DOI:10.13878/j.cnki.jnuist.2017.05.007

刘辉[1,2]　仲红[1]　许艳[1]　周金玉[1]

车联网云环境下多服务器架构的匿名认证及密钥协商协议

摘要

随着车载自组织网(Vehicular Ad-hoc Networks,VANETs)和云计算的发展,越来越多面向车联网用户的移动应用服务应运而生.这些应用服务往往由不同的服务器提供,车辆要从这些服务器获得服务,则必须向不同的服务器提供注册信息.为了实现车辆在多个服务器上的高效认证,本文提出一个车联网云环境下(Vehicular Cloud Computing,VCC)面向多服务器架构的匿名认证协议,协议实现了车辆与服务器的双向认证,并能够保护车辆隐私.

关键词

车联网云;匿名认证;多服务器架构

中图分类号 U495;TP309

文献标志码 A

0　引言

VANETs 是智能交通系统(Intelligent Transportation System,ITS)的核心组成部分[1],是物联网在智能交通领域的具体应用.VANETs 包含两类通信节点:部署在车辆中的车载单元(On-Board Units,OBU)和固定于路边的路侧单元(Road Side Units,RSU).VANETs 使用 DSRC(Dedicated Short Range Communications)协议[2]实现车辆间通信(Vehicle-to-Vehicle,V2V),以及车辆与 RSU 通信(Vehicle-to-Infrastructure,V2I),而车辆经由 RSU 通过 Internet 与应用服务器之间进行通信.VANETs 组成结构如图 1 所示.

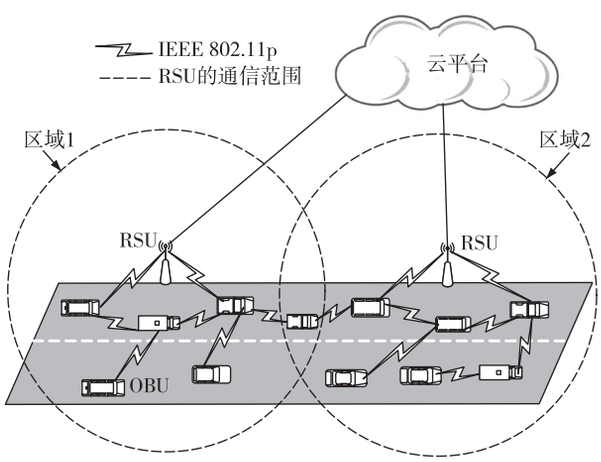

图 1　VANETs 系统模型

Fig. 1　VANETs system model

VANETs 为智能交通带来的便利必然促使 VANETs 成为下一代移动互联网的重要研究内容[3]:VANETs 能使驾乘人员和交通管理人员获得全面实时的交通信息,能够有效解决交通阻塞问题、减少道路交通事故.此外,VANETs 为驾乘人员提供办公、娱乐等服务,能够提高工作效率和生活质量.然而 VANETs 提供的交通状况、办公娱乐等信息通常由不同的服务器提供,车辆要获得这些服务,则必须分别向不同服务器提供注册信息.如果采用传统的单一注册机制,车辆将需要重复注册并记住大量的用户名和密码,这将为车辆及服务器带来

收稿日期 2017-05-31

资助项目 国家自然科学基金(61572001,61702005);安徽省自然科学基金(1708085QF136);安徽大学博士科研启动经费

作者简介

刘辉,男,博士生,实验师,研究方向为物联网安全、无线传感网安全.liuhui@ahu.edu.cn

仲红(通信作者),女,博士,教授,博士生导师,主要研究方向为信息安全和隐私保护.zhongh@ahu.edu.cn

1　安徽大学 计算机科学与技术学院,合肥,230601

2　安徽大学 电子信息工程学院,合肥,230601

极大的不便.针对单一注册机制带来的问题,已有学者提出面向多服务器架构的认证协议,此类协议中用户只需注册一次便可获取多个服务器的访问权限[4-5].然而,文献[4-5]提出的是基于静态身份的多服务器认证协议,容易造成用户信息泄露并可能被追踪,给用户隐私带来威胁.随后,Das 等[6]提出基于动态身份的多服务器认证协议,允许用户改变自己的密码,实现用户身份的匿名性.基于动态身份的多服务器认证协议能够保护用户的身份隐私,近年来得到了广泛研究.2009 年,文献[7]提出一种双向生物认证协议,协议不需要存储秘密信息,减少服务器端和用户端的存储代价.2014 年,He 等[8]利用生物特性,首次提出 3 因子的动态多服务器认证协议,然而 Odelu 等[9]指出 He 等[8]的协议不能抵抗重放攻击和假扮攻击.上述利用生物特征实现的多服务器认证协议需要安装额外设备采集生物特征.2011 年,李曦等[10]使用基于身份密码体制,提出一种基于身份的远程服务器认证协议.2015 年,Amin 等[11]提出一个 3 因子的基于双线性配对的多服务器匿名认证协议,但是协议的注册过程需要权威机构参与.

移动网络信号稳定性差,用户终端的计算能力一般,对多服务器认证协议的安全性和效率有着较高要求,以上面向多服务器架构的匿名认证协议[6-11]并不适用于移动网络环境.2016 年,He 等[12]使用自证书密码体制,提出一个动态多服务器认证协议,协议有着较高的计算效率和通信效率,可用于移动网络环境实现匿名的多服务器认证.然而作为一种特殊的移动网络,VANETs 的通信节点是车辆,有着通信节点众多、节点移动速度快、实时性要求高的特点,文献[12]提出的协议虽然高效,但还不能完全适用于 VANETs 的移动网络环境.2016 年,谢永等[13]首次提出适用于 VANETs 的多服务器匿名认证协议,并指出 VANETs 的移动服务多由云计算服务器提供,进而提出一个车联网云计算平台(Vehicular Cloud Computing,VCC)[14-15]下面向多服务器架构的匿名认证协议.然而,本文研究发现文献[13]提出的协议在双向认证与密钥协商阶段,服务器能够计算出车辆的真实身份,无法对云服务器实现车辆身份的隐私保护.为解决车联网云环境下车辆需要向多个服务器注册以获取应用服务的问题,本文提出一个面向多服务器架构的匿名认证和密钥协商协议,云服务器在向 RC 注册时有着较低的计算代价.此外,云服务器无法计算出车辆的真实身份,能够有效保护车辆隐私.

1 预备知识

1.1 双线性映射

令 G 是 p 阶循环加法群,G_T 是 p 阶循环乘法群.双线性映射 $e:G\times G\rightarrow G_T$ 满足以下 3 个性质:

1) 双线性性:$\forall g,h\in G$ 和 $a,b\in Z_p$,有 $e(g^a,h^b)=e(g,h)^{ab}$;

2) 非退化性:$\exists g\in G$,使得 $e(g,g)$ 在 G_T 中的阶是 p;

3) 可计算性:$\forall g,h\in G$,存在有效算法计算 $e(g,h)\in G_T$.

1.2 复杂性假设

DBDH 假设:在 p 阶循环加法群 G 和 p 阶循环乘法群 G_T 中,双线性映射 $e:G\times G\rightarrow G_T$.随机选择 G 的生成元 g,随机数 $a,b,c\in {}_RZ_p^*$,并将 (g,g^a,g^b,g^c) 和 $Z\in {}_RG_T$ 发送给敌手 A,由 A 判断 Z 是否等于 $e(g,g)^{abc}$,若 $Z=e(g,g)^{abc}$,A 输出 1,否则输出 0.

如果不存在多项式时间算法以不可忽略的优势解决 DBDH 假设,那么 DBDH 假设在群 G,G_T 中成立.A 解决 DBDH 问题的优势为:$Adv=|\Pr[A(g,g^a,g^b,g^c,e(g,g)^{abc})=0]-\Pr[A(g,g^a,g^b,g^c,Z)=0]|$.

1.3 系统模型

本文研究车联网云环境下多服务器匿名认证协议,系统模型如图 2 所示.与文献[13]一样,系统模型包含 3 个参与者:注册中心、云服务器和移动节点(包括车辆和 RSU).

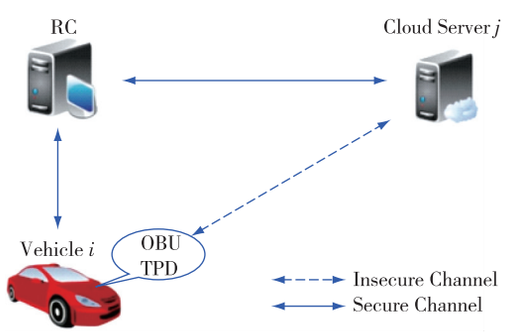

图 2 VCC 环境下多服务器认证系统模型

Fig. 2 System model of multi-servers authentication for VCC

1)注册中心(Register Center,RC):是可信第三方,负责生成系统参数、云服务器和移动节点的密钥,并为车辆分配防篡改设备(Tamper-Proof Device,TPD).

2)云服务器:是半可信第三方,诚实地执行协议但会窃取车辆隐私.为 VANETs 中的移动节点提供各种应用服务器.

3)移动节点:包括车辆和 RSU.车辆在注册中心申请注册,注册通过后,向云服务器提出服务请求,该服务请求由 RSU 转发给云服务器.

1.4 安全要求

一个 VCC 环境下面向多服务器架构的匿名认证协议应满足如下的安全要求[13]:

1)消息认证:在收到消息时,云服务器和车辆能够验证消息发送方的身份,并保证消息在传输过程中没有被篡改.

2)会话密钥协商:云服务器和车辆最终能够协商出一个安全的会话密钥,用来加密后期传输的消息.

3)隐私保护:协议必须保护车辆身份信息不被云服务器获取.云服务器在接收到车辆发布的消息后,无法计算出车辆的身份信息.

4)抵抗各种攻击:协议需要抵抗假扮攻击、重放攻击等各种攻击,以确保 VCC 环境的安全性与可靠性.

需要说明的是,与文献[13]提出的安全要求相比,本文在隐私保护方面要求车辆对云服务器也是匿名的,因此本文协议在隐私保护方面安全性更高.

2 提出协议

为了提高文献[13]的安全性和效率,本节提出一个 VCC 环境下面向多服务器架构的匿名认证协议,该协议包括:系统初始化、注册、双向认证及密钥协商等 3 个阶段.

2.1 系统初始化

注册中 RC 生成系统参数:

1)RC 选择有限域 F_p 上的椭圆曲线 E,并从 E 上选择一个阶为 q 的有限循环群 G,P 为 G 的生成元.

2)RC 选择随机数 $s \in Z_q^*$,计算 $P_{pub}=sP$;选择5个安全的 Hash 函数:$h_0:G \rightarrow \{0,1\}$,$h_1,h_2,h_3,h_4:\{0,1\} \rightarrow Z_q^*$.

3)RC 公开系统参数 $params=(E,q,P,P_{pub},H_0,H_1,H_2,H_3,H_4)$,保密 s 作为系统主密钥.

2.2 注册阶段

这一阶段包括云服务器注册和车辆注册.

2.2.1 云服务器注册

身份标识为 ID_j 的云服务器 Ser_j 向 RC 进行注册.

1)RC 选择随机数 $s_j \in Z_q^*$,计算 $P_j=s_jP$;

2)RC 将(s_j,P_j) 通过安全信道发送给云服务器 Ser_j,Ser_j 公开(ID_j,P_j);

3)RC 将(ID_j,P_j) 记录在服务器列表 SerList 中.

2.2.2 车辆注册

身份标识为 RID_i 的车辆 V_i 向 RC 进行注册.车辆 V_i 将自己的真实身份 RID_i、密码 PW_i 提交给 RC,RC 检查通过后为 V_i 颁发一个防篡改设备 TPD,TPD 中记录车辆的身份 RID_i、密码 PW_i、系统参数 $params$ 和系统主密钥 s.

2.3 双向认证及密钥协商

车辆和云服务器进行双向认证,并协商出会话密钥.

2.3.1 车辆 V_i 向云服务器 Ser_j 发送访问请求

1) V_i 将应用需求发送给 RC,RC 从 SerList 查找并返回服务器 Ser_j 的身份及公钥信息(ID_j,P_j).

2)V_i 向 TPD 输入身份 RID_i 和密码 PW_i,验证通过后,将服务器 Ser_j 的信息(ID_j,P_j) 发送给 TPD.

3)TPD 选择随机数 $u_i \in Z_q^*$,时间戳 T_i,计算 $U_i=u_iP$,$PID_i=RID_i \oplus h_0(u_iP_{pub})$,$h_{it}=h_1(ID_j,PID_i,U_i,T_i)$,$sk_i=u_i+h_{it}s$.

4)OBU 选择随机数 $r_i \in Z_q^*$,计算 $R_i=r_iP$,$h_i=h_2(ID_j,PID_i,U_i,R_i,T_i)$,$\sigma_i=r_i+h_isk_i$.

5)V_i 将请求信息 $Req=(ID_j,PID_i,U_i,R_i,T_i,\sigma_i)$ 发送给云服务器 Ser_j.

2.3.2 云服务器 Ser_j 向车辆 V_i 发送响应消息

1)云服务器 Ser_j 接收到车辆 V_i 发来的请求 Req 后,计算 $h_{it}=h_1(ID_j,PID_i,U_i,T_i)$,$h_i=h_2(ID_j,PID_i,U_i,R_i,T_i)$,并验证如下等式是否成立:

$$\sigma_iP=R_i+h_iU_i+h_ih_{it}P_{pub}, \tag{1}$$

如果等式(1)成立,则签名有效;否则 Ser_j 终止本次会话.

2)Ser_j 选择随机数 $r_j \in Z_q^*$,计算 $R_j=r_jP$,$sk=h_3(r_jR_i,ID_j,PID_i,U_i,T_i)$,$h_j=h_4(PID_i,ID_j,U_i,sk,r_iR_j)$,$\sigma_j=r_j+h_js_j$.

3)Ser_j 将响应信息 $Res=(ID_j,PID_i,R_j,\sigma_j)$ 发送给 V_i.

2.3.3 车辆 V_i 验证云服务器 Ser_j 的响应消息

1) V_i 接收到云服务器 Ser_j 的响应信息 Res 后,计算 $sk=h_3(r_iR_j,ID_j,PID_i,U_i,T_i)$,$h_j=h_4(PID_i,ID_j,U_i,sk,r_iR_j)$,并验证如下等式是否成立:

$$\sigma_jP=R_j+h_jS_j, \tag{2}$$

如果等式(2)成立,则云服务器 Ser_j 验证通过.

2) V_i 得到与云服务器 Ser_j 在时间段 T_i 内的会话密钥 sk.

3 协议分析

3.1 正确性分析

1) 如果等式(1)成立,则车辆 V_i 生成的签名 σ_i 是有效的.

$$\sigma_i P = (r_i + h_i sk_i)P = (r_i + h_i(u_i + h_{it}s))P = R_i + h_i U_i + h_i h_{it} P_{pub}.$$

2) 如果等式(2)成立,则云服务器 Ser_j 的签名 σ_j 是有效的.

$$\sigma_j P = (r_j + h_j s_j)P = R_j + h_j S_j.$$

3) 车辆 V_i 与云服务器 Ser_j 协商的会话密钥 sk 是一致的.

V_i 计算的会话密钥 $sk = h_3(r_i R_j, ID_j, PID_i, U_i, T_i)$;$Ser_j$ 计算的会话密钥 $sk = h_3(r_i R_j, ID_j, PID_i, U_i, T_i)$.

由于 $r_i R_j = r_j R_i = r_i r_j P$,则 V_i 与 Ser_j 协商的会话密钥 sk 是一致的.

3.2 安全性分析

本文在 1.4 节指出 VCC 环境下面向多服务器架构的双向认证协议应满足消息认证、会话密钥协商、隐私保护和抵抗各种攻击等 4 个方面的安全要求.下面将分析本文提出的协议满足 1.4 节提出的安全要求.

1) 消息认证:当车辆 V_i 试图获取云服务器提供的服务时,将发送请求消息 Req,如果其中的 σ_i 满足 $\sigma_i P = R_i + h_i U_i + h_i h_{it} P_{pub}$,则表明 σ_i 包含注册中心给车辆 V_i 颁发的合法私钥,即 V_i 是在 RC 中注册的合法用户,其中 $h_{it} = h_1(ID_j, PID_i, U_i, T_i)$,$h_i = h_2(ID_j, PID_i, U_i, R_i, T_i)$.随后,云服务器 Ser_j 发送响应消息 Res,如果 σ_j 满足 $\sigma_j P = R_j + h_j S_j$,则表明 Ser_j 是 RC 中注册的合法的云服务器,其中 $h_j = h_4(PID_i, ID_j, U_i, sk, r_i R_j)$.

2) 会话密钥协商:云服务器 Ser_j 和车辆 V_i 最终协商的会话密钥 sk,满足 $sk = h_3(r_i R_j, ID_j, PID_i, U_i, T_i) = h_3(r_j R_i, ID_j, PID_i, U_i, T_i)$,其中 r_i 和 r_j 分别是车辆 V_i 和云服务器 Ser_j 选择的随机数,同时由于离散对数的困难性,系统中只有车辆和云服务器才能知道自己选择的随机数 r_i 和 r_j,所以协议最终协商的会话密钥 sk 只有车辆和云服务器知道,因此 sk 是安全的会话密钥.

3) 隐私保护:车辆 V_i 向云服务器发送的请求消息 Req 只含有车辆的假名 $PID_i = RID_i \oplus h_0(u_i P_{pub})$.假名中含有随机数 u_i,因此车辆每次发布请求消息时的假名均不相同,可以防止车辆位置被追踪,实现车辆位置隐私保护.此外,由离散对数困难性可知,假名中含有的值 $h_0(u_i P_{pub})$ 只有车辆 V_i 和注册中心 RC 知道,因此车辆 V_i 的真实身份只有 V_i 和注册中心才能获取,能够实现车辆身份的隐私保护.本文的协议可对攻击者和半可信的云服务器实现车辆身份的隐私保护,而文献[13]的协议只能对攻击者实现车辆身份的隐私保护.

4) 抵抗假扮攻击:若攻击者 Adv 试图伪装成车辆 V_i 登录云服务器,则需要伪造请求消息 $Req = (ID_j, PID_i, U_i, R_i, T_i, \sigma_i)$,其中 σ_i 应满足等式(1),但 Adv 未在 RC 中注册,无法计算出合法的 σ_i.若攻击者 Adv 试图伪装成云服务器 Ser_j 与车辆交互,则需要伪造响应消息 $Res = (ID_j, PID_i, R_j, \sigma_j)$,但只有在 RC 中注册的合法云服务器才能获得 RC 颁发的私钥,故 Adv 无法计算出合法的 σ_j.因此,本协议能够抵抗假扮攻击.

5) 抵抗重放攻击:当车辆 V_i 试图获取云服务器提供的服务时,会选择当前的时间戳 T_i,并根据 T_i 计算请求消息 Req.因此,时间段 T_i',攻击者 Adv 试图重放时间段 T_i 截获的请求消息 Req,将无法通过验证.因此,本协议能够抵抗重放攻击.

3.3 效率分析

本节分析本文协议的计算效率,并与文献[13]提出的面向多服务器架构的双向认证和密钥协商协议进行性能比较.与文献[13]提出的协议一样,本文协议基于非奇异椭圆曲线密码体制设计,无双线性配对操作,因此是高效的.

表 1 较为直观地表明了这 2 个协议在双向认证及密钥协商阶段的计算开销.文献[13]协议中,车辆需要计算 4 个椭圆曲线标量乘法和 5 个单向 Hash 函数,即车辆的计算时间是 $4T_{em}$;云服务器需要计算 5 个椭圆曲线标量乘法和 5 个单向 Hash 函数,即云服务器的计算时间是 $5T_{em}$.本文协议中,车辆需要计算 4 个椭圆曲线标量乘法和 5 个单向 Hash 函数,即车辆的计算时间是 $4T_{em}$;云服务器需要计算 4 个椭圆曲线标量乘法和 4 个单向 Hash 函数,即云服务器的计算时间是 $4T_{em}$.本文在 CPU 主频为 3.20 GHz,操作系统为 Win7,内存为 2 GB 的环境下,实现了椭圆曲线标量乘法运算,运行 1 000 次的平均计算时间

为 0.651 ms.

表 1 2 个协议的计算代价

Table 1 Computation cost comparison between the proposed protocol and protocol in Ref.[13] ms

Protocol	Vehicles	Cloud Server
文献[13]	$4T_{em}\approx 2.604$	$5T_{em}\approx 3.255$
本文协议	$4T_{em}\approx 2.604$	$4T_{em}\approx 2.604$

4 结束语

本文研究了车联网云环境下面向多服务器架构的双向认证及密钥协商协议,并提出一个双向认证协议,能够实现车辆和云服务器间的相互认证.在协议执行过程中,车辆在每次发布服务请求时,将计算并使用不同的假名,能够防止车辆身份被追踪同时实现位置隐私保护.此外,只有注册中心能够恢复出车辆的假名,使得协议不仅能够对攻击者实现车辆身份的隐私保护,同时还能对云服务器保护车辆隐私.

参考文献

References

[1] Zeadally S, Hunt R, Chen Y S, et al. Vehicular ad hoc networks (VANETS): Status, results, and challenges[J]. Telecommunication Systems, 2012, 50(4): 217-241

[2] Dedicated Short Range Communications (DSRC)[EB/OL]. [2017-06-25]. http://Grouper.ieee.org/groups/scc32/dsrc/index.html

[3] Kakkasageri M S, Manvi S S. Information management in vehicular ad hoc networks: A review[J]. Journal of Network and Computer Applications, 2014, 39(1): 334-350

[4] Li L H, Lin L C, Hwang M S. A remote password authentication scheme for multiserver architecture using neural networks[J]. IEEE Transactions on Neural Networks, 2001, 12(6): 1498-1504

[5] Tsaur W J, Wu C C, Lee W B. A smart card-based remote scheme for password authentication in multi-server Internet services[J]. Computer Standards & Interfaces, 2004, 27(1): 39-51

[6] Das M L, Saxena A, Gulati V P. A dynamic ID-based remote user authentication scheme[J]. IEEE Transactions on Consumer Electronics, 2004, 50(2): 629-631

[7] 张凡,冯登国.基于模糊提取的远程双向生物认证[J].计算机研究与发展,2009,46(5):850-856
ZHANG Fan, FENG Dengguo. Fuzzy extractor based remote mutual biometric authentication[J]. Journal of Computer Research and Development, 2009, 46(5): 850-856

[8] He D B, Wang D. Robust biometrics-based authentication scheme for multiserver environment[J]. IEEE Systems Journal, 2014, 9(3): 816-823

[9] Odelu V, Das A K, Goswami A. A secure biometrics-based multi-server authentication protocol using smart cards[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(9): 1953-1966

[10] 李曦,李传锋,朱巍,等.基于身份的多服务器认证密钥协商方案[J].华中科技大学学报(自然科学版),2011,39(1):36-40
LI Xi, LI Chuanfeng, ZHU Wei, et al. Identity-based smart card remote authenticated key agreement protocol for multi-servers[J]. Journal of Huazhong University of Science and Technology (Natural Science Edition), 2011, 39(1): 36-40

[11] Amin R, Biswas G P. Design and analysis of bilinear pairing based mutual authentication and key agreement protocol usable in multi-server environment[J]. Wireless Personal Communications, 2015, 84(1): 439-462

[12] He D B, Zeadally S, Kumar N, et al. Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(9): 2052-2064

[13] 谢永,吴黎兵,张宇波,等.面向车联网的多服务器架构的匿名双向认证与密钥协商协议[J].计算机研究与发展,2016,53(10):2323-2333
XIE Yong, WU Libing, ZHANG Yubo, et al. Anonymous mutual authentication and key agreement protocol in multi-server architecture for VANETs[J]. Journal of Computer Research and Development, 2016, 53(10): 2323-2333

[14] Lee E, Lee E K, Gerla M, et al. Vehicular cloud networking: Architecture and design principles[J]. IEEE Communications Magazine, 2014, 52(2): 148-155

[15] Gerla M, Lee E K, Pau G, et al. Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds[C]// IEEE World Forum on Internet of Things, 2014: 241-246

Anonymous authentication and key agreement protocol in multi-server architecture for vehicular cloud computing

LIU Hui[1,2] ZHONG Hong[1] XU Yan[1] ZHOU Jinyu[1]
1 School of Computer Science and Technology, Anhui University, Hefei 230601
2 School of Electronics and Information Engineering, Anhui University, Hefei 230601

Abstract The development of VANETs and cloud computing brings more and more mobile application services for VANETs. Yet vehicles must provide registration information to different cloud servers to obtain their services. In order to achieve efficient authentication in multi-server architecture, this paper proposes an anonymous authentication and key agreement protocol in multi-server architecture for vehicular cloud computing, which realizes a two-way authentication protocol for vehicles and servers, and protects the privacy of the vehicles at the same time.

Key words vehicular cloud computing; anonymous authentication; multi-server architecture