车载自组网中高效的群组协商通信协议

韩牟[1]，华蕾[1]，王良民[1]，江浩斌[2]，马世典[2]
(1. 江苏大学计算机科学与通信工程学院，江苏 镇江 212013；2. 江苏大学汽车工程研究院，江苏 镇江 212013)

摘 要：提出一种高效的群组协商通信协议,针对节点身份认证的效率问题，采用群内节点自检认证的方式，避免向认证中心发送认证证书，从而提高身份认证的速度；针对通信的机密性和单点失败现象，采用节点协商建立群组的方法，进而实现节点间的可靠通信；针对合法车辆认证次数频繁问题，采用群密钥传输机制，减少合法车辆的认证次数，进而提高节点加入群组的速度。最后，安全性分析和性能分析结果表明，所提方案不但满足车载自组网（VANET, vehicle ad hoc network）通信的基本安全需求，并且在认证时延、传输开销和平均时延方面优于现有方案。

关键词：高效认证；密钥协商；群组通信；车载自组网
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018009

Efficient communication protocol of group negotiation in VANET

HAN Mu[1], HUA Lei[1], WANG Liangmin[1], JIANG Haobin[2], MA Shidian[2]
1. Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China
2. Automotive Engineering Research Institute, Jiangsu University, Zhenjiang 212013, China

Abstract: An efficient communication protocol of group negotiation was proposed. The protocol adopted self-checking authentication in group to avoid the nodes sending certificates to the authentication center which improved the efficiency of identification. At the same time, the group establishment among nodes which through negotiation ensured the communication confidentiality and prevented the phenomenon of single-point failure. Besides, a group key transmission scheme was proposed to reduce the frequency of authentication for legal vehicles and improve the speed of joining in the group. At the end, theoretical analysis and simulation results demonstrate that the proposed protocol not only meets the security requirements of communication in VANET, but also shows much better performance than previous reported schemes on verification delay, transmission overhead and average delay.

Key words: efficient authentication, key negotiation, group communication, vehicle ad hoc network

1 引言

车载自组网的快速发展使人们能够方便快捷地从中获得各类服务，例如舒适服务项目，交通信息、气象信息、加油站或服务区地址、价格信息以及网络接入等；安全服务项目，紧急情况告警、变换车道援助、交叉路口协调、路面情况警告等，进而享受更加安全舒适的驾驶环境[1~4]。网络中的节点包括车辆和路边单元（RSU, road side unit）。每一辆车都安装了车载单元（OBU, on board unit），通过 OBU 车辆能够与外界进行各种通信。然而，由于车载自组网的动态性更强、稳定性更差等特点，

收稿日期：2017-09-05；**修回日期**：2017-12-10
通信作者：马世典，masd@ujs.edu.cn
基金项目：江苏省重点研发计划基金资助项目（No.BE2017035）；江苏省“六大人才高峰”基金资助项目（No.DZXX-012）；江苏省自然科学基金资助项目（No.12KJD580002）；江苏省研究生创新基金资助项目（No.KYLX_1057）
Foundation Items: The Key Research and Development Plan of Jiangsu Province (No.BE2017035), The Six Talent Peaks Project of Jiangsu Province (No.DZXX-012), The Natural Science Foundation of Jiangsu Province (No.12KJD580002), Jiangsu Graduate Innovation Fund (No.KYLX_1057)

使其在通信安全和通信效率方面面临诸多的问题和挑战，尤其是消息的安全性以及节点认证的效率。因此，设计一种既能满足 VANET 的安全需求又高效的通信方案是目前 VANET 研究的重点之一。

首先，一个适用于 VANET 的通信协议需要满足以下几个基本的安全需求。

1) 消息完整性和身份认证性。车辆能够认证消息，并且能够确认该消息确实由发送方发送和签名，没有被恶意车辆篡改。

2) 消息的隐私性。车辆在通信过程中所发送的任何消息均不能泄露任何关于其真实身份的隐私信息。

3) 消息的机密性。车辆发送的消息只能被指定的车辆解读，其他车辆无法获得。

4) 消息的不可否认性。当恶意车辆发送的恶意消息引发交通事故时，相应的权威机构应能够从该恶意消息中揭露出发送方的真实身份并对其进行谴责，进而使该车辆无法否认其发送该条恶意消息。

5) 前后向安全性。当车辆离开通信群后，其无法获得该群的新群密钥，同时新加入群的成员也无法获得该群的原群密钥。

其次，由于车辆移动速度快，导致 VANET 中通信时间短。因此，通信的效率同样至关重要。

目前，为了解决上述 VANET 通信中的安全性问题以及高效通信问题，文献[5]提出了一种新的 PKI（public key infrastructure）方案。该方案根据不同情况将共享密钥对集合分为紧急密钥对集合和匿名密钥对集合，合法车辆可以在不同情况下使用不同密钥对集合中的私钥进行签名，从而满足 VANET 中的安全需求。基于消息聚合算法椭圆曲线零知识证明，文献[6]提出一种通信双方不需交换证书的匿名认证机制解决隐私泄露问题进而保护节点的身份隐私。此外，该机制基于消息聚合算法实现路边单元对消息的批量认证，提高消息认证的效率。文献[7]提出每辆车预装载大量的匿名公私钥对以及公钥证书保护车辆的隐私，但是检查撤销证书列表需要耗费大量的时间。文献[8,9]提出高效的消息认证方案。其中，文献[8]中的方案为合法车辆通过使用共享群签名密钥为自己颁发证书，从而降低消息认证时所产生的平均功耗，但仍存在消息认证速度不够理想的问题。文献[9]基于椭圆曲线密码提出一种不需双线性映射对运算的消息认证方案，降低了签名与验证的计算开销和通信开销。文献[10,11]提出采用群签名方案解决 VANET 中的安全认证问题。较普通的签名，群签名具有更高的隐私性，其不会反映出任何签名者的信息，只有群管理者能够从群签名中追踪到签名者，但由于车辆移动速度快，需要频繁地更新群签名，因此，不适用于 VANET。文献[12]提出一种高效的可撤销群签名方案。该方案采用将子集覆盖框架与 Camenisch-Stadler 方案相结合的方法，以提高签名验证的效率，但方案中成员证书长度复杂度与车辆数目密切相关，使其在车辆数目庞大的 VANET 环境下并不适用。文献[13]提出一种车辆和 RSU 批量验证签名的方法，提高认证速度，但是该方法严重依赖防篡改装置。文献[14]使用 HMAC（hash-based message authentication code）对消息进行认证，保证消息的完整性和认证性，同时引入对称密码减少通信开销，但却引发对称密钥的产生与管理这一新的困难问题。文献[15~18]通过使用基于身份的密码体制减少公钥证书的计算过程。其中，文献[15,16]提出使用批量认证的方法提高了认证效率，但是不具备前向安全性。其中，文献[16]通过减少耗时的映射运算提高认证的效率，但车辆的认证次数过于频繁，耗费大量的时间，并且为可信中心带来了巨大的压力与负担。文献[17]使用 HMAC 和对称密码代替传统、复杂的椭圆曲线密码，加快了消息的认证速度，但同时产生了车辆易被跟踪的问题。文献[18]提出可撤销的群组批量认证的方法，但该方法没有考虑头车辆的安全性。文献[19]提出了 VANET 安全通信框架，该框架采用对称密码和非对称密码相结合的方式，在保证通信安全的同时提高通信效率。

针对上述现有方案存在的问题，本文提出高效的群组协商通信方案。该方案在满足 VANET 安全需求的基础上，通过使用 RSU 和车辆相互自认证的方式代替传统的第三方认证，使用群密钥协商方案以及群密钥传递机制，提高了车辆的认证效率和通信效率。本文的主要贡献如下。

1) 提出一种无认证中心的节点自检认证方法，避免向认证中心进行认证的消息传输。

2) 提出一种密钥传输机制，减少合法车辆的认证次数，进而提高合法节点加入群组的速度。

2　预备知识

2.1　相关数学知识

1) G_1 中的计算性 Diffie-Hellman 问题（CDH problem)

①CDH 问题。已知(P,aP,bP)，其中，$a,b\in Z_q^*$，P 是 G_1 的生成元，由概率多项式时间算法 A 输出 abP，A 成功的概率为

$$succ_{A,G_1}^{\mathrm{CDH}}=\Pr[A(P,aP,bP)=abP] \tag{1}$$

②CDH 假设。对于任意的判定性多项式时间算法(PPT 算法)，A、$succ_{A,G_1}^{\mathrm{CDH}}$ 是可以忽略值。

2) G 中的判定性 Diffie-Hellman 问题（DDH problem)

①DDH 问题。G 中的 DDH 问题，即对于(g, g^x, g^y, g^r)，x、y、$r\in_R G$，存在 PPT，输出值为 0 或 1 的算法 A，当 r=xy 时，输出 0；反之，输出 1。A 成功解决 G 中的 DDH 问题的优势为

$$adv_{A,G}^{\mathrm{DDH}}=\Pr[A(g,g^x,g^y,g^{xy})=1]-\Pr[A(g,g^x,g^y,g^r)=1] \tag{2}$$

②DDH 假设。对于任意 PPT，输出值为 0 或 1 的算法 A，$adv_{A,G}^{\mathrm{DDH}}$ 是可以忽略值。

3) 双线性映射

如果一个映射 $e:G_1\times G_1\to G_2$ 满足以下 3 个性质，则称为双线性映射。

①双线性。对所有的 P、$Q\in G_1$，a、$b\in Z_q^*$，满足 $e(aP,bQ)=e(P,Q)^{ab}$。此性质等价于对所有的 P、Q、$R\in G_1$，满足 $e(P+Q,R)=e(P,R)e(Q,R)$，$e(P,Q+R)=e(P,Q)e(P,R)$。

②非退化性。如果 P 是 G_1 的生成元，则 $e(P,P)$ 是 G_2 的生成元，即满足 $e(P,P)\neq 1$。

③可计算性。对于任意 P、$Q\in G_1$，存在有效的算法计算 $e(P,Q)$。

2.2 系统结构模型

本文的系统结构模型如图 1 所示。其主要由可信度最高的可信中心（TA）、RSU 以及车辆 3 个部分构成。

1) 可信中心（TA）。TA 为整个系统的可信认证中心，具有足够的计算能力和存储能力。其负责车载自组网中所有实体的注册、管理工作，揭露处于交通纠纷事件中车辆的真实身份信息以及公布非法车辆的撤销信息。在本文中，车辆和 RSU 在使用前均需到 TA 处进行注册，获得相关证书及系统参数。

2) 路边单元（RSU）。RSU 均匀分布在路边，与 TA 进行有线通信，与车辆进行无线通信，在相邻的 RSU 之间也能够通信。其主要负责认证处于自身管辖范围内车辆的合法性、协商密钥、建立通信群组以及协助 TA 对违法车辆进行谴责。

3) 车辆。每个车辆都装备有能够存储安全材料以及执行所有加密操作的 OBU。

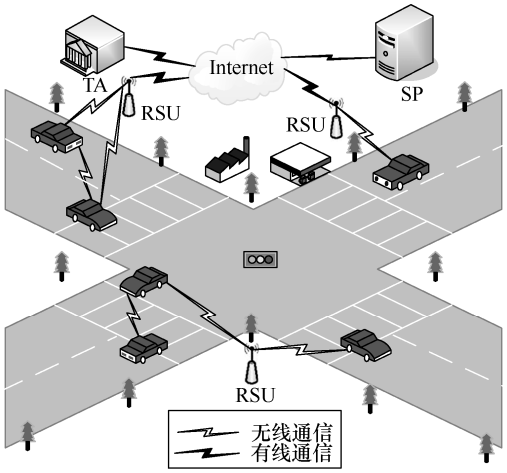


图 1 系统结构模型

2.3 攻击模型

由于车载自组织网络通过无线信道进行通信，使其不可避免地面临许多威胁和攻击，例如，注入虚假错误的消息、篡改消息内容等。因此 VANET 的安全与车辆用户的生命财产息息相关，上述威胁和攻击会造成严重的后果。对此，本文总结了以下几种车载网中主要的攻击类型。这里只讨论对车载自组网内信息传输易遭受的攻击，而不考虑对车辆本身的物理攻击。

1) 假冒攻击。攻击者假冒其他车辆或 RSU 的身份进行通信。

2) 隐私攻击。攻击者通过车载自组网非法地获得其他车辆的敏感信息，从而获得车辆驾驶者的隐私信息，如司机的日常行踪。

3) 窃听攻击。攻击者可以是车辆或 RSU，它们通过非法窃听获得车载自组织网络中的机密数据。

4) 虚假消息攻击。攻击者发布一些错误的信息，这些虚假的消息可能影响接收者对周围情况的判断，从而导致事故的发生。

5) 可否认攻击。当事故发生后，攻击者否认发送过该消息，并使相关部门无法对攻击者进行追责，从而逃避承担事故的责任。

6) 女巫攻击。恶意车辆通过使用多个身份进行攻击，这些身份既可以是盗用其他车辆的身份，也可以是虚假身份。

针对上述几种主要的攻击手段，引言提出的完整性和认证性能够抵抗假冒攻击；隐私性能够抵抗隐私攻击；机密性能够抵抗窃听攻击；不可否认性能够抵抗虚假消息攻击和可否认攻击；针对女巫攻击，可通过对通信实体进行身份认证的方法，达到抵抗女巫攻击的目的。

3　高效的群组协商通信协议

本文的系统设计如图 2 所示，其主要内容包括以下 3 个方面。

1) 系统初始化。生成并公布系统参数，为 RSU 和车辆分发密钥、签名消息、认证参数等。

2) 无认证中心的 RSU 和车辆双向认证。采用无认证中心的双向认证方式，避免向可信中心发送认证证书，减少了认证中心的负担，提高了认证效率，同时使用相邻 RSU 之间传递群密钥的方法，减少合法车辆的认证次数，从而提高了身份认证的速度。

3) 群密钥协商。采用群密钥协商的方式，使合法车辆加入以 RSU 为中心的群，进而进行节点通信。

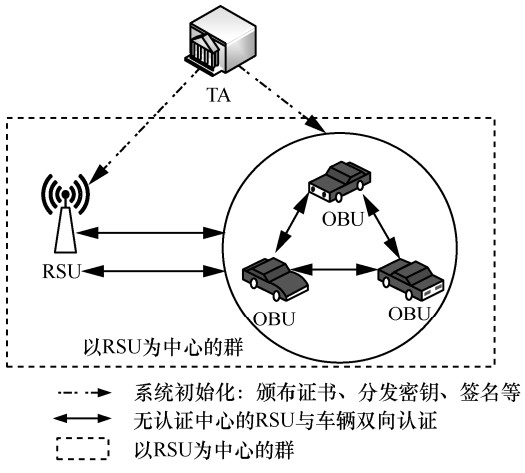


图 2　系统设计

3.1　系统初始化

1) 可信中心（TA）。TA 选择 2 个具有相同大素数阶 q 的群 G_1 和 G_2（G_1 为加法群，G_2 为乘法群）。假设 P 为 G_1 的任意生成元，选择一个特殊的乘法群 G（p 为其安全素数，满足 p=2q+1，q 为 k bit 素数）和循环群 G'=<g>，G'为模 p 的二次剩余类。TA 随机选择 $\psi_{\mathrm{TA}} \in Z_q^*$ 作为私钥 SK_{TA}，并计算出公钥 PK_{TA}=$\Psi_{\mathrm{TA}}P$。TA 定义 2 个散列函数 H_1:$\{0,1\}^* \to G_1$ 和 $h:\{0,1\}^* \to Z_q^*$，一个安全的密码算法 $E(\cdot)$，然后公布整个系统参数 $(G_1, G_2, P, q, e, G, p, g, PK_{\mathrm{TA}}, H_1(\cdot), h(\cdot), E(\cdot))$，并预载到进行注册的 RSU 和车辆中。本文主要符号定义如表 1 所示。

表 1　　主要符号定义

定义	描述
q	比特素数
G_1,G_2	具有相同大素数阶 q 的加法群和乘法群
P, g	加法群 G_1 与循环群 G'的任意生成元
p	特殊乘法群 G 的安全素数
V, TID_V, FID_V	车辆，真名标识，假名标识
RSU, TID_{RSU}	RSU，真名标识
m	消息
Q_U, s_U	U 的认证参数
TS	时间戳
U	实体 U（车辆或 RSU）
$\mathrm{RSU}_{i\pm1}$	RSU_i 附近的 RSU
(PK_U, SK_U)	U 的公钥、私钥
$\sigma_{SK_U}(\cdot)$	U 对数据的签名
GK	群密钥
$VVK_{i,j}$	车辆 V_i 和 V_j 的共享密钥
$HMAC_k(\cdot)$	使用密钥 k 产生的消息认证
$E_k(\cdot)$	用密钥 k 加密

2) 路边单元（RSU）。RSU 使用前需要到 TA 处注册。在注册过程中 TA 给每个 RSU 分配一个真名 TID_{RSU_i}，随机选择 $\xi_i \in Z_q^*$ 作为 RSU 的私钥 SK_{RSU_i}，计算公钥 $PK_{\mathrm{RSU}_i}=\xi_i P$ 和认证参数 $Q_{\mathrm{RSU}_i}=H_1(TID_{\mathrm{RSU}_i})$、$s_{\mathrm{RSU}_i}=\psi_{TA}Q_{\mathrm{RSU}_i}$，然后生成签名 $\sigma_{SK}(PK_{\mathrm{RSU}_i}, TID_{\mathrm{RSU}_i}, Loc_{\mathrm{RSU}_i}, h(Loc_{\mathrm{RSU}_i}))$，其中，$h(Loc_{\mathrm{RSU}_i})$ 是 RSU_i 所在地理位置信息的散列值。随后将附近区域内路边单元 $\mathrm{RSU}_{i\pm1}$ 的公钥一同下载到 RSU_i 中。

3) 车辆。车辆到 TA 处进行注册时，TA 为每辆车 V_i 分配一个真名 TID_{V_i}，计算认证参数 $Q_{V_i}=H_1(TID_{V_i})$、$s_{V_i}=\psi_{\mathrm{TA}}Q_{V_i}$ 并保存。每当车辆进入另一 RSU 的通信范围时，车辆随机选择 $r_i \in Z_q^*$ 作为临时私钥 SK_{V_i}，计算临时公钥 $PK_{V_i}=r_iP$ 以及临时假名 $FID_{V_i}=TID_{V_i} \oplus H_1(r_iPK_{\mathrm{TA}})$，从而保证自身不被攻击者追踪到。

3.2　高效的群组协商通信协议设计

本文所提出的高效群组协商通信协议，其详细设计如图 3 所示，系统初始化后，当目标车辆进入 RSU_1 的通信范围内，首先需要与 RSU_1 进行无身份认证以验证车辆身份的合法性。当身份认证完成后

（即目标车辆为合法车辆），目标车辆将与 RSU_1 协商群密钥加入群 1 进行通信，同时 RSU_1 采用群密钥传递机制将该群的群密钥传递给附近区域的 RSU_2。当目标车辆移动到群 2 时，RSU_2 只需确认该目标车辆是否已经被附近 RSU_1 认证过（即目标车辆是否为合法车辆），若该目标车辆已经完成认证，则直接进行群 2 的密钥协商，否则，对其身份进行进一步的认证。

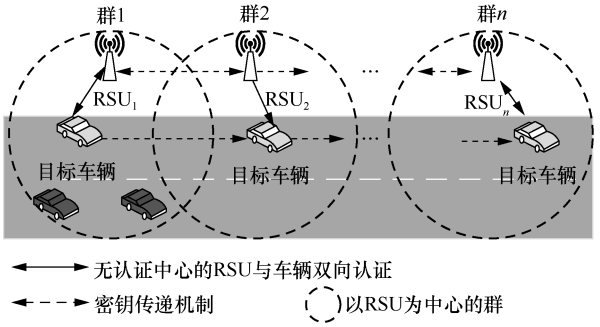


图 3 协议详细设计

3.2.1 车辆和 RSU 双方认证

本文协议中车辆和 RSU 的身份认证是不需 TA 参与的相互自认证方式，同时相邻 RSU 采用群密钥传递机制，减少合法车辆的认证次数。车辆和 RSU 双方认证过程如图 4 所示，信息交互过程如图 5 所示。

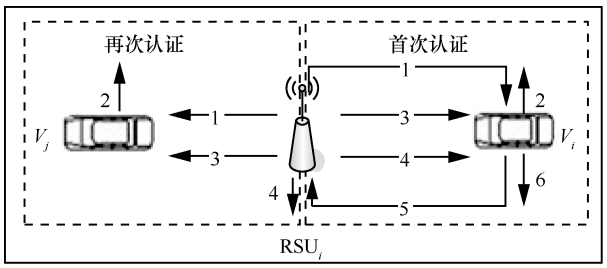


图 4 车辆和 RSU 双方认证过程

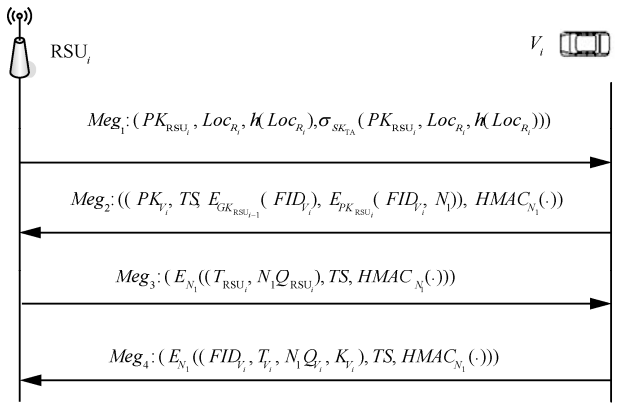


图 5 RSU_i 与 V_i 双向认证信息交互过程

如图 4 所示，车辆进行首次认证时需要进行完整的身份认证过程，其共有 6 步。而已经完成过一次完整认证的车辆，当需要再次认证时，只需要完成前 4 步。

1) RSU_i 周期性向外广播消息 Meg_1：$(PK_{RSU_i}, Loc_{RSU_i}, h(Loc_{RSU_i}), \sigma_{SK_{TA}}(PK_{RSU_i}, Loc_{RSU_i}, h(Loc_{RSU_i})))$。

2) 车辆 V_i 进入 RSU_i 的通信范围时（当车辆处在相邻 2 个 RSU 的交叉混合区域时，则根据信号强度选择与信号强度较强的 RSU 进行双向认证），接收到消息 Meg_1 后，车辆 V_i 从 Meg_1 中获得相应的信息 $PK_{RSU_i}, Loc_{RSU_i}, h(Loc_{RSU_i})$ 以及签名 $\sigma_{SK_{TA}}(PK_{RSU_i}, Loc_{RSU_i}, h(Loc_{RSU_i}))$，然后使用 TA 的公钥 PK_{TA} 验证签名。若签名正确，则车辆 V_i 从 GPS 中取出其当前所处位置的地理信息 Loc_{V_i}，计算 $\Delta L = |Loc_{V_i} - Loc_{RSU_i}|$，并判断 ΔL 是否不大于 600 m。若 $\Delta L \leqslant 600$ m，则 V_i 完成对 RSU_i 的认证，否则，丢弃该消息。

3) 车辆 V_i 完成对路边单元 RSU_i 的认证后选择随机数 N_1，随后发消息 Meg_2: $(PK_{V_i}, TS, E_{GK_{RSU_{i-1}}}(FID_{V_i}), E_{PK_{RSU_i}}(FID_{V_i}, N_1), HMAC_{N_1}(\cdot))$ 给 RSU_i。

4) 当 RSU_i 接收到消息 Meg_2 后，根据消息中的时间戳（TS）计算出时间差 $\Delta t = CT - TS$，其中，CT 为当前时刻，若 Δt 满足网络时延，则 RSU_i 解密信息 $E_{PK_{RSU_i}}(FID_{V_i}, N_1)$，从而，得到车辆的 FID_{V_i}，N_1 计算 $HMAC'_{N_1}(\cdot)$，比较 $HMAC'_{N_1}(\cdot)$ 和消息 Meg_2 中的 $HMAC_{N_1}(\cdot)$，若相等，则使用附近区域 $RSU_{i\pm1}$ 传递的 GK，解密 $E_{GK_{RSU_{i\pm1}}}(FID_{V_i})$ 得到 FID'_{V_i}，比较 FID_{V_i} 和 FID'_{V_i}，若相等，则车辆 V_i 已被附近 $RSU_{i\pm1}$ 完成认证(即车辆 V_i 为合法车辆)，那么车辆 V_i 将进行群密钥协商过程。若不相等，RSU_i 随机选择 $\alpha \in Z_q^*$ 并计算 $T_{RSU_i} = \alpha P$，然后发送消息 Meg_3: $(E_{N_1}((T_{RSU_i}, N_1Q_{RSU_i}), HMAC(\cdot)))$ 给车辆 V_i。

5) V_i 接收到 Meg_3，解密获得 T_{RSU_i}，认证 $HMAC'_{N_1}(\cdot)$。随机选择 $\beta \in Z_q^*$，计算 $T_{V_i} = \beta P$，$K_{V_i} = e(\beta N_1 Q_{RSU_i}, PK_{TA})e(N_1 s_{V_i}, T_{RSU_i})$，发送 Meg_4: $(E_{N_1}((FID_{V_i}, T_{V_i}, N_1Q_{V_i}, K_{V_i}), TS, HMAC_{N_1}(\cdot)))$ 给 RSU_i。

6) RSU_i 接收到 Meg_4 后，首先解密认证 $HMAC_{N_1}(\cdot)$，若认证成功，则根据 T_{V_i}、$N_1Q_{V_i}$、K_{V_i} 计算 $K_{RSU_i} = e(\alpha N_1 Q_{V_i}, PK_{TA})e(N_1 s_{RSU_i}, T_{V_i})$，如果式(3)

成立，则车辆 V_i 为合法车辆。

$$K_{V_i} = K_{\mathrm{RSU}_i} \tag{3}$$

3.2.2 群组密钥的协商和更新

1) 群组密钥协商

完成身份认证后的车辆将进行群密钥协商过程，加入以 RSU 为中心的群，以便与 RSU 和群内其他合法成员进行通信。群密钥协商过程如图 6 所示。

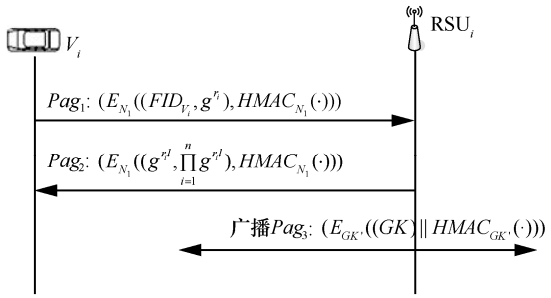


图 6　群密钥协商过程

① V_i 随机选择 $r_i \in Z_{qi}^*$，计算 g^{r_i}，发送 Pag_1: $(E_{N_1}((FID_{V_i}, g^{r_i}), HMAC_{N_1}(\cdot)))$ 给 RSU_i。

②RSU_i 接收 Pag_1，解密获得 FID_{V_i}、g^{r_i}，随机选择 $l \in Z_q^*$，计算 $g^{r_i l}$、$\prod_{i=1}^{n} g^{r_i l}$ 和群密钥 $GK = g^l \prod_{i=1}^{n} g^{r_i l}$，然后发送消息 Pag_2: $(E_{N_1}((g^{r_i l}, \prod_{i=1}^{n} g^{r_i l}), HMAC_{N_1}(\cdot)))$ 给 V_i，并广播 Pag_3: $(E_{GK'}((GK) \| HMAC_{GK'}(\cdot)))$ 给其他群组成员，其中，GK'为以前的群密钥。随后 RSU_i 执行群密钥传输机制。

③V_i 接受消息 Pag_2，解密获得 $g^{r_i l}$、$\prod_{i=1}^{n} g^{r_i l}$，计算 $g^l = (g^{r_i l})^{r_i^{-1}}$，然后获得群密钥 $GK = g^l \prod_{i=1}^{n} g^{r_i l}$。

群密钥更新后，RSU_i 通过有线发送消息 $E_{PK_{\mathrm{RSU}_{i\pm1}}}(GK, \sigma_{PK_{\mathrm{RSU}_i}}(\cdot))$ 给附近的 RSU。

2) 群密钥的更新

为了使处在通信群组中的车辆退出后，不妨碍群内其他车辆的通信，同时不能与群内成员继续进行通信，因此，该通信群组必须执行群密钥的更新过程。该过程如下所示。

①当车辆 V_j 离开 RSU_i 的通信区域时，车辆 V_j 向 RSU_i 主动发送离开消息 $E_{GK}(left, FID_{V_j}, HMAC_{GK}(\cdot))$。当 RSU_i 接收到车辆 V_j 的离开消息后，其随机选择 $l \in Z_q^*$ 计算除 V_j 以外全部群内其他成员的 $g^{r_i l}$、$\prod_{1}^{j-1}\prod_{j+1}^{n} g^{r_i l}$ 并广播消息 Bm_1 $(E_{GK'}((g^{r_1 l}, FID_{V_1}), \cdots, (g^{r_{j-1} l}, FID_{V_{j-1}}), (g^{r_{j+1} l}, FID_{V_{j+1}}), \cdots, (g^{r_n l}, FID_{V_n}), \prod_{1}^{j-1}(\prod_{j+1}^{n} g^{r_i l}), TS, HMAC_{GK'}(\cdot)))$。

②当群内其他成员 V_i 接收到密钥更新消息 Bm_1 时，使用 GK'解密该消息，根据 FID_{V_i} 得到 $g^{r_i l}$、$\prod_{1}^{j-1}\prod_{j+1}^{n} g^{r_i l}$，并计算出 $g^l = (g^{r_i l})^{r_i^{-1}}$，进而更新群密钥 $GK = g^l \prod_{1}^{j-1}\prod_{j+1}^{n} g^{r_i l}$。

4 可行性和安全性

4.1 方案可行性

4.1.1 双向认证的可行性

为了提高车辆身份认证的速度，减少合法车辆的认证次数，本文提出了不需 TA 参与的车辆与 RSU 双向认证方案，其可行性由定理 1 得到保证。

定理 1　在第 3.2.1 节中，RSU_i 是通过式(3)对车辆 V_i 的身份其进行认证的。当且仅当式(3)成立时，车辆 V_i 的身份是合法的。

证明　充分性。当式(3)成立时，车辆 V_i 的身份是合法的（即该车辆是合法车辆）。

由于车辆 V_i 所发送的消息 Meg_4 中，K_{V_i} 的值等于 $e(\beta N_1 Q_{\mathrm{RSU}_i}, PK_{\mathrm{TA}})e(N_1 s_{V_i}, T_{\mathrm{RSU}_i})$，并且 SK_{TA} 是可信中心的私钥，不进行任何的传输，攻击者及非法成员无法获得，根据 CDH 困难问题，非法车辆以及攻击者在不知道 SK_{TA} 的情况下无法计算出 $s_{V_i} = \psi_{\mathrm{TA}} Q_{V_i}$，进而无法获得 K_{V_i} 的值。因此，当式(3)成立时，车辆 V_i 是合法车辆。

必要性。当车辆 V_i 的身份是合法的，式(3)成立。通过如下计算过程可以验证式(3)是否成立。

$$\begin{aligned} K_{V_i} &= e(\beta N_1 Q_{\mathrm{RSU}_i}, PK_{\mathrm{TA}})e(N_1 s_{V_i}, T_{\mathrm{RSU}}) \\ &= e(\beta N_1 H_1(TID_{\mathrm{RSU}_i}), \psi_{\mathrm{TA}} P) \cdot \\ &\quad e(N_1 \psi_{\mathrm{TA}} H_1(TID_{V_i}), \alpha P) \\ &= e(\alpha N_1 H_1(TID_{V_i}) + \beta N_1 H_1(TID_{\mathrm{RSU}_i}), \psi_{\mathrm{TA}} P) \\ &= e(\alpha N_1 Q_{V_i}, PK_{\mathrm{TA}})e(N_1 s_{\mathrm{RSU}_i}, T_{V_i}) \\ &= K_{\mathrm{RSU}_i} \end{aligned} \tag{4}$$

如式(3)所示的计算过程，如果车辆 V_i 的身份是合法的，则式(3)一定成立。因此，必要性证明完成。

通过上述证明，本文提出的车辆与 RSU 双向身份认证方案具有可行性。

4.1.2 群密钥传输机制的可行性

在第 3.2.2 节中采用群密钥传输机制，RSU_i 通过有线通信传输自身群密钥给附近区域的 $\mathrm{RSU}_{i\pm1}$，因此，RSU_i 会存储附近区域 $\mathrm{RSU}_{i\pm1}$ 群的群密钥。当车辆已经认证并加入 $\mathrm{RSU}_{i\pm1}$ 形成的群后，当它进入 RSU_i 的通信范围时，第 3.2.1 节认证过程只会执行步骤 1)~步骤 4)。RSU_i 使用 $\mathrm{RSU}_{i\pm1}$ 发送过来的群密钥解密 $E_{GK_{i\pm1}}(FID_i)$。由于 RSU_i 持有相邻 $\mathrm{RSU}_{i\pm1}$ 的群密钥 $E_{\mathrm{RSU}_{i\pm1}}$，那么当 RSU_i 能够正确解密消息 $E_{GK_{i\pm1}}(FID_i)$ 并获得此车辆的身份信息时，该车辆在进入本群之前，相邻 $\mathrm{RSU}_{i\pm1}$ 一定已经对其完成身份认证并加入相应群组（即该车辆为合法车辆）。此外，由于群密钥首先使用 RSU_i 的公钥进行加密，然后通过有线进行传递，所以群密钥是安全的。因此，群密钥传递机制是可行的。

4.2 方案安全性

4.2.1 消息的完整性和认证性

在本文所提出的通信方案中，消息的完整性和认证性是通过采用 $E_k(M)$ 和消息认证 $HMAC_k(M)$实现的。若攻击者无法获得 $E_k(M)$ 和 $HMAC_k(M)$，那么信息的完整性与认证性得到了保障。

在共享密钥 k 被安全持有的情况下，若攻击者无法伪造消息，则在随机预言机下本方案对存在的伪造攻击是安全的。首先，考虑挑战者和攻击者之间的游戏。

Setup：挑战者给予攻击者一系列参数。

Challenge：挑战者请求攻击者选择一个随机的消息 M 并产生 $E_k(M)$和 $HMAC_k(M)$。

Guess：攻击者将一对 $E_k(M)$和 $HMAC_k(M)$发送给挑战者。

在游戏中，攻击者的优势定义为

$$adv=\Pr[E_k(M)\text{和 }HMAC_k(M)\text{是有效的签名}] \tag{5}$$

在第 3.2.1 节中，$k=N_1$ 为车辆 V_i 和路边单元 RSU_i 共享的密钥。使用 PK_{RSU_i} 加密 N_1 后传递给路边单元 RSU_i。由于只有 RSU_i 拥有对应的私钥 SK_{RSU_i}，则对消息进行解密获得 N_1。因此，任何攻击者都无法获得 N_1 和伪造任何有效信息。

因此，攻击者的优势是微乎其微的，本文方案是安全的。

4.2.2 消息的隐私性

定理 2 该通信协议具有消息的隐私性，即攻击者获取车辆的真实身份并对车辆进行追踪是困难的。

证明 攻击者追踪车辆 V_i，获得其行驶路线。本文方案中，车辆在通信过程中发送的相关信息会涉及隐私，如车辆本身的假名 FID_{V_i}、公钥 PK_{V_i} 以及认证时发送的认证参数 $N_1Q_{V_i}$。由于合法车辆每进入一个 RSU 的通信范围时，车辆都会重新选择 $r_i\in Z_q^*$，计算出临时的私钥 $SK_{V_i}=r_i$、公钥 $PK_{V_i}=r_iP$ 和假名 $FID_{V_i}=TID_{V_i}\oplus H_1(r_iPK_{\mathrm{TA}})$。因此，合法 V_i 在不同的以 RSU 为中心的群组内所使用的公钥和假名是不同的，因此，攻击者无法通过车辆在某一群内的公钥、假名以追踪到某一合法车辆。同样，由于认证参数 $N_1Q_{V_i}$ 中 N_1 在不同的 RSU 范围中亦是改变的，并且根据 CDH 困难问题，攻击者不能从 $N_1Q_{V_i}$ 计算出 Q_{V_i}，所以攻击者也不能通过 $N_1Q_{V_i}$ 跟踪车辆。综上所述，攻击者追踪车辆是困难的。

4.2.3 消息的机密性

本文所提出的通信方案中，车辆在进行群密钥协商的过程中，车辆 V_i 随机选择 r_i 计算出 g^{r_i}，然后对其加密再进行传递，根据 DDH 困难性问题可知，假设攻击者获得 g^{r_i}，但也无法计算出 r_i 的值，进而根据 $g^l=(g^{r_il})^{r_i^{-1}}$ 计算出 g^l。同时由于 l 由 RSU_i 随机选择，攻击者没有办法获得。同样，根据 DDH 困难性问题可知，攻击者根据信息 g^{r_il} 也无法计算出 g^l。综上所述，攻击者无法获得群密钥 $GK=g^l\prod_{i=1}^{n}g^{r_il}$，进而保证了群密钥协商过程中消息的机密性。

在路边单元 RSU_i 与车辆 V_i 进行通信的过程中，消息经过共享密钥 N_1 加密后进行传递，而共享密钥 N_1 是由车辆 V_i 随机产生，然后使用 RSU_i 的公钥加密之后进行转发。根据 CDH 困难性问题可知，攻击者在持有 RSU_i 公钥的情况下无法计算出私钥，进而无法得到共享密钥 N_1，那么攻击者也无法获得使用 N_1 加密过的任何消息，因此保证了路边单元 RSU_i 与车辆 V_i 进行通信过程中消息的机密性。

4.2.4 消息的不可否认性

为了证明当出现意外事故时，该协议能够根据

通信消息协助有关部门进行追责，通信具有不可否认性，给出证明如下所示。

定理 3　不可否认性是指车辆发送某个消息后，其否认曾经发送过该消息是困难的。如交通事故发生后，相关部门在调查该事件时能够找出引发事故的关键消息并揭示出消息的发送车辆，即使该车辆否认其曾经发送过该消息。

证明　在本方案中，发送的每条消息都附有消息发送方的假名 FID_{V_i}，相关部门可以根据该假名，获得该车辆在通信过程中使用的公钥 PK_{V_i}，随后可信中心可根据自己的私钥、车辆的假名及公钥通过计算揭示出车辆的真实身份 ，即

$$\begin{aligned} TID_{V_i} &= FID_{V_i} \oplus H_1(SK_{\mathrm{TA}} \cdot PK_{V_i}) \\ &= TID_{V_i} \oplus H_1(r_i \cdot PK_{\mathrm{TA}}) \oplus H_1(SK_{\mathrm{TA}} \cdot PK_{V_i}) \\ &= TID_{V_i} \end{aligned} \tag{6}$$

综上所述，攻击者否认发送过该消息是困难的。

4.2.5　前后向保密性

为了证明该通信协议具有前后向保密性，即只有现有的群成员拥有当前群的群密钥，其证明如下所示。

定理 4　该通信协议具有前后向保密性，即退出群的车辆获得新的群密钥是困难的，新加入群的车辆获得前向群密钥是困难的。

证明　假设攻击者 V_i 离开 RSU_i 的通信范围，其仍想获得新的群密钥，由于新的群密钥 $GK = g^l \prod_{1}^{j-1}\prod_{j+1}^{n} g^{r_i l}$，所以其必须获得 g^l 和 $\prod_{1}^{j-1}\prod_{j+1}^{n} g^{r_i l}$。根据协议，当攻击者离开群组时，$\mathrm{RSU}_i$ 随机选择新的 $l \in Z_q^*$，广播计算新群密钥的各项数据。根据 DDH 困难问题可知，即使攻击者 V_j 接收到 RSU_i 广播的信息从而获得新群的相关数据 $g^{r_1 l},\cdots,g^{r_{j-1} l},g^{r_{j+1} l},\cdots,g^{r_n l},\prod_{1}^{j-1}\prod_{j+1}^{n} g^{r_i l}$，但无法得到 $g^{r_j l}$，因此攻击者 V_j 无法计算出新的群密钥，从而无法进行群内通信。同样，当攻击者 V_i 加入群组时，RSU 随机选择新的 $l \in Z_q^*$，攻击者无法获得以前的参数 l 计算出原始参数 g^l，进而进一步计算原始群密钥 $GK = g^l \prod_{1}^{j-1}\prod_{j+1}^{n} g^{r_i l}$。

综上所述，攻击者 V_j 获得前后向群密钥是困难的，该通信协议具有前后向保密性。

5　性能分析与仿真

本文实验相关参数采用美国联邦公路管理局提供的真实数据[20]。实验道路场景实验道路长约 900 m，包括 5 个车道和一个辅道，RSU 分别部署在道路的 100 m 和 700 m 处，实验采用 14:40:00~14:45:00 时段的车辆移动数据，实验场景如图 7 所示，主要参数如表 2 所示。

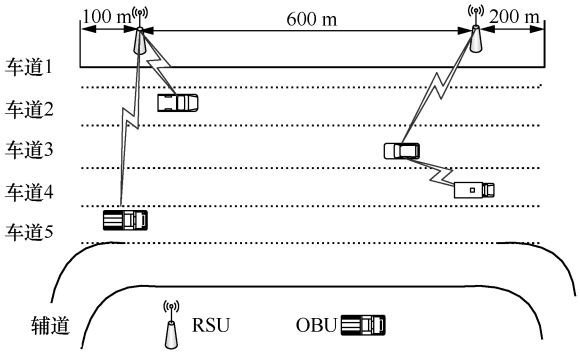


图 7　仿真实验场景

表 2　**仿真参数**

仿真参数	参数值
仿真工具	NS2
区域大小	900 m×30 m
仿真时间	5 min
消息主体大小	200 B
传播间隔	300 ms
变化间隔	0.05 s
RSU 通信范围	600 m
车辆通信范围	300 m
车辆平均移动速度	30 m/s
通信带宽	6 Mbit/s
MAC 协议	IEEE 802.11b

5.1　认证时延

根据文献[11]中所述，实验在英特尔奔腾 3.0 GHz 处理器上运行，得到执行一次点乘操作所需的时间 T_{mul} 为 0.6 ms，执行一次映射到点的散列操作 T_{mtp} 为 0.6 ms，执行一次双线性映射对所需的时间 T_{par} 为 4.5 ms。由于认证中散列、HMAC 运算等消耗的时间极少，故忽略计算它们所需要的时间。因此，本文主要的计算开销为 T_{mul}、T_{mtp} 和 T_{par}。表 3 所示的是 RSU 对 n 辆车（均为非法车辆）进行认证时所需的计算量对比。对比的其他方案中合法车辆每

经过一个 RSU 都需要进行完整的身份认证过程，认证次数频繁。而本文方案通过采用密钥传递机制，使合法车辆仅需进行一次完整的身份认证即可，减少了合法车辆身份认证的次数，进而从整体上提高了认证效率。

表 3　　计算量比较（完成 n 辆车认证）

方案	OBU 计算量	RSU 计算量
CPAS 方案	$4nT_{\text{mul}}$	$(n+1)T_{\text{mul}}+3T_{\text{par}}$
ABAKA 方案	$3nT_{\text{mul}}$	$(4n+3)T_{\text{mul}}$
ARGB 方案	$6nT_{\text{mul}}+2nT_{\text{mtp}}$	$(n+1)T_{\text{mul}}+3T_{\text{par}}+T_{\text{mtp}}$
本文方案	$5nT_{\text{mul}}+nT_{\text{mtp}}+2nT_{\text{par}}$	$4nT_{\text{mul}}+2nT_{\text{par}}$

由于本文提出的认证方案中，如果车辆已被某路段的 RSU 认证过（即该车辆为合法车辆），则当其进入该 RSU 附近其他 RSU 的通信范围，再次进行认证时，该认证过程只需进行到 3.2.1 节方案的步骤 4)即可。因此，当某一车辆以一定的速度经过某个路段时，其仅需完成一次完整的从步骤 1)~步骤 6)的认证过程，而附近的 RSU 对其认证步骤仅需 4 步，且不需进行最为耗时的双线性映射操作，进而提高了认证效率。

如图 8 所示，本文方案与现有通信方案 CPAS 方案[16]、ARGB 方案[18]和 ABAKA 方案[15]的认证时延均随车辆数目的增加呈上升趋势。当 n 辆车中存在 5%和 10%的非法车辆时，本文方案的认证时延均小于其他对比方案。当道路上的非法车辆为 15%时，本文方案的认证时延仍然小于 ARGB 和 ABAKA 方案，并与 CPAS 方案接近。当道路上的非法车辆为 20%时，本文方案仍小于 ARGB 方案的认证时延。进一步发现，当车辆数目为 100 且非法车辆为 5%时，本文方案的认证时延是 CPAS 方案的 76%，是 ABAKA 方案的 56%，是 ARGB 方案的 43%。因此，本文方案前移具有较小的认证时延，且认证效率较高。

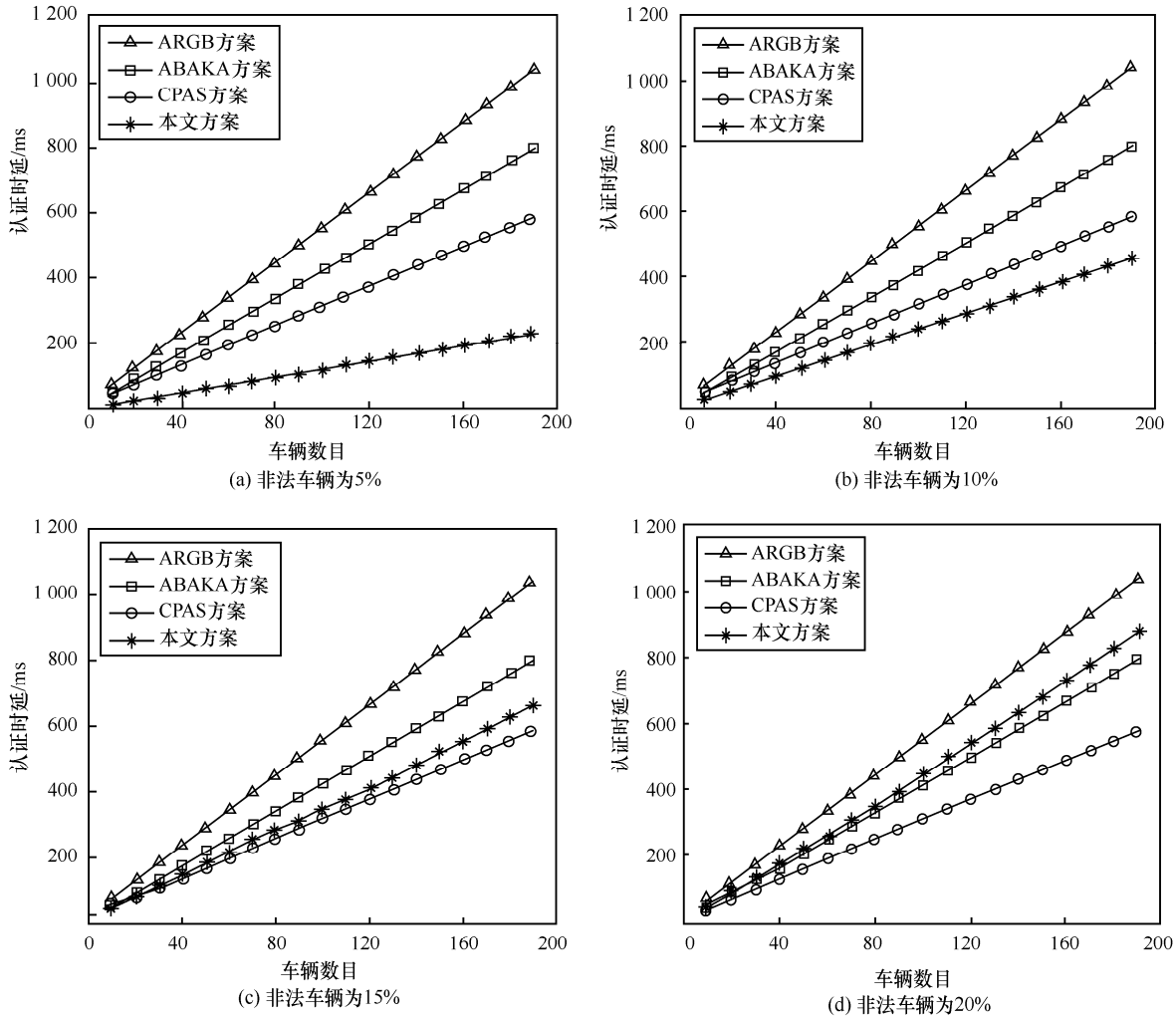


图 8　车辆密度与认证时延

5.2　传输开销

本文方案使用消息的大小表示传输开销。每条消息包括假名、HMAC 和消息主体。其中，假名为 42 B，HMAC 为 16 B，故每条消息（除消息主体外）需额外增加 58 B。本文方案的传输开销与现有方案的传输开销对比结果如表 4 所示。

表 4　传输开销比较（发送信息为 *n*）

方案	OBU → RSU /B
CPAS 方案	208*n*
ABAKA 方案	84*n*
ARGB 方案	63*n*
本文方案	58*n*

图 9 为当车辆数目为 10~190 时，CPAS 方案、ABAKA、ARGB 和本文方案的传输开销对比。从图 9 中可以看出，本文方案的传输开销最小。进一步分析可知，本文方案的通信开销是 CPAS 方案的 27.4%，是 ABAKA 方案的 67.9%，是 ARGB 方案的 88.4%。

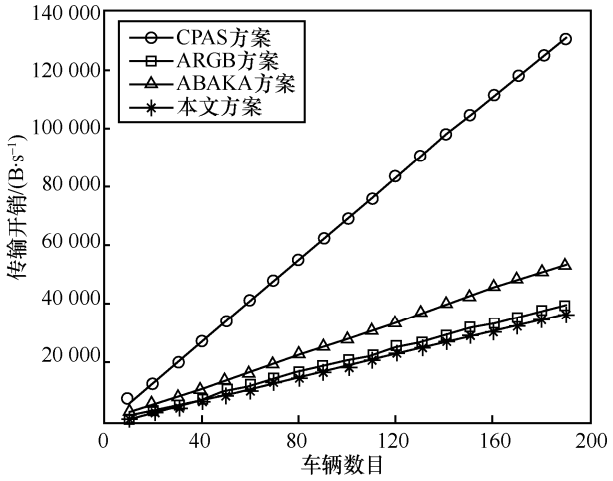


图 9　车辆密度与传输开销

5.3　平均时延

根据文献[17]可知，消息的平均时延的定义如式(7)所示。

$$delay=\frac{1}{N}\sum_{i=1}^{N}\frac{1}{M}\sum_{m=1}^{M}(T_{\text{cream}}^{n\text{-}m}+T_{\text{transmission}}^{n\text{-}m\text{-}k}+T_{\text{verify}}^{n\text{-}m\text{-}k}) \quad (7)$$

其中，车辆的数目为 N，车辆发送的消息数为 m，车辆或 RSU 生成消息所花费的时间为 $T_{\text{cream}}^{n\text{-}m}$，实体 n 向实体 k 发送消息 m 时消息的传输时间为 $T_{\text{transmission}}^{n\text{-}m\text{-}k}$，实体 k 对实体 n 发来的消息 m 进行认证所需的时间为 $T_{\text{verify}}^{n\text{-}m\text{-}k}$。

图 10 所示的是车辆数量对平均时延的影响。其中，本文方案的通信分为车辆与车辆（V-V）的通信和车辆与 RSU（R-V）的通信。从图 10 中可以看出，随着车辆数目的增加，消息的平均时延也随之增加。其中，ABAKA 方案和 ARGB 方案的平均时延较长。当车辆数目为 100 时，ABAKA 方案和 ARGB 方案的平均时延分别为 262 ms、96 ms，而本文方案 R-V 和 V-V 通信平均时延分别为 8.5 ms 和 32 ms，远小于对比方案。

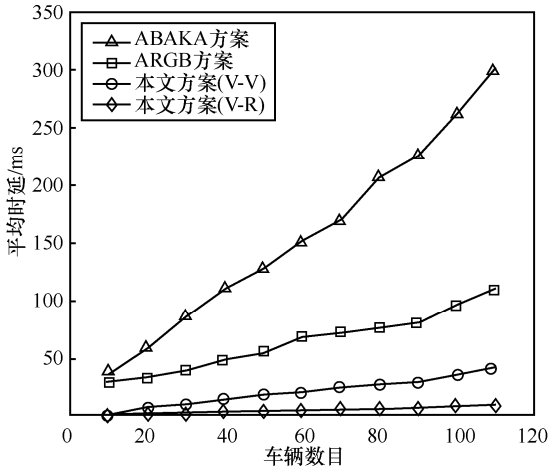


图 10　车辆数量与通信的平均时延

图 11 所示的是当道路上车辆的数目为 60 时，平均时延受车辆的行驶速度的影响。从图 11 中可以看出，平均时延的大小随车辆速度的变化而变化，并且 ABAKA 方案和 ARGB 方案的平均时延受车辆速度的影响较大，而本文方案的平均时延受车辆速度的影响较小。

在本文方案中，非法车辆进行一次完整的协商过程需要 25.338 ms, 其中，身份认证需 24 ms，而密钥协商部分需 1.338 ms，由此可以看出，密钥协商所需的时间远小于身份认证所需的时间。此外，当车辆已经完成过一次完整认证过程之后，对其身份再次认证时仅需进行认证方案的前 4 步，减去了认证过程中计算最为耗时的双线性映射对所需的时间，且群密钥协商中只需进行简单运算，如幂运算、逆运算等。

综上所述，虽然本文方案增加了群密钥协商过程，但其所产生的负荷远小于认证所产生的负荷，因此，本文方案仍然具有较高的效率优势。

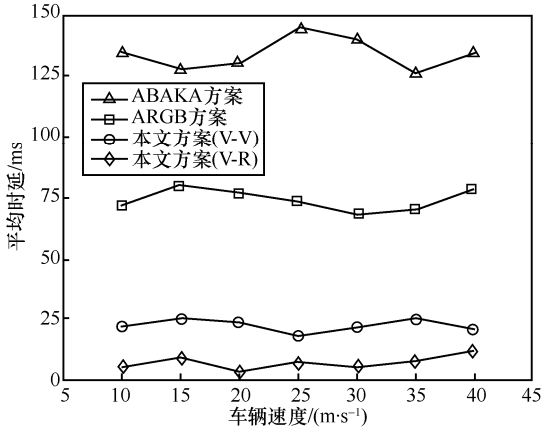


图 11　车辆速度与平均时延

6　结束语

本文提出了一种无认证中心、高效的群组协商通信的方案，该方案具有以下特性。

1) 采用节点自认证的方式，通信过程不需第三方 TA 的参与，从而加快了认证速度。

2) 使用密钥协商产生密钥的方式代替 RSU 分发密钥，解决了通信中存在的单点失败问题。

3) 通过在 RSU 中使用群密钥传递的方式，减少了合法车辆的认证次数。

在将来的工作中，本文将针对在没有路边基础设施（即 RSU）参与的情况下，针对车辆之间自行认证并进行可靠通信的问题展开进一步的研究。

参考文献：

[1] WHAIDUZZAMAN M, SOOKHAK M, GANI A, et al. A survey on vehicular cloud computing[J]. Journal of Network & Computer Applications, 2014, 40(1):325-344.

[2] JIANG S, ZHU X, WANG L. An efficient anonymous batch authentication scheme based on HMAC for VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(8):2193-2204.

[3] BITAM S, MELLOUK A, ZEADALLY S. VANET-cloud: a generic cloud computing model for vehicular ad hoc networks[J]. IEEE Wireless Communications, 2015, 22(1): 96-102.

[4] 宋成, 张明月, 彭维平, 等. 基于双线性对的车联网批量匿名认证方案研究[J]. 通信学报,2017,38(6):49-57.
SONG C, ZHANG M Y, PENG W P, et al. Research on batch anonymous authentication scheme for VANET based on bilinear pairing[J]. Journal on Communications, 2017, 38(6):49-57.

[5] DING Q, LI X, JIANG M, et al. Reputation management in vehicular ad hoc networks[C]//2010 International Conference on Multimedia Technology (ICMT). 2010:1-5.

[6] 李晋国, 林亚平, 李睿, 等. 车载自组织网络中基于椭圆曲线零知识证明的匿名安全认证机制[J]. 通信学报. 2013, 34(5): 52-61.
LI J G, LIN Y P, LI R, et al. Secure anonymous authentication scheme based on elliptic curve and zero-knowledge proof in VANET[J]. Journal on Communications, 2013, 34(5):52-61.

[7] WASEF A, SHEN X. MAAC: message authentication acceleration protocol for vehicular ad hoc networks[C]//Global Telecommunications Conference. 2009: 1-6.

[8] CALANDRIELLO G, PAPADIMITRATOS P, HUBAUX J P, et al. On the performance of secure vehicular communication systems[J]. IEEE Transactions on Dependable & Secure Computing, 2011, 8(6): 898-912.

[9] 吴黎兵, 谢永, 张宇波. 面向车联网高效安全的消息认证方案[J]. 通信学报, 2016, 37(11):1-10.
WU L B, XIE Y, ZHANG Y B. Efficient and secure message authentication scheme for VANET[J]. Journal on Communications, 2016, 37(11): 1-10.

[10] WASEF A, SHEN X. Efficient group signature scheme supporting batch verification for securing vehicular networks[C]//IEEE International Conference on Communications. 2010, 29(16): 1-5.

[11] CHIM T W, YIU S M, HUI L C K, et al. SPECS: secure and privacy enhancing communications schemes for VANETs[J]. Ad Hoc Networks, 2011, 9(2):189-203.

[12] 仲红, 黄丛林, 许艳,等. 高效的可撤销群签名方案[J]. 通信学报, 2016, 37(10):18-24.
ZHONG H, HUANG C L, XU Y, et al. Efficient group signature scheme with revocation[J]. Journal on Communications, 2016, 37(5):18-24.

[13] SUN J, ZHANG C, ZHANG Y, et al. An identity-based security system for user privacy in vehicular ad hoc networks[J]. IEEE Transactions on Parallel & Distributed Systems, 2010, 21(9): 1227-1239.

[14] ZHANG C, LIN X, LU R, et al. An efficient message authentication scheme for vehicular communications[J]. IEEE Transactions on Vehicular Technology, 2008, 57(6):3357-3368.

[15] HUANG J L, YEH L Y, CHIEN H Y. ABAKA: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks[J]. IEEE Transactions on Vehicular Technology, 2011, 60(1):248-262.

[16] SHIM K A. CPAS: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks[J]. IEEE Transactions on Vehicular Technology, 2012, 61(4):1874-1883.

[17] HU C, CHIM T W, YIU S M, et al. Efficient HMAC-based secure communication for VANETs [J]. Computer Networks, 2012, 56(9): 2292-2303.

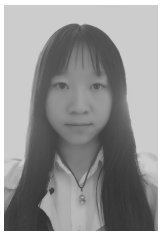
[18] 王良民, 李晓君, 仲红. VANET 中一种可撤销的车辆群组批认证方

法[J]. 中国科学, 2013, 43(10): 1307-1325.
WANG L M, LI X J, ZHONG H. A revocable group batch verification scheme for VANET[J]. Science China, 2013, 43(10): 1307-1325.

[19] WAHAN A A, JUNG L T. Security framework for low latency vanet applications[C]//International Conference on Computer and Information Sciences. 2014:1-6.

[作者简介]

韩牟（1980-），女，吉林省吉林市人，江苏大学副教授、硕士生导师，主要研究方向为密码学、网络安全等。



华蕾（1992-），女，河南南阳人，江苏大学硕士生，主要研究方向为车载网通信安全。

王良民（1977-），男，安徽潜山人，江苏大学教授、博士生导师，主要研究方向为物联网信息处理技术、物联网安全协议、车联网安全结构。

江浩斌（1969-），男，江苏启东人，江苏大学教授、博士生导师，主要研究方向为道路车辆运行安全主动防控技术与理论、智能交通运输技术等。

马世典（1977-），男，安徽萧县人，江苏大学副教授、硕士生导师，主要研究方向为智能网联汽车、交通信息与安全等。