FAPP:一个基于浮动车的 VANETs 隐私保护协议

杨 涛 王亚坤 葛云峰 林 宇
(清华大学生命科学学院 北京 100084)
(国家蛋白质科学研究(北京)设施清华大学基地 北京 100084)

摘 要 车辆自组网(VANETs)是一种物联网在智能交通领域的重要应用形态,近年来已经成为了学术界和工业界的共同研究重点。VANETs 具有诱人的发展前景,但其应用受到安全性和隐私保护的严格制约,因此有关 VANETs 的安全性和隐私保护的文献逐渐成为研究的一个热点,涌现了一大批研究成果,对 VANETs 的实用化具有重要意义。针对车-车(V2V)通信的隐私保护,基于城市交通的浮动车辆,设计了一个可追溯身份隐私保护协议:FAPP。FAPP 采取浮动车辅助成群隐私保护技术:浮动车 F 联合周边车辆自发形成一个群组,F 作为组长,负责认证组员有效性、颁发组密钥和规定组参数;F 将组员秘密发送给自己的消息匿名化处理后,用组密钥对称加密后再转发给其它组员或者其它组。必要时,TRC 能准确定位消息的产生者。安全性和性能分析表明该协议能够很好地满足 VANETs 中车-车通信下条件隐私保护的目标。据我们所知,这是第一个基于城市交通浮动车成群技术的 VANETs 隐私保护协议。

关键词 车辆自组网,浮动车,隐私保护,车辆单元,路边单元,车路通信,车车通信
中图法分类号 TP309 **文献标识码** A

FAPP:A Float-car-aided Privacy-preserving Authentication Protocol for VANETs

YANG Tao WANG Ya-kun GE Yun-feng LIN Yu
(School of Life Sciences, Tsinghua University, Beijing 100084, China)
(Tsinghua University Branch of China National Center for Protein Sciences Beijing, Beijing 100084, China)

Abstract VANETs are one of the most important Internet of Things(IoT) applications in the intelligent transportation field. VANETs have attractive prospects for development. The research about security and privacy of VANETs is becoming a hot spot, and there has been a large number of research results. Using a float-car-aided group forming method, we proposed a float-car aided privacy-preserving communication protocol for VANET(FAPP). In FAPP, the float car F forms a group G which members are the vehicles around it. As a group leader, F takes charge of the verification of the member car through the revocation list from the transportation regulation center(TRC). F generates the session key and determines the configuration for the group, too. F can anonymize the message from the group member, and then send it to other group members or other group leader after inserting a corresponding trace entry into the trace log. If required, trace execution department(TED) can trace out the disputed message's real signer with the cooperation of the TRC. Comparison with other existing schemes in the literature has been performed to show the efficiency and applicability of our scheme and can match the VANET conditional privacy protecting objects well through security analysis.

Keywords VANETs, Float car, Privacy protecting, OBU, RSU, V2I, V2V

1 引言

伴随着 VANETs 快速实用化的号角,如何对 VANET 实施有效的安全保障已经成为一个至关重要的问题,这不仅关系到道路交通的通行效率,而且是关系到生命财产安全、生死攸关的大事。例如,如果攻击者在 VANETs 中注入并不存在的交通事故报告。如果缺乏实用和有效的隐私保护措施,VANETs 系统将面临隐私相关的各种攻击,举步维艰,乃至全面崩溃的巨大危险。因此,文献[1]进一步指出:"隐私保护对信息社会的重要程度堪比环境保护对物理世界的重要程度一样"。

具体说来,由于 VANETs 一般需要认证提供信息的车辆以及保护其所提供信息的完整性(不被篡改),因此在认证的同时,用户将面临如下隐私信息泄漏、隐私权被侵害的危险:

(1)在认证中,某个车辆节点的隐私,如身份、位置等可能被泄漏,因而需要具有隐私保护功能的认证措施,并且为防止虚假信息的攻击,还需要置信元件和防篡改设备(利用预防篡改的硬件以及固件来储存敏感的加密材料以及执行加密操作)。

(2)车辆是一种特殊的私人物品[2],会在一个相当长的时段中陪伴在车主身边,并可能记录下大量的个人信息,而且车辆在很多社会中是一种社会地位的象征,许多个人行为模式

本文受国家自然科学基金项目(61170263,61003230)资助。
杨 涛(1976-),男,博士生,主要研究方向为高性能计算、特殊数字签名技术、车辆自组网安全和隐私保护等,E-mail:ytao@pku.edu.cn。

也可以通过车辆驾驶者的驾驶行为进行推断。

(3)随着定位系统和基于位置服务的普及,完全可以采集到驾驶者的驾车运动模式:当车辆在一个独立的系统中通信时,上述问题还不是很严重;但当大量电子收费系统、运维系统、软件和媒体下载、离线定位系统甚至 Internet 接入时,车辆之间的连接将更加紧密。因此,这种隐私泄露将具有更广泛和更深远的影响。

VANETs 隐私保护领域的先驱者 Raya 曾指出:"VANETs 能否被接受和推广,安全和隐私保护起着关键性(crucial)的作用[3]"。为此,迫切需要对 VANETs 隐私保护进行全面和系统的研究。从汽车制造商角度来看,隐私保护更是一个非常重要的话题,其好坏程度是消费者购车的一个决定性因素。

近年来 VANET 安全和隐私保护的研究越来越得到重视,成为一个研究热点区域,但总的说来,对 VANET 的隐私保护方面的研究还是非常有限,起步也比较晚,属于较新的具有潜质的研究领域。

本文充分挖掘 VANETs 的特点和需求,紧紧围绕 VANET 中的车辆身份隐私保护问题,基于城市交通的浮动车辆(float car),设计了一个可追溯通信隐私保护协议:FAPP。FAPP 是一个用于车-车通信的隐私保护协议,主要用于路边单元没有覆盖的区域和拥堵路段的场景。

2 定义

本文涉及的若干定义列举如下:

定义 1 车辆自组网(Vehicular Ad hoc network,VANETs):其是移动自组网和传感器网技术在交通运输领域的具体应用,通过车与车之间的相互通信(Vehicle-to-Vehicle Communication,V2V)以及车与路边节点相互通信(Vehicle-to-Infrastructure Communication,V2I)来构建一个自组织的、分布式、部署方便、费用低廉、结构开放的车辆间通信网络。在实际实现中,V2V 一般都采用专门为车-车动态高速通信设计的协议 DSRC[4,5] 来实现。

定义 2 条件隐私(conditional privacy):其指通常情况下保护用户隐私信息,但发生事故或纠纷时,可以由权威仲裁方授权开启对肇事者真实身份的追溯过程,并据此实施仲裁和处罚。一般而言,VANET 中安全相关应用涉及的隐私保护都必须是条件隐私,这也是各国交通安全管理的实际需要[7],能有效威慑和惩罚肇事者,切实保证人们生命财产的安全。

定义 3 浮动车(float car):浮动车辆[8,9]主要是指出租车、公交车、巡逻警车、运输车等长期在路面上行驶(出行率高)的车辆,由于其拥有的公用性质,其位置隐私对浮动车而言可以适当放松。浮动车系统具有建设周期短、投资少、覆盖范围大、精度高、实时性强等优势[10]。一般而言,装备了 GPS 和通信等设备的浮动车可以作为城市交通实时统计预测的一种风向标,据相关文献估计,浮动车比率为 1.5%~3%就能很精确地反映整个城市交通的全貌[11,12](截止 2007 年[10],北京市浮动车系统就达到了约 7000 辆出租车,占出租车总量的 1/10以上,达到北京市机动车总量的 2.5%)。因此,国内外很多大中城市都已经启用了浮动车系统,建设有一定的基础设施和采集网络,合理和充分共用浮动车系统的车辆具有很好的成本优势。

定义 4 认证授权中心(Transportation Regulation Center,TRC):其主要职能是负责整个系统的建立、授权、撤销和管理职能(类似 PKI 体制下的 CA),包含整个系统的参数设置和基础信息库(简称基础库)。

定义 5 追溯中心(Trace Execution Department,TED):其主要职能是通过对 TRC 的分权(追溯权)策略,来更好地提供面向安全应用的真实身份追溯服务,该分支需要包含辖区的追溯信息库(简称追溯库)。

定义 6 车辆单元(On-Board Units,OBU):其是部署在车辆中参与通信的嵌入式处理单元,是 VANETs 的最基础实体,相当于通信系统中的移动终端。

定义 7 路边单元(Road Side Units,RSU):其是参与 VANETs 的路边基础设施节点。RSU 使得 VANETs 除了可单独组网实现局部的通信外,还可通过 RSU 作为接入点的网关,连到后备网络(如 Internet),提供更丰富的娱乐、车内办公等服务。

3 相关工作

近年来,VANETs 隐私保护领域涌现了许多文献,提出了不少挑战性的问题和富有创造性的方案。

2004 年,Hubaux 等[13]指出了 VANETs 中的安全和隐私挑战:隐私担忧并没有阻止人们对 Internet、手机网络和电子支付的广泛接受,因此,引导比阻止更有意义。该文献引入了电子车牌作为车辆唯一识别,并指出通过部署 PKI 机制来认证每一条消息和对实体进行双向认证。

2005 年,Raya 等提出了经典的 HAB 协议[14]。主要思想是采用传统成熟的 PKI 技术,利用 TRC 颁发的大量匿名/别名证书,并通过周期性更换证书来隐藏 OBU 的真实身份和防止非法追踪。HAB 的密钥的分发、管理、存储和撤销的代价过高,适用网络规模小,实用性比较差。

2007 年,Lin 等提出的 GSB 方案[15]也是一个早期经典方案:第一次将群签名(基于 Boneh 等的短群签名[16])引入 VANET 隐私保护领域,并结合了基于身份的签名技术[17]。GSB 的优点在于 OBU 中只需要存储一个私钥和群公钥即可,不需要存储大量的假名密钥和证书;同时 TRC 可以实现车辆假名与长期身份的对应,并且 RL 很短且易于更新。GSB 的缺陷是:需要频繁更换群密钥才能撤销车辆身份,其代价过大;验证开销大,消息验证的时间和被撤销的车辆证书的数目存在线性关系,即撤销单个 OBU 验证开销至少需要两次双线性对运算,RL 较大时会导致验证时间过长而难以被实际系统所应用。

2008 年,Lu 等基于双线性对、VLR 群签名[18]和 IBC[19]提出了 ECPP 方案[20],其主要创新在于引入了"路上(on-the-fly)短期群成员证书"(简称路上证书):将 GSB 方案中群的辖区从全局缩小到每个 RSU 级别,RSU 是群首,OBU 是拥有路上证书的群成员。ECPP 还消除了密钥托管的问题。然而,ECPP 协议交互次数多,通信开销较大,还不能满足不可链接性要求;另外,ECPP 还依赖于 RSU 的广泛部署,无法适用于早期的 VANET,应用场景相对比较狭隘。

2010 年,Wasef 等提出了 DCS 方案[21],允许 OBU 按需从 RSU 申请一定数目的证书。DCS 还提出了实现跨域漫游和批验证的一些方法。但 DCS 有一个明显的弱点:恶意

OBU 可以通过交替申请，迅速获取大量假名用于攻击。即使系统识别了这些恶意 OBU，撤销其拥有的众多假名也要付出高昂的代价。

2010 年，Wu 等提出了一个专门针对 V2V 通信隐私保护的 WDG 方案[22]。WDG 基于消息相关群签名（MLGS）[23]，能根据消息关联标志符来对消息进行唯一性签名控制，这样能有效抵御 Sybil 攻击。WDG 还支持对群签名消息真正产生者的授权追溯。WDG 还是面临和 GSB 一样的撤销匹配耗时问题，不能适应实际系统的要求。

2012 年，Yang 等提出了基于单跳代理重签名技术的 TP4RS 方案[24]。该方案利用代理重签名技术克服了签名验证效率和撤销列表过大等问题，在 RSU 普及场景下（城市繁华街区）具有较好的实用性。但是，这个方案对 RSU 这种基础设施的过分依赖也是一个难以克服的问题。

4 FAPP 协议构建

本文提出了一个基于浮动车的 VANETs 隐私保护协议（Float-car Aided Privacy-Preserving communication protocol for VANET，FAPP）。FAPP 是一个针对 V2V 通信设计的可追溯隐私保护协议，基于浮动车辆辅助成群技术，用于基础设施 RSU 未覆盖，但存在浮动车辆活动的区域的隐私保护。

FAPP 协议的构建包含初始化、消息产生和验证、身份追溯和撤销等步骤。以下分别进行详细介绍。

4.1 初始化

认证中心 TRC 初始化系统，并为每个普通车辆 OBU 和浮动车辆 FOBU 建立系统参数。本协议的符号声明如表 1 所列。

表 1 符号声明表

符号	说明
TRC	认证中心
TED	追溯执行部门
RL	被撤销车辆列表
V_i	第 i 辆普通车
F_j	第 j 个浮动车辆
RID_i，PID_i	车辆 V_i 的真实 ID 和伪 ID
TRC^-，TRC^+	TRC 的私钥和公钥
TED^-，TED^+	TED 的私钥和公钥
K_i^-，K_i^+	V_i 的私钥和公钥
F_i^-，F_i^+	F_j 的私钥和公钥
H(.)	哈希函数：$H:\{0,1\}\rightarrow Zq$
Enck()	使用密钥 k 的对称加解密算法
Signk()	使用密钥 k 的公钥签名算法
HMACk()	使用密钥 k 的 HMAC 算法
T_1	TRC 中的追溯表
T_{2j}	F_j 中的追溯表
T_2	TED 中的追溯表
Params	系统公开参数

4.1.1 系统建立

给定一组双线性参数 (G_1, G_2, e, q, P)（P 是 G_1 的生成元），TRC 随机挑选 $TRC^- \in Z_q^*$ 作为 TRC 主密钥，并计算 TRC 公钥 $TRC^+ = TRC^- \cdot P$。TED 随机挑选 $TED^- \in Z_q^*$ 作为 TED 私钥并计算 TED 公钥 $TED^+ = TED^- \cdot P$。再挑选一个安全的哈希函数 $H:\{0,1\}^* \rightarrow G_1$，以及一个以 k 为密钥的安全对称算法 $Enc_k()$，一个以 k 为密钥的安全 HMAC 算法 $HMAC_k()$，一个以 k 为密钥的安全签名算法 $Sign_k()$。设置系统公共参数为 $Params = \{G_1, G_2, e, q, P, TRC^+, TED^-, H, Enc_k(), HMAC_k(), Sign_k()\}$。

4.1.2 OBU 密钥生成

每辆车都有一个真实标识 RID，设 V_i 对应拥有真实标识 RID_i，车辆公私钥对产生步骤如下：

（1）车 V_i 首先随机选择 $K^- \in Z_q^*$ 作为其私钥，并计算 $K^+ = K^- \cdot P$ 为其公钥；

（2）车 V_i 再随机选择 $t_i Z_q^*$ 来决定验证信息 $X_i: a_i = H(t_i P \| RID_i)$，$b_i = (t_i - K_i^- \cdot a_i)$。然后车 V_i 把 K_i^+，RID_i，a_i，b_i 发送给 TRC。

（3）收到 $\{K_i^+, RID_i, a_i, b_i\}$ 后，TRC 首先验证一下等式是否成立：$a_i = H(b_i P + (K_i^+)^{a_i} \| RID_i)$。如果成立，$\{K^+, RID_i\}$ 就作为合法的公钥和真实标识，否则拒绝。最后，TRC 将 $\{K^+, RID_i\}$ 存放在追溯表 T_1 中。

每辆车都预先装载系统公共参数 $Params$。并且，每一辆车 V_i 都在车内的防篡改设备中存储一个公私钥对 (K^+, K^-) 及其相关的匿名证书（TRC 根据车 V_i 的伪标识 PID_i 和公钥 K^+ 来签发）。

4.1.3 FOBU 密钥生成

每辆浮动车都有一个真实标识 RID，设 F_i 对应拥有真实标识 $FRID_i$，车辆公私钥对产生步骤如下：

（1）车 F_i 首先随机选择 $F_i^- \in Z_q^*$ 作为其私钥，并计算 $F^+ = F^- P$ 为其公钥；

（2）车 V_i 再随机选择 $t_i \in Z_q^*$ 来决定验证信息 $X_i: a_i = H(t_i P \| FRID_i)$，$b_i = (t_i - F_i^- \cdot a_i)$。然后车 V_i 把 K_i^+，$FRID_i$，a_i，b_i 发送给 TRC。

（3）收到 $\{K_i^+, FRID_i, a_i, b_i\}$ 后，TRC 首先验证一下等式是否成立：$a_i = H(b_i P + (F_i^+)^{a_i} \| FRID_i)$。如果成立，$\{F^+, FRID_i\}$ 就作为合法的公钥和真实标识，否则拒绝。最后，TRC 将 $\{F^+, FRID_i\}$ 存放在追溯表 T_1 中。

每辆浮动车都预先装载系统公共参数 $Params$。并且，F_i 在车内的防篡改设备中存储一个公私钥对 (F^+, F^-) 及其匿名证书（TRC 根据车 F_i 的伪标识 $FPID_i$ 和公钥 F_i^+ 来签发）。F_i 还需要预装入一个当前系统的 RL 及其更新分发点地址列表。RL 的更新包含如下两种可选方式：

（1）TRC 分布式分发点模式：通过加油站或交通枢纽提供的无线网络，与 RL 更新分发点进行连接和授权更新操作。图 1 给出了分布点模式下的示意图。

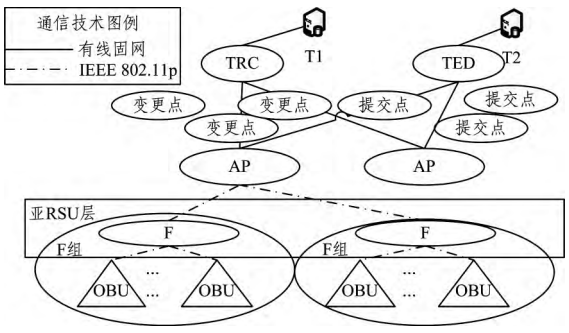

图 1 分布点模式示意图

（2）高等级 RSU 更新模式：在 TRC 授权的高等级 RSU（如加油站或警局型 RSU）辖区进行授权更新操作。图 2 给出了 RSU 模式下的示意图。

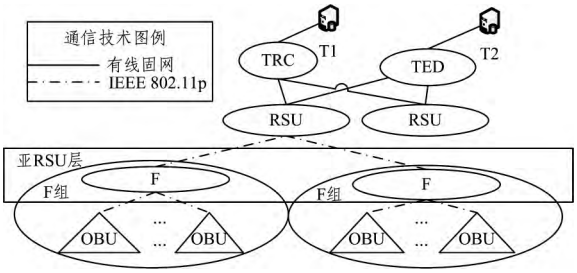

图 2　RSU 模式示意图

4.1.4　RSU 密钥生成

这是一个可选步骤，如果系统选择 TRC 分布式分发点模式和 TED 分布式接收点模式，RSU 密钥生成在本方案中就可以不存在。

TRC 为每一个所属的坐落在地点 L_j 的 RSU_j 随机挑选 $K^-_{RSU_j} \in Z_q^*$，然后计算 $K^+_{RSU_j} = K^-_{RSU_j} P$，并通过秘密渠道将这个公私钥对（$K^+_{RSU_j}$，$K^-_{RSU_j}$）发送给相应的 RSU_j。RSU 的主要作用是向浮动车辆提供撤销列表的安全更新和接受追溯信息的安全提交。

4.1.5　以 FOBU 为组长构建群组

以 FOBU 为组长构建群组的过程可进一步分为 3 个子过程：

（1）FOBU 广播 *Hello* 报文：假定 F_j 定期（如 1 秒钟）给其辖区内的 OBU 广播 $Hello=[R_j \| K^+_{F_j} \| D]$（$R_j$ 是 F_j 给自己产生的一个随机数，代表群的权重因子，D 是代表 F_j 当前的行驶方向）。

（2）OBU 加入群组声明：在收到 FOBU 的广播包后，且判断 FOBU 的方向和本车方向一致的前提下（否则可以认定是逆方向开来的浮动车，群组生命期只能维持在极其短暂的错车时间，这样加入群组就几乎没有意义了），启动加入群组的算法得到 V_i 给 F_j 发送加入群组声明 $M'=[KT_iTED^+ \| Timestamp \| K_i^+]$，具体过程参见算法 1。

（3）FOBU 接受加入确认：F_j 给 V_i 发送接受加入的群组参数报文 M''，具体过程请参见算法 2。

4.2　消息产生

OBU 在产生事件消息后，需要在进行消息通告前对该消息进行可追溯处理，称为消息产生过程。FAPP 的消息产生过程可进一步分为消息产生和群内转发 2 个子过程。

算法 1　V_i 加入 F_j 群组算法

Input：

系统公共参数，Params；

OBU 私钥 K_i^-；

OBU 公钥 K_i^+；

FOBU 公钥 F_j^+

Output：

加密消息 $M'=[Timestamp \| K_i^+]$；

1. V_i 随机挑选 $r_1 \in Z_q^*$；

2. 计算一个会话密钥 $\phi = r_1 \cdot F_j^+$；

3. 计算一个暗示 $\psi = r_1 P$；

4. 构造 $M=[Timestamp \| K_i^+]$；

5. 计算 $M'=(\psi, Enc_\phi(M))$；

6. return M'

算法 2　F_j 对 V_i 加入群组确认算法

Input：

系统公共参数，Params；

撤销列表：RL；

加密消息，M'；

Output：

群组参数报文，M''；

1. F_j 通过计算本次会话密钥 $\phi' = \psi \cdot F_j^-$，并用来解密第一步收到的消息；

2. 通过查找由 TRC 公布的撤销列表 RL，来验证公钥 K_i^+ 的有效性，如果无效则退出；

3. 如果上诉公钥有效，再验证时间戳的正确性，如果错误则退出；

4. 通过以上检查后，F_j 查看是否有现成的未过期的群共享密钥 KG_j，如果没有就随机挑选出 $KG_j \in Z_q^*$ 并构造出群密钥说明报文：$GG=[\omega \| KG_j \| Timestamp]$；

5. 计算 $M''=\phi'$，$Enc_{\phi'}(GG))$；

6. return M''

·消息产生

消息产生是生成消息及其可有效追溯的签名，这里是指 OBU 给组长 FOBU 发送带该 OBU 私钥签名的消息。OBU 签名的消息 M'（安全相关）包含 6 个域：消息标识、载荷、时间戳、F_j 的公钥、V_i 的签名、V_i 的公钥，总共 168 字节，具体格式如表 2 所列。

表 2　OBU 签名的消息格式表

消息标识	载荷	时间戳	F_j 的公钥	V_i 的签名	V_i 的公钥
2 字节	100 字节	4 字节	21 字节	20 字节	21 字节

每个域说明如下：

（1）消息标识：定义了消息的种类，长度为 2 字节；

（2）载荷：包含车辆位置、方向、速度、加/减速度、交通事件、当前时间等信息，长度为 100 字节；

（3）时间戳：消息产生时的确切时间，为了防止消息重放攻击，还能避免单一用户多次报告同一事故时被误判为 Sybil 攻击者，长度为 4 字节；

（4）F_j 的公钥：用于维持群内通信的 FOBU 的公钥（来自于上一节的 FOBU 广播），长度为 21 字节；

（5）V_i 的签名：该车 OBU 对私钥对前 4 个域的签名，长度为 20 字节；

（6）V_i 的公钥：该车 OBU 的公钥，长度为 21 字节。

V_i 的消息产生算法如算法 3 所示。

算法 3　FAPP 的 OBU 消息产生算法

Input：

系统公共参数：Params；

FOBU 公钥：F_j^+；

会话密钥：Φ；

原始消息：m；

Output：

可追溯消息：

$m''=Enc_\phi(ID \| m \| Timestamp \| F_j^+ \| \sigma \| K_i^+)$；

1. 计算 $\sigma = Sign_{K_i^+}(ID \| m \| F_j^+ \| Timetamp)$；

2. 生成 $m'=[ID \| m \| Timestamp \| F_j^+ \| \sigma \| K_i^+]$；

3. 计算 $m''=Enc_\phi(m')$；

4. return m''；

·消息群内转发

FOBU 给辖内所有 OBU 广播上述消息 m'' 即可。F_j 的消息群内转发方式分为两种模式：

（1）分离模式：这是推荐的模式，优点在于能有效节约通信带宽，适合于对实时性和效率要求高的应用。缺点是必须依赖浮动车开辟一定的追溯表空间，并能定期上报给 TED。

本模式下的算法如算法 4 所示。

(2)聚合模式:这种模式不依赖浮动车存储和上报追溯记录,追溯信息都聚合在通信消息中,缺点也比较明显,FOBU 的计算开销增大,且消息的大小被扩大了。本模式下的算法如算法 5 所示。

在分离模式下:TED 需要事先委托 TRC 为 F_j 预装入一个追溯信息提交接受点地址列表。追溯信息的提交包含两种可选方式:(1)TED 分布式接收点模式,即通过加油站或交通枢纽提供的无线网络,与追溯信息提交接受点进行连接和授权提交操作;(2)高等级 RSU 代收模式,即在 TED 授权的高等级 RSU(如加油站或警局型 RSU)辖区进行安全提交操作。

算法 4 FAPP 的消息群内转发算法(分离模式)

Input:

系统公共参数:Params;

FOBU 公钥:F_j^+;

会话密钥:Φ';

群密钥:KG_j;

加密消息:m'';

Output:

群内广播消息:

$m''=[ID \| m \| Timetamp \| HMAC_{KGj}(ID \| m \| Timestamp)]$

1:利用 Φ' 解密 m'' 得到 $[ID \| m \| Timetamp \| F_j^+ \| \sigma \| K_i^+]$;

2:将 $(H(m),\sigma)$ 二元组追加到本地的追溯表 T_{2j} 中;

3:生成 $m''=[ID \| m \| Timetamp \| F_j^+ \| HMAC_{KGj}(ID \| m \| Timestamp \| F_j^+)]$;

4:return m''';

算法 5 FAPP 的消息群内转发算法(聚合模式)

Input:

系统公共参数:Params;

FOBU 公钥:F_j^+;

TED 公钥:TED+;

会话密钥:Φ';

群密钥:KG_j;

加密消息:m'';

Output:

群内广播消息:

$m'''=[ID \| m \| Timestamp \| HMAC_{KG_j}(ID \| m \| Timestamp]$;

1. 利用 Φ' 解密 m'' 得到 $[ID \| m \| Timestamp \| F_j^+ \| \sigma \| K_i^+]$;

2. 计算出 $Tag=Sign_{TED^+}(\sigma)$;

3. 生成 $m'''=[ID \| m \| Timestamp \| F_j^+ \| HMAC_{KG_j}(ID \| m \| Timestamp \| F_j^+) \| Tag]$;

4. return m''';

4.3 消息验证

消息验证是对签名消息进行有效性验证,FAPP 中接收消息的组员用组密钥 KG_j 计算出 $HMAC_{KGj}(ID \| m \| Timestamp \| F_j^+)$,与 m''' 中的 $[HMAC_{KGj}(ID \| m \| Timestamp) \| F_j^+)]$ 比较,如果相等,就作为合法消息接收;否则直接丢弃。

4.4 追溯

如果存在一个伪造的消息 m,就必须要启动追溯来确定消息 m 的签名者的真实身份。

·分离模式的追溯

首先说明一下 TED 中的追溯表 T_2:它是由存储在浮动车辆 F_j 中的 T_{2j} 合并而成的。浮动车辆在条件成熟的场所将 T_{2j} 安全上传至 TED 中进行统一存储,传输方式有通过高等级 RSU 和 TED 分布式上传点两种可选方式,成功上传后释放本地存储空间。FAPP 在分离模式下的追溯过程依赖 FOBU 向 TED 提交本地追溯表 T_{2j} 的过程:

(1)FOBU 经过高级别 RSU,并发出提交追溯表的申请;

(2)RSU 向 FOBU 进行安全身份确认;

(3)FOBU 通过 RSU 和 TED 建立安全通道;

(4)上载 T_{2j} 到 TED 中的 T_2。

这种模式下的追溯算法如算法 6 所示。

算法 6 TED 追溯消息 m 的真实发布者(分离模式)

Input:

系统公共参数,Params;

争议消息,m;

Output:

车辆真实身份,RID_i;

1. TED 匹配公钥:TED 计算 H(m),并通过匹配追溯表 T_2 中符合(H(m),σ)的表项,得到消息的签名 σ^*。逐个利用公钥 K_i^+ 进行解密得到 m',如果 $m=m'$ 则表明找到了符合条件的 K_i^+。

2. TED 向 TRC 申请追溯 OBU:按 TED 的要求,TRC 根据通过匹配本地存储的追溯表 T_1,找到和 K_i^+ 相匹配的 RID_i;

3. return RID_i;

·聚合模式的追溯

这种模式 TED 只是逻辑上对 TRC 进行分权,并没有本地的追溯表的存在。这种模式下的追溯算法如算法 7 所示。

算法 7 TED 追溯消息 m 的真实发布者(聚合模式)

Input:

系统公共参数,Params;

争议消息,m;

Output:

车辆真实身份,RID_i;

1. TED 解密 Tag:通过提取争议消息 m 中的 Tag 部分,用 TED 的私钥对 Tag 进行解密,得到消息的签名 σ。逐个利用公钥 K_i^+ 进行解密得到 m',如果 $m=m'$ 则表明找到了符合条件的 K_i^+。

2. TED 向 TRC 申请追溯 OBU:按 TED 的要求,TRC 根据通过匹配本地存储的追溯表 T_1,找到和 K_i^+ 相匹配的 RID_i;

3. return RID_i;

4.5 身份撤销

FAPP 协议中,身份撤销是由 TRC 将恶意车辆 OBU 对应的公钥 K_i^+ 增加到撤销列表 RL 中即可。然后通过高等级 RSU 或 TRC 分布式发布点两种模式进一步下发给 FOBU,FOBU 在接收到 OBU 的加入群组申请时需要本地查找 RL 来验证 OBU 的有效性。如果该 OBU 在 RL 中,该 OBU 将无法加入群组来产生合法通信。为了增加查询速度,对撤销列表 RL 可以预先建立 Hash 表存储模式,这样查找时只需要一次 Hash 映射操作和一次字符串比较操作即可[25]。

5 协议分析

5.1 正确性分析

FAPP 的正确性由如下定理来保证。

定理 1(会话密钥定理) 公式 $\Phi'=\Phi$ 是成立的。

证明:

$\phi''=\psi F_j^-=r_1 P F_j^-=r_1(F_j^- P)=r_1(F_j^+)=\phi$

5.2 安全性分析

FAPP 协议的安全性分析主要从消息认证、隐私保护、可追溯性、抗攻击性和身份撤销等方面展开:

(1)消息认证方面：合法签名 σ（假设签名消息中包含 OBU_i 的公钥 K_i^+）的产生只能由车辆 V_i 的私钥 K_i^-（该私钥存储在 V_i 的防篡改设备中）来产生，根据数字签名的不可伪造性，敌手伪造 σ 是不可行的。F_j 管理的组用 HMAC 进行消息发布，只有拥有组密钥 GK_j 的组内成员才能构造出合法的 HMAC 群消息。

(2)隐私保护方面：共享的会话密钥 Φ 能保护在组成员 V_i 和组长 F_j 之间的通信保密性，并且，从 ψ 和 F_j^+ 中求出 Φ 是一个 CDH 问题：即给定 P，$\psi=r_1P$ 和 $F_j^+=F_j^-\cdot P$，找出 $\phi=r_1K_j^+\cdot P$ 是困难的。因此，只有和 (K_i^+,σ) 关联的 F_j 才能解开该加密消息。另外，给定一个对某消息的签名 σ，虽然 F_j 只需要用 TRC 的公钥 TRC^+ 来验证其正确性，但如果没有 TRC 的协助来追溯 σ 中消息的真实发布者，则其是一个计算性难题。

(3)可追溯性方面：(a)给定一个有争议的消息签名，只有 TRC 和 TED 合作才能利用前述追溯机制找到发布该消息的真实车辆 OBU。(b)在追溯过程中并不需要实际签名者的任何参与，而是签名消息本身，加上 TRC 和 TED 的追溯记录就具备了完整的认证信息。

(4)抗攻击能力方面：(a)抗消息伪造攻击：协议中成员车辆 V_i 对消息 m 的数字签名是不可伪造的，因此能抵抗消息伪造攻击；(b)抗消息重放攻击：协议中时间戳的应用，可以保证消息的新鲜性，能有效抵御重放消息攻击。

(5)身份撤销方面：(a)撤销的有效性：恶意车辆被发现并确认后，TRC 会公布 RL，在 FOBU 更新 RL 后，恶意车辆将不能再通过 FOBU 参与 VANET 合法通信，无法继续实施伤害；(b)撤销的及时性：撤销的及时性主要依赖浮动车中 RL 更新的及时性。RL 的更新时靠浮动车通过 TRC 分布式分发点或高等级 RSU（如警局、加油站和交通枢纽等）进行通信来获取的。基于浮动车辆的基本运动特性，加上是在城区场景下，其经过以上具备 RL 更新条件的场所的频率应该是不低的（估计至少在 1 个小时以内），所以其 RL 更新的及时性有一定的保障，也不排除有细微的误差范围，这只能靠基础设施的进一步完备来弥补。

5.3 性能分析

OBU 是一种安装在车辆上的计算、存储和通信能力都相对受限的特种设备，而 RSU 相对拥有更好的计算、存储能力和网络条件，因此我们主要针对 OBU 在各个方案中的性能开销进行了比较，这些开销的大小对方案的实用性有重要的影响。

为了使这种性能对比保持统一性和可参照性，特采纳经典的 ECPP 协议中采取的相关性能参数设置：

(1)安全参数设定：双线性对计算采用 Miyaji-Nakabayashi-Takano(MNT)曲线，$k=6$，q 为 160 位长。循环群上的元素长度为 161 位（161bits≈21Bytes）。此外，还设定其它变量均为 32 位（除素域和循环群上的元素、消息类型、组号、身份标识 ID 以外），例如时间戳等。

(2)运算开销设定：为了简化比较，按照惯例，这里我们只考虑诸如双线性对运算、点乘运算等重量级的运算，而忽略那些耗时偏少的运算，如单向 Hash 运算和对称加解密开销等；另外，按照通用做法，还可以忽略可以事先计算好的运算操作。

(3)系统参数开销设定：我们对照的所有方案都需要有一个固化的系统参数，该系统参数的开销都不算大，最多有 1 个系统公钥、加密函数和 Hash 函数的偏差，为了简化比较，突出主题和重点，在分析中都排除这部分开销。

(4)时间戳设定：我们对照的所有方案都需要使用时间戳来防止重放攻击，所以对比时间戳开销意义不大，在分析中都排除这部分开销。

(5)实验参数设定：用 T_{mul} 表示椭圆曲线上的单个标量乘法运算耗时，用 T_{exp} 表示单个幂指运算耗时，T_{par} 表示单个双线性对运算耗时。在 Intel Pentium IV3.0GHZ 机器上：设定 $T_{mul}=0.6$ms，$T_{exp}=0.46$ms，$T_{par}=4.5$ms[26-28]。假定 OBU 装备该计算能力的 CPU。

5.4 计算开销分析

假定 FAPP 采用的签名算法是 ECDSA 标准算法。

·签名操作包括：(1)OBU 签名：需要 1 个 T_{mul} 即可，即 0.6ms；(2)FOBU 匿名化签名：需要一个可忽略的轻量级 HMAC 操作即可。

·验证操作包括：(1)FOBU 验证：需要一个可忽略的 Hash 操作和 RL 比对操作，以及对 OBU 签名进行验证的 2 个 T_{mul}，合计 1.2ms；(2)OBU 验证：需要一个可忽略的轻量级 HMAC 操作即可。

OBU 常规计算（指签名和验证计算）开销对比如表 3 所列。

表 3 OBU 常规计算开销对比

方案	签名(ms)	验证(ms)
HAB	0.5	7.2
GSB	53.7	49.3
ECPP	0.6	20.1
DCS	1.2	24.3
WDG	2.76	7.26
TP^{4}RS	3	22.5
FAPP	0.6	1.2

可以看出，FAPP 协议在计算上的开销表现比较优秀，特别是在验证开销指标上。

5.5 存储开销分析

FAPP 协议的存储开销分析如下：

(1)OBU：需要存储一个私钥（21 字节）和一个公钥（21 字节），总开销为 42 字节。

(2)FOBU：除了需要存储公私钥外（共 42 字节），还需要本地存储 RL（撤销一个车辆需要加入该车的公钥 21 字节）和追溯表 T_{2j}（每个表项（H(m)，σ），其大小为 40 字节），RL 和 T_{2j} 的大小视实际情况而变化。

以北京市为例，假设 500 万辆中即使每年有 5%被撤销，其 RL 的大小约为：$500\times10^4\times5\times10^{-2}\times21=5.25\times10^6$ 字节，约 5.3M 字节，这个大小对 FOBU 而言是完全可以接受的。以浮动车最低 24 小时上传一次 T_{2j} 给 TED 为例，开辟 10M 字节的存储区就能允许 FOBU 每天处理最多 250000 左右的消息记录数目。

5.6 通信开销分析

FAPP 协议的通信开销分析如下：OBU 发出的每个消息由于密码相关操作会产生 2+21+20+21=64（字节）的额外开销。

通信开销对比如表 4 和图 3 所示。

表 4　OBU 常规计算开销对比表

方案	通信开销(字节)
HAB	137
GSB	197
ECPP	189
DCS	209
WDG	133
TP^{4}RS	85
FAPP	64

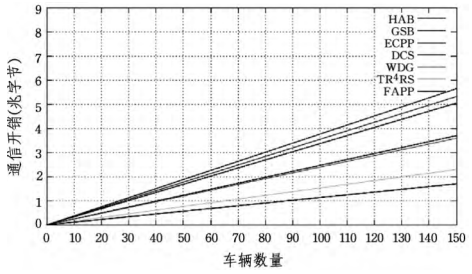

图 3　一分钟 OBU 通信负载额外开销比较图

从上述图表中可以看出，FAPP 的 OBU 通信负载开销是相对最优的，好于 HAB、GSB、ECPP、DCS、WDG、TP^{4}RS 等方案。

5.7　支持城市拥堵场景

假定拥堵场景下一般都发生在有 RSU 的重要地段，这也是很多文献的通用假设。在这些场景中，可能有数以百计的大量车辆集中在一起(设定其中有一定比例的浮动车辆存在应该是比较合理的)。

单纯以 RSU 的处理能力，即使加上批验证和聚合签名等优化技术，也难以承受如此巨大的通信和计算压力。本系统中，浮动车辆的出现可以实现一个 RSU 亚层，合理和充分利用浮动车辆的处理资源可以动态缓解拥堵场景下的性能瓶颈，有效减轻拥堵路段 RSU 所承担的压力：RSU 参照浮动车的 GPS 数据，负责统一指挥拥堵地段的浮动车辆形成一系列通信范围较小的子群组，形成一个类树状结构，以浮动车为子树管理节点，下辖一定数量的叶子节点(普通车)，进行消息预处理和消息融合，再分层分级汇报到根节点(RSU)进行广播、转发和上报等操作。

5.8　脆弱性分析

时间同步是 FAPP 协议的一个脆弱点，该协议对时间准确性的要求比较高，将存在如下问题：(1)FOBU 的时间同步问题：FOBU 本身就标配了 GPS 或国产北斗卫星导航系统，都可以用来进行授时，且覆盖面广、精度高；(2)普通 OBU 的时间同步问题，可通过年审时在 TRC 授权机构完成，也可在高等级 RSU 处完成，还可通过加入 FOBU 组群在组长 F_j 的帮助下来完成。

如果浮动车 F_j 被恶意者控制，不上传其本地存储的 T_{2j} 甚至有能力恶意删除全部或者部分，会造成追溯信息表的缺失，针对这种情况，有如下应对方法：(1)浮动车一般都有 GPS 定位功能，且 TED 能获取该信息，比对现有 RSU 的覆盖范围，如果 F_j 在非 RSU 覆盖范围内活动过，但在规定的最大时间内仍没有到 RSU 处进行 T_{2j} 的上传，TED 将视情况追究 F_j 的责任；(2)普通车辆 OBU 定期将合作过的 FOBU 的公钥序列和对应的时间范围，通过 TED 的公钥加密后通过 RSU 或无线网络上传给 TED，TED 将其作为抽检依据，对符合条件的 F_j 上传的 T_{2j} 进行小概率抽查，如果不符合将继续追查 F_j 的行为和责任；(3)TED 的追查方式主要包括：将派出调查车辆对该 F_j 进行现场检查，如果违规，则进行处理甚至吊销其资格证书；(4)如果浮动车 F_j 被恶意者控制并只是将 T_{2j} 进行窃取并试图分析，这种情况下，由于 F_j 在物理时空上已经和 V_i 接近并产生通信，因此某种意义上 V_i 当时的位置隐私已经暴露，但是其身份隐私还在 TRC 的保护范围之内。

结束语　本文介绍了一个用于 V2V 的隐私保护协议，主要用于 RSU 没有覆盖的区域和城市拥堵路段场景，其基本思想是：因为浮动车辆在城市交通中具有一定代表和覆盖作用，在基础设施 RSU 未覆盖的地域，将浮动车辆作为一种“亚 RSU”而充分利用。采取浮动车辅助成群技术：浮动车 F 利用 V2V 通信，联合在其有效通信半径内且行驶方向一致的车辆自发形成一个群组，F 作为组长，负责认证车辆有效性(通过及时更新撤销列表)、维护组密钥和规定组参数；F 和每个组员都有一个利用认证中心 TRC 颁发的匿名证书协商出的一对一秘密通道，组员将需要传播的消息先利用该通道发送给 F，F 经过消息匿名化处理后，用基于群密钥的对称加密算法加密后再转发给其它组员或者其它组。如果发生消息争议情况，追溯中心 TED 可通过和 TRC 的协作，准确定位到产生该消息车辆的真实身份。

参 考 文 献

[1] Domingo-Ferrer J. Coprivacy: an introduction to the theory and applications of co-operative privacy[J]. SORT: statistics and operations research transactions, 2011: 25-40

[2] Dotzer F. Privacy issues in vehicular ad hoc networks[C]// Privacy Enhancing Technologies. Springer, 2006: 197-209

[3] Raya M, Hubaux J P. Securing vehicular ad hoc networks[J]. Journal of Computer Security, 2007, 15(1): 39-68

[4] 5.9GHz DSRC. Dedicated short range communications[OL]. http://grouper.ieee.org/groups/scc32/dsrc/index.html, 2014

[5] Kenney J B. Dedicated Short-Range Communications (DSRC) Standards in the United States[J]. Proceedings of the IEEE, 2011, 99(7): 1162-1182

[6] Buttyan L, Hubaux J P. Security and cooperation in wireless networks[M]. Cambridge University Press, 2007

[7] 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

[8] Fastenrath D U. Floating car data on a larger scale [C]// ITS World Congress. 1997: 1-10

[9] 秦玲，张剑飞，郭鹏，等. 浮动车交通信息处理与应用系统核心功能及实现[J]. 公路交通科技，2006，7(11)：44-46

[10] 朱丽云，温慧敏，孙建平. 北京市浮动车交通状况信息实时计算系统[J]. 城市交通，2008，6(1)：77-80

[11] 计会凤. 基于浮动车 GPS 数据的动态交通预测与诱导模型研究[D]. 阜新：辽宁工程技术大学，2009

[12] Kerner B S, Demir C, Herrtwich R G, et al. Traffic state detection with floating car data in road networks[C]// 2005 Intelligent Transportation Systems. IEEE, 2005: 44-49

[13] Hubaux J P, Capkun S, Luo J. The security and privacy of smart vehicles[J]. IEEE Security & Privacy Magazine, 2004, 2(3): 49-55

[14] Raya M, Hubaux J P. The security of vehicular ad hoc networks [C]// Proceedings of the 3rd ACM Workshop on Security of Ad

hoc and Sensor Networks. ACM,2005:21-31
[15] 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 Part1):3442-3456
[16] Boneh D,Boyen X,Shacham H. Short group signatures[C]// Advances in Cryptology-CRYPTO 2004. Springer,2004:227-242
[17] Shamir A. Identity-based cryptosystems and signature schemes [C]// Lecture Notes in Computer Science,Advances in cryptology-CRYPTO'84. Springer,1984,196:47-53
[18] Boneh D,Shacham H. Group signatures with verifier-local revocation[C]// 11th ACM Conference on Computer and Communications Security. ACM,2004:168-177
[19] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[C]// Advances in Cryptology — CRYPTO 2001. Springer,2001:213-229
[20] Lu R,Lin X,Zhu H,et al. ECPP:Efficient conditional privacy preservation protocol for secure vehicular communications[C]// INFOCOM'2008. IEEE,2008:1229-1237
[21] Wasef A,Jiang Y,Shen X. DCS:An Efficient Distributed-Certificate-Service Scheme for Vehicular Networks[J]. IEEE Transactions on Vehicular Technology,2010,59(2):533-549
[22] Yang Tao,Xiong Hu,Hu Jian-bin,et al. A traceable privacy-preserving authentication protocol for VANETs based on proxy re-signature[C]// Eighth International Conference on Fuzzy Systems and Knowledge Discovery(FSKD 2011). IEEE,2011,4:2217-2221
[23] Calandriello G, Papadimitratos P, Hubaux J P, et al. Efficient and robust pseudonymous authentication in VANET[C]// Proceedings of the 4th ACM International Workshop on Vehicular Ad hoc Networks(VANET'07). ACM,2007:19-28
[24] 赵宝康.无线传感器网络隐私保护关键技术研究[D].长沙:国防科学技术大学,2009
[25] Scott M. Efficient implementation of crytographic pairings [OL]. http://ecryptss07. rhul. ac. uk/Slides/Thursday/mscottsamos07. pdf,2014
[26] Wasef A,Shen X. Efficient Group Signature Scheme Supporting Batch Verification For Securing Vehicular Networks[C]// IEEE International Conference on Communications(ICC 2010). IEEE,2010:1-5

(上接第 350 页)

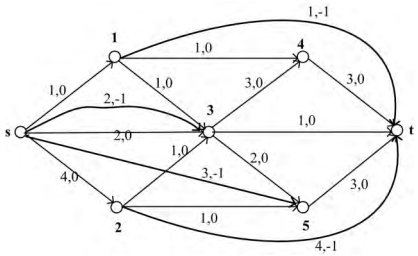

图 4 容量费用网络图 D_2

在容量费用网络图 D_2 中,用文献[2]中所讲述求最小费用最大流方法,取零流为初始可行流,求得最小费用最大流结果如图 5 所示。

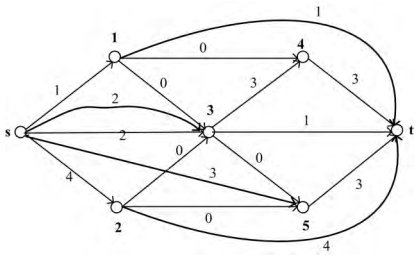

图 5 D_2 最小费用最大流图

(4)在图 5 中,去掉增加的弧$((1,t),(2,t),(s,2),(s,5))$,其余弧上的流量加上网络 D 中对应弧的容量下限c_{ij}(如$f_{s3}=2+c_{s3}=2+3=5$),得容量带上下限的网络图 D 的最大流为 14,如图 6 所示。

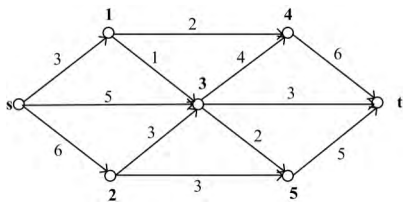

图 6 容量带上下限的网络 D 的最大流图

结束语 通过实例详细说明了将带上下限的网络最大流问题转化为求解网络的最小费用最大流问题算法的方法和步骤,本文所讲的算法更适合顶点集的个数不是很多的有限有向网络图。

参 考 文 献

[1] [美]Johnsonbaugh R. 离散数学[M]. 黄林鹏,译. 北京:电子工业出版社,2009:497-508
[2] 钱颂迪,等. 运筹学[M]. 北京:清华大学出版社,2012:312-320
[3] 胡运权. 运筹学教程权[M]. 北京:清华大学出版社,2007:233-268
[4] 赵礼峰,白睿,等. 求解网络最大流的标号算法[J]. 计算机技术与发展,2001,21(12):113-115
[5] 谢凡荣,贾仁安. 有上下界网络最大流与最小截问题[J]. 运筹管理,2008,17(2):24-31
[6] 张宏斌,等. 运筹学方法及应用[M]. 北京:清华大学出版社,2008:123-133
[7] 王志强,孙小军. 网络最大流的新算法[J]. 计算机工程与设计,2009,30(10):2357-2359
[8] 赵礼峰,白睿. 求解网络最大流问题的标号算法[J]. 计算机技术与发展,2011,21(12):113-115
[9] 库向阳. 点和边有容量约束的网络最小费用最大流算法[J]. 计算机应用研究,2010,27(8):3112-311
[10] 谢政. 网络算法与复杂性理论[M]. 长沙:国防科技大学出版社,2003:116-123
[11] 徐翠霞. 深度优先搜索最大流问题的简单算法[J]. 潍坊学院学报,2006,6(6):30-32
[12] 陈静,单锐. 容差修正网络最大流问题 2F 算法[J]. 长春工业大学学报,2008,29(6):713-716
[13] 谢利民,朱恩强,等. 计算机网络最小割的问题的注记[J]. 数学的实践与认识,2009,39(7):170-171
[14] 高随祥. 图论与网络流理论[M]. 北京:高等教育出版社,2006:292-331