车载自组织网络的无证书匿名认证协议

许俊峰[1] 丁雪峰[2] 司成祥[1] 张 伟[1]
(国家计算机网络应急技术处理协调中心 北京 100029)[1] (四川大学信息管理中心 成都 610065)[2]

摘 要 车载自组织网络在解决世界各地日益加重的各种交通问题中,得到了越来越多的应用,其安全性也成为研究的焦点。基于离散对数困难问题,提出了一个无证书的安全V2R匿名认证协议。新协议既避免了基于传统公钥系统的协议需做证书验证和维护的缺陷,又避免了基于身份的认证协议需要密钥分发的缺陷。与具有相同安全级别的匿名认证协议比较,本协议更为安全高效,因此更适用于无线车载网络。

关键词 车载自组织网络,隐式认证,匿名认证
中图法分类号 TP918.1 **文献标识码** A

Certificateless Anonymous Authentication Protocol for Vehicle Ad-hoc Network

XU Jun-feng[1] DING Xue-feng[2] SI Cheng-xiang[1] ZHANG Wei[1]
(National Computer Network Emergency Response Technical Team Coordination Center of China, Beijing 100029, China)[1]
(Information Management Center, Sichuan University, Chengdu 610065, China)[2]

Abstract Vehicular Ad-hoc networks (VANET) have acquired more and more applications in dealing the aggravating traffic problems all over world. And their security is receiving increasing attention. Based on discrete logarithm problem, a certificateless secure vehicle-to-roadside anonymous authentication protocol was proposed. The proposed protocol combines the advantages of the protocol based on traditional public key cryptosystem (no key escrow) and that based on ID-PKC (implicit authentication). Compared with the protocol at the same security level, the efficiency of the proposed approach is much more efficient. So it is more appropriate for VANET.

Keywords Vehicular ad-hoc network, Implicit authentication, Anonymous authentication

1 引言

随着无线通信技术的发展,人们的生活发生了翻天覆地的变化。近年来,汽车制造商和通信企业通过在车辆上和道路旁安装通信设施来为司机和乘客提供各种各样的服务,包括路况信息服务、安全驾驶信息服务等,以提高道路及驾驶的安全性,优化交通状况。通过在车辆上安装车载通信设备(称为车载通信单元OBUs (onborad units),在道路的关键位置安装路旁通信单元RSUs(roadside units),来构建车载自组织网络VANET(Vehicular Ad Hoc Network)。鉴于无线技术的低成本及易开发的特性,可以在道路旁密集地安装RSUs,它们为车辆提供通信接口;并且RSUs可以连接到因特网的主干网中以提供更为多样的服务,例如TCP服务或者实时多媒体流应用等。

VANET包含两类通信:车辆与车辆的通信V2V (Vehicle-to-Vehicle)和车辆与路旁基础设施的通信V2R (Vehicle-to-Roadside)。这两者都受到企业和学术界越来越多的关注,旨在提供各类服务,提高驾驶安全性,优化交通管理等。

VANET可以带来很多好处,如提供服务,安全驾驶和优化交通等。然而,VANET目前面临各种安全挑战[1]。显然,用户任何恶意行为,包括对信息的修改或重放都能给其他人带来致命的危害。所以目前有很多研究[1,3-14]集中在VANET的安全性上。V2V通信和V2R通信具有不同的安全需求:V2V通信需要满足认证性、条件隐私保护、不可否认性;V2R通信需满足对RSUs的消息完整性、源认证性、不可否认性,以及对OBUs的隐私保护性、认证性、消息完整性、不可否认性。目前有很多研究[1,3,11,14]关注V2R的安全性。已有的对于V2R安全性的研究主要集中在RSUs的消息完整性和认证性上,关注OBUs的条件隐私保护性和不可否认性的研究却很少。而这两者对于V2R通信中的OBUs是非常重要的安全需求。因为OBUs可能从RSUs请求各种付费服务,或者它们可能发送交通相关的信息给RSUs,例如某地某车辆造成交通事故。OBUs可能会提供肇事车辆的牌照,但它们不希望任何第三方能追踪到它们的告发行为。本文致力于解决V2R中OBUs的条件匿名性、认证性以及不可否认性问题。据我们所知,目前还没有任何研究专门解决这个问题。提出了一个新颖的V2R通信中的匿名认证协议。该协议基于一个无证书签名方案,该签名方案集合了传统公钥下签名

到稿日期:2012-12-04 返修日期:2013-04-04 本文受四川省科技支撑计划项目(2012GZ0001),上海市科学技术委员会基金项目(11511505300)资助。

许俊峰(1959-),男,硕士,高级工程师,主要研究方向为网络与信息安全,E-mail:xjf@mail.nisac.gov.cn;丁雪峰(1974-),男,博士,讲师,主要研究方向为计算机网络,E-mail:dingxf@scu.edu.cn(通信作者);司成祥(1982-),男,博士,工程师,主要研究方向为网络与信息安全;张 伟(1985-),男,博士,工程师,主要研究方向为网络与信息安全。

方案无密钥分发的优势和基于身份签名方案的隐式认证的优势。该无证书签名的验证结果是对应于签名者公钥的一个常数。基于此无证书签名方案以及提出的账户索引的概念，我们提出了一个匿名认证协议，协议满足条件隐私保护、认证性以及不可否认性。

本文第 2 节介绍背景知识；第 3 节介绍无证书签名方案；基于该签名方案，第 4 节提出匿名认证协议；第 5 节讨论其安全性及效率；最后总结全文。

2 背景知识

本节介绍一些背景知识，包括双线性对和一个困难问题假设的定义。

假定 q 为一个大素数(如 160 比特)，群 G_1 为由生成元 P 生成的 q 阶加法群，G_2 为 q 阶乘法群。双线性对 $e:G_1\times G_1\rightarrow G_2$ 为具有如下性质的映射[18]：

(1)双线性性：对任意 $P,Q\in G_1$ 和 $a,b\in Z_q^*$，有 $e(aP,bQ)=e(P,Q)^{a,b}$；

(2)非退化性：$e(P,P)\neq 1$，1 是 G_2 的单位元，若 P 为 G_1 的生成元，则 $e(P,P)$ 是 G_2 的生成元；

(3)可计算性：对任意 $(P,Q)\in G_1\times G_1$，存在有效多项式算法计算 $e(P,Q)$。

典型地，G_1 是由定义在有限域 F_p 上的椭圆曲线 E/F_p 上的点构成的 q 阶子群，p 为满足 $q\mid p(p-1)$ 的大素数，G_2 为扩域 F_{p^a} 上的 q 阶乘法子群。可以通过修改 Weil 对[17]和 Tate 对[18]来构造以上的双线性对。

给定一个素数阶 q 的群 G_2，其生成元为 P，假设以下定义在群 G_2 上的问题在多项式时间内是不可解的[19]。

离散对数问题 DLP (Discrete Logarithm Problem)：定义 G_2 上的离散对数问题为，给定 $g,y\in G_2$，解出 $r\in Z_q^*$ 以满足等式 $y=g^r$。

3 无证书签名方案

本节介绍无证书签名方案，它是我们构造 VANET 上匿名认证协议的基础。我们的无证书签名方案由 4 个子算法构成：初始化、提取、签名和验证，具体描述如下。

3.1 初始化

在这个阶段，传输管理中心 TRC(Transportation Regulation Center)扮演半可信密钥生成中心 KGC (Key Generation Center)的角色，负责产生和发布系统公开参数。给定安全参数 k，TRC 执行以下步骤：

1)按照第 2 节的定义产生参数$\{e,E/F_p,q,G_1,G_2,P\}$；

2)随机选取 $s\in Z_q^*$ 作为系统主密钥，设置 $P_{pub}=\{P_{pub}^1,P_{pub}^2\}=(sP,s^{-1}P)$作为系统的公钥；

3)选取两个 Hash 函数 $H_1:\{0,1\}^*\rightarrow Z_q^*$ 和 $H_2:\{0,1\}^*\times G_2\rightarrow Z_q^*$；

4)公布系统参数：$\{e,E/F_p,q,G_1,G_2,P,P_{pub},H_1,H_2\}$，而主密钥 s 保密。

3.2 提取

在这个阶段，产生用户的公私钥。该阶段由以下 4 个步骤构成。

1)产生用户部分私钥

假设 $ID\in\{0,1\}^*$ 是 U_{ID} 用户的身份标识。TRC 产生用户 U_{ID} 的部分私钥 $S_{ID}=\{S_{ID}^1,S_{ID}^2\}=(sH_1(ID)P,sH_1(ID))$，并通过安全信道发送给 U_{ID}。

2)产生用户部分公钥

TRC 产生用户 U_{ID} 的部分公钥 $P_{ID}=s^{-1}H_1(ID)^{-1}P$，并发送给 U_{ID}。

3)产生用户私钥

U_{ID} 随机选取 $x_{ID}\in Z_q^*$，并计算 $SK_{ID}=(SK_{ID}^1,SK_{ID}^2)=(x_{ID},S_{ID}^1,x_{ID},S_{ID}^2)=(x_{ID},sH_1(ID)P,x_{ID}sH_1(ID))$。$SK_{ID}$ 为用户的私钥。

4)产生用户公钥

U_{ID} 计算其完整公钥 $PK_{ID}=(PK_{ID}^1,PK_{ID}^2)=(x_{ID}H_1(ID)P,x_{ID}^{-1}P_{ID})=(x_{ID}H_1(ID)P,x_{ID}^{-1}s^{-1}H_1(ID)^{-1}P)$。可以通过验证等式 $e(PK_{ID}^1,PK_{ID}^2)=e(P_{pub}^2,P)$来验证公钥是否正确。

3.3 签名

U_{ID} 利用私钥 SK_{ID} 对消息 $m\in\{0,1\}^*$ 签名，步骤如下：

1)随机选取 $r\in Z_q^*$ 并计算 $R=rP\in G_1$；

2)计算 $h=H_2(m,R)$和 $S=(r+h)^{-1}SK_{ID}^1$；

U_{ID} 对消息 m 的签名为 $\sigma=(S,R)$。

3.4 验证

给定签名者的公钥，验证者通过下列步骤验证对消息 m 的签名 $\sigma=(S,R)$是否正确：

1)计算 $h=H_2(m,R)$；

2)检查等式 $e(S,R+hP)=e(PK_{ID}^1,P_{pub}^1)$是否成立。

若以上等式成立，则签名正确，否则拒绝接受该签名。

我们可以发现：

$$\begin{aligned}e(S,R+hP)&=e((r+h)^{-1}SK_{ID}^1,(r+h)P)\\&=e(x_{ID}sH_1(ID)P,P)\\&=e(x_{ID}H_1(ID)P,sP)\\&=e(PK_{ID}^1,P_{pub}^1)\end{aligned}$$

而对应于每个用户的公钥，$e(PK_{ID}^1,P_{pub}^1)$是一个常量。

4 VANET 上的匿名认证协议

本节给出我们构造的 VANET 上的匿名认证协议。在协议中，OBU 是能被 RSU 匿名认证的，RSU 可以被 OBU 认证。在它们的认证过程中，RSU 和 OBU 之间会产生一个安全会话密钥，可以将其用于以后它们之间的安全通信中。

4.1 系统模型

在本协议中存在 3 种类型的参与者：传输管理中心 TRC、路旁固定通信单元 RSUs、车载移动通信单元 OBUs。

1)传输管理中心 TRC：其扮演注册中心和部分密钥生成中心的角色，负责 RSUs 和 OBUs 的注册，以及帮助 RSUs 和 OBUs 产生其部分公私钥。TRC 管理一个 OBUs 的账户列表。TRC 是半可信的。

2)RSU：其是安装在路旁关键位置的固定通信单元。它在 TRC 的帮助下产生自己的公私钥。RSU 向 TRC 请求获得 OBUs 的账户列表。它可以与 OBUs 进行认证通信。

3)OBU：其是安装在车辆上的无线通信单元。OBU 在 TRC 的帮助下产生其公私钥，与 RSU 或其他 OBU 进行认证通信。

4.2 协议描述

我们的匿名认证协议基于第 3 节的无证书签名方案，协

议由 3 个阶段构成：初始化、注册和认证。

1)初始化

在这个阶段，给定安全参数 k，TRC 产生系统公私钥对 (P_{pub},S)，设置 $g=e(p,p)$，并发布系统公开参数$\{e,E/F_p,q,G_1,G_2,P,g,P_{pub},H_1,H_2\}$，方法同第 3 节。

2)注册

在这个阶段，TRC 扮演注册中心的角色。RSU 和 OBU 向 TRC 发送注册请求，然后在 TRC 的帮助下产生它们的公私钥，方法同第 3 节。

假设 RSU 的公私钥对为(PK_{RSU},SK_{RSU})，满足：

$$PK_{RSU}=(PK^1_{RSU},PK^2_{RSU})$$
$$=(x_{RSU}H_1(ID_{RSU})P,x^{-1}_{RSU}s^{-1}H_1(ID_{RSU})^{-1}P)$$
$$SK_{RSU}=(SK^1_{RSU},SK^2_{RSU})=(x_{RSU}S^1_{RSU},x_{RSU}S^2_{RSU})$$
$$=(x_{RSU}sH_1(ID_{RSU})P,x_{RSU}sH_1(ID_{RSU}))$$

假设 OBU 的公私钥对为(PK_{OBU},SK_{OBU})，满足：

$$PK_{OBU}=(PK^1_{OBU},PK^2_{OBU})$$
$$=(x_{OBU}H_1(ID_{OBU})P,x^{-1}_{OBU}s^{-1}H_1(ID_{OBU})^{-1}P)$$
$$SK_{OBU}=(SK^1_{OBU},SK^2_{OBU})=(x_{OBU}S^1_{OBU},x_{OBU}S^2_{OBU})$$
$$=(x_{OBU}sH_1(ID_{OBU})P,x_{OBU}sH_1(ID_{OBU}))$$

在本阶段 TRC 为每个 OBU 产生一个秘密账户 Acc_{OBU}，Acc_{OBU}是一个 3 元组$\langle Ind_{OBU},ID_{OBU},Inf_{OBU}\rangle$。$Ind_{OBU}$ 表示 OBU 的账户索引，并且 $Ind_{OBU}=e(PK^1_{OBU},P^1_{pub})$。所以 Ind_{OBU}的值是对应于 OBU 公钥的一个常数。ID_{OBU}是 OBU 的身份标识。Inf_{OBU}记录了与 OBU 的账户 Acc_{OBU}有关的信息，例如其帐目信息，它发送的交通信息，它请求和接受的服务信息等。TRC 为所有的 OBU 账户管理一个账户列表 AL (Account List)。当一个新的 OBU 注册时，它的账户会加入到 AL 中。如果一个 OBU 注销了，其账户也会从 AL 中被删除。TRC 将 AL 通过安全信道发送给 RSU。

TRC 载入两个预先设定的函数：一个 Hash 函数 $H_3:\{0,1\}^*\times G_2\rightarrow\{0,1\}^{l(k)}$和一个消息认证码函数 $MAC_{(\cdot)}()$。

3)认证

在这个阶段 OBU 和 RSU 进行相互认证，由以下 4 个步骤组成。

第 1 步

(1)OBU 随机选取 $r\in Z_q^*$ 并计算 $R=rP,R'=rPK^2_{RSU}$；

(2)OBU 取得当前登录设备的时间戳 T，并计算 $h=H_2(T,ID_{OBU},ID_{RSU},R)$；

(3)OBU 计算 $S=(r+h)^{-1}SK_{OBU}$；

(4)OBU 计算安全会话密钥 $\kappa=H_3(ID_{OBU},ID_{RSU},R)$；

(5)OBU 发送服务请求 $Req=\{R',S,T,ID_{RSU}\}$给 RSU。

第 2 步

当 RSU 收到请求信息 $Req=\{R',S,T,ID_{RSU}\}$时，它首先检查时间戳 T 的有效性。如果 T 无效，则 RSU 拒绝该请求。否则，RSU 计算下列值，并回复 OBU 的请求：

(1)RSU 计算 $R=R'\cdot SK^2_{RSU}$；

(2)RSU 计算 $h=H_2(T,ID_{OBU},ID_{RSU},R)$；

(3)RSU 计算 OBU 的账户索引 $Ind_{OBU}=e(S,R+hP)$；

RSU 从列表 AL 中搜索 Ind_{OBU}。如找到一个对应的条目$\langle Ind_{OBU},ID_{OBU},Inf_{OBU}\rangle$，则返回对应的身份标识 ID_{OBU}；否则，拒绝并关闭此会话。

(4)RSU 计算会话密钥 $\kappa=H_3(ID_{OBU},ID_{RSU},R)$；

(5)RSU 计算 $MAC_\kappa(ID_{OBU},ID_{RSU})$并将其发送给 OBU。

第 3 步

OBU 计算 $\kappa=H_3(ID_{OBU},ID_{RSU},R)$，并验证 $MAC_\kappa(ID_{OBU},ID_{RSU})$的完整性。如果结果是负值，OBU 将结束此会话。否则，OBU 成功认证了 RSU。

经过认证后，RSU 和 OBU 可利用会话密钥进 κ 行安全通信。

5 协议分析

本节将对协议的安全性和性能进行分析。

5.1 安全性分析

从以下几个方面分析协议的安全性。

(1)OBU 匿名

在我们的协议中 OBU 匿名性指除了参与协议的 OBU 和 RSU，任何第三方(包括 TRC)1)不能将特定会话与参与协议的 OBU 相关联；2)不能将两个不同的会话与参与协议的同一 OBU 关联。

注意到协议旨在提供抗恶意敌手(包括 TRC)的 OBU 匿名性。根据协议描述，$Ind_{OBU}=e(PK^1_{OBU},P^1_{pub})$用于标识参与协议的 OBU。而在协议中要计算出 Ind_{OBU}必须恢复 $R=R'\cdot SK^2_{RSU}$。在没有 SK^2_{RSU}的信息的情况下计算 Ind_{OBU}，其困难性相当于解 DLP 问题。任何敌手(包括 TRC)都没有关于 SK^2_{RSU}的任何信息，这就使其(包括 TRC)即使能复制一份帐号列表，也不能计算 Ind_{OBU}，也不能验证签名，因此条件 1)是满足的。

因为 R,R'都是基于随机数来计算的，所以不同的会话会产生不同的请求信息 $Req=\{R',S,T,ID_{RSU}\}$，进而产生不同的会话密钥 κ。因此 $MAC_\kappa(ID_{OBU},ID_{RSU})$是不同的。所以，条件 2)成立。

(2)OBU 不可否认性

我们的协议是基于无证书签名的，而 OBU 发送的签名信息可以作为 RSU 防止 OBU 抵赖的证据。因此协议满足 OBU 的不可否认性。

(3)条件隐私保护

因为协议满足 OBU 匿名性，所以 OBU 在协议中能得到隐私保护。一旦存在纠纷，RSU 就可以通过其保存的签名证据来追踪 OBU 的身份。

(4)相互认证性

在协议中，OBU 通过验证消息认证码 $MAC_\kappa(ID_{OBU},ID_{RSU})$的完整性来认证 RSU；$R$ 是由 OBU 选取随机数 r 计算得到的，而只有 RSU 能够利用其私钥 SK^2_{RSU}从 R'恢复出 R。因此，$\kappa=H_3(ID_{OBU},ID_{RSU},R)$是 OBU 和 RSU 之间共享的密钥。因协议满足 OBU 匿名性，ID_{OBU}是 OBU 和 RSU 之间共享的另一条秘密信息。RSU 能通过发送 $MAC_\kappa(ID_{OBU},ID_{RSU})$表明其掌握秘密信息 ID_{OBU}和会话密钥 κ。

RSU 通过验证 OBU 的签名来认证其身份。我们的无证书签名存在不可伪造性，则没有任何敌手(包括 TRC)能伪装成 OBU。

因此 RSU 与 OBU 之间实现了互相认证。

(5)抗重放攻击

为了抵抗重放攻击，在协议中添加了时间戳。RSU 通过验证 OBU 发送的信息中时间戳的新鲜性来验证是否存在重放攻击。因为 OBU 和 RSU 利用新鲜的会话密钥 κ 构造 $MAC_\kappa(ID_{OBU},ID_{RSU})$，因此 OBU 能验证 RSU 的回复信息

$MAC_\kappa(ID_{OBU}, ID_{RSU})$是否是被重放的。

(6)会话密钥安全性

我们可看出 $R=rP$ 是 OBU 和 RSU 之间共享的秘密值。因此,会话密钥 $\kappa=H_2(ID_{OBU}, ID_{RSU}, R)$也只能由 OBU 和 RSU 共享。RSU 通过返回 $MAC_\kappa(ID_{OBU}, ID_{RSU})$来确认。敌手唯一能获得此会话密钥的途径是离线猜测。敌手构造 $MAC_{\kappa'}(ID_{OBU'}, ID_{RSU})$,然后与 RSU 的回复信息 $MAC_\kappa(ID_{OBU}, ID_{RSU})$比较。假设$|ID_{OBU}|=2$kB,$|\kappa|=160$bit,则一个每秒能计算 10 亿次 Hash 运算的敌手需 2.29×2^{120}年才能获得该会话密钥。因此我们构造的会话密钥是安全的。

5.2 性能分析

本节将我们的协议与 Lin 等人的基于身份的协议[3]、Xiong 等人的基于证书的协议[14]做性能比较。这些协议是仅有的对 V2R 安全通信具体实施的 3 个协议。

在比较计算性能时,我们采用 MIRACL[15]中密码操作的运行时间作为比较依据。假设服务器平台采用带有 512M bytes 内存和 Windows XP 操作系统的 PIV 3 GHZ 处理器。而移动通信单元采用 206 MHz StrongARM 处理器。如果服务器的密码操作运行时间用 ts 来表示,则用户端的密码操作运行时间为 $tc=ts\times2100/206$[16]。对于基于双线性对的协议,为了达到 1024 比特 RSA 相同等级的安全性,我们采用定义在超椭圆曲线 $E/F_p: y^3=x^3+x$(其内置阶 embedding degree 为 2)上的 Tate 对。q 为 160 比特的 Solinas 素数,$q=2^{159}+2^{17}+1$,p 为 512 比特的素数满足 $p+1=12pr$。

密码操作的运行时间如表 1 所列,其中 *Pairing* 表示双线性对运算,*Sca-Mul* 表示 G_1 上的标量乘运算,*Exp* 表示 G_2 上的指数运算。

表 1 不同平台上各种密码操作运行时间(单位:毫秒)

	Sca-Mul	Exp	Pairing
服务器端	0.83	11.20	20.01
用户端	8.46	114.17	203.99

我们假设 RSUs 采用服务器端的平台,而 OBUs 采用客户端的平台。在 Lin 等人的基于身份的协议中,OBU 的签名需要 2 个 G_2 上的指数运算,RSU 的验证需要 2 个 G_1 上的标量乘运算、2 个 G_2 上的指数运算和 1 个双线性对运算;在 Xiong 等人的协议中,OBU 的签名需要 3 个 G_2 上的 2 个指数运算,RSU 验证需要 4 个双线性对运算;在我们的协议中,OBU 签名需要 3 个 G_1 上的标量乘运算,RSU 验证需要 2 个 G_1 上的标量乘运算和 1 个双线性对运算。3 个协议需要的运算开销比较如表 2 所列。

表 2 3 个协议的计算开销比较(单位:毫秒)

协议	签名	验证
Lin 等人的协议	228.34	44.07
Xiong 等人的协议	342.51	80.04
我们的协议	25.38	21.67

由于在 VANET 中,OBU 是移动的通信单元,其计算资源是有限的,因此当我们考虑这些认证协议的性能时,主要考虑 OBU 计算开销。通过表 2,我们得到新协议 OBU 的计算开销是 Lin 等人的协议的 11.11%,新协议 OBU 的计算开销是 Xiong 等人的协议的 7.41%。因而我们的协议大大减少了计算开销,因此更适用于 VANET。

结束语 本文为 VANET 通信提出了一个安全的匿名认证协议。我们的匿名认证协议是基于无证书签名方案,因此具有无需公钥证书和无需密钥分发的优势。我们的协议满足匿名认证性、条件隐私保护性、抗重放攻击、相互认证性等。在协议中还能在通信双方之间建立安全会话密钥。与相同安全级别的同类型协议比较,我们的协议效率明显提高,因此非常适合于车载自组织网络。

参 考 文 献

[1] 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

[2] Misener J A. Vehicle- infrastructure integration(VII)[J]. Intellimotion, 2005, 11(2): 1-3

[3] Lin X, Sun X, Ho P-H, et al. GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications[J]. IEEE Transactions on Vehicular Technology, 2007, 56(6): 3442-3456

[4] Lin X, Lu R, Zhang C, et al. Security in Vehicular Ad Hoc Networks[J]. IEEE Communications Magazine, 2008, 46(4): 88-95

[5] Lin X, Sun X, Wang X, et al. TSVC: Timed Efficient and Secure Vehicular Communications with Privacy Preserving[J]. IEEE Transactions on Wireless Communications, 2008, 7(12): 4987-4998

[6] Lu R, Lin X, Zhu H, et al. ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications[A]// The 27th IEEE International Conference on Computer Communications, 2008[C]. Phoenix, Arizona, USA: Springer-Verlag, 2008: 15-17

[7] Zhang C, Lin X, Lu R, et al. RAISE: An Efficient RSU-aided Message Authentication Scheme in Vehicular Communication Networks[A]// IEEE International Conference on Communications (ICC'08), 2008[C]. Beijing, China: Springer-Verlag, 2008: 19-23

[8] 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

[9] Xi Y, Sha K, Shi W, et al. Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks[A]// Eighth International Symposium on Autonomous Decentralized Systems (ISADS'07), 2007[C]. New york: Springer-Verlag, 2007: 344-351

[10] Mak T K, Laberteaux K P, Sengupta R. A Multi-Channel VANET Providing Concurrent Safety and Commercial Services[A]// Proceedings of 2nd ACM International Workshop on Vehicular Ad Hoc Networks, 2005[C]. Cologne, Germany: Sringer-Verlag, 2005: 1-9

[11] Raya M, Hubaux J P. The security of vehicular ad hoc networks [A]//3rd ACM workshop on Security of ad hoc and sensor networks, 2005[C]. New York: Springer-Verlag, 2005: 11-21

[12] Xu Q, Mak T, Ko J, et al. Medium Access Control Protocol Design for Vehicle-Vehicle Safety Messages[J]. IEEE Transactions on Vehicular Technology, 2007, 56(2): 499-518

[13] Hubaux J P, Capkun S, Jun L. The Security and Privacy of Smart Vehicles[J]. IEEE Security and Privacy Magazine, 2004, 2(3): 49-55

[14] Xiong Hu, Qin Zhi-guang, Li Fa-gen. Secure Vehicle-to-roadside Communication Protocol Using Certificate-based Cryptosystem [J]. IETE Technical Review, 2010, 27(3): 214-219

(下转第 173 页)

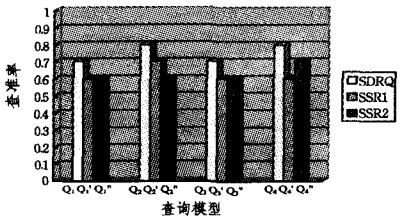

图 6 查准率

综上可以看出，本文提出的方法在权重分配和语义距离评估方面是合理的。一方面，通过对查询及 RDF 的预处理，可以在很大程度上减少由于查询松弛及同源词替换导致的时间性能上的不足，另一方面，在查准率以及查全率上，本文的方法均有良好的表现。

结束语 为了解决 RDF 查询返回结果为空或少量的问题，本文提出基于语义的 RDF 近似查询的处理方法。首先，初始查询通过 RDFS 蕴含规则进行松弛，之后利用权重对松弛查询进行语义选择并进行同源词替换，最后利用语义距离选取与初始查询在语义上相近的结果。在此基础上，给出基于语义的 RDF 近似查询处理的算法。实验结果表明，本文提出的方法能够为用户提高更多更为准确的查询结果，并且有较好的查询响应时间。目前 RDF 查询(包括近似查询)方法主要关注的是 RDF 显式表示的信息，基于推理机制的 RDF 查询能够抽取出 RDF 非显式表示、但能由 RDF 显式表示信息推导出的信息。未来我们将为本文提出的近似查询方法提供推理机制。

参 考 文 献

[1] Berners-Lee T, Handler J, Lassila O. The Semantic Web[M]. Scientific American, 2001, 184: 34-43

[2] Miller E, Swick R, Brickley D. Resource Description Framework RDF[C]// Recommendation, W3C. 2004

[3] Clark K G. RDF Data Access Use Cases and Requirements[C]// W3C Working Draft. March 2005

[4] Hurtado C A, Poulovassilis A, Wood P T. A relaxed approach to RDF querying[C]// Proceedings of the 5th International Semantic Web Conference. LNCS, 2006, 4273: 314-328

[5] Hurtado C A, Poulovassilis A, Wood P T. Query relaxation in RDF[J]. Journal of Data Semantics, 2008, 10: 31-61

[6] Poulovassilis A, Wood P T. Combining approximation and relaxation in semantic web path queries[C]// Proceedings of the 2010 International Semantic Web Conference. LNCS, 2010, 6496: 631-646

[7] Huang H, Liu C F, Zhou X F. Computing relaxed answers on RDF databases[C]// Proceedings of the 9th International Conference on Web Information Systems Engineering. LNCS, 2008, 5175: 163-175

[8] Andreasen T, Bulskov H, Knappe R. From ontology over similarity to query evaluation[C]// Proceedings of the 2nd CoLogNETElsNET Symposium-Questions and Answers: Theoretical and Applied Perspectives. 2003: 39-50

[9] Maedche A, Staab S. Measuring similarity between ontologies [C]// Proceedings of the 13th International Conference on Knowledge Engineering and Knowledge Management. LNCS, 2002, 2473: 251-263

[10] Guo Y, Pan Z, Hein J. An evaluation of knowledge base systems for large OWL datasets[C]// Proceedings of the 3rd International Semantic Web Conference. LNCS, 2004, 3298: 274-288

[11] Jena S D B[OL]. http://jena.hpl.hp.com/wiki/SDB

[12] Zhu L, Ma Q, Liu C N. Semantic-distance based evaluation of ranking queries over relational databases[J]. Journal of Intelligent Information Systems, 2010, 31: 415-445

(上接第 151 页)

[13] Boneh D, Crescenzo G, Ostrovsky R, et al. Public key encryption with keyword search[C]// Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt'04). 2004: 506-522

[14] Abdalla M, Bellare M, Catalano D, et al. Searchable Encryption Revisited: Consistency Properties, Ration to Anonymous IBE, and Extensions[C]// Proceedings of International Cryptology Conference (CRYPTO'05). LNCS 3621, 2005: 205-222

[15] Hwang Y H, Lee P J. Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-User System[C]// Proceedings of International Conference on Pairing-Based Cryptography(Pairing'07). LNCS 4575, 2007: 2-22

[16] Yang Y J, Bao F, Ding X H, et al. Multiuser private queries over encrypted databases[J]. Journal of Applied Cryptography, 2009, 1(4): 309-319

[17] Yang Y J, Lu H B, Weng J. Multi-user private keyword search for cloud computing[C]// Proceedings of Third IEEE International Conference on Cloud Computing Technology and Science (CloudCom'11). 2011: 264-271

[18] DARPA Information Science and Technology Study Group. Privacy with security[R]. Technical report. http://www.cs.berkeley.edu/-tygar/papers/ISAT-final- briefing.pdf, 2002-12

[19] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing[J]. Journal of Cryptology, 2004, 17(4): 297-319

[20] Zhu R, Yang G M, Wong D. An efficient identity-based key exchange protocol with KGS forward secrecy for low-power devices[C]// Proceedings of Internet and Network Economics First International workshop (WINE'05). LNCS 3828, 2005: 500-509

(上接第 155 页)

[15] Shamus Software Ltd., Miracl library [OL]. http://www.shamus.ie/index.php? page=home

[16] Ren K, Lou W, Zeng K, et al. On broadcast authentication in wireless sensornetworks[J]. IEEE Trans. on Wireless Commun., 2007, 6(11): 4136-4144

[17] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[A]// CRYPTO 2001, 2001[C]. New York: Springer-Verlag, 2001: 213-229

[18] Barreto P, Kim H, Bynn B, et al. Efficient algorithms for pairing-based cryptosystems[A]// CRYPTO 2002, 2002[C]. New York: Springer-Verlag, 2002: 354-368

[19] Bao F, Deng R H, Zhu H. Variations of Diffie-Hellman problem [A]// Proc. ICS, 2003[C]. New York: Springer-Verlag, 2003: 301-312