DOI：10.7652/xjtuxb201302010

采用群组密钥管理的分布式车联网信息认证方案

刘辉，李晖
（西安电子科技大学计算机网络与信息安全教育部重点实验室，710071，西安）

摘要：鉴于车联网在提高驾驶安全性和道路通行效率方面起到的重要作用，针对车联网中的信息安全和隐私保护问题，提出了一个基于群组密钥管理的分布式信息认证方案。该方案使用高效的笔名签名来保护隐私；车辆使用基于无证书签密技术来获取密钥；密钥管理分区进行，减轻了密钥管理中心的负担；证书吊销列表实行属地化管理，解决了违规车辆的召回问题；采用批量验证技术降低了车辆的计算开销，使得信息认证的效率提高30 %以上。安全性分析和仿真实验结果表明，该方案和现有车联网认证方案相比具有较高的安全性、可行性和鲁棒性。

关键词：车载通信；群签名；签密
中图分类号：TN918 **文献标志码**：A **文章编号**：0253-987X(2013)02-0058-05

A Distributed Authentication Protocol for VANET

LIU Hui, LI Hui
(Key Laboratory of Computer Networks and Information Security, Ministry of Education, Xidian University, Xi'an 710071, China)

Abstract: Vehicular ad hoc networks (VANET) are vital to enhance safety and efficiency in transportation systems. A distributed and group-based message authentication scheme is proposed to resolve information security and privacy-preserving problem in VANET, Efficient pseudonym signature is employed in the scheme to preserve privacy; and the certificateless signature technology is used to help vehicles to secretly receive a secret key. Management for secret keys is based on groups to reduce the burden of key distribution centre (KDC). The certificate revocation list (CRL) is locally managed to solve the problem of vehicle recall. Moreover, batch technique is employed to accelerate the verification, and the efficiency is improved over 30%. Extensive simulations are conducted to confirm the efficiency of the scheme in various application scenarios. The results show that the scheme is more secure, feasible and robust than other existing schemes.

Keywords: vehicular communication; group signature; signcryption

随着移动网络和信息处理技术的快速发展，车载通信网作为一种新型的移动自组网，将成为智能交通领域发展的一座里程碑，它可以大大减少道路交通安全事故的发生，提高道路通行效率，还可以接入因特网提供天气预报、加油站、旅馆等信息服务。这种以短距离无线通信(DSRC)标准、车辆环境无线接入(WAVE)标准和802.11p为基础的网络，由车载通信单元(OBU)和路边基础设施(RSU)组成，RSU部署在道路两侧或十字路口，OBU安装在每一辆车上，车辆可以周期性地广播安全信息，例如交通事故、路况信息、紧急刹车和转向等，进行车间通信(V2V)和对RSU通信(V2R)。车载网的部署和实施有着巨大的

收稿日期：2012-06-02。 作者简介：刘辉(1979—)，男，讲师；李晖(通信作者)，男，教授，博士生导师。 基金项目：国家自然科学基金资助项目(61103143，61003300)；陕西省自然科学基金资助项目(2011JQ8042)。
网络出版时间：2012-11-02 网络出版地址：http://www.cnki.net/kcms/detail/61.1069.T.20121102.1836.003.html

社会和经济效益，近年来引起了工业界和学术界的高度关注，产生了许多重要的研究成果[1-3]。但是，这项技术的发展也面临着许多挑战，主要是在确保信息的完整性和可追溯性的同时，要保护好司乘人员的隐私，并且要满足实时处理的需求。由于不法分子和自私人员可能会利用车载网传播伪造信息来满足自己的需要，所以必须使用数字签名机制确保传输的信息来自于真实可靠的车辆，但是这些信息通常包括车辆的位置、方向和时间等，很容易被人获知，这样会威胁到司乘人员的隐私。

为了解决这些问题，已经有许多代表性的研究成果[4-7]，大多都使用了很耗时的数学运算，严重影响大规模车载网的部署实施，并且不满足安全信息必须快速处理的需求。这些方案大致分为两类，其中文献[8-10]等采用了基于笔名认证的技术，但是每辆车需要事先储存大量的匿名证书，才能满足保护隐私的需求，因此大大加重了认证中心的证书管理的负担，为了减轻证书管理的负担，另外一些方案[11-13]采用了群签名来保护隐私，但是证书召回是很困难的问题。还有学者提出使用基于身份的签名体制[7]，但此类协议要求系统的主密钥储存在一种理想化的防篡改硬件中，现实中很难实现，并且容易受到边信道攻击。

本文提出了一种分布式的基于笔名认证的安全协议，能够解决车载网信息快速验证的问题，同时很好地保护了司乘人员的隐私。方案采用了移动通信群组管理的模式，对笔名证书属地化管理，在本地行驶的合法汽车采用高效无证书混合签密[14]的方式，可以定期通过就近的 RSU 向证书中心申请临时笔名，然后进行车联网信息传输，所有由本地笔名签署的信息进行批量验证，因此可以大大提高信息验证的效率。

1　预备知识

1.1　双线性对

设 G_1 和 G_2 分别表示阶为素数 q 的加法循环群和乘法循环群，p 是 G_1 的一个生成元。如果映射 $e: G_1 \times G_2 \rightarrow G_2$ 满足下列性质，则称为双线性对。①双线性性：对任意 $a, b \in Z_q^*$，$e(aP, bP) = e(P, P)^{ab}$。②非退化性：$e(P, P) \neq 1_{G_2}$。③可计算性：对所有的 $P, Q \in G_1$，都能有效计算 $e(P, Q)$。双线性对 e 可以通过有限域上的超椭圆曲线的 Tate 对或 Wail 对来构造。

1.2　Diffie-Hellman 问题

CDH(Computational Diffie-Hellman)问题：任给 (aP, bP)，其中 $a, b \in Z_q^*$，计算 abP。BDH(Bilinear Diffie-Hellman)问题：任给 (aP, bP, cP)，其中 $a, b, c \in Z_q^*$，计算 $e(P, P)^{abc} e(P, P)^{abc}$。

2　本文方案

2.1　系统初始化

选取两个阶为素数 q 的循环群 G_1 和 G_2，$e: G_1 \times G_1 \rightarrow G_2$ 是一个双线性对，P 是 G_1 的一个生成元，g_2 是 G_2 的一个生成元；随机选取 $s \in Z_q^*$ 作为系统的主密钥，并且计算 $P_0 = sP$；选取两个哈希函数 $H_1: \{0,1\}^* \rightarrow G_1$ 和 $H_2: Z_q^* \times G_2 \times G_1 \rightarrow \{0,1\}^\lambda$；选取一种对称加密算法 (E, D)，该算法满足可认证性和机密性，其密钥空间为 $\{0,1\}^\lambda$。系统的公共参数为 $(G_1, G_2, q, e, g_2, P, P_0, H_1, H_2, E, D, \lambda)$，系统的私钥是 s。

2.2　车辆注册和群登记

每辆车在入户时可以获得一个身份，例如电子车牌或车牌号，每个地区或城市称作一个群，群的身份可以是地区编号，这样每辆车和每个地区在部署车联网前都有了自己的身份 ID，系统通过如下计算为每辆车和每个群管理中心生成它们的部分私钥：$D_{\mathrm{ID}} = sH_1(\mathrm{ID})$。然后，每辆车和每个群随机选取 $x_{\mathrm{ID}} \in Z_q^*$，作为自己的另一部分私钥，并计算公钥 $P_{\mathrm{ID}} = x_{\mathrm{ID}} P$，每个 ID 的完整私钥为 $S_{\mathrm{ID}} = (D_{\mathrm{ID}}, x_{\mathrm{ID}})$。

2.3　车辆笔名获取

车辆会定期向群密钥中心申请临时笔名，或者当车辆驶入一个新的群之后也会向驶入群的密钥中心申请临时笔名，发出的请求信息中包含时间戳 TS、公钥 P_r 和自己的身份 ID_r，并且用群公钥进行加密，群密钥中心收到信息解密后首先检查时间戳，若时间超过设定值，则予以丢弃；否则，再检查申请车辆 ID_r 是否在违规车辆召回列表中，若在其中，将丢弃申请信息，若不在其中则通过如下运算为申请车辆颁发一个笔名：①令 g_2 是 G_2 的生成元，随机选取 $x \in Z_q^*$，计算临时笔名 $T = g_2^x$；②随机选取 $r \in Z_q^*$，令 $Q_r = H_1(\mathrm{ID}_r)$，计算 $K = H_2(r, e(D_s, Q_r), x_s P_r)$，其中 (D_s, x_s) 是群密钥中心的完整私钥；③计算 $c = E_K(T \| T_S \| \mathrm{ID}_2 r \| x)$；④输出并发送 (c, r)。

申请车辆收到 (c, r) 后，使用群的身份和公钥 (ID_s, P_s) 以及自己的私钥 (D_r, x_r) 对 (c, r) 进行解签，运算如下：①令 $Q_s = H_1(\mathrm{ID}_s)$，计算 $K = H_2(r, e(Q_s, D_r), x_r P_s)$；②计算 $T \| T_S \| \mathrm{ID}_r \| x = D_k(c)$。

群密钥中心向申请车辆发出笔名 T 和与之对应的签名私钥 x 之后，会将笔名和申请车辆的身份存入证书列表。

2.4 车辆信息签名

车辆收到临时笔名和签名私钥之后，就可以对发出的安全信息 M 进行签名，并且只有同一个群的成员才能发送和接收信息，信息格式是 $(M \| \sigma \| T_S \| T)$，其中 σ 是发送信息的车辆对 M 的签名，$\sigma = H_1(M)^x$。

2.5 车辆信息验证

车联网内车辆收到由同一个群的车辆发出的信息后，需要进行验证，验证之前先根据信息附带的时间戳核对信息的时效性，在有效期内的信息通过对运算进行验证，假如收到信息 $(M \| \sigma \| T_S \| T)$，若 $e(H_1(M), T) = e(\sigma, g_2)$，则接受该信息；若等式不成立，则予以丢弃。

由于所有车辆几乎每 300 ms 都要广播一次安全信息，所以车联网内信息的验证效率必须非常高。为了在短时间内验证大批量的安全信息，必须采用批量验证技术，假如收到 n 个信息 $\{M_i, T_i, \sigma_i, T_i\}$，$i = 1, \cdots, n$，则批量验证算法如下：①检查所有时间 T_i 的有效性，如果 T_i 过期，就拒绝接收该信息，在下面的运算中将其丢弃；②计算 $C_1 = e\left(\prod_{i=1}^{n} H_1(M)_i, \prod_{i=1}^{n} T_i\right)$；③计算 $C_2 = e\left(\prod_{i=1}^{n} \sigma_i, g_2^n\right)$；④如果 $C_1 = C_2$，就接收所有信息，否则不予接收。

根据使用的批量验证技术，每辆车对同一段时间在一个群内接收的所有信息进行验证所花费的代价几乎等同于一条信息的验证代价，因此车辆不会因接收的信息太多而来不及验证，从而解决了车联网对于安全信息认证必须快速的问题。

2.6 违法车辆追踪

车联网中如果存在恶意的车辆，可能会发布伪造的安全信息给其他车辆，故意误导交通甚至导致交通事故的发生，如果出现这种情况，群密钥管理中心会通过下面的步骤揭示恶意车辆的身份：①从 $(M \| \sigma \| T_S \| T)$ 中提取车辆笔名 T；②在数据库中查找车辆身份和笔名的对照 (ID, T)；③更新车辆召回列表和证书列表，并将违法车辆的身份通知给所有其他群的密钥管理中心，该车辆在下次申请笔名时都予以拒绝，并将违法车辆记录在案，实施惩罚。

3 安全性和效率分析

本文方案满足信息的可认证性。所有通过申请并获得笔名的车辆发出的信息都会附带签名，没有签名的信息不会被接受，因此所有车联网中传输的信息都可被认为来自真实的车辆，并且在传输途中不会被篡改，引入的数字签名保证了信息的完整性和可认证性。同时，本文方案具备信息的可追踪性，一旦有车辆发布伪造或虚假信息，遭到举报后，群密钥管理中心会通过车辆的真实身份和笔名的对照表，找到违法车辆，将其加入违法车辆召回列表，通知所有的群密钥中心，使其不能进行下一次的笔名申请，并在车辆年检时实施惩罚。

本文方案能够保护司乘人员的隐私。所有的车辆在进行车联网通信之前，都要向群密钥管理中心申请笔名，并且会定期更新，群密钥管理中心对笔名的发送采用无证书签密的方式发送，保证了笔名来源的真实性和可认证性，并且敌手不会从截获的密文中获得车辆的身份和笔名对应的签名密钥，因此车辆身份和笔名的对应关系只存放在密钥管理中心，外界无法从车辆发出的签名信息中获得车辆的身份，而且笔名是定期更换的，所以敌手也无法从车辆发出的签名信息中获得车辆的行踪。

本文方案能够抵抗边信道攻击和拒绝服务攻击。协议中笔名对应的签名密钥保存在车辆的防篡改设备中，如果长期不更新这个签名密钥，可能会给敌手留下恢复密钥的机会，以致能够跟踪车辆，但是需要注意的是，实际上敌手只是偶尔发动边信道攻击，因此大多数情况下，在敌手积累了足够多的信息之前，受到攻击的车辆已经更换了自己的笔名和签名密钥。本文方案建议周期地更新车辆的签名密钥，在最坏的情况下，即使敌手破解了车辆的签名密钥，那也只能是更新前的一段时间。另外，该方案采用了无证书管理的方式，大大减轻了密钥管理中心的负担。车联网中信息的认证采用了批量认证技术，使得认证时间减少为接近原来的 $1/n$（n 为需要认证信息的个数），因此能够有效地对付拒绝服务攻击和分布式拒绝服务攻击。

无证书体制下存在两类攻击：第一类攻击是由普通的攻击者造成的，他不知道密钥管理中心的私钥，但可以替换任何用户的公钥；第二类攻击者是指好奇但诚实的密钥管理中心，他们已经知道部分用户的私钥，但不替换任何用户公钥。假定对称加密方案 (E, D) 具有可认证性，则本文采用的无证书签密算法在随机预言机模型和 BDH 及 CDH 困难性假设下对两类攻击者都能满足可认证性的安全需求；如果 (E, D) 又具有机密性，那么本文方案在随机

预言机模型和 BDH 及 CDH 困难性假设下对两类攻击者都能满足机密性的安全需求[14]。

车辆获取签名密钥时，密钥中心的运算只包括一个对运算和一个点乘运算，车辆进行的运算也是包括一个对运算和一个点乘运算，因此本文方案在签密和解签密认证的效率上比其他方案高，而且密文长度也最短。对于 80 b 的安全级别，群元素的长度为 320 b，有限域元素的长度是 160 b，那么密文长度比其他方案至少短 416 b，这非常适合于车载网的通信环境。

4　仿真实验

实验使用了仿真工具 NS2 的 2.34 版本，仿真时间为 200 s，移动节点为 10～120 个，静止节点为 8 个，车辆速度范围为 0～120 km/h，OBU 通信距离为 300 m，RSU 通信范围为 1 km，数据链路层协议为 802.11p，路由协议为 GSR。模拟路况如图 1 所示，仿真区域为 5 km×5 km。

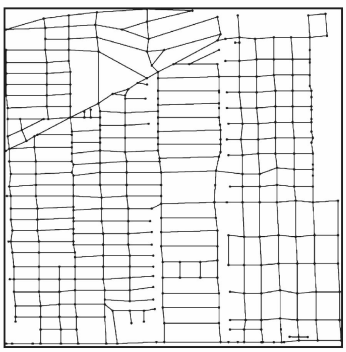

图 1　仿真实验交通路况

将本文方案的实验结果与现有方案 ECPP[12] 和 GISS[11] 的结果进行比较。首先是车辆获取签名密钥花费的时间比较，如表 1 所示，ECPP 方案中车辆获取签名证书需要花费两个来回的时间，本文方案则只需要一个来回时间，包括车辆发出请求、密钥中心计算临时笔名和发送笔名给车辆的时间。由表 1 可以看出，本文方案明显减少了车辆笔名的申请时间。

本文方案中 RSU 负责接收车辆签名密钥的申请并转发给密钥管理中心，然后密钥管理中心将生成的车辆笔名传给相应的 RSU，并由 RSU 发送给申请车辆，RSU 成功完成任务的比例等于收到笔名的车辆数除以发送申请的次数，由表 2 可以看出，本文方案中 RSU 转发笔名的成功率可以达到 80％以上，远远大于 ECPP 和 GSIS 方案的成功率。

表 1　车辆获取签名密钥花费时间　　ms

车辆数	时间	
	ECPP 方案	本文方案
10	5.9	4.0
20	6.0	4.1
30	6.4	4.3
40	6.9	5.0
50	7.2	5.5
60	7.9	6.1
70	8.4	7.0

表 2　RSU 转发数据的成功率　　％

车辆数	成功率		
	ECPP 方案	GSIS 方案	本文方案
20	49.3	67.5	84.3
40	37.5	65.9	79.6
60	29.8	64.3	75.5
80	26.7	63.5	72.5
100	25.5	61.2	70.6
120	23.2	57.6	68.3

车辆采纳一条信息需要的总时延包括信息的签名运算时间、信息传输时间和信息验证时间。本文方案中信息签名算法和验证算法的时间复杂度小于 ECPP 和 GSIS 方案，并且使用了信息批量验证，因此平均信息时延大大减少，另外，方案中信息签名的大小为 160 B，使得信息的传输时间能够减少，表 3 中反映本文方案的信息时延能够节约 30 ％以上。

表 3　平均信息延迟　　ms

车辆数	平均信息延迟		
	ECPP 方案	GSIS 方案	本文方案
10	236	187	102
20	501	399	196
30	782	596	371
40	886	780	595
50	932	893	733
60	1 085	1 018	801

表 4 表明，随着单跳范围内（即 300 m 范围内）车辆的增多，端到端传递的信息时延变化不大，变化幅度控制在 15 ms 以内，这远远小于可容忍的最大端到端时延（100 ms），但是随着车辆密度的增大，车载自组织网内的丢包率会逐渐增大，尤其是当车辆密度达到 120 辆/300 m 时，丢包率高达 63 ％，然而这样的车辆密度只是在实验中才会出现，实际中即使出现最严重的交通拥堵，车辆密度最多也不会超

过60辆/300 m(每辆车长度为4 m左右,再加上前后车间距离2 m)。况且这种情况下,丢失的数据包包含了大量的重复发送的数据。因此,正常情况下车辆密度低于50辆/300 m,小于18 %的丢包率是完全可以接受的。

表4 车辆密度对网络性能的影响

车辆密度 辆/300 m	端到端时延 /ms	平均丢包率 /%
10	11.5	2.3
20	13.6	4.7
40	17.2	15.2
60	18.5	37.2
80	20.1	45.3
100	22.0	54.5
120	24.5	63.0

5 结 论

本文基于高效的无证书签密算法和笔名签名的算法,提出了一种车联网信息认证方案,能够满足车联网主要的安全需求,例如可认证性、可追踪性和匿名保护等;采用了批量验证的技术能够节约车联网信息认证的时间,满足了智能交通中对安全信息必须反应迅速的要求,并且提出的方案能够在规模上进行快速的升级和扩充,很好地适应了车联网从部署初期到大规模应用的发展要求。另外,对于违法车辆笔名的召回仍然采用了传统的召回列表的方式。如何快速地召回这些笔名,仍然是一个比较棘手的问题。

参考文献:

[1] MOHARRUM M A, AL DARAISEH A A. Toward secure vehicular ad-hoc networks: a survey [J]. IETE Technical Review, 2012, 29(1): 80-89.

[2] LIN Xiaodong, LU Rongxing, ZHANG Chenxi, et al. Security in vehicular ad hoc networks [J]. IEEE Communications Magazine, 2008, 46(4): 88-95.

[3] RAYA M, PAPADIMITRATOS P, HUBAUX J P. Securing vehicular communications [J]. IEEE Wireless Communications, 2006, 13(5): 8-15.

[4] DAZA V, DOMINGO-FERRER J, SEBE F, et al. Trustworthy privacy-preserving car-generated announcements in vehicular ad hoc networks [J]. IEEE Transactions on Vehicular Technology, 2009, 58(4): 1876-1886.

[5] PAPADIMITRATOS P, BUTTYAN T, HOLCZER T, et al. Securing vehicular communications systems: design and architecture [J]. IEEE Communication Magazine, 2008, 46(11): 100-109.

[6] WU Qianhong, DOMINGO-FERRER J, GONZALEZ-NICOLAS U. Balanced trustworthyness, safety, and privacy in vehicle-to-vehicle communications [J]. IEEE Transactions on Vehicular Technology, 2010, 59(2), 559-573.

[7] ZHANG Chenxi, LU Rongxing, LIN Xiaodong, et al. An efficient identity-based batch verification scheme for vehicular sensor networks [C]// Proceedings of the 2008 IEEE INFOCOM. Piscataway, NJ, USA: IEEE Computer Society Press, 2008: 246-250.

[8] CALANDRIELLO G, PAPADIMITRATOS P, HUBAUX J A. Efficient and robust pseudonymous authentication in VANET [C]// Proceedings of the 2007 ACM VANET. New York, USA: ACM, 2007: 19-28.

[9] RAYA M, HUBAUX J. The security of vehicular ad hoc networks [C] // Proceedings of the 2005 ACM SASN. New York, USA: ACM, 2005: 11-21.

[10] RAYA M, HUBAUX J. Securing vehicular ad hoc networks [J]. Journal of Computer Security, 2007, 15(1): 39-68.

[11] LIN Xiaodong, SUN Xing, HO Pin-han, et al. GSIS: a secure and privacy preserving protocol for vehicular communications [J]. IEEE Transactions on Vehicular Technology, 2007, 56(6): 3442-3456.

[12] LU Rongxing, LIN Xiaodong, SHEN Xuemin, et al. ECPP: efficient conditional privacy preservation protocol for secure vehicular communications [C] // Proceedings of the 2008 IEEE INFOCOM. Piscataway, NJ, USA: IEEE Computer Society Press, 2008: 1229-1237.

[13] 刘辉, 李晖, 马占欣. 一个安全高效的车载网信息认证方案 [J]. 西南交通大学学报, 2011, 46(2): 315-320.
LIU Hui, LI Hui, MA Zhanxin. Efficient and secure authentication scheme for vehicular Ad Hoc networks [J]. Journal of Southwest Jiaotong University. 2011, 46(2): 315-320.

[14] 孙云霞, 李晖. 高效无证书混合签密 [J]. 软件学报, 2011, 22(7): 1690-1698.
SUN Yunxia, LI Hui. Efficient certificateless hybrid signcryption [J]. Journal of Software, 2011, 22(7): 1690-1698.

(编辑 武红江)