一种基于IBE的车联网安全通信方法

A Secure Communication Method for IOV Based on IBE

施君宇，江俊桦，吴　旭，曹含磊〔中移（苏州）软件技术有限公司，江苏 苏州 215010〕
Shi Junyu，Jiang Junhua，Wu Xu，Cao Hanlei〔China Mobile（Suzhou）Software Technology Co.，Ltd.，Suzhou 215010，China〕

摘　要：
在当今汽车工业和无线通信领域，车联网的通信安全已成为专家学者研究的热点问题。对相关文献进行研究后，基于身份加密机制（IBE）提出了一种可用于车联网安全通信的算法。该算法结合了现有的公钥体系和基于身份的加密（IBE）技术，使车辆能够使用假身份来隐藏其真实来源，从而有效防止信息被篡改或者车辆真实身份被暴露，确保车联网中通信的安全。

关键词：
车联网；通信安全；身份加密机制
doi：10.12045/j.issn.1007-3043.2025.01.010
文章编号：1007-3043（2025）01-0051-04
中图分类号：TN929.5
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
In today's automotive industry and wireless communication field，the communication security of the Internet of Vehicles also becomes a hot topic of research for experts and scholars. After studying relevant literatures，it proposes an algorithm based on Identity-based encryption（IBE）that can be used for secure communication in the Internet of Vehicles. This algorithm combines existing public key systems and identity based encryption（IBE）technology，enabling vehicles to use fake identities to hide their true sources，so as to effectively prevent information tampering or the exposure of the vehicle's true identity，and ensure the security of communication in the Internet of Vehicles.

Keywords：
IOV；Communication security；IBE

引用格式：施君宇，江俊桦，吴旭，等. 一种基于IBE的车联网安全通信方法[J]. 邮电设计技术，2025（1）：51-54.

0 引言

当今时代是一个万物互联的时代，在交通领域，车联网（IOV）则走在了时代前列，甚至被写入了工信部的“十四五”规划中。车联网的内涵和外延也在不断发展演进，这既为人们提供了便捷舒适的服务，也标志着交通网络的一场革命。车联网（IOV）又称车载自组网，其概念源于物联网，即车辆物联网。它以行驶中的车辆为信息感知对象，借助新一代信息通信技术，实现车与X（即车与车、人、路、服务平台）之间的网络连接，提升车辆整体的智能驾驶水平，为用户提供安全、舒适、智能、高效的驾驶体验与交通服务，同时提高交通运行效率，从而提高社会交通服务的智能化水平[1]。车联网中有不同类型的通信参与者，如车辆（V）、路边单元（RSU）、证书颁发机构（CA）等，它们可以实现不同类型的通信，如车辆之间的通信（V2V）、车辆与RSU之间的通信（V2R）等，也可以扩展为V2X，实现车辆和行人、智能物体等之间的通信，其中V2V通信发挥主要作用，通过车辆交换不同类型的信息，如安全信息和非安全信息。然而，这也带来了关于隐私保护、信息安全、通信时延等诸多挑战[2]。

V2V的通信安全需要考虑多方面的因素，既要保

收稿日期：2024-11-18

证信息准确、及时地送达正确的接收方且不被窃听，同时也要保证信源的隐私，还要防范恶意攻击，避免信息被伪造或者篡改。车联网面临各种潜在的攻击方式。攻击者可能采用不同的攻击手段，如针对个人隐私的攻击，侵犯到地理位置和真实身份等隐私；也可能破坏车联网正常的通信，修改传递的信息，以破坏其完整性；还可能通过窃听手段，获取保密的通信内容[3-4]。

1 研究现状

在近十来年的研究中，已经有许多专家学者提出了不同的解决方案来解决V2V通信中的安全问题。这些方案的底层原理大致分为以下3种类型。

a）基于硬件的解决方案。这类方案利用信道化和可证明分布函数在物理层识别攻击，其偏向应对物理层的攻击，而忽略更高层的攻击[5]。

b）基于身份认证的解决方案。不同的解决方案都会利用一个可信权威[6-8]。该权威负责将密钥分发给车辆，其中一些解决方案利用证书，而另一些解决方案可能处理不够及时，可信权威必须充当中间人，这导致了网络中的延迟和瓶颈。此外，还有一些解决方案没有考虑假名的使用，从而忽视了车辆的隐私保障[9]。

c）基于信任机制的解决方案[10-12]。相关文献提出网络中每辆车都与一个信任值相关联，并可能根据车辆行为而变化，还存在可信第三方（TTP）或相互组信任管理，根据其信任值评估和隔离攻击者。然而，这些解决方案的可靠性往往是暂时的，因为攻击者可以前期先采取正常的行为来提高其信任值，而可信第三方后续可能会因此妥协[13]。

本文将采用一种加密通信机制来解决这个问题，该机制利用了现有的公钥体系和基于身份加密（IBE）算法，通过这套方法，车辆完全可以使用假身份来隐藏其真实来源并保证通信安全。

2 系统架构

车联网（IOV）没有定义标准化的体系结构，本文参照主流的IOV架构。如图1所示，它由配备专用短距离通信（DSRC）板的车辆（V）组成，这些DSRC板被固定为干预防护设备（TPD），通常被称为车载单元（OBU）。DSRC是标准Wi-Fi的改进形式，称为802.11p，它使用5.9 GHz频段，整个模块被称为车载网

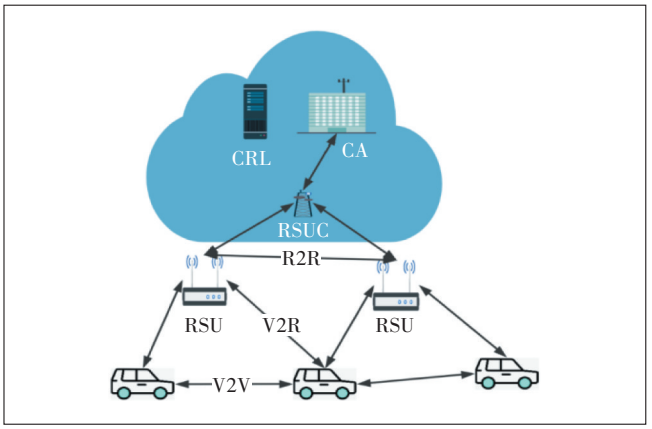

图1　IOV常见架构

络中的无线接入（WAVE）[14-15]。汽车可以移动的地方如停车场、道路等，将在路的两侧部署路边单元（RSU），通常这些RSU都具备了一定的计算能力和无线通信能力。

交通管理局（TA）作为该架构的底层管理方，负责车辆注册。车辆被购买后需在TA进行注册，并在其数据库中创建一个条目，其中包含车辆所有信息、司机信息和其他关键数据。RSU需要部署在一条站点线上，用于本地和全局的切换管理，它们与RSU控制器（RSUC）相互连接；RSUC充当交换站，也可以为TA和CA传输数据。

认证机构（CA）为每一辆在TA注册后的车辆创建一个公钥证书，其中包含公钥信息以及过期时间。该公钥证书同样可以被RSU获悉，同时CA会有一个存证书撤销列表（CRL）的数据库。如果发现有的车辆是攻击者，RSU可以使用该列表发送吊销请求。

3 基于IBE的通信安全保障方法

本文采用了一种混合方法，即每辆车都要处理CA颁发的公钥证书，但在其顶层设计中使用IBE，以避免每次验证证书造成的延迟。

本文的方法主要分为5个阶段。

步骤1：车辆注册并获取密钥对，如图2所示。车辆在其车载单元（OBU）配置完成后不久，生成公钥、私钥对PU、PR，并将其与车辆详细信息一起发送给认证机构（CA），同时将其公钥证书的唯一标识符也发送给CA。CA验证详细信息后，将其存储到数据库中，并向车辆颁发其公钥证书。这一步骤在车辆的生命周期中只进行一次，除非硬件发生更改或证书过期。

步骤2：RSU发挥密钥中心的作用。RSU每隔一

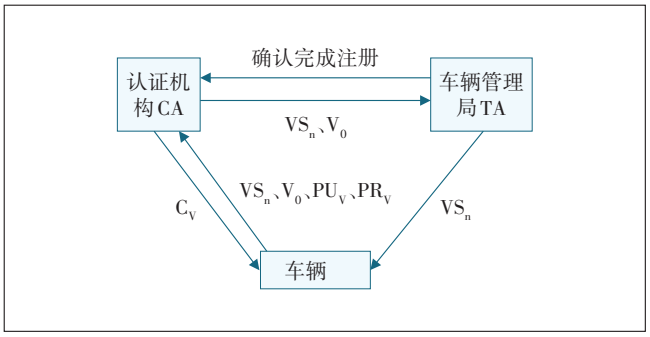

图2　车辆注册示意

段时间重新生成主密钥MS_R，同时每次车辆从一个RSU移动到另一个RSU时，每个RSU都会进行相应配置（见图3）。

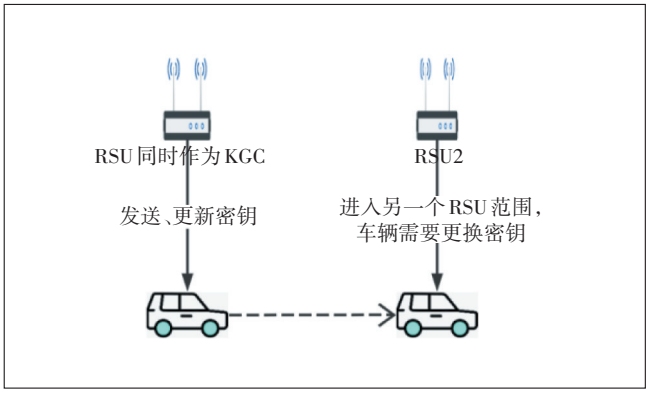

图3　密钥生成、交换示意

作为密钥生成中心（KGC），RSU选择一个主密钥MS_R，并负责确认全局参数：四元组(p, G_1, G_T, e)，其中，p是一个质数，G_1为由p生成的循环加法群，G_T为具有相同p阶的乘法组，g是G的原根，e为满足$G_1 \times G_1 \rightarrow G_T$的双线性映射。

这里的全局参数同样可以表达为(P, Q, H_1, H_2)，其中，H_1是将车辆信息的字符串映射为G的哈希函数，$H_1 = [0,1]^l \rightarrow G$；$H_2$是将$G_T$中元素映射成回字符串的哈希函数，$H_2 = G_T \rightarrow [0,1]^l$。

令$MS_R = a, Q = g^a$

步骤3：车辆通过假名保护隐私信息。在RSU注册的车辆持有公钥，但当车辆需要联网建立通信通道时，它不会直接公布其公钥，而是通过向RSU展示公钥证书获得保护性“假名”。这些假名可以随意更改，遵循一定的命名模式或完全随机，以使车辆匿名。

a）当车辆V_1进入新的RSU区域时，它会发送其公钥证书给RSU。RSU验证证书及其有效期，并产生一组假名（P_{id1}、P_{id2}、P_{id3}，……P_{idn}）供V_1通信。

b）V_1车辆主动变更假名。V_1发送其P_{id}给RSU，RSU通过计算$SK_{id} = \left(H_1(P_{id})\right)^a$，生成密钥$SK_{id}$。

步骤4：加密通信。在某些情况下，一些消息需要加密传输，以保证其安全性和完整性。具体将采用如下过程加密。

汽车V_1和V_2准备通信。如果车辆V_2想要发送机密信息M_2给V_1（M_2是一个二进制字符串）。且V_2拥有从RSU获取的全局信息(p, G_1, G_T, e)，同时已知V_1的假名，那么V_2通过以下算法生成加密文本CT_2：

$$C_1 = g^r$$

$$C_2 = M_2 \oplus H_2(e(H_1(P_{id}), Q)^r)$$

$$CT_2 = [C_1 \| C_2]$$

其中r是每次发起通信时随机产生的随机数（确保攻击者不会通过破解历史密钥获取规律从而得到后续密钥）。

然后V_2发送密文CT_2给V_1。

步骤5：V_1车解密。V_1接收到CT_2后，使用其密钥SK_{id}解密消息（可以明确知道的元素是C_1、C_2、SK_{id}），通过以下算式就可解密出M_2。

$$M_2 = C_2 \oplus H_2(e(SK_{id}, C_1))$$

具体的解密过程如下（利用抽象双线性配对的双线性）：

$$\text{解密信息} = C_2 \oplus H_2(e(SK_{id}, C_1))$$

将$C_2 = M_2 \oplus H_2(e(H_1(P_{id}) \cdot Q)^r)$代入得到

$$\text{解密信息} = M_2 \oplus H_2(e(H_1(P_{id}), Q)^r) \oplus H_2(e(SK_{id}, C_1))$$

再将$C_1 = g^r$，$SK_{id} = (H_1(P_{id}))^a$代入得到

$$\text{解密信息} =$$

$$M_2 \oplus H_2(e(H_1(P_{id}), Q)^r) \oplus H_2(e((H_1(P_{id}))^a, g^r)) =$$

$$M_2 \oplus H_2(e(H_1(P_{id}), g^a)^r) \oplus H_2(e((H_1(P_{id}))^a, g^r)) =$$

$$M_2 \oplus H_2(e(H_1(P_{id}), g))^{ar} \oplus H_2(e(H_1(P_{id}), g))^{ar} = M_2$$

可见V_1可以得到准确的M_2消息。

4　安全性论证

为了证明本方法的安全性，我们在系统中模拟了一个危险的攻击者（V_A）。V_A拥有所有车辆应有的计算能力和通信技术，它甚至会伪装成正常车辆行驶，但它的目标是妨碍交通、篡改信息、跟踪车辆、窃取真实身份。

a）尝试攻破保密性：当车辆V_2想要发送消息M给V_1时，它会对消息进行加密并发送$CT_2 = [C_1 \| C_2]$给V_1，

如果V_A试图解密信息，则它至少需要从C_1中获悉随机数r的具体值，这相当于从已知的P_{id}计算出SK_{id}，这是一个解离散对数难题，其难度已有数学证明，并广泛应用于密码学。因此，本系统保障了消息的保密性。

b）尝试攻破完整性。车辆V_2发送密文$CT_2 = [C_1 \| C_2]$。假设在到达V_1之前，V_A就捕获了消息，并尝试通过准备好的M来修改消息C_2，并准备$C_2\hat{} = M_2 \oplus H_2(e(H_1(P_{id}), Q)^r)$，通过一个随机的$r\hat{}$和预先计算$C_1\hat{} = gr\hat{}$并发送给$V_1$，那么$V_1$得到了篡改后的消息：

$$M_2\hat{} = C_2\hat{} \oplus H_2(e(SK_{id}, C_1\hat{}))$$

这样，车辆V_1无法通过C_1还原出有效信息。因此，V_A即使篡改信息但还是无法欺骗V_1。该方案最终保证了信息的完整性。

c）匿名攻击。在IOV中，所有的车辆应该保持匿名性，因为对手可能会跟踪车辆并了解其驾驶模式、行为模式，甚至可能对司机实施一些危险行为，如绑架、跟踪、诈骗等。而对于V_A来说，要获得车辆V_{id}的真实身份，它必须获得C_1并知道P_{id}的证书，而只有RSU拥有这些数据。RSU本身就是一个防篡改设备，这对V_A来说获得这些数据是不可能的。

同时，车辆进入新的RSU管理范围就会获得新的假名，这意味着假名每次都在变化。因此，从假名还原车辆真实身份信息，在数学原理和现有技术条件下，几乎是不可能实现的。

5 总结

本文提出的方法可以有效保证车联网中通信的安全性，防止信息被篡改或者车辆真实身份被暴露。在未来的车联网通信系统中，该方法拥有较好的使用前景。后续也将继续研究优化相关算法，探索更低的计算复杂度和通信开销等[16-17]。

参考文献：

[1] 井骁. 浅析车联网技术与应用[J]. 上海汽车，2019(4)：9-12.
[2] 黄语骁. 车联网网络安全技术研究[J]. 电子世界，2018(19)：49-50.
[3] DI，HAN，BO，et al. Secure V2V Communications via Relays：Resource Allocation and Performance Analysis[J]. IEEE Wireless Communications Letters，2017，6(3)：342-345.
[4] 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.
[5] NARAYANA V L，BHARATHI C R. Identity based cryptography for mobile ad hoc networks[J/OL]. [2024-04-09]. https://www.researchgate.net/publication/316681172_Identity_based_cryptography_for_mobile_ad_hoc_networks.
[6] LEE C C，LAI Y M. Toward a secure batch verification with group testing for VANET[J]. Wireless networks，2013(6)：19.
[7] TANGADE S，MANVI S S. Scalable and privacy-preserving authentication protocol for secure vehicular communications[C]//2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). IEEE，2016.
[8] CUI H，DENG R H，WANG G. An Attribute-Based Framework for Secure Communications in Vehicular Ad Hoc Networks[C]//Ad Hoc Networks. IEEE，2019.
[9] AZEES M，VIJAYAKUMAR P，DEBORAH L J. Comprehensive survey on security services in vehicular ad-hoc networks[J]. IET Intelligent Transport Systems，2016，10(6)：379-388.
[10] BONEH D，FRANKLIN M. Identity-Based Encryption from the Weil Pairing[C]//Annual International Cryptology Conference. Springer，Berlin，Heidelberg，2001.
[11] NARAYANA V，BHARATHI C. Effective multi-mode routing mechanism with master-slave technique and reduction of packet droppings using 2-ACK scheme in MANETS[J].Modelling，Measurement and Control A，2018，91 (2)：73-76. DOI：10.18280/mmc_a.910207.
[12] L N V，A PEDA GOPI，N. ASHOK KUMAR. Different techniques for hiding the text information using text steganography techniques：A survey[J].Ingénierie des Systèmesd'Information，2018，23(6)：115-125.
[13] GOPI A P，NARAYANA V L，KUMAR N A. Dynamic load balancing for client server assignment in distributed system using genetical gorithm[J/OL].[2024-04-09]. https://www.researchgate.net/publication/330690960_Dynamic_load_balancing_for_client_server_assignment_in_distributed_system_using_genetical_gorithm.
[14] ALAM K M，SAINI M，SADDIK A E. Toward Social Internet of Vehicles：Concept，Architecture，and Applications[J]. IEEE Access，2015，3：343-357.
[15] 楼吉汉，张伟，詹源，等. 一种基于Wi-Fi的DSRC技术[C]//2014第9届中国智能交通年会大会论文集. 中国智能交通协会，2014.
[16] 徐元杰，吴建华，龚一轩. 简析车联网网络安全[C]//第39次全国计算机安全学术交流会论文集.2024.
[17] 王怡暄. 基于区块链的车联网隐私保护认证方案研究[D]. 兰州：兰州理工大学，2023.

作者简介：
施君宇，工程师，硕士，主要从事云计算技术服务相关工作；江俊桦，工程师，硕士，主要从事云计算技术服务相关工作；吴旭，学士，主要从事云存储、网络安全相关工作；曹含磊，学士，主要从事云安全、网络安全相关工作。