•可信计算与信息安全•

DOI:10.15961/j.jsuese.201700619

车联网中基于群签名的身份认证协议研究

郑明辉,段洋洋,吕含笑

(湖北民族学院 信息工程学院,湖北 恩施 445000)

摘　要:针对车联网中的车辆单元的隐私信息泄露而被非法分子跟踪攻击的问题,通过分析车联网的拓扑结构及其通信特征,提出了一个基于轻量级群签名的车辆身份认证协议,以对车辆身份进行快速且高效的匿名认证。协议的内容共分为5个阶段:在初始化阶段,由车联网系统产生群的公/私钥对和系统参数,并利用路旁辅助设施将群公钥和系统参数分发给车载单元,群私钥由群管理者保管;在车辆单元入网阶段,车辆单元将自己的身份信息通过盲签名技术提交给群管理者,认证通过后由群管理者为车辆单元颁发群证书;在协同通信阶段,拥有群证书的车辆成员利用它的有效证书和群公钥对其状态信息进行签名,并利用车载传感器发送给附近的车辆单元,实现与周边车辆的协同驾驶;在消息验证阶段,只有合法的车辆成员才能利用群公钥打开它所接收到的状态信息,但无法得知该消息发送者的真实身份,以此实现车辆间的匿名通信;在签名验证阶段,当某个车辆成员为了独享道路资源发布虚假消息导致交通事故时,群管理者利用其预留的群私钥将该消息的签名打开,即可遍历出对应的车辆成员进行问责。作者采用改进后的轻量级群签名技术,能够做到群公钥和群签名的长度不依赖群成员的个数;以零知识证明作为成员身份验证的手段,可以提高群中成员之间的认证速度。先对协议的安全性从数学的角度作了分析和证明,再搭建了由100台PC机组成的局域网仿真平台模拟车联网中的车辆单元之间的协同通信。实验结果表明本协议在100个车辆用户的局域网中完成身份认证的时间约为7 ms,且在认证时间开销上优于所对比的方案,较大程度地降低了车载单元在身份认证过程中的存储和计算负担。

关键词:车联网;隐私保护;群签名;身份认证

中图分类号:TN918.1;TN918.91　　**文献标志码**:A　　**文章编号**:2096-3246(2018)04-0130-05

Research on Identity Authentication Protocol Group Signature-based in Internet of Vehicles

ZHENG Minghui, *DUAN Yangyang*, *LYU Hanxiao*

(School of Info. Eng., Hubei Univ. For Nationalities., Enshi 445000, China)

Abstract: In order to solve the problem of illegal member's tracking attack, which caused by the vehicle units' privacy disclosure in vehicular ad hoc networks (VANETs), a vehicle identity authentication protocol based on lightweight group signature was proposed by analysis of topology and communication characteristics of VANETs in this paper, which can authenticate the vehicles anonymously in a fast and efficient way. The protocol has five stages. In the initialization phase, the public/private key pairs and system parameters of the group were generated by the VANETs system, then the group public key and system parameters were distributed to the on-board units by the roadside auxiliary facilities. The group private key was kept by the group manager. When a vehicle unit entered VANETs, the unit's own identity was submitted to the group manager by the blind signature. A group certificate would be distributed to the vehicle unit by the group manager when authentication passed. In the cooperative communication stage, the vehicle member who owned the group certificates signed the state information with the valid certificate and group public key, then sent it to the nearby vehicle units by the car sensors, and achieved cooperative driving with surrounding vehicles. In the message verification stage, only can the legal vehicle members open the received status information by using group public key, but couldn't know the true identity of the message sender. In this way, the anonymous communication among vehicles was realized. In the stage of signature verification, when a vehicle unit broadcasted a false message for the purpose of exclusively using road resource and caused traffic accident,

收稿日期:2017 – 08 – 04

基金项目:国家自然科学基金资助项目(61472121);湖北省创新群体项目资助(2016CFA021)

作者简介:郑明辉(1972—),男,教授,博士. 研究方向:信息安全. E-mail: mhzheng3@163.com

网络出版时间:2018 – 07 – 11 14 : 58 : 00　　**网络出版地址**: http://kns.cnki.net/kcms/detail/51.1773.TB.20180711.1458.008.html

the group manager can open the signature of the message by using the group private key, and traversed the corresponding vehicle members to carry on the accountability. The innovation of the paper was the usage of improved lightweight group signature technology, which could ensure that the length of group public key and group signature didn't depend on the number of group members. Zero knowledge proof was also used as a means of membership authentication which improved the speed of authentication among the members. The security of the protocol was analyzed and proved mathematically in this paper, and a LAN simulation platform composed of 100 PC machines was built to simulate the cooperative communication among vehicle units in VANETs. The experimental results showed that authentication time of the protocol was about 7 ms among 100 vehicle users. The performance of the proposed protocol is superior to the contrasted schemes. It greatly reduced the storage and calculation burden of the vehicle units during the process of identity authentication.

Key words: VANETs; privacy protection; group signature; identity authentication

车联网(vehicular ad hoc networks)是由车辆子网、网络运营商和服务基础设施3部分构成[1],用于实现车辆之间的协同通信并保护车主的位置隐私。在提高用户驾乘体验的同时,也会导致车辆用户的的位置隐私信息泄露的问题。

Samarati等[2]利用k–匿名打乱车辆身份信息保护车主的位置隐私信息。该方案在理想的欧式空间且车辆数足够多的场景中优势明显,但在实际中并不适用,也不能抵抗敌手基于概率统计的攻击; Beresford[3–4]首次提出了mix-zones的概念,为用户定义一个可以变更假名的混合区域,用于车辆的位置隐私保护。Butty等[5]首次将mix-zones方案应用到车联网的位置隐私保护中,将特定区域部署成为mix-zones,车辆在该区域内变更假名后以另一个身份退出该mix-zones空间,此时,敌手很难将车辆的前后两个假名关联起来跟踪车辆,从而达到了车辆之间的匿名通信与协同驾驶的目的; Palanisamy[6]指出了基于位置的mix-zones方案在实际应用中并不可行,并进一步论证了该方案模型易于受敌手基于长期观察的概率统计及已有知识的时序攻击和转移攻击。Raya等[7]最早提出了适用于车联网的别名验证机制,车辆以一定的周期更换别名后签发报文,接收方对收到报文的匿名证书进行验证以判定该报文的合法性,实现车辆间的匿名性通信与身份认证。基于数字签名的假名变更方案虽然能够提供良好的可验证性和防抵赖性,但是,要对车联网通信中的每一条消息都进行数字签名和认证无疑会增加受限车载单元的通信开销和存储负担,因此,该方案对于即时通信要求极高的车联网而言并不适用。为了减轻车载单元的计算和存储负担, Freudiger等[8]提出了"只有在不可被监控的区域中变更假名才有效"的假名变更方案,即加密的mix-zones,该方案能够防止非法成员对于车联网内部细节的窥探,有效地抵抗了来自mix-zones空间外部非法敌手的攻击,但不能抵抗来自车联网中内部合法成员的恶意攻击,同时,空间密钥的分发和更新机动性能较差。

较之欧美国家,中国对于车联网的研究起步稍晚,2009年,在全国GPS运营商大会上提出了车联网概念。梅颖[9]针对车联网中存在的隐私问题提出了一个隐私保护访问控制方案,车辆用户先在认证机构处注册一个不包含其任何身份信息的令牌,待车辆进入到特定区域时向认证机构出示其令牌,相互认证通过后才能建立会话,但是当要求建立会话通信的车辆单元过多时,该方案的通信性能较低。杨威等[10]从当前受限设备的存储空间和计算能力出发,对轻量级密码的依据原理和实现机制进行了综述,但是并没有针对适用于车辆单元的认证技术展开论述。Zhao等[11]方案采用盲认证的技术保护车辆位置隐私信息,随着车辆数的增加,车辆成员与路旁辅助设施之间的身份认证时间消耗会迅速增加,因此,无法适用于车辆拥堵的车联网。Camenish等[12]运用知识签名,并以离散对数和RSA算法作为群体身份认证的理论基础,对传统的群签名方案做了优化,优化后的方案首次实现了群公钥不变且能够自由地增加新成员;该方案的签名长度,签名算法,验证算法以及打开算法的计算量与群成员的数量不相关,大大降低了签名的时空开销。对于受限设备的车载单元而言,无论是在存储负荷上,还是计算开销上都达到了轻量级通信的水平。

综上所述,数字签名是实现身份认证的方便且可靠的方案,但其签名长度和计算复杂性是制约它在车联网中大规模应用的主要瓶颈。因此,作者通过对车联网的拓扑结构和通信特征的分析,结合轻量级群签名的优点提出一种高效的身份认证协议。通过设计协议内容,并搭建仿真平台进行验证,可以证明本协议能够实现车辆间轻量级的快速匿名通信。

1　基于群签名的身份认证协议设计

1.1　协议内容介绍

本协议的内容可描述为:在系统初始化阶段,车联网建立车辆群资源G(group),生成群公/私钥对并借助路旁辅助单元将群公钥广播给群中车辆GN(group

number)；车辆V_i(vehicle)在进入mix-zone时发起加入群请求，群管理者GM(group manager)验证其身份合法后颁发群证书GC(group certification)，待双方相互认证完成后车辆成为合法群成员；此时，车辆就可以代表整个群对自己的身份和位置信息进行签名GS(group signature)并广播给周围的车辆；在进行协同通信时，车辆只需证明自己是车联网中合法的群成员即可；在身份验证阶段，邻近车辆只需对接收的消息信源进行签名验证，即可判断接收消息的合法性并及时调整自己的驾驶状态；在产生纠纷时，群管理者利用群私钥将有争议的签名打开以确认签名者的身份。协议的流程如图1所示。

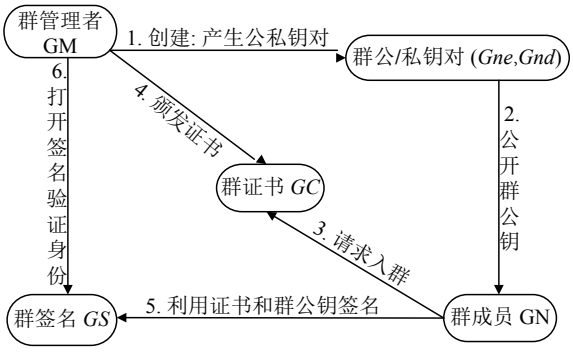

图 1 协议流程图

Fig. 1 Protocol flowchart

1.2 协议实现步骤

协议详细步骤如下：

1)系统初始化

由车联网管理者GM建立车辆群资源G，即一个mix-zones覆盖区域，并由RSA算法计算产生相应的群公钥(Gne)和群私钥(Gnd)以及表示群成员私钥长度的系统安全性参数α、λ、ε；然后，通过路旁单元将公开参数$(n,e,\mathrm{G},g,\alpha,\lambda,\varepsilon)$公布给车联网中的车辆$V_i$，由GM保存群私钥对($Gnd$)，留待以后打开或追踪车辆身份的签名时用。

2)车辆进入车联网

设有车辆V_i进入车联网，需要选取自己的私钥x，做如下计算：

$$y=\alpha^x(\bmod n) \tag{1}$$

$$z=g^y \tag{2}$$

将y和z及对z的签名发送给GM以证明其拥有满足知识签名$y=\alpha^x(\bmod n)$的密钥x；接着，GM验证V_i发送过来的y和z的合法性以确认其知道x，并保存V_i的参数对(y,z)用于将来打开群签名；此时，GM给车辆V_i颁发成员证书$GC=(y+1)^{Gne}(\bmod n)$，同样地，车辆V_i对证书GC的合法性进行验证后即可进入车联网，并享受由车联网提供的服务。

3)车辆签名进行协同通信

这是车联网中车辆之间实现协同驾驶并保证其位置隐私的关键。即进入到车联网中的车辆V_i就可以向邻近车辆证明自己是合法成员，并对其状态信息，如当前位置、行驶方向、当前车速和加速度等信息进行签名后，包装成数据包向周边车辆广播发送：

$$\tilde{g}=\tilde{g}^{\gamma},\gamma\in Z_n^* \tag{3}$$

$$\tilde{z}=\tilde{g}^{y}(\bmod n) \tag{4}$$

$$\lambda_1=\mathrm{SKLOGLOG}[\beta:\tilde{z}=\tilde{g}^{\alpha^{\beta}}](m) \tag{5}$$

$$\lambda_2=\mathrm{SKROOTLOG}[\beta:\tilde{z}\tilde{g}=\tilde{g}^{\beta^{e}}](m) \tag{6}$$

式中，λ_1和λ_2是车辆单元基于双离散对数(SKLOGLOG)和离散对数e次方根的知识签名(SKROOTLOG)。最终签名消息为$(\tilde{g},\tilde{z},\lambda_1,\lambda_2)$。

4)验证接收信息的信源合法性

验证签名时，只需要通过知识签名验证消息来源是否合法。

5)责任纠纷处理

当有车辆为了独享基于位置的服务或者占有道路资源而发送欺骗信息导致交通事故，交通警察机构要追究肇事者责任时，只需要打开群签名，通过步骤3)进行身份验证。所以，群管理员只需遍历所有的群成员，找到使签名公式成立的成员参数就可以知道是哪个群成员做的群签名。

1.3 协议性能评估

1)安全性证明

对于本协议的安全性分析，其实质是考量基于知识签名的签名者利用数学知识和公共信息在非交互和不泄露某个秘钥的前提下向别人证明该成员知道秘钥。故对于本协议在匿名通信的安全性证明可以转换为对基于双离散对数的知识签名算法的安全性证明。

基于双离散对数的知识签名可表示为$\mathrm{SKLOGLOG}[\beta:y=g^{\alpha^{\beta}}](m)$，它是针对$y=g^{\alpha^x}(\bmod n)$提出来的。其中，$y$为公钥，$g$、$\alpha$、$n$为公开的系统参数，$m$为消息。用户只要能够给出知识签名$(c,s_1,s_2,\cdots,s_k)$满足下列等式，就表示其知道私钥$x$。

$$c=\mathrm{H}(m\|y\|g\|\alpha\|p_1\|p_2\|\cdots\|p_k) \tag{7}$$

式中：H为Hash函数；

$$p_i=\begin{cases}g^{\alpha^{s_i}}(\bmod n), & c_i=0;\\ y^{\alpha^{s_i}}(\bmod n), & c_i=1\end{cases} \tag{8}$$

其中，$i=1,2,\cdots,k$。操作过程如下：

①随机选择k个正整数$r_1,r_2,\cdots,r_k$。

②根据式(7)计算c，其中，$p_i=g^{\alpha^{r_i}}(\bmod n)$。

③计算s_i：

$$s_i = r_i - c_i \times x \tag{9}$$

式中，c_i为c转化成二进制数后的第i位上的数字。

④得到用户对密钥x的知识签名为$(c, s_1, s_2, \cdots, s_k)$。

不难发现，若用户拥有私钥x，则可以通过以上操作步骤计算得出知识签名$(c, s_1, s_2, \cdots, s_k)$；若用户不知道私钥$x$，则在计算上不太可能找到满足上述条件的$(c, s_1, s_2, \cdots, s_k)$，至少在计算上是困难的。从而证明了非法用户是不可能伪造一个满足上述条件的身份，从而保障了用户间的匿名通信是安全的。于是本协议的安全性得以证明。

2）协议正确性分析

在发生争议需要确认车主身份并追究相关责任时，只需要借助RSA签名算法将引发争议的签名打开即可。具体做法如下：

①利用由群管理者GM预留的群私钥(Gnd)对产生争议的签名$(\tilde{g}, \tilde{z}, \lambda_1, \lambda_2)$进行解密：$(\tilde{g}, \tilde{z}, \lambda_1, \lambda_2)^{Gnd} \equiv m' (\mathrm{mod}\, n)$，得到明文$m'$；

②提取出m'中车辆身份信息，由群管理者GM遍历车辆在加入群时所预留的身份信息作比对，找出相应签名的责任人。

2　实验仿真与结果分析

在由100台PC机搭建的局域网仿真平台上，选用512位的群密钥，模拟车联网中的车辆之间的协同通信的场景。

在搭建好的仿真环境中，对本文所提协议进行测试，得到车辆单元在完成身份认证时所消耗的时间与车辆数的关系，如图2所示。

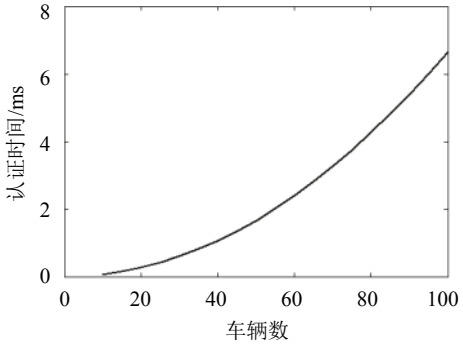

图 2　车辆认证所需时间与车辆数的关系

Fig. 2　Relation between the time required for vehicle identification and the number of vehicles

由图2可以看出，本文所提协议在完成100个车辆单元的身份认证时间约为7 ms。尽管认证时间的消耗随着车辆数量规模的增大而增大，但整体变化幅度不大。这是因为本方案所采用的短群签名技术具有如下特点：在不改变群公钥的前提下能够自由地增加群成员，而且签名长度及其验证打开算法的计算量也与群成员数不相关，从而可以大幅度地降低成员在进行身份认证的时空开销。

采用本方案与Zhao等[11]方案和Yoon等[13]方案对车辆完成认证的时间开销进行比较，结果如图3所示。

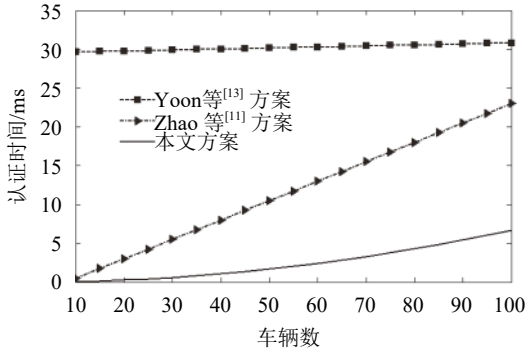

图 3　本方案与其他两种方案的时耗比较

Fig. 3　Comparison of the scheme and other's scheme in certification time consumption

由图3可知，在100个车辆数范围内，本方案的认证时间消耗最少，能够满足车联网对实时性通信的需求。Zhao等[11]方案中使用的是可撤销群签名技术，其认证消耗的时间与群的规模大小密切相关，故其认证所消耗的时间会随着车辆数的增大而急剧上升，从而降低了车辆间的认证效率。因此，该方案只有在群成员数极少的情况下才可以表现出成员身份认证速度极快的优越性，但这在车联网的具体实施中并不适用。Yoon等[13]方案采用基于ID签名的批量验证技术，车辆单元数越多，该方案的优势越明显，但在100个车辆数范围内，表现欠佳。

3　结　论

作者从车联网的结构特征以及车辆之间对通信时效性的需求切入，采用轻量级的群签名技术解决了车联网中对即时通信要求极高和车辆身份快速高效认证的问题。对协议的安全性和正确性作了数学上的理论分析，证明本协议能够保护车载单元的位置隐私；通过设计实验方案进行仿真，表明本方案可以满足车联网通信时效性的要求；同时，在身份认证速度指标上本方案优于Zhao和Yoon等方案。本方案的不足之处为：1）普通的PC机上进行的静态仿真，而现实中的车联网是一个拓扑结构随时都在变化的场景而且车载单元的计算能力也较为薄弱，故实际应用中的表现要比实验结果差；2）由于实验环境的条件限制，只在100个PC机的局域网中进行测试。以上局限性有待下一步研究改善。

参考文献:

[1] Zhang Jianming,Zhao Yujuan,Jiang Haobin,et al.Research on protection technology for location privacy in VANET[J]. Journal on Communications,2012,33(8):180–189.[张建明,赵玉娟,江浩斌,等.车辆自组网的位置隐私保护技术研究[J].通信学报,2012,33(8):180–189.]

[2] Samarati P,Sweeney L.Generalizing data to provide anonymity when disclosing information(abstract)[C]//Proceedings of the Seventeenth ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems.New York: ACM,1998:188.

[3] Beresford A R,Stajano F.Location privacy in pervasive computing[J].IEEE Pervasive Computing,2003,2(1):46–55.

[4] Beresford A R,Stajano F.Mix zones:User privacy in location-aware services[C]//Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops.Orlando,Florida:IEEE,2004:127.

[5] Buttyán L,Holczer T,Vajda N.On the effectiveness of changing pseudonyms to provide location privacy in VANETS[M]// Security and Privacy in Ad-Hoc and Sensor Networks. Heidelberg:Springer-Verlag,2007:129–141.

[6] Palanisamy B,Liu L.MobiMix:Protecting location privacy with mix-zones over road networks[C]//Proceedings of the 2011 IEEE 27th International Conference on Data Engineering.Hannover:IEEE,2011:494–505.

[7] Raya M,Hubaux J P.Securing vehicular ad hoc networks[J]. Journal of Computer Security(Special Issue on Security of Ad-hoc and Sensor Networks),2007,15(1):39–68.

[8] Freudiger J,Raya M,Félegyházi M,et al.Mix-zones for location privacy in vehicular networks[C]//Proceedings of the 2007 ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS).Vancouver: ACM,2007:1–7.

[9] Mei Ying.Research on the privacy preservation for VANETS[D].Wuhan:University of Science and Technology,2014.[梅颖.车联网隐私保护研究[D].武汉:华中科技大学,2014.]

[10] Yang Wei,Wan Wunan,Chen Yun,et al.Review on lightweight cryptography suitable for constrained devices[J]. Journal of Computer Applications,2014,34(7):1871–1877.[杨威,万武南,陈运,等.适用于受限设备的轻量级密码综述[J].计算机应用,2014,34(7):1871–1877.]

[11] Zhao Zhen,Chen Jie,Zhang Yueyu,et al.An efficient revocable group signature scheme in vehicular ad hoc networks[J]. KSII Transactions on Internet & Information Systems,2015, 9(10):4250–4267.

[12] Camenisch J,Stadler M.Efficient group signature schemes for large groups (extended abstract)[M]//Advances in Cryptology—CRYPTO'97.Heidelberg:Springer-Verlag,1997:410–424.

[13] Yoon H J,Cheon J H,Kim Y.Batch verifications with ID-based signatures[M]//Information Security and Cryptology—ICISC 2004.Heidelberg:Springer-Verlag,2004: 233–248.

（编辑　赵　婧）

引用格式: Zheng Minghui,Duan Yangyang,Lyu Hanxiao.Research on identity authentication protocol group signature-based in internet of vehicles[J].Advanced Engineering Sciences,2018,50(4):130–134.[郑明辉,段洋洋,吕含笑.车联网中基于群签名的身份认证协议研究[J].工程科学与技术,2018,50(4):130–134.]