到消息后，验证时间戳和消息类型。保存$< \text{ID}_B, k_0, C_\eta >$并通过安全通道将$< \text{ID}_{R_{\text{num}}}, C_\eta, \text{ID}_B, k_0, t_{11}, \text{res}_7 >$发送给其他RSU。

3.4　边缘认证协议流程

当边缘认证域建立后，车辆再次与TA认证时，TA会优先检查该车辆是否已加入认证域，如果车辆存在于已激活的某个认证域中，则向其发送$< \text{ID}_B, k_0 >$，让车辆的OBU下次认证时可以直接利用边缘认证域进行身份认证。如果车辆不存在于任何认证域，则利用图4协议完成认证，其中TA执行RSU_j的计算任务。对于本地车辆，车辆在上一个RSU完成认证后，所有认证域中的RSU节点利用$\text{num} = ((\sum_{j_3=1}^{L} s_{j_3}) \text{mod} L) + 1$选举出一个新节点$\text{RSU}_j$作为下一个RSU范围内的认证节点，并将会话密钥更新为$k_i = h(k_{i-1}) \oplus h(\text{num})$，其中$k_{i-1}$表示上一次认证的会话密钥，$k_i$表示当前会话密钥。车辆收到广播后，同步更新$k_i$，然后利用切比雪夫混沌映射完成边缘认证，认证过程如图4所示，具体步骤如下：

步骤1　本地车辆OBU_i查询目标RSU的临时公钥T_{r_2}，生成随机数r_k，计算$\nu = T_{r_k}(x) \text{mod} p'$，$\iota = T_{r_1}(x) \text{mod} p'$，$M = T_{r_k}(T_{r_2}) \text{mod} p'$，$N = \nu \oplus (\text{ID}_{V_i} || T_{V_i})$, $Q = \nu \oplus \iota$, $\text{Auth} = T_{r_1}(T_{\vartheta \cdot h(\nu)}(T_{r_2})) \text{mod} p'$，其中$r_1$和$\iota$为$\text{OBU}_i$的临时私钥和公钥，$p'$为某个安全的大素数。然后向目标RSU发送认证消息$< M, N, Q, \text{Auth} >$。

步骤2　RSU_n收到认证消息后，选择随机数r_m，利用$T_{r_2}(\nu') \text{mod} p' = M$计算$\nu'$，利用$\text{ID}'_{V_i} || T'_{V_i} = N \oplus \nu'$恢复$\text{OBU}_i$的ID和时间戳$T'_{V_i}$，在$C_\eta$中查找$\text{ID}_{V_i}$对应的$\vartheta'$，继续计算$\iota' = Q \oplus \nu'$，$\text{Auth}' = T_{r_2 \cdot \vartheta' \cdot h(\nu')}(\iota') \text{mod} p'$，验证$\text{Auth}' = \text{Auth}$是否成立，若成立则计算$\upsilon = T_{r_m}(x) \text{mod} p'$, $\text{Res} = T_{r_m \cdot \vartheta' \cdot h(\text{ID}_{R_n} || \text{ID}_{V_i})}(\nu') \text{mod} p'$，并向$\text{OBU}_i$发送响应消息$< \text{Res}, \upsilon >$。否则拒绝认证。

步骤3　OBU_i收到响应消息后，计算$\text{Res}' = T_{r_k \cdot \vartheta \cdot h(\text{ID}_{R_n} || \text{ID}_{V_i})}(\upsilon) \text{mod} p'$，并验证$\text{Res}' = \text{Res}$是否成立，若成立则计算会话密钥$k_{r_k - r_m} = T_{r_k}(\upsilon) \text{mod} p'$, $\text{Au} = T_{r_1 \cdot h(\text{ID}_{R_n} || \text{ID}_{V_i})}(\upsilon) \text{mod} p'$，向$\text{RSU}_n$发送消息$< \text{Au} >$。若等式不成立则拒绝消息。

步骤4　RSU_j收到消息后计算$\text{Au}' = T_{r_m \cdot h(\text{ID}_{R_i} || \text{ID}_{V_i})}(\iota') \text{mod} p'$，验证$\text{Au}' = \text{Au}$是否成立，若成立则认证通过，计算会话密钥为$k_{r_m - r_k} = T_{r_m}(\nu') \text{mod} p'$。否则认证失败。

3.5　认证记录的更新

每当车辆认证时，随机选择认证区域中的RSU与车辆完成身份认证。RSU将认证记录打包成

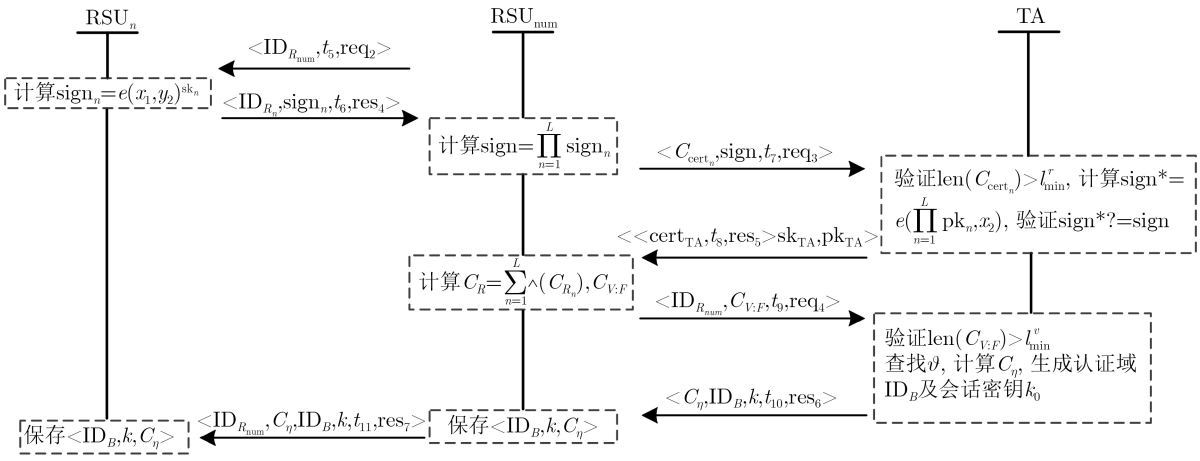

图 3 认证域的申请

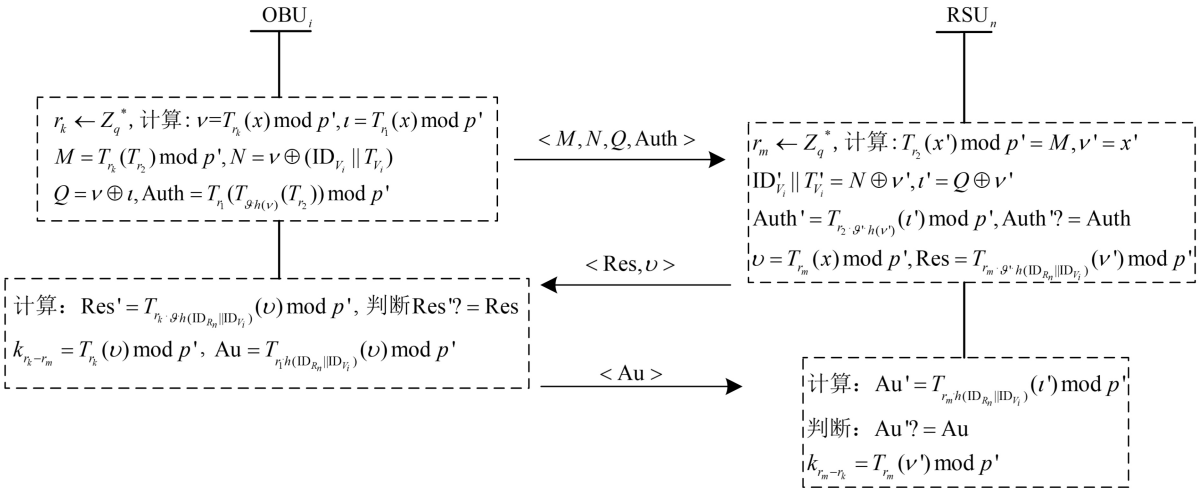

图 4 边缘认证

数据块后用会话密钥k_i加密进行广播，其他RSU对认证记录进行检查，若无误则将其加入自己的内存池，否则发出拒绝消息，若大多数RSU拒绝则对广播的数据块进行身份追溯。数据块结构如图5所示。RSU对认证记录的同步保存确保了认证的不可篡改性，可及时发现车辆的异常认证行为，也可以避免RSU的恶意认证。

版本号	哈希值	时间戳	随机数
认证列表			
RSU的ID	OBU1的ID	认证时间	
RSU的ID	OBU2的ID	认证时间	
RSU的ID	OBU3的ID	认证时间	
…	…	…	

图 5 认证区域数据块结构

4 安全性分析

4.1 基于随机预言机的安全性证明

为了证明协议的安全性，本节基于随机预言机的模型[13]分别计算了攻击者$\mathcal{A}$伪造认证消息M_1或M_3获得RSU的认证，和正常OBU发送认证消息M_1时，$\mathcal{A}$成功伪造响应消息M_2这3种情况下$\mathcal{A}$的优势。

定理1 假设存在概率多项式时间(Probabilistic Polynomial Time, PPT)攻击者能以ε的概率伪造消息M_1，则挑战者$\mathcal{C}$能以不可忽略的概率ε_1破解计算离散对数(Compute Discrete Logarithm, CDL)问题[14]。定义$\varepsilon_1 \geq (1-\frac{1}{q_{\mathrm{h}}^2})^{q_{\mathrm{e}}} \cdot (1-\frac{1}{q_{\mathrm{s}}}) \cdot (1-\frac{1}{q_{\mathrm{e}}}) \cdot \frac{1}{q} \cdot \frac{1}{q_{\mathrm{e}}} \cdot \varepsilon$，其中$q_{\mathrm{h}}$表示哈希询问的上界，$q_{\mathrm{e}}$表示extract询问的上界，$q_{\mathrm{s}}$表示send询问的上界，$q$表示密钥池的深度。

证明 假设存在CDL实体T，满足$Q = T_s(x) \bmod p$，且$\mathcal{C}$不知s。$\mathcal{C}$通过维护L_h列表记录随机预言机的回答，通过维护L_ϑ列表记录extract返回的OBU$_i$的认证密钥，通过维护L_s列表记录实体之间交换的信息，通过L_r列表记录extract返回的私钥。所有列表初始为空，$\mathcal{C}$公布2个列表：$\mathrm{ID}_{V_i} = \{\mathrm{ID}_{V_1}, \mathrm{ID}_{V_2}, \cdots, \mathrm{ID}_{V_{q_e}}\}$，$\mathrm{ID}_{R_i} = \{\mathrm{ID}_{R_1}, \mathrm{ID}_{R_2}, \cdots, \mathrm{ID}_{R_{q_e}}\}$。$\mathcal{A}$选择$\mathrm{ID}_{V_i}*$作为伪造消息的对象。

$\mathcal{C}$运行以下程序对$\mathcal{A}$的询问做出回答。$h(x)$：$\mathcal{A}$在h上询问x，$\mathcal{C}$先检查L_h中是否存在记录$(x, h(x))$，如果存在则返回$h(x)$给$\mathcal{A}$，否则$\mathcal{C}$随机选择r，并将r返回给$\mathcal{A}$，同时在L_h中添加记录(x, r)。extract(ϑ_{V_i})：如果$V_i \neq V_i*$，$\mathcal{C}$随机选择$\mathrm{pw}_{V_i}, \mathrm{date}, T_{\mathrm{sk_{TA}}}, r_t$，询问$h$得到$\vartheta = h(h(\mathrm{ID}_{V_i} || \mathrm{pw}_{V_i}) || \mathrm{date}) \cdot h(h(T_{\mathrm{sk_{TA}}}) || r_t))$的值，在$L_\vartheta$中搜索$(\mathrm{ID}_{V_i}, \vartheta)$，如果不存在，则在$L_\vartheta$中添加记录$(\mathrm{ID}_{V_i}, \vartheta)$，向$\mathcal{A}$返回$(\mathrm{ID}_{V_i}, \vartheta)$。如果存在，则提取$\vartheta$，此时若$h(h(\mathrm{ID}_{V_i} || \mathrm{pw}_{V_i}) || \mathrm{date}) \cdot h(h(T_{\mathrm{sk_{TA}}}) || r_t)) \neq \vartheta$，则$\mathcal{C}$终止程序。否则$\mathcal{C}$成功计算认证密钥$\vartheta$，向$\mathcal{A}$返回$(\mathrm{ID}_{V_i}, \vartheta)$。如果$V_i = V_i*$，$\mathcal{C}$直接终止程序。extract$(\mathrm{ID}_{V_i})$：如果$V_i \neq V_i*$，$\mathcal{C}$随机选择$r_1$，计算$T_{r_1} = T_{r_1}(x) \bmod p$，在$L_r$中搜索$(\mathrm{ID}_{V_i}, r, T_r)$，如果不存在，则在$L_r$中添加记录$(\mathrm{ID}_{V_i}, r_1, T_{r_1})$，向$\mathcal{A}$返回$(\mathrm{ID}_{V_i}, r_1)$。如果存在，则提取$r$，此时若$T_{r_1} \neq T_r$或$T_{r_1} = T_r$且$r_1 \neq r$，则$\mathcal{C}$终止程序。否则$\mathcal{C}$成功计算$V_i$的私钥$r_1$，向$\mathcal{A}$返回$(\mathrm{ID}_{V_i}, r_1)$。如果$V_i = V_i*$，$\mathcal{C}$直接终止程序。extract$(\mathrm{ID}_{R_i})$：$\mathcal{C}$随机选择$r_2$，计算$T_{r_2} = T_{r_2}(x) \bmod p'$，在$L_r$中搜索$(\mathrm{ID}_{R_i}, r, T_r)$，如果不存在，则在$L_r$中添加记录$(\mathrm{ID}_{R_i}, r_2, T_{r_2})$，向$\mathcal{A}$返回$(\mathrm{ID}_{R_i}, r_2)$。如果存在，则提取$r$，此时若$T_{r_2} \neq T_r$或$T_{r_2} = T_r$且

$r_2 \neq r$，则$\mathcal{C}$终止程序。否则$\mathcal{C}$成功计算R_i的私钥r_2，向$\mathcal{A}$返回(ID_{R_i}, r_2)。

$\mathcal{A}$可以发送以下4种send询问模拟攻击者的能力。send$(V_i{}^k, \mathrm{start})$：如果$V_i = V_i*$，$\mathcal{C}$返回$\perp$并终止程序，如果$V_i \neq V_i*$，则$\mathcal{C}$利用extract$(\vartheta_{V_i})$中的方法生成$\vartheta$，利用extract$(\mathrm{ID}_{V_i})$中的方法计算$V_i$的私钥$r_1$，并在$L_r$中添加记录$(\mathrm{ID}_{V_i}, r_1, T_{r_1})$，然后利用得到的$\vartheta, r_1$和随机数$r_k$计算认证消息$< M, N, Q, \mathrm{Auth} >$。$\mathcal{C}$在$L_s$中添加记录$(\mathrm{ID}_{V_i}, k, r_k, \vartheta)$，同时向$\mathcal{A}$返回$< M, N, Q, \mathrm{Auth} >$。send$(R_j{}^m, (M, N, Q, \mathrm{Auth}))$：$\mathcal{C}$在$L_r$中搜索$\mathrm{ID}_{R_i}$，如果不存在，则利用extract$(\mathrm{ID}_{R_i})$中的方法生成$R_i$的私钥$r_2$，并在$L_r$中添加记录$(\mathrm{ID}_{R_i}, r_2, T_{r_2})$，利用extract$(\vartheta_{V_i})$计算$\vartheta$，然后按照协议中的方法计算$\nu', \mathrm{ID}_{V_i}{}', \iota'$，最后通过上述结果计算$\mathrm{Auth}' = T_{r_2 \cdot \vartheta' \cdot h(\nu')}(\iota'))\mathrm{mod}p'$，并验证$\mathrm{Auth}' = \mathrm{Auth}$是否成立，如果不成立则拒绝消息，如果等式成立且$V_i \neq V_i*$，则$\mathcal{C}$随机选择$r_m$并在$L_s$中添加记录$(\mathrm{ID}_{R_i}, m, r_m)$，然后按照协议计算$(\mathrm{Res}, \upsilon)$，最后将其返回给$\mathcal{A}$。send$(V_i{}^k, (\mathrm{Res}, \upsilon))$：$\mathcal{C}$收到该询问后，在$L_s$中搜索$(\mathrm{ID}_{V_i}, k, r_k, \vartheta)$，计算$\mathrm{Res}' = T_{r_k \cdot \vartheta \cdot h(\mathrm{ID}_{R_i} || \mathrm{ID}_{V_i})}(\upsilon))\mathrm{mod}p'$，并验证$\mathrm{Res}' = \mathrm{Res}$是否成立。如果成立则$\mathcal{C}$成功认证$\mathcal{A}$，然后在$L_r$中搜索$(\mathrm{ID}_{V_i}, r_1, T_{r_1})$，计算$\mathrm{Au} = T_{r_1 \cdot h(\mathrm{ID}_{R_i} || \mathrm{ID}_{V_i})}(\upsilon))\mathrm{mod}p'$，向$\mathcal{A}$返回Au。否则$\mathcal{C}$拒绝消息。send$(R_j{}^m, (\mathrm{Au}))$：$\mathcal{C}$收到该询问后，在$\mathrm{L}_s$中搜索$(\mathrm{ID}_{R_i}, m, r_m)$，计算$\mathrm{Au}' = T_{r_m \cdot h(\mathrm{ID}_{R_i} || \mathrm{ID}_{V_i})}(\iota'))\mathrm{mod}p$，验证$\mathrm{Au}' = \mathrm{Au}$是否成立。如果成立则$\mathcal{C}$成功认证$\mathcal{A}$，否则$\mathcal{C}$拒绝消息。reveal$(\prod_P^i)$：$\mathcal{C}$将在成功运行所有查询后，向$\mathcal{A}$返回正确会话密钥SK，否则返回$\perp$。

为了计算攻击者$\mathcal{A}$的优势，定义以下事件：E_1：仿真过程不会在中途被终止。E_2：$\mathcal{A}$成功向$\mathcal{C}$发送send$(R_j{}^m, M_1)$，其中$M_1 = (M, N, Q, \mathrm{Auth})$是一个合法的认证消息，并且extract$(\mathrm{ID}_{V_i})$从未被询问过。$E_3$：在伪造的认证消息中，$\mathrm{ID}_{V_i} = \mathrm{ID}_{V_i}^*$。仿真过程在以下4种情况下被终止：(1)在extract(ϑ_{V_i})中发生哈希冲突，即$h(h(\mathrm{ID}_{V_i} || \mathrm{pw}_{V_i}) || \mathrm{date}) \cdot h(h(T_{\mathrm{sk_{TA}}}) || r_t)) \neq \vartheta$，其概率为$1/q_h^2$。(2)$\mathcal{C}$由extract$(\mathrm{ID}_{V_i})$提取密钥时，生成的$r_1$满足$T_{r_1} \neq T_r$或$T_{r_1} = T_r$且$r_1 \neq r$，其概率为$(1 - 1/q)$。(3)$\mathcal{C}$执行extract$(\mathrm{ID}_{V_i}^*)$，其概率为$1/q_\mathrm{e}$。(4)$\mathcal{C}$执行send$(V_i{}^k, \mathrm{start})$其中$\mathrm{ID}_{V_i} = \mathrm{ID}_{V_i}*$，其概率为$1/q_s$。因此，存在以下关系：$P[E_1] = (1 - 1/q_h^2)^{q_e} \cdot (1 - 1/q_s) \cdot (1 - 1/q_e) \cdot 1/q P[E_2|E_1] \geq \epsilon$, $P[E_3|E_2 \wedge E_1] = 1/q_e$, $\epsilon_1 = P[E_3 \wedge E_2 \wedge E_1] = P[E_3|E_2 \wedge E_1] \cdot P[E_2|E_1] \cdot P[E_1] \geq (1 - 1/q_h^2)^{q_e} \cdot (1 - 1/q_s) \cdot (1 - 1/q_e) \cdot 1/q \cdot 1/q_e \cdot \epsilon$。其结果与定理1相同，定理1得证。

定理2　假设存在PPT攻击者能以ϵ的概率伪造消息M_2，则挑战者$\mathcal{C}$能以不可忽略的概率ϵ_2解决CDL问题，并且$\epsilon_2 = \epsilon_1$。

证明　在定理1中，攻击者$\mathcal{A}$利用extract(ϑ_{V_i})提取ϑ，利用extract(ID_{V_i})提取V_i的私钥r_1，然后利用send$(V_i{}^k, \mathrm{start})$中的方法伪造认证消息$M_1$，而对于$M_2$，$\mathcal{A}$计算Res需要先求出$\vartheta'$和$\nu'$，其中$\nu'$需要由$T_{r_2}(x')\mathrm{mod}p' = M$求出，所以$\mathcal{A}$同样需要利用extract$(\mathrm{ID}_{R_i})$提取$R_i$的私钥$r_2$，利用extract$(\vartheta_{V_i})$提取$\vartheta'$。因此，定理1与定理2是对称的，定理1被证明成立，所以定理2同样成立，且$\epsilon_2 = \epsilon_1$。

定理3　假设存在PPT攻击者能以ϵ的概率伪造消息M_3，则挑战者$\mathcal{C}$能以不可忽略的概率ϵ_3破解CDL问题，并且$\epsilon_3 > \epsilon_1$。

证明　在定理1中，攻击者$\mathcal{A}$利用extract(ϑ_{V_i})提取ϑ，利用extract(ID_{V_i})提取V_i的私钥r_1，然后利用send$(V_i{}^k, \mathrm{start})$中的方法伪造认证消息$M_1$，对于$M_3$，$\mathcal{A}$计算Au只需要利用extract$(\mathrm{ID}_{V_i})$提取$V_i$的私钥$r_1$，显然定理3的证明是定理1的子证明，因此定理1成立则定理3必成立，并且$\epsilon_3 > \epsilon_1$。

定理4　假设存在PPT攻击者可以赢得上述游戏，并能以不可忽略的概率输出$\mathrm{SK}' = \mathrm{SK}$，则存在挑战者$\mathcal{C}$能以不可忽略的概率解决CDL问题。

证明　为了分析会话密钥的安全性，定义以下事件：E_V：$\mathcal{A}$从Test询问中得出正确的会话密钥；E_R：针对实体$\prod_V^i$的Test询问被正确调用；E_{SK}：针对实体$\prod_R^i$的Test询问被正确调用。E_V表示$\mathcal{A}$成功仿冒车辆V_i发送认证消息，当E_V发生时，$\mathcal{A}$生成随机数r_k已被$\mathcal{C}$认证，当收到$\mathcal{C}$返回的υ，$\mathcal{A}$可以直接利用$k_{r_k - r_m} = T_{r_k}(\upsilon)\mathrm{mod}p'$得到会话密钥SK。同理当$E_R$发生时，$\mathcal{A}$可以直接利用$k_{r_m - r_k} = T_{r_m}(\nu')\mathrm{mod}p'$得到会话密钥SK，所以$P[E_{\mathrm{SK}}] = P[E_V \vee E_R]$，即$\mathcal{A}$得出会话密钥等效于仿冒$V_i$或$R_i$成功发送认证消息，由定理1和定理2，同样等效于解决CDL问题。

4.2 其他安全性讨论

IoV系统规定认证协议除了需要进行形式化安全证明外，还需要满足一些基本安全需求[15]，同时能够抵御常见的恶意攻击[16]，下面将对本文所设计协议进行相关安全性讨论。

(1)可以抵御重放攻击。

证明　假设攻击者$\mathcal{A}$通过窃听获取历史认证消息$< M, N, Q, \mathrm{Auth} >$，将其发送给RSU进行认证请求。$\mathrm{RSU}_j$验证通过后生成随机数$r_m$，计算$< \mathrm{Res}, \upsilon >$，并将该消息传回给$\mathcal{A}$，此时$\mathcal{A}$需要正确计算Au才能通过后续验证，然而计算Au需要OBU_i的私钥r_1，

$\mathcal{A}$只能通过公钥ι计算r_1，这属于CDL困难性问题，所以可以抵御重放攻击。

(2)可以抵御仿冒攻击。

证明 由定理1和定理2可知，攻击者$\mathcal{A}$无法仿冒成OBU发送认证消息，也无法仿冒成RSU进行认证，因此$\mathcal{A}$更加无法仿冒成OBU向RSU发送消息同时仿冒成RSU向OBU发送消息，所以可以抵御仿冒攻击。

(3)匿名性与可追溯性。

证明 本文所提协议没有为车辆设定假名，而是采用令OBU_i发送的认证消息中不直接包含车辆真实ID的方式，任意$\mathcal{A}$无法从交互的消息中获取OBU_i的真实ID。而RSU可以利用$\mathrm{ID}_{V_i}'||T_{V_i}' = N \oplus \nu'$恢复车辆ID(RSU可以追溯出车辆的真实身份)，由于计算ν'需要RSU的私钥r_2，因此$\mathcal{A}$成功恢复OBU_i的ID等效于解决CDL。所以所提认证协议具有可追溯性与更优的匿名性。

(4)会话密钥的前向安全和后向安全。

证明 群会话密钥的前向和后向安全：车辆每次完成认证后，系统都会将会话密钥更新为$k_i = h(k_{i-1}) \oplus h(\mathrm{num})$，假设车辆在RSU之间的切换时间间隔为$\tau'$，一次哈希运算的时间为$\Delta t$，则攻击者$\mathcal{A}$成功猜测$k_i$的概率为$p = \lim\limits_{l_h \to l_4} \dfrac{\tau'}{2^{l_h}\Delta t} \le \varepsilon$，即当哈希函数的位宽大于$l_4$时，$\mathcal{A}$在$\tau'$时间内正确猜出$k_i$的概率可以忽略。此外，由于$h(\mathrm{num})$输出均匀，攻击者$\mathcal{A}$无法由$k_i$推测$k_{i-1}$，也无法由$k_i$推测$k_{i+1}$，这可以保证传输数据的前向和后向安全。车辆临时会话密钥的前向安全和后向安全：临时会话密钥$\mathrm{sk}_i = k_{r_k - r_m} = k_{r_m - r_k} = T_{r_k}(T_{r_m}))\mathrm{mod}p$，其中$r_k$和$r_m$是临时生成的两个随机数，因此$\mathrm{sk}_i$也是随机的，所以无法由$\mathrm{sk}_i$求出$\mathrm{sk}_{i-1}$或$\mathrm{sk}_{i+1}$，这保证了会话密钥$\mathrm{sk}_i$的前向安全和后向安全。

5 仿真性能对比分析

5.1 认证时延对比

本节对本文协议的认证时延与文献[11]方案、文献[12]方案、文献[13]方案和文献[7]方案进行了对比。定义T_{h},T_{mul},T_{p},T_{e},T_{chev}分别表示单次的哈希运算、椭圆曲线中的点乘运算、双线性映射、模指数运算和切比雪夫映射的计算时间。本文在配置为Intel(R) Core(TM) i5-9500, RAM为2.00 GB的Win10环境下，于VS2010中使用密码学库OpenSSL-1.1.1h对文中所使用到的密码学操作进行模拟，测得$T_{\mathrm{h}} \approx 0.008\ 0$ ms, $T_{\mathrm{mul}} \approx 0.051\ 4$ ms, $T_{\mathrm{p}} \approx 1.254\ 1$ ms, $T_{\mathrm{e}} \approx 0.173\ 2$ ms, $T_{\mathrm{chev}} \approx 0.033\ 6$ ms。通过实验数据可以分别计算5种方案在用户端和边缘服务器端的计算时延，结果如表1所示。各方案在用户端的时延比较如图6所示，可见除文献[12]方案和文献[7]方案外，其他3种方案的用户端时延都处于较低水平，这可以很好地满足IoV中车辆节点计算能力有限的要求。在边缘服务器端的时延如图7所示，显然本文的计算时延远远低于文献[11]方案和文献[12]方案，相比于文献[13]方案和文献[7]方案分别提高了约86.42%, 45.57%，这主要是由于本文避免了耗时的双线性映射运算，并通过使用切比雪夫混沌映射避免了椭圆曲线中的点乘运算，从而大大降低了计算时延。

5.2 通信轮数及通信开销对比

本节对本文协议的通信轮数及通信开销与上述方案进行了对比。定义W_{H},W_{p},W_{mul},$W_{\mathrm{Z_q}}$,W_{ID},W_{T},W_{R},W_{chev}分别表示哈希函数、双线性映射、椭圆曲线点乘、数域Z_q、用户ID、时间戳、随机数和切比雪夫映射的输出位宽。根据文献[16]，本文设$|W_{\mathrm{H}}| = 256$ bit, $|W_{\mathrm{p}}| = 1\ 024$ bit, $|W_{\mathrm{mul}}| = 1\ 024$ bit, $|W_{\mathrm{Z_q}}| = 160$ bit, $|W_{\mathrm{ID}}| = 256$ bit, $|W_{\mathrm{T}}| = 32$ bit, $|W_{\mathrm{R}}| = 128$ bit, $|W_{\mathrm{chev}}| = 480$ bit。通过分析计算得各方案的通信轮数及通信开销如表2所示，开销对比如图8所示。由通信轮数可以看出文献[13]方案和文献[7]方案仅需进行2轮通信就可以完成认证，然而这两种方案均利用用户端与边缘服务器端同步的时间戳防止重放攻击，当攻击者发动去同步攻击时，文献[13]方案和文献[7]方案将无法利用时间戳判断是否属于重放攻击，而文献[12]方案与本文方案均采用2次验证的方式提高抵御重放攻击的能力。在通信开销方面，本文与文献[7]方案接近，相比于文献[11]方案、文献[12]方案、文献[13]方案分别提

表 1 认证时延对比(ms)

方案	用户端	边缘服务器端
文献[11]	$5T_{\mathrm{h}} + T_{\mathrm{e}} + 4T_{\mathrm{mul}} \approx 0.418\ 8$	$4T_{\mathrm{h}} + 2T_{\mathrm{e}} + 4T_{\mathrm{p}} + 2T_{\mathrm{mul}} \approx 5.497\ 6$
文献[12]	$7T_{\mathrm{h}} + 2T_{\mathrm{e}} + 2T_{\mathrm{p}} + 4T_{\mathrm{mul}} \approx 3.116\ 2$	$5T_{\mathrm{h}} + 2T_{\mathrm{e}} + 4T_{\mathrm{p}} + 3T_{\mathrm{mul}} \approx 5.557\ 0$
文献[13]	$5T_{\mathrm{h}} + T_{\mathrm{e}} + 4T_{\mathrm{mul}} \approx 0.418\ 8$	$5T_{\mathrm{h}} + T_{\mathrm{p}} + 6T_{\mathrm{mul}} \approx 1.602\ 5$
文献[7]	$10T_{\mathrm{h}} + 30T_{\mathrm{mul}} \approx 1.622\ 0$	$5T_{\mathrm{h}} + 7T_{\mathrm{mul}} \approx 0.399\ 8$
本文	$2T_{\mathrm{h}} + 8T_{\mathrm{chev}} \approx 0.284\ 8$	$2T_{\mathrm{h}} + 6T_{\mathrm{chev}} \approx 0.217\ 6$

高了27.08%, 40.34%, 29.05%，显然本文具有更低的通信量。

6　结束语

本文提出一种高效的匿名安全分布式认证协议。通过RSU之间的3次广播构建了边缘认证区并利用TA完成了对区域合法性的检验，从而解决传统IoV分布式系统中边缘RSU可信程度不高的问题，利用切比雪夫混沌映射设计了本地车辆的分布式匿名认证协议，并利用随机预言机模型对协议的安全性进行了形式化的证明。最后的仿真结果说明了本文所提方案在认证效率和通信成本上具有一定的优势。

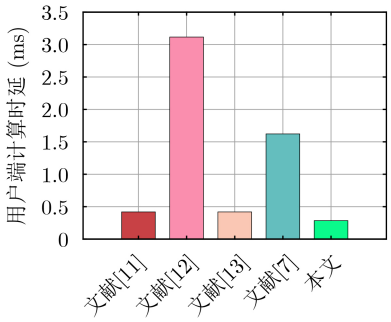

图 6 各方案下的用户端计算时延

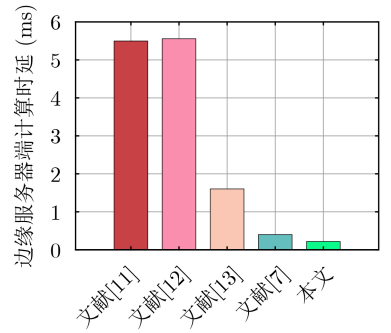

图 7 各方案下的边缘服务器端计算时延

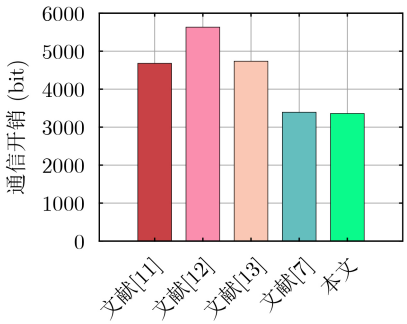

图 8 各方案下的通信开销

表 2　通信轮数及通信开销对比

方案	通信轮数	通信开销(bit)
文献[11]	4	$3\|W_{\text{mul}}\|+\|W_{\text{P}}\|+\|W_{\text{H}}\|+\|W_{\text{ID}}\|=4\,608$
文献[12]	4	$4\|W_{\text{mul}}\|+\|W_{\text{P}}\|+\|W_{\text{H}}\|+\|W_{\text{ID}}\|=5\,632$
文献[13]	2	$4\|W_{\text{mul}}\|+2\|W_{\text{T}}\|+2\|W_{\text{Z}_{\text{q}}}\|+\|W_{\text{ID}}\|=4\,736$
文献[7]	2	$2\|W_{\text{mul}}\|+2\|W_{\text{T}}\|+4\|W_{\text{ID}}\|+2\|W_{\text{R}}\|=3\,392$
本文	3	$7\|W_{\text{chev}}\|=3\,360$

参 考 文 献

[1] SUN Yunchuan, WU Lei, WU Shizhong, *et al*. Security and privacy in the internet of vehicles[C]. Proceedings of 2015 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI), Beijing, China, 2015: 116–121. doi: 10.1109/IIKI.2015.33.

[2] YING Bidi and NAYAK A. Anonymous and lightweight authentication for secure vehicular networks[J]. *IEEE Transactions on Vehicular Technology*, 2017, 66(12): 10626–10636. doi: 10.1109/TVT.2017.2744182.

[3] CHEN C M, XIANG Bin, LIU Yining, *et al*. A secure authentication protocol for internet of vehicles[J]. *IEEE Access*, 2019, 7: 12047–12057. doi: 10.1109/ACCESS.2019.2891105.

[4] CUI Jie, WANG Yali, ZHANG Jing, *et al*. Full session key agreement scheme based on chaotic map in vehicular Ad hoc networks[J]. *IEEE Transactions on Vehicular Technology*, 2020, 69(8): 8914–8924. doi: 10.1109/TVT.2020.2997694.

[5] WEI Lu, CUI Jie, ZHONG Hong, *et al*. Proven secure tree-based authenticated key agreement for securing V2V and V2I communications in VANETs[J]. *IEEE Transactions on Mobile Computing*, 2022, 21(9): 3280–3297. doi: 10.1109/TMC.2021.3056712.

[6] CHUANG M C and LEE J F. TEAM: Trust-extended authentication mechanism for vehicular Ad hoc networks[J]. *IEEE Systems Journal*, 2014, 8(3): 749–758. doi: 10.1109/JSYST.2012.2231792.

[7] YAO Yingying, CHANG Xiaolin, MIŠIĆ J, *et al*. BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services[J]. *IEEE Internet of Things Journal*, 2019, 6(2): 3775–3784. doi: 10.1109/JIOT.2019.2892009.

[8] 刘雪艳, 王力, 郇丽娟, 等. 车联网环境下无证书匿名认证方案[J]. 电子与信息学报, 2022, 44(1): 295–304. doi: 10.11999/JEIT201069.

LIU Xueyan, WANG Li, HUAN Lijuan, *et al*. Certificateless anonymous authentication scheme for internet of vehicles[J]. *Journal of Electronics & Information Technology*, 2022, 44(1): 295–304. doi: 10.11999/JEIT201069.

[9] LI Jiangtao, LI Yufeng, CAO Chenhong, *et al*. Conditional anonymous authentication with abuse-resistant tracing and distributed trust for internet of vehicles[J]. *IEEE Internet of*

Things Journal, 2022, 9(11): 8749–8762. doi: 10.1109/JIOT.2021.3116422.

[10] VIJAYAKUMAR P, AZEES M, KOZLOV S A, *et al*. An anonymous batch authentication and key exchange protocols for 6G enabled VANETs[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2022, 23(2): 1630–1638. doi: 10.1109/TITS.2021.3099488.

[11] TSAI J L and LO N W. A privacy-aware authentication scheme for distributed mobile cloud computing services[J]. *IEEE Systems Journal*, 2015, 9(3): 805–815. doi: 10.1109/JSYST.2014.2322973.

[12] IRSHAD A, SHER M, AHMAD H F, *et al*. An improved multi-server authentication scheme for distributed mobile cloud computing services[J]. *KSII Transactions on Internet and Information Systems*, 2016, 10(12): 6092–6115. doi: 10.3837/TIIS.2016.12.021.

[13] JIA Xiaoying, HE Debiao, KUMAR N, *et al*. A provably secure and efficient identity-based anonymous authentication scheme for mobile edge computing[J]. *IEEE Systems Journal*, 2020, 14(1): 560–571. doi: 10.1109/JSYST.2019.2896064.

[14] KUMAR A and OM H. An enhanced and provably secure authentication protocol using Chebyshev chaotic maps for multi-server environment[J]. *Multimedia Tools and Applications*, 2021, 80(9): 14163–14189. doi: 10.1007/s11042-020-10320-x.

[15] BAGGA P, DAS A K, WAZID M, *et al*. Authentication protocols in Internet of vehicles: Taxonomy, analysis, and challenges[J]. *IEEE Access*, 2020, 8: 54314–54344. doi: 10.1109/ACCESS.2020.2981397.

[16] LAI Chengzhe, ZHANG Min, CAO Jie, *et al*. SPIR: A secure and privacy-preserving incentive scheme for reliable real-time map updates[J]. *IEEE Internet of Things Journal*, 2020, 7(1): 416–428. doi: 10.1109/JIOT.2019.2953188.

张海波：男，博士，副教授，研究方向为车联网、区块链、安全认证等.

兰 凯：男，硕士生，研究方向为车联网、认证协议、密钥协商等.

黄宏武：男，硕士，研究方向为车联网、认证协议等.

王汝言：男，博士，教授，研究方向为泛在网络、多媒体信息处理等.

邹 灿：男，硕士，高级咨询顾问，研究方向为大数据、信息安全、数字经济等.

责任编辑：余 蓉