

## 基于签密和区块链的车联网电子证据共享方案

杨小东<sup>1</sup>, 席婉婷<sup>1</sup>, 王嘉琪<sup>1</sup>, 陈艾佳<sup>1</sup>, 王彩芬<sup>2</sup>

(1. 西北师范大学计算机科学与工程学院, 甘肃 兰州 730070;

2. 深圳技术大学大数据与互联网学院, 广东 深圳 518118)

**摘要:** 针对车联网电子证据共享中的隐私和安全性问题, 提出了一种基于签密和区块链的车联网电子证据共享方案。所提方案将证据密文和证据报告分别存储于云服务器和区块链, 以实现电子证据的安全存储与共享。利用基于身份的签密技术保证了数据的机密性, 运用代理重加密技术实现了保险公司对车联网电子证据的共享。引入聚合签名技术, 降低了多个车辆用户签名验证的计算开销; 采用信誉激励机制提高了电子证据的可靠性。安全性分析表明, 所提方案满足数据的机密性、完整性、可验证性和不可伪造性。与现有方案相比, 所提方案在计算开销方面具有一定优越性。

**关键词:** 车联网; 电子证据; 基于身份的签密; 代理重加密; 区块链; 聚合签名

**中图分类号:** TP309.7

**文献标识码:** A

**DOI:** 10.11959/j.issn.1000-436x.2021237

## Electronic evidence sharing scheme of Internet of vehicles based on signcryption and blockchain

YANG Xiaodong<sup>1</sup>, XI Wanting<sup>1</sup>, WANG Jiaqi<sup>1</sup>, CHEN Aijia<sup>1</sup>, WANG Caifen<sup>2</sup>

1. College of Computer Science & Engineering, Northwest Normal University, Lanzhou 730070, China

2. College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China

**Abstract:** To solve the problems of privacy and security in the electronic evidence sharing of Internet of vehicles, a sharing scheme of electronic evidence in the Internet of vehicles based on signcryption and blockchain was proposed. The evidence ciphertext and the evidence report were stored in the cloud server and the block chain respectively to realize the secure storage and sharing of the electronic evidence. The identity-based signcryption technology was used to ensure the confidentiality of data, and the proxy re-encryption technology was used to realize the sharing of electronic evidence of Internet of vehicles by insurance companies. The aggregation signature technique was introduced to reduce the computation cost of multi vehicle user signature verification. The reliability of electronic evidence was improved by using credibility incentive mechanism. Security analysis shows that the proposed scheme achieves data confidentiality, integrity, verifiability and unforgeability. Compared with the existing schemes, the proposed scheme has certain advantages in terms of computational overhead.

**Keywords:** Internet of vehicles, electronic evidence, identity-based signcryption, proxy re-encryption, blockchain, signature aggregation

收稿日期: 2021-09-04; 修回日期: 2021-12-03

基金项目: 国家自然科学基金资助项目 (No.61662069, No.61562077, No.61702552); 中国博士后科学基金资助项目 (No.2017M610817); 兰州市科技计划基金资助项目 (No.2013-4-22); 西北师范大学青年教师科研能力提升计划基金资助项目 (No.NWNU-LKQN-14-7)

**Foundation Items:** The National Natural Science Foundation of China (No.61662069, No.61562077, No.61702552), China Postdoctoral Science Foundation Funded Project (No.2017M610817), The Science and Technology Project of Lanzhou City (No.2013-4-22), The Research Ability Improvement Project of Young Teachers of Northwest Normal University (No.NWNU-LKQN-14-7)

## 1 引言

车联网<sup>[1]</sup>是车、路、人协同的开放融合网络，是借助现代通信技术实现信息共享的移动通信系统。车联网中车辆行驶数据、交通状态数据和交通事故数据的共享，不仅能够实现路况监测以避免交通混乱，也能够为交通执法部门和保险公司等提供重要信息。例如，交通执法部门可以通过车辆行驶数据调查事故原因；保险公司可以将交通事故数据作为理赔证据等。然而，车联网数据在促进智慧交通发展的同时，也面临着严峻的数据安全挑战。由于车联网数据具有巨大的经济价值，恶意用户利用车联网进行非法行为的情况频频发生<sup>[2]</sup>，数据被窃取或伪造可能会造成车联网交通事故难以定责等问题。

电子证据<sup>[3]</sup>作为一种新型的证据，是利用电子设备进行传递、存储和共享的一切形式的证据。传统证据的提取依赖于人工，人工取证费时费力且效率极低；而电子证据具有收集迅速、易于保存、占用空间少和便于审查核实的特点，它的共享则能够更高效地解决车联网交通事故的追责及赔偿等问题。然而，电子证据因其本身较脆弱且依赖存储介质，易被丢失、修改和伪造<sup>[4]</sup>。如发生肇事类交通事故时，无有效证据或责任人故意伪造证据会导致定责困难或追责出现偏颇。保险公司的赔偿可能随之出现偏差造成重大利益损失，且追责有失公允也会导致司法部门公信力下降。因此，电子证据共享过程中的隐私泄露与数据安全问题亟待解决。

基于身份的签密<sup>[5]</sup>和代理重加密技术<sup>[6]</sup>可以通过对数据加密来解决数据隐私与安全问题。基于身份的签密具有更短的密文和更小的计算开销，对数据既签名又加密保证了数据的机密性和不可否认性。代理重加密技术使用重加密密钥进行密文转换，将授权者的密文转换成被授权者可以解密的密文，实现了第三方用户对授权方数据的共享。然而，基于身份的签密和代理重加密技术依赖于半可信第三方，通常存在数据存储中心化的问题。云服务器通常在执行用户命令的同时，仍对用户的信息保持好奇，因此其是半可信的。集中化存储的云服务器很容易遭到不法分子的攻击，造成隐私数据的篡改、丢失或泄露<sup>[7]</sup>。

区块链技术<sup>[8]</sup>是一种具有去中心化、数据难以篡改、可追溯、不可伪造等特性的信任机制，为电

子证据在车联网中的共享提供了新的去中心化的解决方案。区块链技术可以在防止证据被篡改的同时，实现电子证据的分布式安全存储。然而，区块链技术现阶段存在性能瓶颈<sup>[9]</sup>，无法大规模存储车联网电子证据数据。随着区块链交易数据的增长，节点记录数据的时间也不断延长，数据确认的时延也会越来越高，因此单纯使用区块链存储和共享车联网电子证据存在效率低下的问题。

针对上述问题，本文提出了基于签密和区块链技术的车联网电子证据共享方案。该方案采用链上存储证据报告、链下存储证据密文的方式，将云的海量存储能力和区块链的难以篡改性结合进行优势互补；利用基于身份的签密和代理重加密技术对电子证据进行加密，实现了证据的机密性、身份可验证性和不可否认性。同时，通过管理车辆用户的信誉值，提高了数据的可靠性；采用聚合签名技术降低了签名验证的计算开销。

## 2 相关工作

电子取证逐渐替代传统人工取证，一定程度上解决了证据收集依赖人工、取证效率低下、证据容易失真等问题。但是目前还面临着安全和隐私挑战，如证据提供车辆的隐私保护问题和电子证据易受攻击被篡改和伪造的问题。因此，车联网电子证据共享成为公共法治及智慧交通领域重点关注的研究课题之一。

为了解决数据隐私泄露和共享安全问题，Malone 等<sup>[10]</sup>在数字签名体制<sup>[11]</sup>的基础上利用双线性对计算构造了第一个基于身份的签密方案，保证了数据的机密性、消息的完整性和不可否认性；但其明文的签名在密文中可见，Libert 等<sup>[12]</sup>随后指出该方案是不安全的。Karati 等<sup>[13]</sup>介绍了一种新的基于身份的双线性对签名加密方案，实现了身份的可追溯性；但由于其计算量大不适合在交通场景中短时间内对大量车辆签名进行验证。Boneh 等<sup>[14]</sup>提出的聚合签名解决了多个签名的验证问题，签名验证者仅需验证聚合后的一个签名即可，提高了系统中签名的验证速率。Blaze 等<sup>[15]</sup>提出代理重加密机制实现了密文转换，解决了实际应用中的细粒度解密权限分配问题；但该方案的授权人与代理人可以串通获取授权人的私钥，即存在合谋攻击安全风险。Hundera 等<sup>[16]</sup>和 Luo 等<sup>[17]</sup>将云计算技术引入代理重签密方案，降低了大量数据的存储成本，满足了云

端数据的机密性和完整性的安全需求；但其方案仍消耗较高的计算成本，且存在数据存储中心化和数据易被篡改的问题。

区块链技术的出现为数据易被篡改和伪造的问题提供了一种新的解决方案<sup>[18-19]</sup>，区块链能够确保数据的去中心化存储、难以篡改和不可伪造。Zhang 等<sup>[20]</sup>提出了一个基于区块链的云取证方案，该方案在提供证据同时可实现身份的隐私保护；但方案的效率和安全均受限于中心信任节点。Malamas 等<sup>[21]</sup>提出了一种基于移动物联网的取证框架，利用区块链获取证据保证了证据完整性和可靠性；但密钥管理技术烦琐，无法适用于车联网场景。Huang 等<sup>[22]</sup>提出了一种基于区块链的云计算电子取证模型，该模型可以防止取证各方的串谋篡改；但不能满足并发请求，算法效率需要进一步优化。Oham 等<sup>[23]</sup>利用区块链技术存取证据，提出了一种自动车辆归责框架，该框架能够解决车辆与司法部门间在交通事故中的信任问题，但无法避免数据确认时延高的问题。Li 等<sup>[24]</sup>对电子证据加密实现了数据的安全存储及细粒度访问控制，通过区块链技术保证了数据记录的防篡改；但该方案存在大量双线性对运算，计算开销较大并不高效。

为此，本文基于签密和区块链技术提出了一个新的车联网电子证据共享方案。利用云服务器存储

电子证据密文，区块链存储包含证据哈希值及签名等的证据报告，这样既能防止云服务器伪造或篡改证据，又能减轻区块链的存储负担。使用基于身份的签密和代理重加密算法加密电子证据保证数据机密性，为所有进行通信的实体生成匿名身份以保护其身份隐私。因此，本文方案既解决了车联网电子证据的安全共享问题，又实现了证人即车辆用户的隐私保护需求，使电子证据共享更加高效、安全。

### 3 车联网电子证据共享模型

本节首先重点介绍了模型的逻辑框架与实体功能，然后给出车联网电子证据共享模型的设计目标。

#### 3.1 模型的逻辑框架与实体功能

本文提出将区块链与云服务器相结合，实现数据的链上（区块链）+链下（云服务器）混合存储；同时，利用签密和代理重加密技术，实现了车辆用户的隐私保护和电子证据的安全共享。如图 1 所示，基于区块链的车联网电子证据共享模型包括可信机构（TA, trusted authority）、认证机构（CA, certification authority）、车辆（ $V_i$ , vehicle）、路边单元（RSU, road-side unit）、区块链（BC, blockchain）、云服务器（CS, cloud server）和保险公司（IC, insurance company）7 个实体，其中 TA 对应图 1 中的车辆管理所，CA 对应图 1 中的交通警察局。

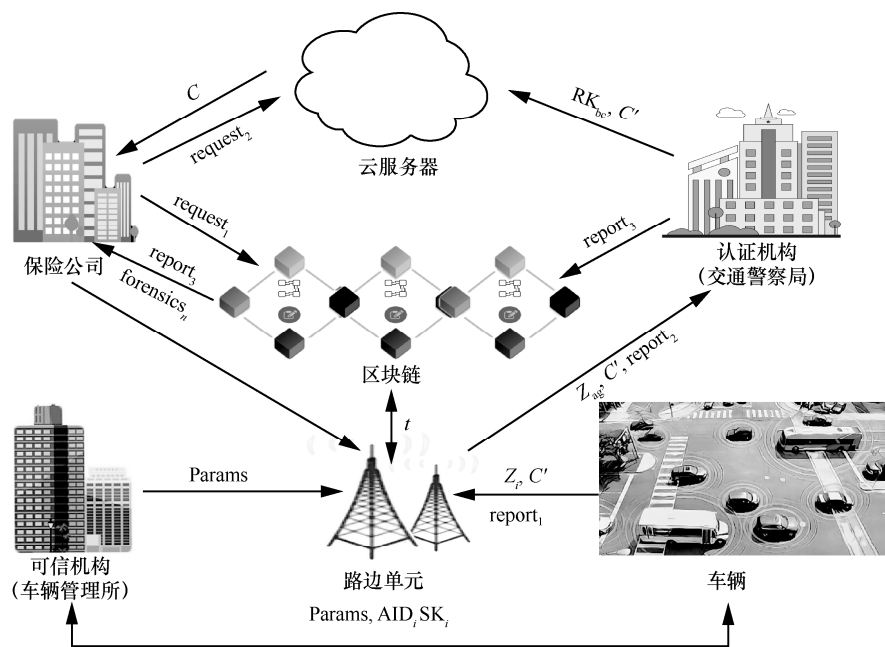


图 1 车联网电子证据共享模型框架

各个实体的具体介绍如下。

- 1) 可信机构：负责进行全局设置，车辆和路边单元需到车辆管理所登记注册。
- 2) 认证机构：负责生成代理密钥，管理并更新车辆的信誉值。
- 3) 车辆：参与取证任务，负责收集证据并对其进行签密。
- 4) 路边单元：负责验证每个车辆的签名，并将有效的一组车辆签名进行聚合。
- 5) 区块链：负责将证据报告存储在记录池中，保险公司需先入链查找证据报告，再根据报告请求云服务器返回证据密文。
- 6) 云服务器：负责进行代理重加密并存储证据密文，具有足够的存储和计算资源。云服务器验证证据密文的有效性，无效则拒绝存储。
- 7) 保险公司：将取证任务委托给路边单元，通过云服务器获取证据密文并解密得到有效证据，对提供有效证据的车辆给予报酬奖励。

### 3.2 模型的设计目标

该模型旨在达到如下设计目标。

- 1) 数据共享。采用云存储和加密技术实现了多对多的共享，车辆用户将电子证据加密存储在云服务器中，保险公司通过解密获取电子证据。车辆用户借助云服务器将电子证据共享给需要有效证据的保险公司。
- 2) 隐私保护。利用基于身份的签密技术，为车辆生成匿名身份进行交互使其真实身份不被泄露，同时也通过加密数据在共享过程中保护电子证据的数据隐私。
- 3) 安全高效。采用了区块链和云计算相结合的混合存储以保证证据数据的安全。区块链中的数据记录的防篡改性以及云服务器强大的存储、计算能力可以确保电子证据的安全存储。聚合签名和代理重加密技术的应用能够很好地提高方案效率，实现数据高效共享。

## 4 方案的详细构造及设计

方案主要包括系统初始化、实体注册、证据收集、证据上传、证据访问和激励机制 6 个步骤。

### 4.1 系统初始化

TA 选择一个安全参数  $1^k$  并执行如下操作。

- 1) TA 选择一个素数  $p$ ，2 个阶为  $p$  的循环群  $G_0$  和  $G_T$ ，其中  $G$  是群  $G_0$  的生成元。循环群满足双

线性映射  $e: G_0 \times G_0 \rightarrow G_T$ 。

- 2) TA 选择 4 个安全的哈希函数： $H_1: \{0,1\}^* \rightarrow G_0$ ， $H_2: G_0 \times G_T \rightarrow Z_p^*$ ， $H_3: G_0 \times G_0 \times G_0 \times G_T \times G_T \rightarrow Z_p^*$  和  $H_4: G_0 \times G_0 \times G_T \rightarrow Z_p^*$ 。

- 3) TA 选择随机数  $\alpha \in Z_p^*$  作为主密钥，并设置  $P_{\text{pub}} = \alpha G$  作为系统公钥。

- 4) TA 秘密保存主密钥  $\text{msk} = \alpha$ ，公开全局参数  $\text{Params} = \{G_0, G_T, e, G, P_{\text{pub}}, H_1, H_2, H_3, H_4\}$ ，并将区块链记录池初始化为空。

### 4.2 实体注册

车辆都需要在 TA 处进行登记注册。车辆通过安全信道将自己的真实身份发送给 TA，对于真实身份为  $\text{RID}_i$  的车辆用户，TA 为其生成匿名身份  $\text{AID}_i$  来保护身份隐私，具体注册步骤如下。

- 1) TA 选择哈希函数  $H_1: \{0,1\}^* \rightarrow G_0$ ，计算  $\text{AID}_i = H_1(\text{RID}_i)$ ， $\text{AID}_i$  为车辆用户的匿名身份，TA 秘密保存注册信息表  $\text{registry} = \{\text{RID}_i, \text{AID}_i\}$ 。

- 2) TA 根据车辆匿名身份  $\text{AID}_i$ ，计算  $\text{SK}_i = \text{mskAID}_i = \alpha \text{AID}_i$  作为车辆用户的私钥。

- 3) TA 将车辆匿名身份和用户私钥  $\{\text{AID}_i, \text{SK}_i\}$  通过一个安全信道发送给用户。

- 4) 如果进行取证任务的车辆用户出现任何违规或非法行为，TA 可以根据  $\text{AID}_i$  查询注册信息表  $\text{registry}$  来曝光该车辆的真实身份以进行追查。

- 5) 区块链节点向 TA 实名注册，TA 创建创世块并广播给整个区块链网络，区块链节点记录创世块。

### 4.3 证据收集

路边单元 RSU 接受 IC 委托的取证任务后，邀请事故路段车辆进行如下证据收集操作。

- 1) IC 将取证任务  $\text{forensics}_n = \{n, \text{AID}_c, u_n\}$  委托给 RSU，其中包括取证任务编号  $n$ 、保险公司匿名身份  $\text{AID}_c$  和取证车辆信誉值要求  $u_n$ 。

- 2) RSU 邀请事故发生路段周围车辆  $(V_1, V_2, \dots, V_j)$  收集事故相关证据数据附上签名并上传。经过事故路段但无证据的车辆  $V_j$  驶离该路段也可将任务附上签名广播给周围的车辆，以提高取证任务完成的效率。

- 3) RSU 将车辆收集的事故相关证据发送至 CA，由 CA 的交通执法人员根据  $\text{forensics}_n$  筛选出有效的证据，并对相关证据数据进行代理重加密；

若无有效证据则由 RSU 继续广播证据收集任务。

#### 4.4 证据上传

车辆、路边单元和认证机构执行以下流程向区块链网络和云服务器安全地上传证据数据。

##### 1) 车辆签密

取证车辆对行车记录仪拍到的现场照片、视频以及事故车辆行驶状态数据等证据进行签密, 以保证其他实体交互过程中是不知道证据明文的。无证据车辆将取证任务附上签名广播给周围车辆。

① 取证车辆  $V_i$  选取随机数  $\varepsilon \in Z_p^*$ , 获取当前设备的时间戳  $t \in \{0,1\}^*$  作为登录令牌, 计算  $X = \varepsilon AID_i$ ,  $Y = H_2(X, M || t)$  和  $Z_i = (\varepsilon + Y)SK_i$  得到签名  $\sigma_i = (Z_i, G)$ , 其中证据  $M \in G_T$ 。

② 车辆  $V_i$  计算  $S = e(\varepsilon SK_i, AID_b)$ ,  $y = MS$ ,  $U = H_3(X, Z_i, y, AID_i, AID_b)$  和  $R = \varepsilon U$ , 其中  $AID_b$  是 CA 的匿名身份。 $V_i$  对证据数据  $M$  加密生成一级密文  $C' = (X, Z_i, y, R)$ 。车辆  $V_i$  生成证据报告 1, 即  $report_1 = \{n, Z_i, H_2(M), t\}$ , 并上传  $Z_i$ 、一级密文  $C'$  及  $report_1$  至路边单元 RSU。

③ 离开事故路段 RSU 范围的无证据车辆  $V_f$  将取证任务发送给目前路段的  $RSU_{now}$ , 由  $RSU_{now}$  将  $forensics_n$  作为消息广播给周围车辆。 $RSU_{now}$  选取随机数  $\psi \in Z_p^*$ , 计算  $SK_R = mskH_1(RID_R) = \alpha AID_R$ ,  $X_R = \psi AID_R$ ,  $Y_R = H_2(X_R, forensics_n)$  和  $Z_R = (\psi + Y_R)SK_R$ , 得到签名  $\sigma_R = (Z_R, G)$ , 将  $\{forensics_n, Z_R\}$  广播给周围车辆, 收到消息的车辆通过计算  $e(Z_R, G) = e(X_R + Y_R AID_R, P_{pub})$  对签名是否有效进行验证。

##### 2) 聚合签名生成

路边单元验证车辆签名是否合法, 并为持有合法签名的一组车辆进行如下操作生成聚合签名。

① RSU 在区块链账本和本地数据库中查找  $t$  是否已经存在。如果存在, 则拒绝该车辆提供的证据, 避免重复存证; 否则, RSU 继续进行聚合签名。

② RSU 首先对每个车辆的签名  $\sigma_i = (Z_i, G)$  ( $1 \leq i \leq j$ ) 通过计算等式  $e(Z_i, G) = e(X + YAID_i, P_{pub})$  进行验证。若等式成立, 则该签名合法, RSU 将持有合法签名的一组车辆的匿名身份生成列表  $V_{legal} = \{AID_1, AID_2, \dots, AID_j\}$ , RSU 为该组车辆生

成聚合签名  $\sigma_{ag} = (Z_{ag}, G)$ , 其中  $Z_{ag} = \sum_{i=1}^j Z_i$ 。若验

证失败, 则签名无效, 该车辆存在上传虚假证据的可能, RSU 可将车辆匿名身份举报给 TA, TA 可以公开该车辆真实身份, CA 也相应地降低该车辆的信誉值。

③ 车辆身份验证通过后, RSU 生成证据报告 2, 即  $report_2 = \{n, Z_{ag}, V_{legal}, AID_c, H_2(M), t\}$ , 并将  $Z_{ag}$ 、一级密文  $C'$  及  $report_2$  上传至 CA。

##### 3) 代理重加密及密文存储

CA 对聚合签名进行验证, 若签名合法, 则执行以下操作进行代理重加密, 并将经过签密和代理重加密的证据密文进行如下存储。

① 交通执法人员根据  $forensics_n$ 、证据报告和信誉值  $value_i$  筛选出有效的证据, 其中 CA 管理的车辆信誉值初始均为相同数值, 仅提交过证据的车辆的匿名身份会被 CA 保存, 并对该车辆的信誉值进行更新。

② CA 通过计算  $e(Z_{ag}, G) = e(\sum_{i=1}^j X + YAID_i, P_{pub})$

对聚合签名  $\sigma_{ag}$  进行批量验证。如果验证通过, 则签名合法, CA 生成重加密密钥进行代理重加密; 否则, 聚合/签名无效, 该 RSU 节点存在被非法攻陷的可能, CA 可向 TA 举报该 RSU 节点。

③ CA 计算  $W = H_4(e(SK_b, AID_c), AID_b, AID_c)$  和  $RK_{bc} = W - SK_b$  生成重加密密钥  $RK_{bc}$ 。

④ CA 记录当前时间戳  $T_s$ , 生成并向区块链网络中发送证据报告 3, 即  $report_3 = \{n, \sigma_{ag}, AID_i, AID_b, AID_c, H_2(M), t, T_s, value_i\}$ 。CA 将  $report_3$  存入区块链记录池中, 并通过安全信道将重加密密钥  $RK_{bc}$  及一级密文  $C'$  发送给云服务器 CS。

⑤ CS 通过重加密密钥对  $C'$  进行代理重加密, CS 计算  $U = H_3(X, Z_i, y, AID_i, AID_b)$ , 验证等式  $e(R, AID_i) = e(U, X)$  是否成立, 若验证通过则计算  $y' = ye(XRK_{bc})$ , 生成二级密文  $C = (X, Z_i, y')$  并存储。其中, CS 通过等式  $e(R, AID_i) = e(U, X)$  来检验证据密文的有效性, 若密文无效则拒绝重加密和存储密文。

#### 4.5 证据访问

保险公司 IC 发送访问请求, 在接收到云服务器 CS 的证据密文后, 执行解密操作获取证据明文, 具体步骤如下。

1) IC 根据取证编号、伪名以及当前时间戳  $T_s$  向区块链网络请求访问证据报告, 数据请求为

$\text{request}_1 = \{n, \text{AID}_c, T_s, P_{\text{pub}}\}$ , 持有相应数据记录的区块链节点向 IC 返回证据报告  $\text{report}_3$ 。

2) IC 根据证据报告向云服务器发送  $\text{request}_2$  请求证据密文, 云服务器向保险公司返回证据密文  $C$ 。

3) IC 对证据密文  $C$  进行解密, IC 通过计算  $W = H_4(e(\text{AID}_b, \text{SK}_c), \text{AID}_b, \text{AID}_c)$ ,  $S' = e(X, W)$  和  $M = y'(S')^{-1}$  解密得到有效证据  $M$ 。

4) IC 通过计算  $Y = H_2(X, M)$  可以验证证据完整性; 通过等式  $e(Z_i, G) = e(X + \text{YAID}_i, P_{\text{pub}})$  可以对证据源进行身份验证。

#### 4.6 激励机制

保险公司 IC 根据证据报告中车辆信誉值  $\text{value}_i$  的高低对证据进行评估。IC 通过奖励机制来刺激、鼓励更多车辆收集并提供有效证据。一旦该有效证据被 IC 成功接受, 则对对应的车辆用户进行报酬奖励。

CA 初始时根据信誉感知激励机制为不同的车辆  $V_i$  设置不同的信誉值。当 IC 发布取证任务并且车辆  $V_i$  竞争参与这些任务时, 感知平台会根据  $V_i$  的信誉值  $\text{value}_i$  进行选择, 优先交由信誉值高的  $V_i$  参与取证任务。对  $V_i$  的信誉值  $\text{value}_i$  进行更新后,  $V_i$  可再次进入下一轮的任务竞争中。通过该激励机制, 可以刺激车辆用户提高任务完成率和参与率。

当有取证任务要处理时, CA 为每个不同的取证任务设置一个信誉阈值, 用  $u_n$  表示。IC 为鼓励更多  $V_i$  参与完成取证任务, 会在每个任务处理完成后为对应  $V_i$  提供奖励报酬。报酬函数用  $P_n = \frac{1}{a(l(r)+1)} u_n B(r)$  来表示, 其中  $a$  为正常数,  $B$  为初始成本预算。通过这种方式, 保险公司初始时会提供很高的报酬来鼓励车辆用户参与取证任务, 随着车辆用户参与的比例  $l(r)$  越来越高, 报酬会慢慢趋于平稳。

## 5 安全性分析

本节将从正确性、机密性、不可伪造性这 3 个方面对本文所提方案进行安全性分析。

### 5.1 正确性

#### 1) 签名的正确性验证

路边单元 RSU 需要对车辆  $V_i$  的签名进行正确性验证, 以确保提供证据的该车辆身份是合法的。RSU 计算式(1)进行验证, 当等式成立时车辆  $V_i$  的身份才合

法, 其对电子证据的签名才有效。具体证明如下。

$$\begin{aligned} e(Z_i, G) &= e((\varepsilon + Y)\text{SK}_i, G) = \\ e(\varepsilon\text{mskAID}_i + \text{YSK}_i, G) &= \\ e(X + \text{YAID}_i, G\text{msk}) &= e(X + \text{YAID}_i, P_{\text{pub}}) \end{aligned} \quad (1)$$

验证得出等式成立, 即该车辆签名有效。路边单元 RSU 将所有合法车辆的签名聚合起来形成新签名发送给 CA, CA 同样需要验证聚合签名是否有效。当验证等式  $e(Z_{\text{ag}}, G) = e(\sum_{i=1}^j X + \text{YAID}_i, P_{\text{pub}})$  成立时, 该聚合签名有效。

#### 2) 证据密文解密正确性验证

云服务器 CS 通过重加密密钥  $\text{RK}_{bc}$  对一级密文进行代理重加密后的密文为  $C = (X, Z_i, y')$ 。保险公司 IC 向云服务器请求获取证据密文后, 根据 CA 的匿名身份  $\text{AID}_b$  和 IC 的私钥  $\text{SK}_c$  计算  $W = H_4(e(\text{AID}_b, \text{SK}_c), \text{AID}_b, \text{AID}_c)$  和  $S' = e(X, W)$ 。IC 通过式(2)可以计算得到证据明文, 具体证明如下。

$$\begin{aligned} y'(S')^{-1} &= ye(X, \text{RK}_{bc})e(X, W)^{-1} = \\ Me(\varepsilon\text{SK}_c, \text{AID}_i)e(X, (W - \text{SK}_c))e(X, W)^{-1} &= \\ \frac{Me(X, \text{SK}_c)e(X, (W - \text{SK}_c))}{e(X, W)} &= \frac{Me(X, W)}{e(X, W)} = M \end{aligned} \quad (2)$$

IC 可以通过解密计算  $y'(S')^{-1} = M$  得到证据明文, 即本文方案的证据密文解密正确。

### 5.2 机密性

本文将基于身份的签密与代理重加密结合起来, 保证了车联网环境下电子证据共享过程中的机密性。机密性是指除了提供证据的车辆及使用证据的保险公司外, 其他实体都不知道证据的具体内容。在本文中, 车辆用户  $V_i$  对电子证据  $M$  进行签密, 将加密后的一级证据密文  $C'$  发送给 CA; CA 生成代理重加密密钥  $\text{RK}_{bc}$  发送给云服务器 CS, CS 对一级密文代理重加密后进行密文存储。当保险公司 IC 希望访问一起事故的电子证据时, 根据取证编号  $n$ 、公司伪名  $\text{AID}_c$  等生成访问请求  $\text{request}_1$ 。IC 将访问请求发送给区块链网络以获取证据报告  $\text{report}_3$ , 再根据证据报告向云请求证据密文  $C$ , 最终解密得到电子证据明文。由于  $V_i$  收集的证据经过了 CS 的代理重加密, 因此只有被授权的合法保险公司  $\text{RID}_c$  才能正确解密证据密文, 其他实体无法获取任何有关电子证据的具体内容。具体证明过程见附录 1。

### 5.3 不可伪造性

在传统车联网数据共享方案中, 由于云服务器是半可信的且存在响应时延的问题, 因此车辆将证据全部发送至云服务器进行处理会存在较大安全风险。本文利用云服务器和区块链混合存储以及基于身份的签名技术, 保证了电子证据的不可伪造性。车辆  $V_i$  上传的证据报告和保险公司 IC 的访问记录对所有区块链实体公开可见, 并且所有链上的数据都具有公开可验证、防篡改性。只要数据被记录在车联网区块链上, 就不会被轻易地伪造和篡改。车辆  $V_i$  进行数据交互时使用的都是匿名身份  $AID_i$ , 非法攻击者即使成功冒充身份, 也会因为不知道系统主密钥  $\alpha$  而不能生成用户私钥  $SK_i$ 。因此, 非法攻击者无法伪造合法的车辆用户签名  $\sigma_i = (Z_i, G)$ , 而伪造的无效签名则不能通过等式  $e(Z_i, G) = e(X + YAID_i, P_{pub})$  的完整性验证。具体证明过程见附录 2。

## 6 性能分析

本节分析了方案的激励性, 并从计算开销方面对所提方案与现有方案进行分析和比较。

### 6.1 激励机制

本文方案引入信誉值是为了使取证任务快速被车辆用户处理完成, 即在更短的时间内获得更高的任务完成比率。在图 2 中可以看出在一段时间内本文信誉激励机制能很快地处理完取证任务, 并在处理任务速度方面具有较好的稳定性。通过设置取证任务的信誉值, 区别划分车辆用户, 选择信誉值高的车辆用户来处理取证任务。这样通过影响取证任务的信誉阈值  $u_n$  和保险公司支付的报酬  $P_n$ , 从而使车辆用户参与比例  $I(r)$  不断增大, 并最终趋于平稳。

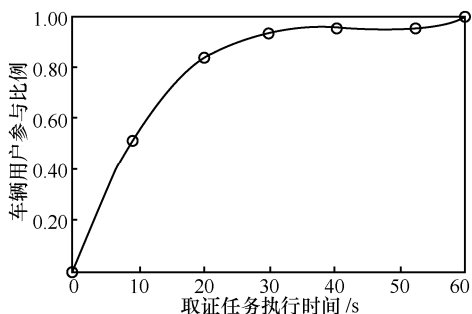


图 2 取证任务完成趋势 ( $I(r)$  稳定前)

在保证取证任务顺利处理完成的基础上, 减少保险公司支付给车辆用户的报酬  $P_n$ , 从而保险公司可以降低对车辆用户奖励的预算, 减少成本的投

入。当参与车辆足够多时不需要再对车辆用户进行激励。图 3 表明  $I(r)$  稳定后的一段时间内, 在保证取证任务顺利完成的基础上, 可以减少保险公司支付给车辆用户的报酬  $P_n$ , 从而使其投入成本减少。综上所述, 本文中选择了信誉高的车辆用户处理取证任务, 使车辆用户参与比例  $I(r)$  不断增大, 保险公司需要支付给车辆用户的报酬  $P_n$  逐渐减少; 即该信誉激励机制在有效提高任务处理效率的同时, 降低了保险公司的成本开销。

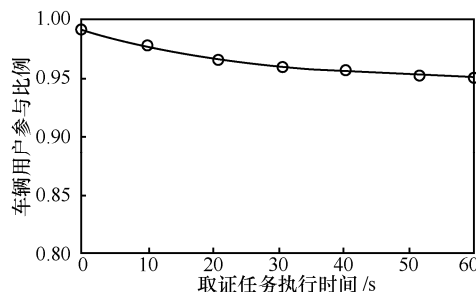


图 3 取证任务完成趋势 ( $I(r)$  稳定后)

### 6.2 计算开销

本节采用对比分析的方式, 将本文方案与 Yu 等<sup>[6]</sup>方案、Hundera 等<sup>[16]</sup>方案和 Luo 等<sup>[17]</sup>方案的计算开销进行了比较。由于这些方案是在双线性对上构建的, 因此通过评估标量乘法运算、指数运算和双线性对运算消耗的时间来比较不同方案的计算开销。各个方案的加解密算法计算开销如表 1 所示, 其中,  $M$  表示一个标量乘运算,  $E$  表示一个指数运算,  $P$  表示一个双线性运算。

表 1 方案计算开销比较

方案	代理密钥生成	加密	解密
Yu 等方案	$2M+2P+1E$	$3M+1P+1E$	$1M+4P+1E$
Hundera 等方案	$2M+2P$	$2M$	$2M+4P$
Luo 等方案	$2M+1P$	$2M+1P+3E$	$2M+1P+3E$
本文方案	$1P$	$4M+1P$	$1M+4P$

本文仿真实验在 Intel Core i5-7400 CPU@3 GHz 平台上使用 Pairing-Based Crypto (PBC) 函数库实现, 所使用硬件环境为 4 GB 处理器内存和 64 位 Windows 10 操作系统。通过仿真实验对比了本文方案及相关 3 种方案的计算开销, 对比结果如图 4 所示。本文方案生成代理密钥、加密和解密消耗的总时间为 151.96 ms, 是 4 个方案中计算开销最少的, 因此本文车联网电子证据共享方案是高效的。

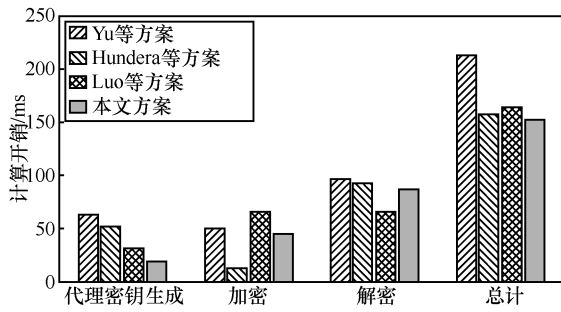


图 4 各方案计算开销比较结果

### 6.3 签名验证

在使用更高效方案对电子证据加解密的同时，本文使用的聚合签名技术也降低了计算开销。聚合签名技术是将不同消息上不同用户分别签署的多个签名聚合成一个短签名。聚合签名进行验证后，验证者可以判断所接收签名的有效性，很大程度上提高了消息验证的效率。本文方案中单个签名验证和聚合签名验证的计算开销比较如表 2 所示，其中  $j$  为单个签名的个数。

表 2 单个签名验证和聚合签名验证的计算开销比较

验证方式	验证计算开销
单个签名验证	$jM + 2jP$
聚合签名验证	$jM + 2P$

通过实验对比本文方案中单个签名验证和聚合签名验证的计算开销，结果如图 5 所示。当存在多个签名时，聚合签名的验证时间远小于单个签名累加的验证时间。因此，本文方案中采用的聚合签名技术极大地降低了签名验证的开销，使电子证据共享方案更加高效。

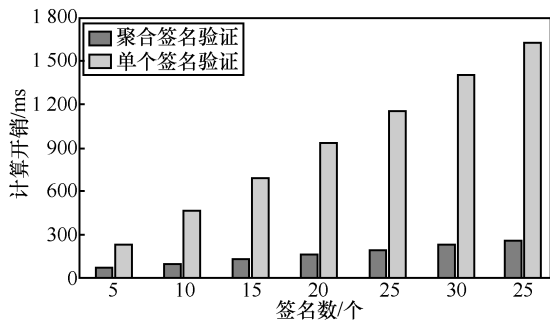


图 5 签名验证开销比较

## 7 结束语

本文针对车联网电子证据共享中的隐私安全和效率问题，提出了一种基于区块链的车联网电

子证据共享方案。该方案不仅实现了证据数据的隐私保护及安全共享，也保证了证据上传者与各实体的匿名交互。借助区块链记录所有证据报告，确保了电子证据不会被篡改和伪造。采用聚合签名和代理重加密技术，使方案具有更优的计算高效性和可靠性。引入信誉激励机制，在有效提高任务处理效率的同时，减少了保险公司支付奖励报酬的成本。最后，通过仿真从计算开销等方面验证了方案的高效性。目前本文匿名交互不足以完全保护用户隐私，只能保证真名被隐藏，无法阻止敌手进行会话链接来判断两次不同的匿名会话来自相同的车辆。在未来的工作中，将继续结合车联网应用场景设计出更安全、高效的隐私保护方案。

## 附录 1 机密性证明

**定理 1** 如果 DBDH 问题是困难的，则本文签密方案在适应性选择密文攻击下满足机密性，即不存在一个攻击者能在多项式时间内以不可忽略的优势攻破本文方案。

**证明** 如果存在一个概率多项式时间敌手  $\mathcal{A}$  可以以不可忽略的优势  $\tau$  选择性地攻破本文方案，那么能够构造一个概率多项式时间算法使挑战者  $\mathcal{B}$  以不可忽略的优势攻破 DBDH 假设。即给定挑战者  $\mathcal{B}$  一个随机的 DBDH 问题实例  $(G, aG, bG, cG, X \in G_T)$ ， $\mathcal{B}$  判断等式  $Z = e(G, G)^{abc}$  是否成立。

**系统建立。**挑战者  $\mathcal{B}$  运行系统初始化算法，将挑战参数  $\text{Params} = \{G_0, G_T, e, G, P_{\text{pub}}, H_1, H_2, H_3, H_4\}$  发送给攻击者  $\mathcal{A}$ 。

**阶段 1**  $\mathcal{A}$  可以对挑战者  $\mathcal{B}$  做有限次数的适应性询问。 $\mathcal{A}$  首先对身份  $\text{AID}_i$  做  $H_1$  询问后，才能将其询问结果用于其他询问。 $\mathcal{A}$  不可以利用签密询问的结果来进行解密询问。

**$H_1$  询问。**当  $\mathcal{A}$  输入数据  $(\text{RID}_i, \text{AID}_i, h_i)$ ， $\mathcal{B}$  以此格式设置列表  $L_1$ 。当  $\mathcal{A}$  查询  $H_1(\text{RID}_i, \text{AID}_i)$  时，若  $(\text{RID}_i, \text{AID}_i, h_i)$  在列表  $L_1$  中存在，则返回  $h_i$  给  $\mathcal{A}$ ；否则， $\mathcal{B}$  随机选取  $h_i \in Z_p^*$ ，添加记录  $(\text{RID}_i, \text{AID}_i, h_i)$  至列表  $L_1$  中并返回  $h_i$  给  $\mathcal{A}$ 。

**$H_2$  询问。**当  $\mathcal{A}$  输入数据  $(\text{AID}_i, \varepsilon, M, t, \text{SK}_i, h_2, Z_i)$ ， $\mathcal{B}$  以此格式设置列表  $L_2$ 。当  $\mathcal{A}$  查询  $H_2(\text{AID}_i, \varepsilon, M, t, \text{SK}_i)$  时，若  $L_2$  中有相对应的记录  $(\text{AID}_i, \varepsilon, M, t, \text{SK}_i, h_2)$ ，则返回  $h_2$  给  $\mathcal{A}$ ；否则， $\mathcal{B}$  随机选择  $\sigma \in \{0, 1\}$ ，其中  $\sigma = (Z_i, G)$ 。当  $\sigma = 0$  时， $\mathcal{B}$  随机选取  $h_2 \in Z_p^*$ ，添加记录  $(\text{AID}_i, \varepsilon, M, t, \text{SK}_i, h_2, Z_i)$  至列表  $L_2$  中并返回  $h_2$  给  $\mathcal{A}$ ；当  $\sigma = 1$  时，令  $h_2 = \perp$  并返回  $\perp$  给  $\mathcal{A}$ 。

$H_3$  询问。当  $\mathcal{A}$  输入数据  $(AID_b, \varepsilon, M, SK_i, Z_i, h_3, C')$ ,  $\mathcal{B}$  以此格式设置列表  $L_3$ 。当  $\mathcal{A}$  查询  $H_3(AID_b, \varepsilon, M, SK_i, Z_i)$  时, 若  $L_3$  中有相对应的记录  $(AID_b, \varepsilon, M, SK_i, Z_i, h_3)$ , 则返回  $h_3$  给  $\mathcal{A}$ ; 否则,  $\mathcal{B}$  随机选择  $C' \in \{0, 1\}$ 。当  $C' = 0$  时,  $\mathcal{B}$  随机选取  $h_3 \in Z_p^*$ , 添加  $(AID_b, \varepsilon, M, SK_i, Z_i, h_3, C')$  至列表  $L_3$  中并返回  $h_3$  给  $\mathcal{A}$ ; 当  $C' = 1$  时, 令  $h_3 = \perp$  并返回  $\perp$  给  $\mathcal{A}$ 。

$H_4$  询问。当  $\mathcal{A}$  输入数据  $(AID_c, \varepsilon, M, SK_b, Z_i, RK_{bc}, h_4, C)$ ,  $\mathcal{B}$  以此格式设置列表  $L_4$ 。当  $\mathcal{A}$  查询  $H_4(AID_c, \varepsilon, M, SK_b, Z_i, RK_{bc})$  时, 若  $L_4$  中有相对应的记录  $(AID_c, \varepsilon, M, SK_b, Z_i, RK_{bc}, h_4)$ , 则返回  $h_4$  给  $\mathcal{A}$ ; 否则,  $\mathcal{B}$  随机选择  $C \in \{0, 1\}$ 。当  $C = 0$  时,  $\mathcal{B}$  随机选取  $h_4 \in Z_p^*$ , 添加  $(AID_c, \varepsilon, M, SK_b, Z_i, RK_{bc}, h_4, C)$  至列表  $L_4$  中并返回  $h_4$  给  $\mathcal{A}$ ; 当  $C = 1$  时, 令  $h_4 = \perp$  并返回  $\perp$  给  $\mathcal{A}$ 。

私钥询问。当  $\mathcal{B}$  收到关于车辆  $RID_i$  的私钥询问时,  $\mathcal{B}$  在列表  $L_1$  中寻找相对应的记录  $(RID_i, AID_i)$ 。如果车辆身份  $RID_i$  属于路边单元邀请的一组车辆  $V^*$ ,  $\mathcal{B}$  计算私钥  $SK_i = \alpha AID_i$  并将其返回  $\mathcal{A}$ ; 否则, 挑战者  $\mathcal{B}$  失败并终止挑战。

签密询问。当  $\mathcal{B}$  收到  $(RID_1, RID_2, M)$  的签密询问时, 如果  $RID_1 \neq RID_i$  且  $RID_2 \neq RID_b$ , 则调用签密步骤回答  $\mathcal{A}$ ; 若  $RID_1 = RID_i$  且  $RID_2 = RID_b$ ,  $\mathcal{B}$  根据下列方法给出一级密文。

**步骤 1**  $\mathcal{B}$  选取随机数  $\varepsilon \in Z_p^*$ , 计算  $X = \varepsilon AID_i$ ,  $Y = H_2(X, M || t)$  和  $Z_i = (\varepsilon + Y)SK_i$ ;

**步骤 2** 计算  $S = e(\varepsilon SK_i, AID_b)$  和  $y = MS$ ;

**步骤 3** 将  $U = H_3(X, Z_i, y, AID_i, AID_b)$  存储在列表  $L_3$  中, 若发生碰撞, 重做步骤 1~步骤 3;

**步骤 4** 计算  $R = \varepsilon U$  并输出一级密文  $C' = (X, Z_i, y, R)$ ;

重加密密钥询问。当  $\mathcal{B}$  收到  $(RID_2, RID_3)$  的重加密密钥询问时,  $\mathcal{B}$  在列表  $L_4$  中寻找相对应的记录。如果  $RID_2 \neq RID_b$  且  $RID_3 \neq RID_c$ , 而且表中存在记录  $(AID_3, SK_2, RK_{bc})$ , 则返回  $RK_{bc}$ 。如果  $RID_2 = RID_b$  且  $RID_3 = RID_c$ , 则  $\mathcal{B}$  设置  $AID_b = H_1(RID_b)$  和  $AID_c = H_1(RID_c)$ , 计算  $W = H_4(e(SK_b, AID_c), AID_b, AID_c)$  和  $RK_{bc} = W - SK_b$ , 最后挑战者  $\mathcal{B}$  将重加密密钥  $RK_{bc}$  返回给  $\mathcal{A}$ ; 否则, 挑战者  $\mathcal{B}$  失败并终止挑战。

重加密询问。当  $\mathcal{B}$  收到  $(RID_2, RID_3, C')$  的重加密询问时, 如果  $RID_2 \neq RID_b$  且  $RID_3 \neq RID_c$ , 则调用重加密步骤回答  $\mathcal{A}$ ; 若  $RID_2 = RID_b$  且  $RID_3 = RID_c$ ,  $\mathcal{B}$  执行如下步骤得到二级密文。

**步骤 1** 计算  $AID_i = H_1(RID_i)$ ;

**步骤 2** 在列表  $L_3$  中查询  $U = H_3(X, Z_i, y, AID_i, AID_b)$

并计算  $y' = ye(XRK_{bc})$ ;

**步骤 3** 返回二级密文  $C = (X, Z_i, y')$  给  $\mathcal{A}$ 。

解密询问。挑战者  $\mathcal{B}$  接收到  $\mathcal{A}$  关于密文的解密询问时, 如果满足  $RID_2 \neq RID_b$  且  $RID_3 \neq RID_c$ , 那么  $\mathcal{B}$  执行解密操作并将其结果返回给  $\mathcal{A}$ ; 否则,  $\mathcal{B}$  输出  $\perp$ , 即输入的密文无效, 无法执行解密操作。如果  $RID_2 = RID_b$  且  $RID_3 = RID_c$ , 则挑战者  $\mathcal{B}$  执行如下步骤获取证据明文。

**步骤 1** 计算  $SK_c = \alpha AID_c$ ;

**步骤 2** 计算  $W = H_4(e(AID_b, SK_c), AID_b, AID_c)$  和  $S' = e(X, W)$ ;

**步骤 3** 计算证据明文  $M = y'(S')^{-1}$  并将结果返回给攻击者  $\mathcal{A}$ 。

挑战。  $\mathcal{A}$  选取长度相等的消息  $M_0$  和  $M_1$ , 将其发送给  $\mathcal{B}$ 。  $\mathcal{B}$  选择  $\mu \in \{0, 1\}$  并按照以下步骤计算密文  $C^*$ 。

**步骤 1** 随机选择  $\theta \in Z_p^*$ , 计算  $X = \theta AID_i$ ,  $Y = H_2(X, M)$  和  $Z_i = (\theta + Y)SK_i$ ;

**步骤 2** 计算  $S = e(\theta SK_i, AID_b)$ ,  $y = MS$ ,  $U = H_3(X, Z_i, y, AID_i, AID_b)$  和  $R = \theta U$ ;

**步骤 3** 输出一级密文  $C'' = (X, Z_i, y, R)$ ;

**步骤 4** 计算  $W = H_4(e(SK_b, AID_c), AID_b, AID_c)$  并生成重加密密钥  $RK_{bc} = W - SK_b$ ;

**步骤 5** 计算  $U = H_3(X, Z_i, y, AID_i, AID_b)$  和  $y' = ye(XRK_{bc})$ ;

**步骤 6** 生成二级密文  $C^* = (X, Z_i, y')$ 。

**阶段 2**  $\mathcal{A}$  继续进行同阶段 1 中的各种适应性询问, 但是  $\mathcal{A}$  不可以对目标身份做私钥询问。

响应。如果  $\mu' = \mu$ , 则  $\mathcal{B}$  输出 1; 若  $\mu' \neq \mu$ , 则  $\mathcal{B}$  输出 0。

如果  $Z = e(G, G)^{abc}$ , 则  $C^*$  是有效密文, 因此  $\mathcal{A}$  有优势  $\tau$  区分  $\mu$ , 有  $\Pr[\mu' = \mu | Z = e(G, G)^{abc}] = \frac{1}{2} + \tau$ 。如果  $Z \neq e(G, G)^{abc}$ , 那么  $\mu = 1$  或  $\mu = 0$  时, 密文每个部分具有一样的概率分布, 也就是说, 在区分  $\mu$  上的优势是可以忽略的, 所以  $\Pr[\mu' = \mu | Z \neq e(G, G)^{abc}] = 1/2$ 。

假设在多项式时间  $t$  内,  $\mathcal{A}$  最多进行  $q_s$  次签密询问、 $q_{rk}$  次代理密钥询问、 $q_r$  次重加密询问、 $q_d$  次解密询问和  $q_{H_i} (i=1, 2, 3, 4)$  次哈希询问。  $\mathcal{B}$  在多项式时间  $t' < t + O(q_{rk} + q_s + q_r q_{H_2} + q_d q_{H_2}) t_p$  内成功解决 DBDH 的概率为  $\tau' > (\tau - q_s(q_s + q_{H_2})2^{l-k}) / 2q_{H_1}$ , 即挑战者  $\mathcal{B}$  能够以一个不可忽略的优势解决 DBDH 问题。但这一问题已被证明是困难的, 所以攻击者  $\mathcal{A}$  能以不可忽略的优势  $\tau$  攻击本文方案这一假设不成立, 本文方案满足机密性要求。证毕。

## 附录 2 不可伪造性证明

**定理 2** 如果 CDH 困难问题成立, 本文所提方案可以抵抗适应性选择消息攻击下的存在性伪造攻击, 即不存在一个攻击者以不可忽略的优势攻破本文方案。

**证明** 如果存在一个多项式时间的敌手  $\mathcal{A}$  在适应性选择消息攻击下以不可忽略的优势攻破了本文方案, 那么能够构造一个多项式时间算法使挑战者  $\mathcal{B}$  以不可忽略的优势攻破 CDH 问题, 即给定  $\mathcal{B}$  已知  $(aG, bG)$ , 最终可以计算出  $abG$ 。

**系统建立。**挑战者  $\mathcal{B}$  进行系统初始化, 设置系统公钥为  $P_{\text{pub}} = \alpha G$ , 生成系统参数 Params 并将其发送给  $\mathcal{A}$ 。 $\mathcal{B}$  维护和更新列表  $L_1, L_2, L_3, L_4$ , 其分别对应  $H_1, H_2, H_3, H_4$  的询问结果。

**阶段 1**  $\mathcal{A}$  必须首先对身份  $\text{RID}_i$  做  $H_1$  询问之后, 才能将其用做其他询问。 $\mathcal{A}$  不可以利用签名询问的结果来进行解签名询问。 $H_1, H_2, H_3$  和  $H_4$  询问与定理 1 中同理。

**私钥询问。**当  $\mathcal{A}$  对身份为  $\text{RID}_i$  的车辆进行私钥询问时,  $\mathcal{B}$  在列表  $L_1$  中寻找相对应的记录  $(\text{RID}_i, \text{AID}_i)$ 。如果身份为  $\text{RID}_i$  的车辆属于路边单元邀请的车辆组  $V^*$ ,  $\mathcal{B}$  计算私钥  $\text{SK}_i = \alpha \text{AID}_i$  并将其返回  $\mathcal{A}$ ; 否则, 挑战者  $\mathcal{B}$  失败并终止挑战。

**签名询问。** $\mathcal{A}$  对  $(\text{RID}_i, M)$  的签名进行询问, 挑战者  $\mathcal{B}$  选取随机数  $\varepsilon \in Z_p^*$ , 根据  $\text{RID}_i$  的私钥  $\text{SK}_i$  来执行  $H_2$  询问; 计算得到  $X = \varepsilon \text{AID}_i$ ,  $Y = H_2(X, M || t)$  和  $Z_i = (\varepsilon + Y)\text{SK}_i$  对应列表  $L_2$  中  $(\text{AID}_i, \varepsilon, M, t, \text{SK}_i, h_2, Z_i)$ , 则  $\mathcal{B}$  将签名  $\sigma = (Z_i, G)$  返回  $\mathcal{A}$ 。

**解签名询问。**挑战者  $\mathcal{B}$  接收到  $\mathcal{A}$  关于签名的解签名询问时, 如果满足  $\text{RID}_2 \neq \text{RID}_b$  且  $\text{RID}_3 \neq \text{RID}_c$ , 那么  $\mathcal{B}$  执行解密操作并将其结果返回给  $\mathcal{A}$ ; 否则,  $\mathcal{B}$  输出  $\perp$ , 即输入的密文无效, 无法执行解密操作。

**伪造。**最后  $\mathcal{A}$  输出一个有效的签名  $(\text{RID}_i, M, \sigma)$ ,  $\mathcal{B}$  计算得到  $Y = H_2(X, M)$ , 其中  $X = \varepsilon \text{AID}_i$  是  $\text{RID}_i$  的原始签名公钥。 $\mathcal{A}$  验证等式  $e(Z_i, G) = e(X + Y\text{AID}_i, P_{\text{pub}})$  是否成立, 若不成立则  $\mathcal{B}$  失败并终止挑战; 否则, 得到等式  $e(Z_i^*, G) = e(X + Y^*\text{AID}_i, P_{\text{pub}})$ , 其中  $\sigma^* = (Z_i^*, G)$ 。若签名  $\sigma = \sigma^*$ , 那么  $\mathcal{B}$  能够解决 CDH 困难问题,  $\mathcal{B}$  可以输出  $abG = (Y - Y^*)^{-1}(Z_i - Z_i^*)$ 。

假设在多项式时间  $t$  内,  $\mathcal{A}$  最多进行  $q_s$  次签名询问、 $q_{\text{sk}}$  次密钥询问、 $q_u$  次解签名询问和  $q_{H_i} (i = 1, 2, 3, 4)$  次哈希询问。与定理 1 的概率分析过程相同, 挑战者  $\mathcal{B}$  成功在多项式时间  $t' < 120686q_{H_1}q_{H_2}(t + O(q_{\text{sk}} + q_s + q_uq_{H_2})t_p)2^k / \tau(2^k - 1)$  内解决 CDH 的概率为  $\tau' > 10(q_s + 1)(q_s + q_{H_2})q_{H_1} / (2^k - 1)$ , 即如

果  $\mathcal{A}$  能成功伪造合法的签名, 则挑战者  $\mathcal{B}$  能够解决 CDH 困难问题。但 CDH 问题已被证明是困难的, 所以攻击者  $\mathcal{A}$  无法以可忽略的概率伪造有效的签名欺骗挑战者, 证明了本文方案的签名算法是安全的。证毕。

### 参考文献:

- [1] ZHOU H B, XU W C, CHEN J C, et al. Evolutionary V2X technologies toward the Internet of vehicles: challenges and opportunities[J]. Proceedings of the IEEE, 2020, 108(2): 308-323.
- [2] SUN Y C, WU L, WU S Z, et al. Attacks and countermeasures in the Internet of vehicles[J]. Annals of Telecommunications, 2017, 72(5): 283-295.
- [3] CASEY E. The chequered past and risky future of digital forensics[J]. Australian Journal of Forensic Sciences, 2019, 51(6): 649-664.
- [4] VAN B E, LIU V T. Digital evidence: challenging the presumption of reliability[J]. Journal of Digital Forensic Practice, 2006, 1(1): 19-26.
- [5] BOYEN X. Multipurpose identity-based signcryption[C]//Advances in Cryptology - CRYPTO 2003. Berlin: Springer, 2003: 383-399.
- [6] YU H F, WANG Z C, LI J M, et al. Identity-based proxy signcryption protocol with universal composability[J]. Security and Communication Networks, 2018: 1-11.
- [7] KUMAR R, GOYAL R. On cloud security requirements, threats, vulnerabilities and countermeasures: a survey[J]. Computer Science Review, 2019, 33: 1-48.
- [8] HERBADJI A, GOUMIDI H, HARBI Y, et al. Blockchain for Internet of vehicles security[C]//Blockchain for Cybersecurity and Privacy. First edition. Boca Raton: CRC Press, 2020: 159-197.
- [9] 蔡振华, 林嘉韵, 刘芳. 区块链存储: 技术与挑战[J]. 网络与信息安全学报, 2020, 6(5): 11-20.
- [10] CAI Z H, LIN J Y, LIU F. Blockchain storage: technologies and challenges [J]. Chinese Journal of Network and Information Security, 2020, 6(5): 11-20.
- [11] MALONE L J. Identity-based signcryption[J]. IACR Cryptology ePrint Archive, 2002: 98.
- [12] BELLARE M, NAMPREMPRE C, NEVEN G. Security proofs for identity-based identification and Signature schemes[J]. Journal of Cryptology, 2009, 22(1): 1-61.
- [13] LIBERT B, QUISQUATER J J. A new identity based signcryption scheme from pairings[C]//Proceedings of 2003 IEEE Information Theory Workshop (Cat. No.03EX674). Piscataway: IEEE Press, 2003: 155-158.
- [14] KARATI A, ISLAM S H, BISWAS G P, et al. Provably secure identity-based signcryption scheme for crowdsourced industrial Internet of things environments[J]. IEEE Internet of Things Journal, 2018, 5(4): 2904-2914.
- [15] BONEH D, GENTRY C, LYNN B, et al. Aggregate and verifiably encrypted signatures from bilinear maps[C]//Lecture Notes in Computer Science. Berlin: Springer, 2003: 416-432.
- [16] BLAZE M, BLEUMER G, STRAUSS M. Divertible protocols and atomic proxy cryptography[C]//Lecture Notes in Computer Science. Berlin: Springer, 1998: 127-144.
- [17] HUNDERA N W, MEI Q, XIONG H, et al. A secure and efficient identity-based proxy signcryption in cloud data sharing[J]. KSII Transactions on Internet and Information Systems, 2020, 14(1):

- 455-472.
- [17] LUO W, MA W P. Secure and efficient proxy re-encryption scheme based on key-homomorphic constrained PRFs in cloud computing[J]. Cluster Computing, 2019, 22(2): 541-551.
- [18] 曾诗钦, 霍如, 黄韬, 等. 区块链技术研究综述: 原理、进展与应用[J]. 通信学报, 2020, 41(1): 134-151.  
ZENG S Q, HUO R, HUANG T, et al. Survey of blockchain: principle, progress and application[J]. Journal on Communications, 2020, 41(1): 134-151.
- [19] ZHANG P Y, ZHOU M C. Security and trust in blockchains: architecture, key technologies, and open issues[J]. IEEE Transactions on Computational Social Systems, 2020, 7(3): 790-801.
- [20] ZHANG Y, WU S Y, JIN B, et al. A blockchain-based process provenance for cloud forensics[C]//Proceedings of 2017 3rd IEEE International Conference on Computer and Communications (ICCC). Piscataway: IEEE Press, 2017: 2470-2473.
- [21] MALAMAS V, DASAKLIS T, KOTZANIKOLAOU P, et al. A forensics-by-design management framework for medical devices based on blockchain[C]//Proceedings of 2019 IEEE World Congress on Services (SERVICES). Piscataway: IEEE Press, 2019: 35-40.
- [22] 黄晓芳, 徐蕾, 杨茜. 一种区块链的云计算电子取证模型[J]. 北京邮电大学学报, 2017, 40(6): 120-124.  
HUANG X F, XU L, YANG X. Blockchain model of cloud Forensics (MT)[J]. Journal of Beijing University of Posts and Telecommunications, 2017, 40(6): 120-124.
- [23] OHAM C, KANHERE S S, JURDAK R, et al. A blockchain based liability attribution framework for autonomous vehicles[EB]. 2018.
- [24] 李萌, 司成祥, 祝烈煌. 基于区块链的安全车联网数字取证系统[J].

物联网学报, 2020, 4(2): 49-57.

LI M, SI C X, ZHU L H. Secure vehicular digital forensics system based on blockchain[J]. Chinese Journal on Internet of Things, 2020, 4(2): 49-57.

#### [作者简介]



杨小东 (1981- ), 男, 甘肃天水人, 博士, 西北师范大学教授, 主要研究方向为代理重签名和云计算安全。

席婉婷 (1997- ), 女, 陕西铜川人, 西北师范大学硕士生, 主要研究方向为车联网安全与隐私保护。

王嘉琪 (1997- ), 女, 甘肃兰州人, 西北师范大学硕士生, 主要研究方向为可搜索加密与隐私保护。

陈艾佳 (1995- ), 女, 甘肃兰州人, 西北师范大学硕士生, 主要研究方向为网络与信息安全。

王彩芬 (1963- ), 女, 河北安国人, 博士, 深圳技术大学教授, 主要研究方向为密码学与信息安全。

# 通 信 学 报

## 2021 年 (第 42 卷) 总目次

### 专题: 面向未来移动网络的大规模组网关键技术

	期	编号	页码
面向大规模物联网的随机接入: 现状、挑战与机遇.....			
..... 范平志, 李 里, 陈 欢, 程高峰, 杨林杰, 汤小波	4	[2021098](1)	
面向未来移动网络密集连接的关键技术综述.....			
..... 钱志鸿, 肖 琳, 王 雪	4	[2021094](22)	
大规模无线通信网络移动边缘计算和缓存研究.....			
..... 黄永明, 郑 冲, 张征明, 尤肖虎	4	[2021096](44)	
面向 B5G/6G 的三三三网络体系架构和优化学习机制.....			
..... 朱近康, 柴名扬, 周武旻	4	[2021095](62)	
联合时域-波束域非正交多址接入.....			
..... 张朝阳, 吴佳佳, 王 珏, 周 楚	4	[2021099](76)	
工业物联网中大规模受损边缘计算网络修复机制.....			
..... 田 辉, 伍 浩, 田 洋, 任建阳, 崔亚娟, 艾文宝, 袁健华	4	[2021100](89)	
基于无标度网络的车联网连通性研究.....			
..... 韩 涛, 贺 威, 代 俊, 左 勇, 杨 旻, 葛晓虎	4	[2021101](100)	
面向密集多波束组网的卫星通信系统资源调度算法.....			
..... 何元智, 彭 聪, 于季弘, 刘 韵	4	[2021102](109)	
基于自私行为分析的超密集 D2D 中继选择算法.....			
..... 王义君, 张有旭, 刘大鹄, 陈桂芬	4	[2021103](119)	

### 专题: 卫星通信技术

卫星互联网若干关键技术研究.....			
..... 张更新, 王运峰, 丁晓进, 洪 涛, 刘子威, 张 晨	8	[2021156](1)	
高动态卫星 DSSS 信号 Turbo 迭代捕获算法.....			
..... 姜春晓, 王佳蔚	8	[2021153](15)	
基于正交时频空技术的低轨卫星通信的安全分析.....			
..... 李 赞, 胡俊凡, 李 兵, 石 嘉, 司江勃	8	[2021158](25)	
卫星互联网路由技术现状及展望.....			
..... 朱立东, 张 勇, 贾高一	8	[2021166](33)	
基于邻居卫星负载状态的低轨卫星分布式路由算法.....			
..... 杨明川, 薛冠昌, 李清毅	8	[2021165](43)	

### 专题: 确定性网络

基于软件定义的时间敏感网络跨域调度机制.....			
..... 汪 硕, 黄玉栋, 黄 韬, 霍 如, 刘韵洁	10	[2021182](1)	
针对工业控制拓扑的确定性局部多点故障检测方法.....			
..... 梁若舟, 赵曦滨, 万 海	10	[2021202](10)	
结合 SDN 控制器的 TSN 周期性带宽预留值计算方法.....			
..... 苏建忠, 张华宇, 朱海龙	10	[2021204](23)	
基于 SRv6 的确定性网络服务共享保护方案.....			
..... 李硕朋, 方 娟, 陈 肯	10	[2021203](32)	

面向工业互联网的 5G-U 与时间敏感网络融合架构与技术.....		
.....蔡岳平, 李 栋, 许 驰, 王 振, 张潇文	10	[2021161](43)

**专题：计算机通信与网络系统安全技术**

对抗机器学习在网络入侵检测领域的应用.....	刘奇旭, 王君楠, 尹 捷, 陈艳辉, 刘嘉熹	11	[2021193](1)
上下文感知的安卓应用程序漏洞检测研究.....	秦佳伟, 张 华, 严寒冰, 何能强, 涂腾飞	11	[2021198](13)
基于区块链和联邦学习的边缘计算隐私保护方法.....			
.....方 晨, 郭渊博, 王一丰, 胡永进, 马佳利, 张 晗, 胡阳阳	11	[2021190](28)	
SDN 控制层泛洪防御机制研究：检测与缓解.....	周启钊, 于俊清, 李 冬	11	[2021191](41)
面向理性用户的秘密重构设计模型.....	刘 海, 田有亮, 唐 莹, Jianbing Ni, 马建峰	11	[2021195](54)

**学 术 论 文**

基于动态概率攻击图的云环境攻击场景构建方法.....	王文娟, 杜学绘, 单棣斌	1	[2021004](1)
车载边缘计算中任务卸载和服务缓存的联合智能优化.....			
.....刘 雷, 陈 晨, 冯 杰, 裴庆祺, 何 辞, 窦志斌	1	[2021017](18)	
基于 Worker 权重差分进化与 Top-k 排序的结果汇聚算法.....	邢玉萍, 詹永照	1	[2021010](27)
面向进程控制流劫持攻击的拟态防御方法.....	潘传幸, 张 铮, 马博林, 姚 远, 季新生	1	[2021013](37)
基于并联 DPMZM 的大动态范围微波光子混频系统.....	高永胜, 史芳静, 谭佳俊, 樊养余	1	[2021003](48)
支持冷启动用户推荐的区块链服务发布方案.....	董学文, 刘昊哲, 乔 慧, 郑佳伟	1	[2021032](57)
面向 6G 的雾无线接入网内生安全数据共享机制研究.....	刘 杨, 李 珺, 陈文韵, 彭木根	1	[2021005](67)
基于稳健卡尔曼滤波的倾斜探测电离层 MUF 短期预报方法.....	李国军, 郑广发, 叶昌荣, 周银萍	1	[2021011](79)
YOLOv3-A: 基于注意力机制的交通标志检测网络.....	郭 璠, 张泳祥, 唐 璘, 李伟清	1	[2021031](87)
基于 Highway-BiLSTM 网络的汉语谓语中心词识别研究.....			
.....黄瑞章, 靳文繁, 陈艳平, 秦永彬, 郑庆华	1	[2021027](100)	
格上基于身份的增量签名方案.....	田苗苗, 陈 静, 仲 红	1	[2021037](108)
制造云服务组合中支持服务关联的 QoS 感知评估模型.....	谢晓兰, 曾兰英, 翟青海	1	[2021021](118)
基于同态加密的 DBSCAN 聚类隐私保护方案.....	贾春福, 李瑞琪, 王雅飞	2	[2021026](1)
安全高效的两方协同 ECDSA 签名方案.....	王 婧, 吴黎兵, 罗 敏, 何德彪	2	[2021019](12)
车联网中基于 MEC 的 V2X 协同缓存和资源分配.....	李方伟, 张海波, 王子心	2	[2021007](26)
基于分时 MDP 的出租车载客预测推荐技术研究.....	王 桐, 高 山, 龚慧雯, 孙 博	2	[2021002](37)
基于多目标效用优化的分布式数据交易算法.....			
.....黄小红, 张 勇, 闪德胜, 钱叶魁, 韩 璐, 李丹丹, 丛 群	2	[2021034](52)	

基于 CAZAC 序列的低复杂度抗频偏同步算法	宫丰奎, 文 妮, 李 果, 高 洋	2	[2021038](64)
分布式排队中退避树的深度优先遍历算法	王文鼎, 张延贺, 吴 炜, 柏 琛, 王 斌	2	[2021044](72)
基于判别式受限玻尔兹曼机的数字调制识别	李正权, 林 媛, 李梦雅, 刘 洋, 吴 琼, 邢 松	2	[2021012](81)
基于多尺度近端特征拼接网络的高光谱图像分类方法	高红民, 曹雪莹, 陈忠昊, 花再军, 李臣明, 陈 月	2	[2021024](92)
通信特定辐射源识别的多特征融合分类方法	何遵文, 侯 帅, 张万成, 张 焱	2	[2021028](103)
基于相对熵和 $K$ -means 的形状相似差分隐私轨迹保护机制	朱素霞, 刘抒伦, 孙广路	2	[2021008](113)
物联网数据收集中无人机路径智能规划	付 澍, 杨祥月, 张海君, 陈 晨, 喻 鹏, 简 鑫, 刘 敏	2	[2021036](124)
高误码率下 LDPC 稀疏校验矩阵重建	吴昭军, 张立民, 钟兆根, 刘仁鑫	3	[2021009](1)
基于 NTRU 的多密钥同态代理重加密方案及其应用	李瑞琪, 贾春福, 王雅飞	3	[2021023](11)
基于对抗补丁的可泛化的 Grad-CAM 攻击方法	司念文, 张文林, 屈 丹, 常禾雨, 李盛祥, 牛 铜	3	[2021025](23)
基于层级注意力机制的链接预测模型研究	赵晓娟, 贾 焰, 李爱平, 陈 恺	3	[2021057](36)
LTE 和 Wi-Fi 网络的双时间尺度未授权频谱划分算法	吴伟华, 刘润滋, 杨清海	3	[2021059](45)
多源异构数据融合的城市私家车流量预测研究	刘晨曦, 王 东, 陈慧玲, 李仁发	3	[2021018](54)
基于信道相关性的物理层安全性能分析	吴宣利, 许智聪, 王禹辰, 李 勇	3	[2021066](65)
基于高性能包处理架构 VPP 的带内网络遥测系统	潘 恬, 林兴晨, 张 娇, 黄 韬, 刘韵洁	3	[2021016](75)
基于 PSO 优化模糊 C 均值的 WSN 分簇路由算法	孙爱晶, 李世昌, 张艺才	3	[2021053](91)
基于无线供能反向散射通信系统安全性的稳健机会约束优化算法设计	郝万明, 谢金坤, 孙钢灿, 朱政宇, 周一青	3	[2021048](100)
分层超立方网络的可靠性评估	刘西蒙, 张郁芳, 周书明, 李小燕	3	[2021064](111)
基于执行体划分的防御增强型动态异构冗余架构	吴 铤, 胡程楠, 陈庆南, 陈安邦, 郑秋华	3	[2021022](122)
轻量级密码算法 TWINE 的唯密文故障分析	李 玮, 汪梦林, 谷大武, 李嘉耀, 蔡天培, 徐光伟	3	[2021039](135)
基于上下文学习的电力物联网接入控制方法	周振宇, 贾泽晗, 廖海君, 赵雄文, 张 磊	3	[2021062](150)
雾计算中细粒度属性更新的外包计算访问控制方案	杜瑞忠, 闫沛文, 刘 妍	3	[2021063](160)
负载约束的 C-V2X 车辆缓存节点选择算法	徐哲鑫, 高楷蒙, 贾文康, 吴 怡	3	[2021065](171)
D2D 协作边缘缓存系统中基于传输时延的缓存策略	蔡 艳, 吴 凡, 朱洪波	3	[2021042](183)
SQLMVED: 基于多变体执行的 SQL 注入运行时防御系统	马博林, 张 铮, 刘 浩, 邬江兴	4	[2021046](127)

云环境下安全的可验证多关键词搜索加密方案.....  
.....张键红, 武梦龙, 王 晶, 刘 沛, 姜正涛, 彭长根 4 [2021054](139)

基于 Pignistic 概率转换和奇异值分解的证据冲突度量方法.....  
.....郭兴林, 孙振晓, 周昱瑶, 漆莲芝, 张 谊 4 [2021086](150)

基于信誉积分的路况信息共享中共谋攻击节点检测方法..... 玄世昌, 汤 浩, 杨 武 4 [2021051](158)

类 MARS 密码结构的线性特性及其优化设计..... 王念平, 洪礼荣 4 [2021068](169)

基于基扩展模型的改进正则化正交匹配追踪 V2X 快时变 SC-FDMA 信道估计..... 廖 勇, 蔡志镛 4 [2021081](177)

基于 IRS 辅助的 SWIPT 物联网系统安全波束成形设计.....  
.....朱政宇, 徐金雷, 孙钢灿, 王 宁, 郝万明 4 [2021060](185)

频谱知识图谱: 面向未来频谱管理的智能引擎..... 孙佳琛, 王金龙, 丁国如, 陈 瑾, 龚玉萍 5 [2021084](1)

基于区间决策图的威胁处置策略快速匹配..... 张玲翠, 李凤华, 房 梁, 郭云川, 李子孚 5 [2021074](13)

基于 LSTM 与改进残差网络优化的异常流量检测方法..... 麻文刚, 张亚东, 郭 进 5 [2021109](23)

基于多特征自适应融合的区块链异常交易检测方法..... 朱会娟, 陈锦富, 李致远, 殷尚男 5 [2021030](41)

基于最小能耗的多无人机无线网络安全数据卸载策略..... 崔高峰, 徐媛媛, 张尚宏, 王卫东 5 [2021085](51)

基于散射体信息的室内 NLOS 多站协作定位算法.....  
.....谢良波, 李 升, 周 牧, 李 泽, 田增山, 王 亚, 付长友 5 [2021070](63)

具有可撤销功能的属性协同访问控制方案..... 彭长根, 彭宗凤, 丁红发, 田有亮, 刘荣飞 5 [2021058](75)

基于 SWIPT 的吞吐量最优化 NOMA 全双工中继选择策略..... 李陶深, 施安妮, 王 哲, 何 璐 5 [2021061](87)

结合粒子滤波及度量学习的目标跟踪方法..... 王洪雁, 张莉彬, 陈国强, 汪祖民, 管志远 5 [2021087](98)

基于连续干扰消除和交替方向乘子法的混合预编码设计.....  
.....赵雄文, 刘 瑶, 张 钰, 耿绥燕, 秦 鹏, 周振宇 5 [2021114](111)

基于信息熵与遗传算法的并行关联规则增量挖掘算法..... 毛伊敏, 邓千虎, 陈志刚 5 [2021052](122)

基于 BCP 的联合委托学习模型及协议..... 高 胜, 向 康, 田有亮, 谭伟杰, 冯 涛, 吴晓雪 5 [2021089](137)

面向海洋观测传感网的计算卸载方法研究..... 苏 新, 薛溟阳, 周一青, 朱金秀 5 [2021067](149)

多智能体协作场景下基于强化学习值分解的计算卸载策略.....  
.....张 鹏, 田 辉, 赵鹏涛, 贺 硕, 童一帆 6 [2021121](1)

联邦学习中基于时分多址接入的用户调度策略..... 陶梅霞, 王 栋, 孙 瑞, 张乃夫 6 [2021056](16)

区块链 PCN 的高效路由策略..... 霍 如, 倪 东, 卢 华, 夏云峰, 汪 硕, 黄 韬, 刘韵洁 6 [2021113](30)

基于深度确定性策略梯度的随机路由防御方法..... 徐潇雨, 胡 浩, 张红旗, 刘玉岭 6 [2021093](41)

城市场景中车联网时空数据分析及其通达性方法.....  
.....程久军, 原桂远, 崔 杰, 周爱国, 吕 博, 李光耀 6 [2021110](52)

基于 DRL 的联邦学习节点选择方法 .....	贺文晨, 郭少勇, 邱雪松, 陈连栋, 张素香	6	[2021111](62)
基于改进灰狼优化的复杂网络重要节点识别算法 .....	顾秋阳, 吴宝, 孙兆洋, 池仁勇	6	[2021088](72)
基于有监督判别投影的网络安全数据降维算法 .....	郭方方, 吕宏武, 任威霖, 王瑞妮	6	[2021117](84)
下行 MIMO 广播信道中基于偏袒干扰消除的回溯干扰对齐方案 .....			
.....	李劲夫, 冯文江, 王文收, 蒋卫恒, 杨崇海	6	[2021092](94)
差分隐私下多重一致性约束问题的逼近方法 .....	蔡剑平, 刘西蒙, 熊金波, 应作斌, 吴英杰	6	[2021122](107)
基于多智能体元强化学习的车联网协同服务缓存和计算卸载 .....	宁兆龙, 张凯源, 王小洁, 郭磊	6	[2021104](118)
基于属性签名标识的 SDN 数据包转发验证方案 .....	常朝稳, 金建树, 韩培胜, 祝现威	6	[2021079](131)
具有可信约束的分布式存储因果一致性模型 .....	田俊峰, 张俊涛, 王彦磊	6	[2021091](145)
源节点电池容量受限的菱形信道最优传输策略 .....	李陶深, 孙莉, 王哲	6	[2021069](158)
基于虚拟机字节码注入的 Android 应用程序隐私保护机制 .....	宋宇波, 陈琪, 宋睿, 胡爱群	6	[2021115](171)
基于威胁情报的网络安全态势感知模型 .....	张红斌, 尹彦, 赵冬梅, 刘滨	6	[2021106](182)
车联网中视频语义驱动的资源分配算法 .....	陈九九, 冯春燕, 郭彩丽, 杨洋, 孙启政, 朱美逸	7	[2021080](1)
自适应的时空多样性联合调度策略设计 .....	全青, 郭云飞, 霍树民, 王亚文, 蔺羽佳, 张凯	7	[2021119](12)
智能变电站通信业务优先级及其队列调度方法 .....			
.....	李俊娥, 陆秋余, 刘剑, 袁凯, 田薇, 彭弼君	7	[2021107](25)
基于犹豫模糊集的不等长序列识别方法及应用 .....	李双明, 关欣, 孙贵东	7	[2021118](41)
公有云中身份基多源 IoT 终端数据 PDP 方案 .....	王化群, 刘哲, 何德彪, 李继国	7	[2021077](52)
基于高阶路径相似度的复杂网络链路预测方法 .....	顾秋阳, 吴宝, 池仁勇	7	[2021055](61)
基于端址重载的 SDN 包转发验证 .....	吴平, 常朝稳, 马莹莹	7	[2021108](70)
基于一维 CNN 的多入多出 OSTBC 信号协作调制识别 .....	安泽亮, 张天骐, 马宝泽, 邓盼, 徐雨晴	7	[2021142](84)
基于生成对抗网络的僵尸网络检测 .....	邹福泰, 谭越, 王林, 蒋永康	7	[2021082](95)
多接收机自由扩散分子通信信道建模 .....	孙卓, 鲍煦, 林颀, 张文策	7	[2021151](107)
基于结构链逆向的内存碎片文件雕刻算法 .....	李炳龙, 周振宇, 张宇, 张和禹, 常朝稳	7	[2021143](117)
基于无证书签密的车联网社会网络安全通信机制 .....	张文波, 黄文华, 冯景瑜	7	[2021144](128)
基于深度图嵌入的无人机自组网链路预测 .....	舒坚, 王启宁, 刘琳岚	7	[2021083](137)
基于公交车缓存的车联网位置隐私保护方案 .....	崔杰, 陈学峰, 张静, 魏璐, 仲红	7	[2021132](150)
基于谱聚类的异构蜂窝超密集网络高效资源分配算法 .....			
.....	王雪, 刘京, 孙佳妮, 张继真, 钱志鸿	7	[2021141](162)
基于深度学习的传感云 sink 节点最优能效 SWIPT 波束成形设计 .....			
.....	王哲, 李陶深, 葛丽娜, 张桂芬, 吴敏	7	[2021131](176)

认知容量收集网络中网络切片频谱共享策略.....	黄 杰, 杨 凡, 谢应昭, 左 迅, 邱 天	7	[2021137](189)
基于张量分解的卷积盲源分离方法 .....	马宝泽, 张天骐, 安泽亮, 邓 盼	8	[2021140](52)
基于深度学习的压缩感知 FDD 大规模 MIMO 系统稀疏信道估计算法.....	.....黄 源, 何怡刚, 吴裕庭, 程彤彤, 隋永波, 宁曙光	8	[2021128](61)
动态密码结构抵抗差分密码分析能力评估.....	王念平, 郭祉成	8	[2021112](70)
高效的决策树隐私分类服务协议 .....	马立川, 彭佳怡, 裴庆祺, 朱浩瑾	8	[2021149](80)
视频主观观测实验启发的 HEVC 感知帧内码率控制 .....	.....公衍超, 王 玲, 刘 颖, 杨楷芳, 林庆帆, 王富平	8	[2021146](90)
基于密钥协商的防范 DHCP 中间人攻击方案 .....	姚志强, 竺智荣, 叶帼华	8	[2021154](103)
多径环境下联合时间反演和 PCA 降维的阵列幅相误差校正 .....	李方伟, 鲁佳文, 王明月	8	[2021145](111)
隐私保护的 VANET 警告信息发布协议 .....	刘 辉, 刘鑫衍, 许 艳, 仲 红, 王 梦	8	[2021135](120)
知识图与行为图混合嵌入的学习者偏好预测 .....	李晓光, 宫 磊, 李晓莉, 张 昕, 于 戈	8	[2021125](130)
雾计算中基于无配对 CP-ABE 可验证的访问控制方案.....	董江涛, 闫沛文, 杜瑞忠	8	[2021162](139)
在线目标分类及自适应模板更新的孪生网络跟踪算法.....	陈志旺, 张忠新, 宋 娟, 雷海鹏, 彭 勇	8	[2021127](151)
基于差分隐私的连续位置隐私保护机制.....	李洪涛, 任晓宇, 王 洁, 马建峰	8	[2021123](164)
基于描述语境特征词与改进 GSDMM 模型的服务聚类方法.....	胡 强, 沈嘉吉, 荆广辉, 杜军威	8	[2021150](176)
软件异构冗余执行系统的安全能力分析.....	马博林, 张 铮, 任 权, 张高斐, 邬江兴	9	[2021176](1)
基于物理层网络编码的无人机中继网络资源优化.....	杨君一, 李 博, 张钦宇	9	[2021172](12)
基于随机时变图的时间确定性网络路由算法.....	王 鹏, 张修社, 索 龙, 史可懿	9	[2021138](21)
采用定长节点分类窗口的低误码平台 LT 编码算法 .....	宋 鑫, 程乃平, 倪淑燕, 廖育荣, 雷拓峰	9	[2021155](31)
IoT 下 CapBAC 规则语义表示及其时间间隔粗糙性分析 .....	梁晓艳, 杜瑞忠	9	[2021075](43)
基于差分隐私的轨迹隐私保护方案 .....	陈 思, 付安民, 苏 铨, 孙怀江	9	[2021168](54)
图神经网络的标签翻转对抗攻击 .....	吴翼腾, 刘 伟, 于洪涛	9	[2021167](65)
基于运行时验证的边缘服务器 DoS 攻击检测方法.....	于 斌, 张 南, 陆 旭, 段振华, 田 聪	9	[2021169](75)
天地一体化信息安全动态赋能架构.....	张玲翠, 许瑶冰, 李风华, 房 梁, 郭云川, 李子孚	9	[2021180](87)
结合图像加密与深度学习的高容量图像隐写算法.....	杨晓元, 毕新亮, 刘 佳, 黄思远	9	[2021134](96)
通用可组合框架下的公平理性委托计算.....	田有亮, 蒋小霞	9	[2021126](106)
编排图驱动的区块链业务过程管理框架.....	俞东进, 韦懿杰, 孙笑笑, 倪 可, 沈沪军	9	[2021171](120)
ERDOF: 基于相对熵权密度离群因子的离群点检测算法.....	.....张忠平, 刘伟雄, 张玉婷, 邓 禹, 魏棉鑫	9	[2021152](133)
基于轮廓自动生成的构造式图像隐写方法.....	周志立, 王美民, 杨高波, 朱剑宇, 孙星明	9	[2021174](144)

素数阶群上基于非对称的身份基环签名	侯红霞, 张明瑞, 赵艳琦, 董晓丽	9	[2021159](155)
基于时变钟差消除的室内载波相位定位算法	范绍帅, 荣志强, 田辉, 李立华, 秦晓琦	9	[2021164](165)
基于同义词扩展和标签传递机制的文本无载体信息隐藏方法	张祯, 倪嘉铭, 姚晔, 龚礼春, 王玉娟, 吴国华	9	[2021139](173)
基于 DNN 的 Sub-6 GHz 辅助毫米波网络功率分配算法	孙长印, 刘李延, 江帆, 姜静	9	[2021170](184)
部分频带干扰下的 OFDM 系统干扰检测与分集抑制算法	李果, 文妮, 宫丰奎, 张剑, 张思瀚	9	[2021173](194)
支持差异化可协商的数据通信机制	寇文龙, 李凤华, 董秀则, 曹晓刚, 耿魁, 李青	10	[2021183](55)
加密去重场景下基于 AONT 和 NTRU 的密钥更新方案	贾春福, 哈冠雄, 武少强, 陈杭, 李瑞琪	10	[2021187](67)
云计算中基于时间和隐私保护的撤销可追踪的数据共享方案	张嘉伟, 马建峰, 马卓, 李腾	10	[2021206](81)
毫米波 MIMO 系统中基于自适应梯度算法的混合预编码	张煜, 张治, 董晓岱	10	[2021207](95)
语义引导的遮挡行人再识别注意力网络	任雪娜, 张冬明, 包秀国, 李冰	10	[2021184](106)
基于 Telemetry 架构的数据中心网络纳秒级时间同步	张千里, 张超凡, 王继龙, 唐翔宇, 沈钰晨, 王会	10	[2021147](117)
融合注意力胶囊的深度因子分解机模型	顾亦然, 姚朱鹏, 杨海根	10	[2021185](130)
基于区块链的多用户环境中公钥可搜索加密方案	郑东, 朱天泽, 郭瑞	10	[2021130](140)
大规模 MIMO-TRDMA 系统中的改进 SOR 信号检测算法	王明月, 李方伟, 景小荣, 张海波, 熊军洲	10	[2021205](153)
基于关联信息提取的恶意域名检测方法	张斌, 廖仁杰	10	[2021181](162)
基于 NLP 的文本相似度检测方法	代晓丽, 刘世峰, 宫大庆	10	[2021192](173)
基于分圆陪集的量子 BCH 码的构造	邢莉娟, 李卓	10	[2021194](182)
混合智能反射表面结构辅助的毫米波通信信道估计	傅友华, 陈栋	10	[2021197](189)
面向正常拟合迁移学习模型的成员推理攻击	陈晋音, 上官文昌, 张京京, 郑海斌, 郑雅羽, 张旭鸿	10	[2021209](197)
端到端时延上限确定的服务链部署算法	王泽南, 张娇, 汪硕, 黄韬, F.Richard Yu	11	[2021189](66)
基于矩阵填充问题的五轮零知识身份认证方案	王后珍, 蔡鑫伟, 郭岩, 张焕国	11	[2021212](79)
面向无人机网络的属性代理签名方案	贺蕾, 马建峰, 魏大卫	11	[2021210](87)
人工智能物联网中面向智能任务的语义通信方法	刘传宏, 郭彩丽, 杨洋, 冯春燕, 孙启政, 陈九九	11	[2021214](97)
基于有效 AP 选择和多分类 LDA 的室内定位算法	刘桂岐, 钱志鸿, 李华亮, 孙佳妮, 冯一诺, 王雪	11	[2021211](109)

基于实例结构的不完备多标签学习 ..... 陈天柱, 李风华, 郭云川, 李子孚 11 [2021186](121)

深度学习数据窃取攻击在数据沙箱模式下的威胁分析与防御方法研究 .....  
..... 潘鹤中, 韩培义, 向夏雨, 段少明, 庄荣飞, 刘川意 11 [2021215](133)

基于拓扑分析的区域级网络抗毁性研究 ..... 安常青, 刘玉家, 王 会, 郑志延, 喻 涛, 王继龙 11 [2021179](145)

基于 CSI 张量分解的室内 Wi-Fi 指纹定位方法 ..... 周 牧, 龙玥辛, 蒲巧林, 王 勇, 何 维 11 [2021218](159)

基于去噪复数 FastICA 和稀疏重构的相干信号欠定 DOA 估计 ..... 侯 进, 李昀喆, 李天宇 11 [2021219](172)

面向无人机雷达通信一体化系统的轨迹与资源联合优化 .....  
..... 范绍帅, 王煜菲, 田 辉, Jie Zhang, 史金鑫 11 [2021201](182)

多核低冗余表示学习的稳健多视图子空间聚类方法 .....  
..... 李 骛, 王 卓, 于晓洋, 陈德运, 张英涛, 孙广路 11 [2021217](193)

捕获效应下基于比特检测的多分支树 RFID 标签识别协议 .....  
..... 张莉涓, 范明秋, 雷 磊, 王 勇, 袁代数 11 [2021216](205)

QML: 一种混合空间索引结构 ..... 崔 栋, 温巧燕, 张 华, 王华伟 12 [2021229](1)

基于身份的可穿戴签名方案 ..... 杨冬梅, 陈 越, 魏江宏, 胡学先 12 [2021223](17)

基于旋转置乱的索引跳频抗干扰加密方法 ..... 鲁信金, 雷 菁, 施育鑫 12 [2021239](27)

基于 Bartlett 和多分类 F 检验侧信道泄露评估 ..... 王娅茹, 唐 明 12 [2021235](35)

OFDM 中一种有效的基于分段非线性压扩的 PAPR 抑制算法 .....  
..... 邢智童, 李 云, 彭德义, 张本思, 刘凯明, 刘元安 12 [2021230](44)

MIMO-OFDM 系统的信道与脉冲噪声联合估计方法 ..... 吕新荣, 李有明, 国 强 12 [2021238](54)

基于无线信道信息的 5G 与 TSN 联合调度机制研究 .....  
..... 孙 雷, 王健全, 林尚静, 马彰超, 李 卫, Qilian Liang, 黄 蓉 12 [2021224](65)

基于路由状态因果链的域间路由不稳定溯源检测方法 .....  
..... 陈 迪, 邱 菡, 张万里, 朱会虎, 朱俊虎, 王清贤 12 [2021221](76)

基于不完全重合信号的单快拍 DOA 估计算法研究 ..... 曲明超, 司伟建, 袁雅芝 12 [2021232](88)

面向 B5G 网络的高效切换认证与安全密钥更新机制 .....  
..... 崔琪楣, 赵文静, 顾晓阳, 朱增宝, 朱晓喧, 陶小峰, 倪 巍 12 [2021240](96)

基于多时间段优化贝叶斯网络的车载容迟网络路由算法 ..... 吴家皋, 郭亚航, 蔡沈磊, 刘林峰 12 [2021222](109)

脉冲噪声下基于平滑循环相关熵谱的调制识别方法 ..... 戴江安, 栾声扬, 赵明龙, 张兆军, 邱天爽 12 [2021231](121)

Cell-Free 大规模 MIMO 系统中基于传输时延的缓存策略研究 .....  
..... 王 蕊, 申 敏, 何 云, 刘香燕 12 [2021234](134)

基于干扰对齐的 NGSO 星座系统同频干扰抑制 .....  
..... 杜 冰, 李家旺, 王先梅, 李 伟, 刘向南, 张海君 12 [2021236](144)

低开销的 NB-IoT 节点群组身份安全认证协议 .....	常相茂, 占俊, 王志伟	12	[2021228](152)
周期为 $N \equiv 1(\text{mod}4)$ 的平衡最优几乎二元序列对 .....	彭秀平, 李红晓, 王仕德, 林洪彬	12	[2021078](163)
IRS 辅助的认知反向散射通信网络性能增强方案 .....	吕斌, 曹怡, 李健, 齐婷	12	[2021233](172)
基于残差密集网络的频谱感知方法 .....	盖建新, 薛宪峰, 南瑞祥, 吴静谊	12	[2021220](182)
基于区块链的双重可验证云存储方案 .....	冯涛, 孔繁琪, 柳春岩, 马蓉, Maher Albettar	12	[2021225](192)
基于三维双流网络的视频目标移除篡改取证 .....	熊礼治, 曹梦琦, 付章杰	12	[2021226](202)

## 综 述

未来网络技术与发展趋势综述 .....	黄韬, 刘江, 汪硕, 张晨, 刘韵洁	1	[2021006](130)
区块链网络安全保障: 攻击与防御 .....	江沛佩, 王骞, 陈艳姣, 李琦, 沈超	1	[2021035](151)
机器学习在信道建模中的应用综述 .....	刘留, 张建华, 樊圆圆, 于力, 张嘉驰	2	[2021001](134)
移动设备加密流量的用户信息探测研究展望 .....	张腾飞, 余顺争	2	[2021040](154)
面向自动驾驶的边缘计算技术研究综述 .....	吕品, 许嘉, 李陶深, 徐文彪	3	[2021045](190)
DNS 隐蔽信道综述 .....	刁嘉文, 方滨兴, 崔翔, 王忠儒, 甘蕊灵, 冯林, 姜海	5	[2021090](164)
拟态多执行体调度算法研究进展 .....	朱正彬, 刘勤让, 刘冬培, 王崇	5	[2021072](179)
面向隐私保护的非聚合式数据共享综述 .....	李尤慧子, 殷昱煜, 高洪皓, 金一, 王新珩	6	[2021120](195)
高精度室内定位研究评述及未来演进展望 .....	王慧强, 高凯旋, 吕宏武	7	[2021136](198)
物联网安全研究综述: 威胁、检测与防御 .....	杨毅宇, 周威, 赵尚儒, 刘聪, 张宇辉, 王鹤, 王文杰, 张玉清	8	[2021124](188)
基于强化学习的移动视频流业务码率自适应算法研究进展 .....	杜丽娜, 卓力, 杨硕, 李嘉锋, 张菁	9	[2021178](205)
自编码器及其应用综述 .....	来杰, 王晓丹, 向前, 宋亚飞, 权文	9	[2021160](218)
工业互联网感知通信控制协同融合技术研究综述 .....	田辉, 贺硕, 林尚静, 范绍帅, 聂高峰, 蒋秀蓉	10	[2021177](211)
轨道角动量光信号处理研究进展 .....	刘俊, 王健	11	[2021148](217)
云虚拟化平台可信证明技术研究综述 .....	涂碧波, 程杰, 夏豪骏, 张坤, 孙瑞娜	12	[2021213](212)

## 学 术 通 信

基于 ARIMA-RNN 组合模型的云服务器老化预测方法 .....	孟海宁, 童新宇, 石月开, 朱磊, 冯锴, 黑新宏	1	[2021015](163)
非线性光谱展宽载波的湍流信道高速传输特性 .....	王天枢, 张莹, 于策, 董芳, 马万卓, 刘显著	1	[2021014](172)

基于短包通信的 NOMA 下行链路安全传输 .....	孙钢灿, 赵少柯, 郝万明, 朱政宇	2	[2021041](168)
DWB-AES: 基于 AES 的动态白盒实现方法 .....	王 滨, 陈 思, 陈加栋, 王 星	2	[2021020](177)
RBFT: 基于 Raft 集群的拜占庭容错共识机制 .....	黄冬艳, 李 浪, 陈 斌, 王 波	3	[2021043](209)
基于属性的多授权中心身份认证方案 .....	唐 飞, 包佳立, 黄永洪, 黄 东, 王惠莅	3	[2021047](220)
基于多通道 GAN 的图像去噪算法 .....	王洪雁, 杨 晓, 姜艳超, 汪祖民	3	[2021049](229)
高带外抑制特性微波陶瓷波导滤波器的设计 .....	梁 飞, 蒙顺良, 吕文中	4	[2021029](194)
基于深度学习的电离层参数预测研究 .....	冯蕴天, 吴 霞, 许 雄, 张荣庆	4	[2021097](202)
基于深度强化学习的能源互联网智能巡检任务分配机制 .....			
.....徐思雅, 邢逸斐, 郭少勇, 杨 超, 邱雪松, 孟洛明		5	[2021071](191)
基于区块链的分布式 EHR 细粒度可追溯方案 .....	应作斌, 斯元平, 马建峰, 刘西蒙	5	[2021033](205)
基于网络编码的协作恢复机制线性可解性研究 .....	殷 俊, 沙雪琪, 王 磊, 张登银, 杨余旺	5	[2021050](216)
车联网中可证安全的匿名可追溯快速组认证协议 .....	张海波, 黄宏武, 刘开健, 贺晓帆	6	[2021073](213)
低功耗蓝牙 5.0 邻居发现协议时延模型研究 .....	骆冰清, 王佩佩, 王正康, 孙知信	6	[2021105](226)
快时变 FDD 大规模 MIMO 系统智能 CSI 反馈方法 .....	廖 勇, 王 帅, 孙 宁	7	[2021129](211)
适用于再生编码分布式存储的轻量型隐私保护审计方案 .....			
.....刘光军, 郭网媚, 熊金波, 刘西蒙, 董长宇		7	[2021116](220)
基于深层信息散度最大化的说话人确认方法 .....	陈 晨, 彤娅峰, 季超群, 陈德运, 何勇军	7	[2021133](231)
基于区块链的铁路工程施工安全监测数据共享关键技术研究 .....			
.....刘玉红, 杨 亮, 朴春慧, 张志国		8	[2021076](206)
内存与片上渗透缓存之间数据迁移的理论分析 .....			
.....胡九川, 范东睿, 程建聪, 严 龙, 叶笑春, 李灵枝, 万良易, 钟海斌		8	[2021157](217)
基于均值漂移图聚类的复杂网络社区发现方法 .....	郭飞鹏, 卢琦蓓, 孙兆洋	9	[2021163](231)
基于 CPN 的安全协议形式化建模及安全分析方法 .....	龚 翔, 冯 涛, 杜谨泽	9	[2021175](240)
基于 NOMA-MEC 系统的信息年龄最小化研究 .....	李保罡, 武文静, 段 晓, 戚银城	10	[2021200](222)
基于深度学习的广义频分复用系统时频双选择信道估计 .....	王 莹, 任 军, 史 可, 林 彬	10	[2021188](233)
混合双跳 PLC-FSO 通信系统的性能分析 .....	陈生海, 言小琴, 黎 赛, 杨 亮	10	[2021199](243)
双粒度轻量级漏洞代码切片方法评估模型 .....	张 炳, 文 峥, 赵宇轩, 王 莹, 任家东	11	[2021196](233)
基于空间感知的多级损失目标跟踪对抗攻击方法 .....			
.....程 旭, 王莹莹, 张年杰, 付章杰, 陈北京, 赵国英		11	[2021208](242)
基于块对角化的通信雷达频谱共存设计 .....	韩凯峰, 黄立涛, 陈 力, 王志勤	12	[2021227](226)
基于签密和区块链的车联网电子证据共享方案 .....	杨小东, 席婉婷, 王嘉琪, 陈艾佳, 王彩芬	12	[2021237](236)

# Journal on Communications

## Contents List Vol.42 (2021)

### Topics: Strategic Technologies to Massive Connecting for the Future Mobile Networks

	No.	Pages
Random access for massive Internet of things: current status, challenges and opportunities .....		
..... <i>FAN Pingzhi, LI Li, CHEN Huan, CHENG Gaofeng, YANG Linjie, TANG Xiaobo</i>	4	[2021098](1)
Review on strategic technology of dense connection for the future mobile network.....		
..... <i>QIAN Zhihong, XIAO Lin, WANG Xue</i>	4	[2021094](22)
Research on mobile edge computing and caching in massive wireless communication network.....		
..... <i>HUANG Yongming, ZHENG Chong, ZHANG Zhengming, YOU Xiaohu</i>	4	[2021096](44)
Three-three-three network architecture and learning optimization mechanism for B5G/6G.....		
..... <i>ZHU Jinkang, CHAI Mingyang, ZHOU Wuyang</i>	4	[2021095](62)
Joint time and beam domain non-orthogonal multiple access .....		
..... <i>ZHANG Zhaoyang, WU Jiajia, WANG Jue, ZHOU Chu</i>	4	[2021099](76)
Recovery mechanism of large-scale damaged edge computing network in industrial Internet of things.....		
..... <i>TIAN Hui, WU Hao, TIAN Yang, REN Jianyang, CUI Yajuan, AI Wenbao, YUAN Jianhua</i>	4	[2021100](89)
Connectivity analysis of IoV based on scale-free network .....		
..... <i>HAN Tao, HE Wei, DAI Jun, ZUO Yong, YANG Yang, GE Xiaohu</i>	4	[2021101](100)
Resource scheduling algorithm of satellite communication system for future multi-beam dense networking .....		
..... <i>HE Yuanzhi, PENG Cong, YU Jihong, LIU Yun</i>	4	[2021102](109)
Relay selection algorithm based on selfish behavior analysis in ultra-dense D2D .....		
..... <i>WANG Yijun, ZHANG Youxu, LIU Dakun, CHEN Guifen</i>	4	[2021103](119)

### Topics: Satellite Communications Technology

Research on several key technologies of satellite Internet.....		
..... <i>ZHANG Gengxin, WANG Yunfeng, DIGN Xiaojin, HONG Tao, LIU Ziwei, ZHANG Chen</i>	8	[2021156](1)
Turbo iterative acquisition algorithm for satellite high-mobility DSSS signal .....		
..... <i>JIANG Chunxiao, WANG Jiawei</i>	8	[2021153](15)
Secrecy analysis for orthogonal time frequency space technique based LEO satellite communication.....		
..... <i>LI Zan, HU Junfan, LI Bing, SHI Jia, SI Jiangbo</i>	8	[2021158](25)
Current status and future prospects of routing technologies for satellite Internet.....		
..... <i>ZHU Lidong, ZHANG Yong, JIA Gaoyi</i>	8	[2021166](33)
Neighbor satellite load based low orbit satellite distributed routing algorithm .....		
..... <i>YANG Mingchuan, XUE Guanchang, LI Qingyi</i>	8	[2021165](43)



Short-term prediction method of oblique sounding ionosphere MUF based on robust Kalman filter .....	LI Guojun, ZHENG Guangfa, YE Changrong, ZHOU Yiping	1	[2021011](79)
YOLOv3-A: a traffic sign detection network based on attention mechanism.....	GUO Fan, ZHANG Yongxiang, TANG Jin, LI Weiqing	1	[2021031](87)
Research on Chinese predicate head recognition based on Highway-BiLSTM network.....	HUANG Ruizhang, JIN Wenfan, CHEN Yanping, QIN Yongbin, ZHENG Qinghua	1	[2021027](100)
Identity-based incremental signature scheme from lattices .....	TIAN Miaomiao, CHEN Jing, ZHONG Hong	1	[2021037](108)
QoS aware evaluation model supporting service correlation in manufacturing cloud service composition .....	XIE Xiaolan, ZENG Lanying, ZHAI Qinghai	1	[2021021](118)
Privacy protection scheme of DBSCAN clustering based on homomorphic encryption .....	JIA Chunfu, LI Ruiqi, WANG Yafei	2	[2021026](1)
Secure and efficient two-party ECDSA signature scheme .....	WANG Jing, WU Libing, LUO Min, HE Debiao	2	[2021019](12)
V2X collaborative caching and resource allocation in MEC-based IoV.....	LI Fangwei, ZHANG Haibo, WANG Zixin	2	[2021007](26)
Research on forecast and recommendation technology of taxi passengers based on time-varying Markov decision process .....	WANG Tong, GAO Shan, GONG Huiwen, SUN Bo	2	[2021002](37)
Distributed data trading algorithm based on multi-objective utility optimization .....	HUANG Xiaohong, ZHANG Yong, SHAN Desheng, QIAN Yekui, HAN Lu, LI Dandan, CONG Qun	2	[2021034](52)
Low-complexity and frequency-offset-robust synchronization algorithm based on CAZAC sequence .....	GONG Fengkui, WEN Ni, LI Guo, GAO Yang	2	[2021038](64)
Depth first traversal algorithm for the back-off tree of distributed queuing .....	WANG Wennai, ZHANG Yanhe, WU Wei, BAI Chen, WANG Bin	2	[2021044](72)
Digital modulation recognition based on discriminative restricted Boltzmann machine .....	LI Zhengquan, LIN Yuan, LI Mengya, LIU Yang, WU Qiong, XING Song	2	[2021012](81)
Hyperspectral image classification method based on multi-scale proximal feature concatenate network .....	GAO Hongmin, CAO Xueying, CHEN Zhonghao, HUA Zaijun, LI Chenming, CHEN Yue	2	[2021024](92)
Multi-feature fusion classification method for communication specific emitter identification .....	HE Zunwen, HOU Shuai, ZHANG Wancheng, ZHANG Yan	2	[2021028](103)
Shape similarity differential privacy trajectory protection mechanism based on relative entropy and K-means .....	ZHU Suxia, LIU Shulun, SUN Guanglu	2	[2021008](113)
UAV path intelligent planning in IoT data collection .....	FU Shu, YANG Xiangyue, ZHANG Haijun, CHEN Chen, YU Peng, JIAN Xin, LIU Min	2	[2021036](124)
Reconstruction of sparse check matrix for LDPC at high bit error rate .....	WU Zhaojun, ZHANG Limin, ZHONG Zhaogen, LIU Renxin	3	[2021009](1)
Multi-key homomorphic proxy re-encryption scheme based on NTRU and its application .....	LI Ruiqi, JIA Chunfu, WANG Yafei	3	[2021023](11)
Generalized Grad-CAM attacking method based on adversarial patch .....	SI Nianwen, ZHANG Wenlin, QU Dan, CHANG Heyu, LI Shengxiang, NIU Tong	3	[2021025](23)
Research on link prediction model based on hierarchical attention mechanism .....	ZHAO Xiaojuan, JIA Yan, LI Aiping, CHEN Kai	3	[2021057](36)
Two-timescale unlicensed spectrum partitioning algorithm between LTE and Wi-Fi network.....	WU Weihua, LIU Runzi, YANG Qinghai	3	[2021059](45)

Study of forecasting urban private car volumes based on multi-source heterogeneous data fusion.....			
.....	<i>LIU Chenxi, WANG Dong, CHEN Huiling, LI Renfa</i>	3	[2021018](54)
Performance analysis of physical layer security based on channel correlation.....			
.....	<i>WU Xuanli, XU Zhicong, WANG Yuchen, LI Yong</i>	3	[2021066](65)
In-band network telemetry system based on high-performance packet processing architecture VPP.....			
.....	<i>PAN Tian, LIN Xingchen, ZHANG Jiao, HUANG Tao, LIU Yunjie</i>	3	[2021016](75)
WSN clustering routing algorithm based on particle PSO optimized fuzzy C-means.....			
.....	<i>SUN Aijing, LI Shichang, ZHANG Yicai</i>	3	[2021053](91)
Robust chance-constrained optimization algorithm design for secure wireless powered backscatter Communication system.....	<i>HAO Wanming, XIE Jinkun, SUN Gangcan, ZHU Zhengyu, ZHOU Yiqing</i>	3	[2021048](100)
Reliability evaluation of hierarchical hypercube network.....			
.....	<i>LIU Ximeng, ZHANG Yufang, ZHOU Shuming, LI Xiaoyan</i>	3	[2021064](111)
Defense-enhanced dynamic heterogeneous redundancy architecture based on executor partition.....			
.....	<i>WU Ting, HU Chengnan, CHEN Qingnan, CHEN Anbang, ZHENG Qiuhua</i>	3	[2021022](122)
Ciphertext-only fault analysis of the TWINE lightweight cryptosystem algorithm.....			
.....	<i>LI Wei, WANG Menglin, GU Dawu, LI Jiayao, CAI Tianpei, XU Guangwei</i>	3	[2021039](135)
Context-aware learning-based access control method for power IoT.....			
.....	<i>ZHOU Zhenyu, JIA Zehan, LIAO Haijun, ZHAO Xiongwen, ZHANG Lei</i>	3	[2021062](150)
Fine-grained attribute update and outsourcing computing access control scheme in fog computing.....			
.....	<i>DU Ruizhong, YAN Peiwen, LIU Yan</i>	3	[2021063](160)
Vehicular cache nodes selection algorithm under load constraint in C-V2X.....			
.....	<i>XU Zhixin, GAO Kaimeng, JIA Wenkang, WU Yi</i>	3	[2021065](171)
Caching strategy based on transmission delay for D2D cooperative edge caching system.....			
.....	<i>CAI Yan, WU Fan, ZHU Hongbo</i>	3	[2021042](183)
SQLMVED: SQL injection runtime prevention system based on multi-variant execution.....			
.....	<i>MA Bolin, ZHANG Zheng, LIU Hao, WU Jiangxing</i>	4	[2021046](127)
Secure and verifiable multi-keyword searchable encryption scheme in cloud.....			
.....	<i>ZHANG Jianhong, WU Menglong, WANG Jing, LIU Pei, JIANG Zhengtao, PENG Changgen</i>	4	[2021054](139)
Evidence conflict measurement method based on Pignistic probability transformation and singular value decomposition.....	<i>GUO Xinglin, SUN Zhenxiao, ZHOU Yuyao, QI Lianzhi, ZHANG Yi</i>	4	[2021086](150)
Method for detecting collusion attack node in road condition information sharing based on reputation point.....			
.....	<i>XUAN Shichang, TANG Hao, YANG Wu</i>	4	[2021051](158)
Linear property and optimal design of MARS-like cryptographic structure.....			
.....	<i>WANG Nianping, HONG Lirong</i>	4	[2021068](169)
Basis expansion model-based improved regularized orthogonal matching pursuit channel estimation for V2X fast time-varying SC-FDMA.....	<i>LIAO Yong, CAI Zhirong</i>	4	[2021081](177)
Secure beamforming design for IRS-assisted SWIPT Internet of things system.....			
.....	<i>ZHU Zhengyu, XU Jinlei, SUN Gangcan, WANG Ning, HAO Wanming</i>	4	[2021060](185)
Spectrum knowledge graph: an intelligent engine facing future spectrum management.....			
.....	<i>SUN Jiachen, WANG Jinlong, DING Guoru, CHEN Jin, GONG Yuping</i>	5	[2021084](1)
Fastly match threat response policies based on interval decision diagram.....			
.....	<i>ZHANG Lingcui, LI Fenghua, FANG Liang, GUO Yunchuan, LI Zifu</i>	5	[2021074](13)

Abnormal traffic detection method based on LSTM and improved residual neural network optimization .....	MA Wengang, ZHANG Yadong, GUO Jin	5	[2021109](23)
Block-chain abnormal transaction detection method based on adaptive multi-feature fusion .....	ZHU Huijuan, CHEN Jinfu, LI Zhiyuan, YIN Shangnan	5	[2021030](41)
Secure data offloading strategy for multi-UAV wireless networks based on minimum energy consumption.....	CUI Gaofeng, XU Yuanyuan, ZHANG Shanghong, WANG Weidong	5	[2021085](51)
Scatterer information based indoor NLOS multiple base station cooperative localization algorithm .....	XIE Liangbo, LI Sheng, ZHOU Mu, LI Ze, TIAN Zengshan, WANG Ya, FU Changyou	5	[2021070](63)
Attribute-based revocable collaborative access control scheme .....	PENG Changgen, PENG Zongfeng, DING Hongfa, TIAN Youliang, LIU Rongfei	5	[2021058](75)
Optimal relay selection for full duplex SWIPT-NOMA systems with maximal throughput.....	LI Taoshen, SHI Anni, WANG Zhe, HE Lu	5	[2021061](87)
Approach of target tracking combining particle filter and metric learning.....	WANG Hongyan, ZHANG Libin, CHEN Guoqiang, WANG Zumin, GUAN Zhiyuan	5	[2021087](98)
Design of hybrid precoding with successive interference cancellation and alternating direction method of multipliers.....	ZHAO Xiongwen, LIU Yao, ZHANG Yu, GENG Suiyan, QIN Peng, ZHOU Zhenyu	5	[2021114](111)
Parallel association rules incremental mining algorithm based on information entropy and genetic algorithm .....	MAO Yimin, DENG Qianhu, CHEN Zhigang	5	[2021052](122)
BCP-based joint delegation learning model and protocol.....	GAO Sheng, XIANG Kang, TIAN Youliang, TAN Weijie, FENG Tao, WU Xiaoxue	5	[2021089](137)
Research on computing offloading method for maritime observation monitoring sensor network .....	SU Xin, XUE Haoyang, ZHOU Yiqing, ZHU Jinxiu	5	[2021067](149)
Computation offloading strategy in multi-agent cooperation scenario based on reinforcement learning with value-decomposition.....	ZHANG Peng, TIAN Hui, ZHAO Pengtao, HE Shuo, TONG Yifan	6	[2021121](1)
TDMA-based user scheduling policies for federated learning.....	TAO Meixia, WANG Dong, SUN Rui, ZHANG Naifu	6	[2021056](16)
Efficient routing strategy of blockchain-based payment channel network .....	HUO Ru, NI Dong, LU Hua, XIA Yunfeng, WANG Shuo, HUANG Tao, LIU Yunjie	6	[2021113](30)
Random routing defense method based on deep deterministic policy gradient .....	XU Xiaoyu, HU Hao, ZHANG Hongqi, LIU Yuling	6	[2021093](41)
Spatio-temporal data analysis and accessibility method for IoV in an urban scene.....	CHENG Jiujun, YUAN Guiyuan, CUI Jie, ZHOU Aiguo, LYU Bo, LI Guangyao	6	[2021110](52)
Node selection method in federated learning based on deep reinforcement learning .....	HE Wenchen, GUO Shaoyong, QIU Xuesong, CHEN Liandong, ZHANG Suxiang	6	[2021111](62)
Key node identification algorithm for complex network based on improved grey wolf optimization.....	GU Qiuyang, WU Bao, SUN Zhaoyang, CHI Renyong	6	[2021088](72)
Reduction algorithm based on supervised discriminant projection for network security data .....	GUO Fangfang, LYU Hongwu, REN Weilin, WANG Ruini	6	[2021117](84)
Partial interference elimination based retrospective interference alignment scheme in the downlink MIMO broadcast channel.....	LI Jingfu, FENG Wenjiang, WANG Wenshou, JIANG Weiheng, YANG Chonghai	6	[2021092](94)
Approximation method of multiple consistency constraint under differential privacy .....	CAI Jianping, LIU Ximeng, XIONG Jinbo, YING Zuobin, WU Yingjie	6	[2021122](107)

Cooperative service caching and peer offloading in Internet of vehicles based on multi-agent meta-reinforcement learning.....	<i>NING Zhaolong, ZHANG Kaiyuan, WANG Xiaojie, GUO Lei</i>	6	[2021104](118)
Software-defined network packet forwarding verification scheme based on attribute-based signatures identification.....	<i>CHANG Chaowen, JIN Jianshu, HAN Peisheng, ZHU Xianwei</i>	6	[2021079](131)
Distributed storage causal consistency model with trusted constraint.....	<i>TIAN Junfeng, ZHANG Juntao, WANG Yanbiao</i>	6	[2021091](145)
Optimal transmission strategy of diamond channel with limited battery capacity of source node.....	<i>LI Taoshen, SUN Li, WANG Zhe</i>	6	[2021069](158)
Android application privacy protection mechanism based on virtual machine bytecode injection.....	<i>SONG Yubo, CHEN Qi, SONG Rui, HU Aiqun</i>	6	[2021115](171)
Network security situational awareness model based on threat intelligence.....	<i>ZHANG Hongbin, YIN Yan, ZHAO Dongmei, LIU Bin</i>	6	[2021106](182)
Video semantics-driven resource allocation algorithm in Internet of vehicles.....	<i>CHEN Jiujiu, FENG Chunyan, GUO Caili, YANG Yang, SUN Qizheng, ZHU Meiyi</i>	7	[2021080](1)
Design of self-adaptive spatio-temporal diversity joint scheduling strategy.....	<i>TONG Qing, GUO Yunfei, HUO Shumin, WANG Yawen, MAN Yujia, ZHANG Kai</i>	7	[2021119](12)
Communication service priority in smart substation and its queue scheduling method.....	<i>LI Jun'e, LU Qiuyu, LIU Jian, YUAN Kai, TIAN Wei, PENG Bijun</i>	7	[2021107](25)
Recognition method based on hesitant fuzzy set for unequal length sequences and its application.....	<i>LI Shuangming, GUAN Xin, SUN Guidong</i>	7	[2021118](41)
Identity-based provable data possession scheme for multi-source IoT terminal data in public cloud.....	<i>WANG Huaqun, LIU Zhe, HE Debiao, LI Jiguo</i>	7	[2021077](52)
Link prediction method based on the similarity of high path.....	<i>GU Qiuyang, WU Bao, CHI Renyong</i>	7	[2021055](61)
Port address overloading based packet forwarding verification in SDN.....	<i>WU Ping, CHANG Chaowen, MA Yingying</i>	7	[2021108](70)
Cooperative modulation recognition based on one-dimensional convolutional neural network for MIMO-OSTBC signal.....	<i>AN Zeliang, ZHANG Tianqi, MA Baoze, DENG Pan, XU Yuqing</i>	7	[2021142](84)
Botnet detection based on generative adversarial network.....	<i>ZOU Futai, TAN Yue, WANG Lin, JIANG Yongkang</i>	7	[2021082](95)
Channel modeling of molecular communication via free diffusion with multiple receiver.....	<i>SUN Zhuo, BAO Xu, LIN Jie, ZHANG Wence</i>	7	[2021151](107)
Memory fragment file carving algorithm based on the reverse of the structure chain.....	<i>LI Binglong, ZHOU Zhenyu, ZHANG Yu, ZHANG Heyu, CHANG Chaowen</i>	7	[2021143](117)
Secure communication mechanism for VSN based on certificateless signcryption.....	<i>ZHANG Wenbo, HUANG Wenhua, FENG Jingyu</i>	7	[2021144](128)
UAV ad hoc network link prediction based on deep graph embedding.....	<i>SHU Jian, WANG Qining, LIU Linlan</i>	7	[2021083](137)
Bus cache-based location privacy protection scheme in the Internet of vehicles.....	<i>CUI Jie, CHEN Xuefeng, ZHANG Jing, WEI Lu, ZHONG Hong</i>	7	[2021132](150)
Spectral clustering-based energy-efficient resource allocation algorithm in heterogeneous cellular ultra-dense network.....	<i>WANG Xue, LIU Jing, SUN Jiani, ZHANG Jizhen, QIAN Zhihong</i>	7	[2021141](162)

Optimal energy-efficiency beamforming design for SWIPT-enabled sink in sensor cloud based on deep learning .....	WANG Zhe, LI Taoshen, GE Lina, ZHANG Guifen, WU Min	7	[2021131](176)
Network slicing with spectrum sharing strategy in cognitive capacity harvesting network .....	HUANG Jie, YANG Fan, XIE Yingzhao, ZUO Xun, QIU Tian	7	[2021137](189)
Convolutive blind source separation method based on tensor decomposition .....	MA Baoze, ZHANG Tianqi, AN Zeliang, DENG Pan	8	[2021140](52)
Deep learning for compressed sensing based sparse channel estimation in FDD massive MIMO systems .....	HUANG Yuan, HE Yigang, WU Yuting, CHENG Tongtong, SUI Yongbo, NING Shuguang	8	[2021128](61)
Security evaluation against differential cryptanalysis for dynamic cryptographic structure .....	WANG Nianping, GUO Zhicheng	8	[2021112](70)
Efficient privacy-preserving decision tree classification protocol .....	MA Lichuan, PENG Jiayi, PEI Qingqi, ZHU Haojin	8	[2021149](80)
HEVC perceptual intra-frame rate control inspired by video subjective observation experiment .....	GONG Yanchao, WANG Ling, LIU Ying, YANG Kaifang, LIN Qingfan, WANG Fuping	8	[2021146](90)
Achieving resist against DHCP man-in-the-middle attack scheme based on key agreement .....	YAO Zhiqiang, ZHU Zhirong, YE Guohua	8	[2021154](103)
Gain and phase errors calibration for joint time reversal and PCA dimensionality reduction over multipath environment .....	LI Fangwei, LU Jiawen, WANG Mingyue	8	[2021145](111)
Privacy protection of warning message publishing protocol in VANET .....	LIU Hui, LIU Xinyan, XU Yan, ZHONG Hong, WANG Meng	8	[2021135](120)
Learner preferences prediction with mixture embedding of knowledge and behavior graph .....	LI Xiaoguang, GONG Lei, LI Xiaoli, ZHANG Xin, YU Ge	8	[2021125](130)
Verifiable access control scheme based on unpaired CP-ABE in fog computing .....	DONG Jiangtao, YAN Peiwen, DU Ruizhong	8	[2021162](139)
Tracking algorithm of Siamese network based on online target classification and adaptive template update .....	CHEN Zhiwang, ZHANG Zhongxin, SONG Juan, LEI Haipeng, PENG Yong	8	[2021127](151)
Continuous location privacy protection mechanism based on differential privacy .....	LI Hongtao, REN Xiaoyu, WANG Jie, MA Jianfeng	8	[2021123](164)
Service clustering method based on description context feature words and improved GSDMM model .....	HU Qiang, SHEN Jiaji, JING Guanghui, DU Junwei	8	[2021150](176)
Security capability analysis of software-based heterogeneous redundant execution system .....	MA Bolin, ZHANG Zheng, REN Quan, ZHANG Gaofei, WU Jiangxing	9	[2021176](1)
Resource optimization for UAV relay networks based on physical-layer network coding .....	YANG Junyi, LI Bo, ZHANG Qinyu	9	[2021172](12)
Time deterministic network routing algorithm based on stochastic temporal graph .....	WANG Peng, ZHANG Xiushe, SUO Long, SHI Keyi	9	[2021138](21)
Low error floor LT coding algorithm by using fixed-length node classification window .....	SONG Xin, CHENG Naiping, NI Shuyan, LIAO Yurong, LEI Tuofeng	9	[2021155](31)
Semantic representation and interval roughness analysis of IoT CapBAC rules .....	LIANG Xiaoyan, DU Ruizhong	9	[2021075](43)
Trajectory privacy protection scheme based on differential privacy .....	CHEN Si, FU Anmin, SU Mang, SUN Huaijiang	9	[2021168](54)

Label flipping adversarial attack on graph neural network .....	<i>WU Yiteng, LIU Wei, YU Hongtao</i>	9	[2021167](65)
Runtime verification approach for DoS attack detection in edge servers .....	<i>YU Bin, ZHANG Nan, LU Xu, DUAN Zhenhua, TIAN Cong</i>	9	[2021169](75)
Dynamic security-empowering architecture for space-ground integration information network .....	<i>ZHANG Lingcui, XU Yaobing, LI Fenghua, FANG Liang, GUO Yunchuan, LI Zifu</i>	9	[2021180](87)
High-capacity image steganography algorithm combining image encryption and deep learning .....	<i>YANG Xiaoyuan, BI Xinliang, LIU Jia, HUANG Siyuan</i>	9	[2021134](96)
Fair and rational delegation of computation in the universally composable framework .....	<i>TIAN Youliang, JIANG Xiaoxia</i>	9	[2021126](106)
Choreography-driven business process management framework based on blockchain .....	<i>YU Dongjin, WEI Yijie, SUN Xiaoxiao, NI Ke, SHEN Hujun</i>	9	[2021171](120)
ERDOF: outlier detection algorithm based on entropy weight distance and relative density outlier factor .....	<i>ZHANG Zhongping, LIU Weixiong, ZHANG Yuting, DENG Yu, WEI Mianxin</i>	9	[2021152](133)
Generative steganography method based on auto-generation of contours .....	<i>ZHOU Zhili, WANG Meimin, YANG Gaobo, ZHU Jianyu, SUN Xingming</i>	9	[2021174](144)
ID-based ring signature on prime order group from asymmetric pairing .....	<i>HOU Hongxia, ZHANG Mingrui, ZHAO Yanqi, DONG Xiaoli</i>	9	[2021159](155)
Indoor carrier phase positioning algorithm based on time-varying clock error elimination .....	<i>FAN Shaoshuai, RONG Zhiqiang, TIAN Hui, LI Lihua, QIN Xiaoyi</i>	9	[2021164](165)
Text coverless information hiding method based on synonyms expansion and label delivery mechanism .....	<i>ZHANG Zhen, NI Jiaming, YAO Ye, GONG Lichun, WANG Yujuan, WU Guohua</i>	9	[2021139](173)
DNN-based Sub-6 GHz assisted millimeter wave network power allocation algorithm .....	<i>SUN Changyin, LIU Liyan, JIANG Fan, JIANG Jing</i>	9	[2021170](184)
Interference detection and diversity suppression algorithm of OFDM system under partial-band jamming .....	<i>LI Guo, WEN Ni, GONG Fengkui, ZHANG Jian, ZHANG Sihan</i>	9	[2021173](194)
Differentiated and negotiable mechanism for data communication .....	<i>KOU Wenlong, LI Fenghua, DONG Xiuze, CAO Xiaogang, GENG Kui, LI Qing</i>	10	[2021183](55)
AONT-and-NTRU-based rekeying scheme for encrypted deduplication .....	<i>JIA Chunfu, HA Guanxiong, WU Shaoqiang, CHEN Hang, LI Ruiqi</i>	10	[2021187](67)
Time-based and privacy protection revocable and traceable data sharing scheme in cloud computing .....	<i>ZHANG Jiawei, MA Jianfeng, MA Zhuo, LI Teng</i>	10	[2021206](81)
Adaptive gradient algorithm for hybrid precoding in mmWave MIMO system .....	<i>ZHANG Yu, ZHANG Zhi, DONG Xiaodai</i>	10	[2021207](95)
Semantic guidance attention network for occluded person re-identification .....	<i>REN Xuena, ZHANG Dongming, BAO Xiuguo, LI Bing</i>	10	[2021184](106)
Nanosecond level time synchronization in datacenter network based on Telemetry architecture .....	<i>ZHANG Qianli, ZHANG Chaofan, WANG Jilong, TANG Xiangyu, SHEN Zhengchen, WANG Hui</i>	10	[2021147](117)
Deep factorization machine model based on attention capsule .....	<i>GU Yiran, YAO Zhupeng, YANG Haigen</i>	10	[2021185](130)
Public key searchable encryption scheme in blockchain-enabled multi-user environment .....	<i>ZHENG Dong, ZHU Tianze, GUO Rui</i>	10	[2021130](140)
Improved SOR signal detection algorithm in massive MIMO-TRDMA systems .....	<i>WANG Mingyue, LI Fangwei, JING Xiaorong, ZHANG Haibo, XIONG Junzhou</i>	10	[2021205](153)

Malicious domain name detection method based on associated information extraction	10	[2021181](162)
..... ZHANG Bin, LIAO Renjie		
Text similarity detection method based on NLP	10	[2021192](173)
..... DAI Xiaoli, LIU Shifeng, GONG Daqing		
Construction of quantum BCH code based on cyclotomic coset	10	[2021194](182)
..... XING Lijuan, LI Zhuo		
Channel estimation for hybrid intelligent reflecting surface structure assisted mmWave communications	10	[2021197](189)
..... FU Youhua, CHEN Dong		
Membership inference attacks against transfer learning for generalized model	10	[2021209](197)
..... CHEN Jinyin, SHANGGUAN Wenchang, ZHANG Jingjing, ZHENG Haibin, ZHENG Yayu, ZHANG Xuhong		
Service chain deployment algorithms for deterministic end-to-end delay upper bound	11	[2021189](66)
..... WANG Ze'nan, ZHANG Jiao, WANG Shuo, HUANG Tao, F.Richard Yu		
5-pass zero-knowledge identity authentication scheme based on matrix completion problem	11	[2021212](79)
..... WANG Houzhen, CAI Xinwei, GUO Yan, ZHANG Huanguo		
Attribute-based proxy signature scheme for unmanned aerial vehicle networks	11	[2021210](87)
..... HE Lei, MA Jianfeng, WEI Dawei		
Intelligent task-oriented semantic communication method in artificial intelligence of things	11	[2021214](97)
..... LIU Chuanhong, GUO Caili, YANG Yang, FENG Chunyan, SUN Qizheng, CHEN Jiujiu		
Indoor positioning algorithm based on effective AP selection and multi-class LDA	11	[2021211](109)
..... LIU Guiqi, QIAN Zhihong, LI Hualiang, SUN Jiani, FENG Yinuo, WANG Xue		
Instance structure based multi-label learning with missing labels	11	[2021186](121)
..... CHEN Tianzhu, LI Fenghua, GUO Yunchuan, LI Zifu		
Threat analysis and defense methods of deep-learning-based data theft in data sandbox mode	11	[2021215](133)
..... PAN Hezhong, HAN Peiyi, XIANG Xiayu, DUAN Shaoming, ZHUANG Rongfei, LIU Chuanyi		
Research on the invulnerability of regional network based on topology analysis	11	[2021179](145)
..... AN Changqing, LIU Yujia, WANG Hui, ZHENG Zhiyan, YU Tao, WANG Jilong		
Indoor Wi-Fi fingerprint localization method based on CSI tensor decomposition	11	[2021218](159)
..... ZHOU Mu, LONG Yuexin, PU Qiaolin, WANG Yong, HE Wei		
Underdetermined DOA estimation of coherent signals based on denoising complex FastICA and sparse reconstruction	11	[2021219](172)
..... HOU Jin, LI Yunzhe, LI Tianyu		
Joint optimization of trajectory and resource allocation for UAV integrated radar and communication system	11	[2021201](182)
..... FAN Shaoshuai, WANG Yufei, TIAN Hui, Jie Zhang, SHI Jinxin		
Robust multiview subspace clustering method based on multi-kernel low-redundancy representation learning	11	[2021217](193)
..... LI Ao, WANG Zhuo, YU Xiaoyang, CHEN Deyun, ZHANG Yingtao, SUN Guanglu		
Capture-aware bit-detecting $M$ -ary tree protocol for RFID tag identification	11	[2021216](205)
..... ZHANG Lijuan, FAN Mingqiu, LEI Lei, WANG Yong, YUAN Daishu		
QML: a hybrid spatial index structure	12	[2021229](1)
..... CUI Dong, WEN Qiaoyan, ZHANG Hua, WANG Huawei		
Identity-based puncturable signature scheme	12	[2021223](17)
..... YANG Dongmei, CHEN Yue, WEI Jianghong, HU Xuexian		
Index modulation aided frequency hopping anti-jamming and encryption method based on rotation scrambling	12	[2021239](27)
..... LU Xinjin, LEI Jing, SHI Yuxin		
Side channel leakage assessment with the Bartlett and multi-classes F-test	12	[2021235](35)
..... WANG Yaru, TANG Ming		
Efficient PAPR reduction algorithm in OFDM based on nonlinear piecewise companding	12	[2021230](44)
..... XING Zhitong, LI Yun, PENG Deyi, ZHANG Benshi, LIU Kaiming, LIU Yuan'an		

Joint channel and impulsive noise estimation method for MIMO-OFDM systems .....  
 ..... *LYU Xinrong, LI Youming, GUO Qiang* 12 [2021238](54)

Research on 5G-TSN joint scheduling mechanism based on radio channel information .....  
 ..... *SUN Lei, WANG Jianquan, LIN Shangjing, MA Zhangchao, LI Wei, Qilian Liang, HUANG Rong* 12 [2021224](65)

Interdomain routing instability traceable detection method based on route state causal chain .....  
 ..... *CHEN Di, QIU Han, ZHANG Wanli, ZHU Huihu, ZHU Junhu, WANG Qingxian* 12 [2021221](76)

Research on single snapshot DOA estimation algorithm based on incompletely overlapped signal .....  
 ..... *QU Mingchao, SI Weijian, YUAN Yazhi* 12 [2021232](88)

Efficient handover authentication and secure key-updating mechanism for B5G networks .....  
 ..... *CUI Qimei, ZHAO Wenjing, GU Xiaoyang, ZHU Zengbao, ZHU Xiaoxuan, TAO Xiaofeng, NI Wei* 12 [2021240](96)

Vehicular delay tolerant network routing algorithm based on optimized multi-period Bayesian network .....  
 ..... *WU Jiagao, GUO Yahang, CAI Shenlei, LIU Linfeng* 12 [2021222](109)

Pol-CCES based modulation recognition method under impulsive noise .....  
 ..... *DAI Jiang'an, LUAN Shengyang, ZHAO Minglong, ZHANG Zhaojun, QIU Tianshuang* 12 [2021231](121)

Research on caching strategy based on transmission delay in Cell-Free massive MIMO systems .....  
 ..... *WANG Rui, SHEN Min, HE Yun, LIU Xiangyan* 12 [2021234](134)

Suppression of co-channel interference in NGSO constellation system with interference alignment .....  
 ..... *DU Bing, LI Jiawang, WANG Xianmei, LI Wei, LIU Xiangnan, ZHANG Haijun* 12 [2021236](144)

Low-cost group-based identity security authentication protocol for NB-IoT nodes .....  
 ..... *CHANG Xiangmao, ZHAN Jun, WANG Zhiwei* 12 [2021228](152)

Balanced optimal almost binary sequence pairs of period  $N \equiv 1(\text{mod}4)$  .....  
 ..... *PENG Xiuping, LI Hongxiao, WANG Shide, LIN Hongbin* 12 [2021078](163)

Performance enhancement scheme for IRS-assisted cognitive backscatter communication network .....  
 ..... *LYU Bin, CAO Yi, LI Jian, QI Ting* 12 [2021233](172)

Spectrum sensing method based on residual dense network .....  
 ..... *GAI Jianxin, XUE Xianfeng, NAN Ruixiang, WU Jingyi* 12 [2021220](182)

Dual verifiable cloud storage scheme based on blockchain .....  
 ..... *FENG Tao, KONG Fanqi, LIU Chunyan, MA Rong, Maher Albettar* 12 [2021225](192)

Forensic of video object removal tamper based on 3D dual-stream network .....  
 ..... *XIONG Lizhi, CAO Mengqi, FU Zhangjie* 12 [2021226](202)

### Comprehensive Reviews

Survey of the future network technology and trend .....  
 ..... *HUANG Tao, LIU Jiang, WANG Shuo, ZHANG Chen, LIU Yunjie* 1 [2021006](130)

Securing guarantee of the blockchain network: attacks and countermeasures .....  
 ..... *JIANG Peipei, WANG Qian, CHEN Yanjiao, LI Qi, SHEN Chao* 1 [2021035](151)

Survey of application of machine learning in wireless channel modeling .....  
 ..... *LIU Liu, ZHANG Jianhua, FAN Yuanyuan, YU Li, ZHANG Jiachi* 2 [2021001](134)

Research prospects of user information detection from encrypted traffic of mobile devices .....  
 ..... *ZHANG Tengfei, YU Shunzheng* 2 [2021040](154)

Survey on edge computing technology for autonomous driving .....		
..... <i>LYU Pin, XU Jia, LI Taoshen, XU Wenbiao</i>	3	[2021045](190)
Survey of DNS covert channel .....		
..... <i>DIAO Jiawen, FANG Binxing, CUI Xiang, WANG Zhongru, GAN Ruiling, FENG Lin, JIANG Hai</i>	5	[2021090](164)
Research progress of mimic multi-execution scheduling algorithm .....		
..... <i>ZHU Zhengbin, LIU Qinrang, LIU Dongpei, WANG Chong</i>	5	[2021072](179)
Survey on privacy protection in non-aggregated data sharing .....		
..... <i>LI Youhuizi, YIN Yuyu, GAO Honghao, JIN Yi, WANG Xinheng</i>	6	[2021120](195)
Survey of high-precision localization and the prospect of future evolution .....		
..... <i>WANG Huiqiang, GAO Kaixuan, LYU Hongwu</i>	7	[2021136](198)
Survey of IoT security research: threats, detection and defense .....		
..... <i>YANG Yiyu, ZHOU Wei, ZHAO Shangru, LIU Cong, ZHANG Yuhui, WANG He, WANG Wenjie, ZHANG Yuqing</i>	8	[2021124](188)
Survey on reinforcement learning based adaptive bit rate algorithm for mobile video streaming services .....		
..... <i>DU Li'na, ZHUO Li, YANG Shuo, LI Jiafeng, ZHANG Jing</i>	9	[2021178](205)
Review on autoencoder and its application .....		
..... <i>LAI Jie, WANG Xiaodan, XIANG Qian, SONG Yafei, QUAN Wen</i>	9	[2021160](218)
Survey on cooperative fusion technologies with perception, communication and control coupled in industrial Internet .....		
..... <i>TIAN Hui, HE Shuo, LIN Shangjing, FAN Shaoshuai, NIE Gaofeng, JIANG Xiurong</i>	10	[2021177](211)
Research progress of optical signal processing with orbital angular momentum .....		
..... <i>LIU Jun, WANG Jian</i>	11	[2021148](217)
Overview of research on trusted attestation technology of cloud virtualization platform .....		
..... <i>TU Bibo, CHENG Jie, XIA Haojun, ZHANG Kun, SUN Ruina</i>	12	[2021213](212)

## Correspondences

Cloud server aging prediction method based on hybrid model of auto-regressive integrated moving average and recurrent neural network .....		
..... <i>MENG Haining, TONG Xinyu, SHI Yuekai, ZHU Lei, FENG Kai, HEI Xinhong</i>	1	[2021015](163)
High-speed transmission characteristics of nonlinear spectral broadening carrier in turbulent channel .....		
..... <i>WANG Tianshu, ZHANG Ying, YU Ce, DONG Fang, MA Wanzhuo, LIU Xianzhu</i>	1	[2021014](172)
Secure transmission for NOMA downlink based on short packet communication .....		
..... <i>SUN Gangcan, ZHAO Shaoke, HAO Wanming, ZHU Zhengyu</i>	2	[2021041](168)
DWB-AES: an implementation of dynamic white-box based on AES .....		
..... <i>WANG Bin, CHEN Si, CHEN Jiadong, WANG Xing</i>	2	[2021020](177)
RBFT: a new Byzantine fault-tolerant consensus mechanism based on Raft cluster .....		
..... <i>HUANG Dongyan, LI Lang, CHEN Bin, WANG Bo</i>	3	[2021043](209)
Multi-authority attribute-based identification scheme .....		
..... <i>TANG Fei, BAO Jiali, HUANG Yonghong, HUANG Dong, WANG Huili</i>	3	[2021047](220)
Image denoising algorithm based on multi-channel GAN .....		
..... <i>WANG Hongyan, YANG Xiao, JIANG Yanchao, WANG Zumin</i>	3	[2021049](229)
Design of microwave ceramic waveguide filter with high out-of-band suppression characteristics .....		
..... <i>LIANG Fei, MENG Shunliang, LYU Wenzhong</i>	4	[2021029](194)

Research on ionospheric parameters prediction based on deep learning .....  
..... *FENG Yuntian, WU Xia, XU Xiong, ZHANG Rongqing* 4 [2021097](202)

Deep reinforcement learning based task allocation mechanism for intelligent inspection in energy Internet.....  
..... *XU Siya, XING Yifei, GUO Shaoyong, YANG Chao, QIU Xuesong, MENG Luoming* 5 [2021071](191)

Blockchain-based distributed EHR fine-grained traceability scheme.....  
..... *YING Zuobin, SI Yuanping, MA JianFeng, LIU Ximeng* 5 [2021033](205)

Research on linear solvability of network coding based cooperative recovery scheme.....  
..... *YIN Jun, SHA Xueqi, WANG Lei, ZHANG Dengyin, YANG Yuwang* 5 [2021050](216)

Verifiably secure fast group authentication protocol with anonymous traceability for Internet of vehicles .....  
..... *ZHANG Haibo, HUANG Hongwu, LIU Kaijian, HE Xiaofan* 6 [2021073](213)

Latency model of neighbor discovery based on Bluetooth low energy 5.0.....  
..... *LUO Bingqing, WANG Peipei, WANG Zhengkang, SUN Zhixin* 6 [2021105](226)

Intelligent CSI feedback method for fast time-varying FDD massive MIMO system.....  
..... *LIAO Yong, WANG Shuai, SUN Ning* 7 [2021129](211)

Lightweight privacy protection data auditing scheme for regenerating-coding-based distributed storage .....  
..... *LIU Guangjun, GUO Wangmei, XIONG Jinbo, LIU Ximeng, DONG Changyu* 7 [2021116](220)

Speaker verification method based on deep information divergence maximization .....  
..... *CHEN Chen, RONG Yafeng, JI Chaoqun, CHEN Deyun, HE Yongjun* 7 [2021133](231)

Research on key technologies of safety monitoring data sharing for railway engineering construction based  
on blockchain ..... *LIU Yuhong, YANG Liang, PIAO Chunhui, ZHANG Zhiguo* 8 [2021076](206)

Theoretical analysis for the data immigration between memory and processor percolation cache.....  
..... *HU Jiuchuan, FAN Dongrui, CHENG Jiancong, YAN Long, YE Xiaochun, LI Lingzhi, WAN Liangyi, ZHONG Haibin* 8 [2021157](217)

Complex network community discovery method based on mean shift graph clustering .....  
..... *GUO Feipeng, LU Qibei, SUN Zhaoyang* 9 [2021163](231)

Formal modeling and security analysis method of security protocol based on CPN .....  
..... *GONG Xiang, FENG Tao, DU Jinze* 9 [2021175](240)

Research on the minimizing of information age based on NOMA-MEC system .....  
..... *LI Baogang, WU Wenjing, DUAN Xiao, QI Yincheng* 10 [2021200](222)

Doubly-selective channel estimation for generalized frequency division multiplexing systems based on deep  
learning..... *WANG Ying, REN Jun, SHI Ke, LIN Bin* 10 [2021188](233)

Performance analysis of dual-hop PLC-FSO communication system .....  
..... *CHEN Shenghai, YAN Xiaoqin, LI Sai, YANG Liang* 10 [2021199](243)

Dual-granularity lightweight model for vulnerability code slicing method assessment .....  
..... *ZHANG Bing, WEN Zheng, ZHAO Yuxuan, WANG Ning, REN Jiadong* 11 [2021196](233)

Multi-level loss object tracking adversarial attack method based on spatial perception.....  
..... *CHENG Xu, WANG Yingying, ZHANG Nianjie, FU Zhangjie, CHEN Beijing, ZHAO Guoying* 11 [2021208](242)

Communication-radar coexistence design based on block diagonalization .....  
..... *HAN Kaifeng, HUANG Litao, CHEN Li, WANG Zhiqin* 12 [2021227](226)

Electronic evidence sharing scheme of Internet of vehicles based on signcryption and blockchain.....  
..... *YANG Xiaodong, XI Wanting, WANG Jiaqi, CHEN Aijia, WANG Caifen* 12 [2021237](236)

## 致 谢

《通信学报》自 1980 年创刊以来,承蒙各位专家学者的支持和厚爱,为我刊审阅了大量来稿。在新年到来之际,我们谨向 2021 年关心和支持我刊,在百忙中为我刊审稿的专家学者致以崇高的敬意和深深的感谢。希望各位专家能继续支持我们的工作,感谢你们付出的辛勤劳动! 恭祝各位专家新年快乐!

### 2021 审稿专家名单

(如有遗漏敬请包涵,排名不分先后)

艾 渤 安 鹏 白恩健 白智全 包建荣 包晓安 鲍 煦 边 山 蔡文郁 曹春杰 曹桂兴 曹海林  
曹利峰 曹腾飞 曹卫平 曾 琦 柴争义 常晓林 陈本辉 陈 朝 陈 晨 陈德运 陈东明 陈芳炯  
陈 刚 陈海光 陈海华 陈后金 陈嘉兴 陈 晶 陈 恺 陈鲁生 陈美娟 陈 翔 陈燕俐 陈玉玲  
陈 哲 陈智雄 程 剑 程杰仁 程庆丰 崔琪楣 代 彬 邓晓衡 丁恩杰 丁进良 丁举鹏 丁 群  
丁世飞 丁宇新 董 俊 董丽华 董晓梅 董学文 董 颖 董振江 杜 蛟 杜军平 杜瑞颖 杜瑞忠  
杜之波 方 箭 方 娟 方 巍 冯景瑜 冯 径 冯友宏 付安民 付绍静 付 伟 付永钢 付 钰  
傅友华 高建彬 高 隼 高振国 高志鹏 龚 俭 龚 征 谷大武 顾仁涛 官 科 管 武 桂 冠  
郭 滨 郭方方 郭 磊 郭 庆 郭迎春 韩益亮 何海涛 贺鹏飞 洪 飞 洪劲松 洪 伟 胡东辉  
胡青松 胡学先 胡轶宁 胡永健 胡 勇 胡致远 华 光 华惊宇 黄传河 黄冬艳 黄海生 黄华军  
黄开枝 黄梦醒 黄 韬 黄添强 黄欣沂 霍树民 吉根林 纪其进 贾春福 贾 敏 简 鑫 姜 明  
姜 禹 蒋 鹏 蒋卫恒 金澈清 金晨辉 靳小龙 巨 刚 康海燕 柯品惠 寇 广 赖英旭 兰巨龙  
李爱平 李晨亮 李春国 李德识 李 枫 李古月 李光辉 李 海 李 鹤 李 晖 李建华 李建江  
李 剑 李军怀 李领治 李 宁 李 强 李仁发 李融林 李少谦 李陶深 李婉婷 李伟生 李旭杰  
李 璇 李兴华 李 伊 李勇军 李玉峰 李 云 李正权 李致远 廖 勇 林金朝 林 敏 刘安丰  
刘 飞 刘功亮 刘光军 刘宏展 刘建华 刘连山 刘林峰 刘 留 刘 淼 刘乃安 刘奇旭 刘绍辉  
刘婷婷 刘万涛 刘西蒙 刘玉玲 刘玉岭 刘 渊 刘媛妮 龙 军 卢建民 罗 彪 罗智勇 吕文俊  
马昌社 马东堂 马建峰 马 礼 马 啸 牛少彰 牛奕龙 潘海为 潘 俊 庞辽军 裴 超 裴庆祺  
彭 伟 彭 鑫 普园媛 亓 晋 齐丽娜 钱 峰 钱丽萍 钱亚冠 钱志鸿 乔 蕊 秦宝东 秦 川

卿朝进 邱恭安 邱卫东 曲海鹏 任艳丽 阮 彤 沙学军 尚凤军 余 堃 申利民 沈海澜 沈 航  
 沈 华 沈连丰 沈玉龙 沈振萍 谌 刚 盛泳潘 宋广佳 宋铁成 苏 新 孙 聪 孙国林 谈 玲  
 谭晓衡 汤红波 唐 飞 唐振民 陶小峰 滕志军 田海博 田 辉 田有亮 田增山 万鸣华 汪春霆  
 汪 定 汪 俊 汪一鸣 王 安 王 琛 王尔申 王风宇 王 刚 王高丽 王公仆 王海涛 王海舟  
 王 恒 王洪玉 王 健 王 鹃 王汝言 王瑞锦 王尚广 王仕果 王天枢 王 威 王 巍 王兴元  
 王 毅 王永建 王 勇 王占山 王昭顺 魏 杰 魏忠诚 文伟平 吴 铤 吴 帆 吴 凡 吴 昊  
 吴家皋 吴礼发 吴 蒙 吴 强 吴 巍 吴晓平 吴宣利 吴 怡 吴哲夫 吴振强 武小年 席 亮  
 夏金祥 夏 琦 肖 斌 肖利民 肖绍球 肖 泳 谢绒娜 谢显中 谢 永 邢成文 熊 钢 熊金波  
 熊 余 徐启建 徐少毅 徐位凯 徐雅斌 徐煜华 许文俊 许晓荣 玄世昌 薛广涛 延志伟 闫成新  
 颜学雄 阳春华 杨东升 杨高波 杨恒伏 杨宏宇 杨家轩 杨 健 杨 洁 杨 军 杨 亮 杨万扣  
 杨 维 杨亚涛 杨 哲 杨 震 叶阿勇 叶 苗 于银辉 余礼苏 余翔宇 袁 琪 袁 征 詹 杰  
 张成文 张大龙 张大伟 张 迪 张海波 张海君 张 恒 张焕国 张建敏 张 军 张 科 张 磊  
 张立军 张连明 张 琳 张 平 张士兵 张 涛 张 薇 张 伟 张伟哲 张文彬 张艳硕 张友春  
 张玉军 张玉清 张长江 张治中 赵海涛 赵 亮 赵瑞杰 赵小敏 赵永利 赵 跃 郑福春 郑国强  
 郑 凯 郑学强 郑作亚 仲 红 周建江 周南润 周四望 周亚建 周一青 周 宇 周志刚 朱风华  
 朱 辉 朱建明 朱立东 朱 琦 朱巧明 朱政宇 邹北骥 邹德清

## 2020 年《通信学报》优秀论文

(排名不分先后)

- 曾诗钦, 霍如, 黄韬, 等. 区块链技术研究综述: 原理、进展与应用[J]. 通信学报, 2020, 41(1):134-151.  
ZENG S Q, HUO R, HUANG T, et al. Survey of blockchain: principle, progress and application[J]. Journal on Communications, 2020, 41(1):134-151.
- 袁亮, 俞啸, 丁恩杰, 等. 矿山物联网人-机-环状态感知关键技术研究[J]. 通信学报, 2020, 41(2):1-12.  
YUAN L, YU X, DING E J, et al. Research on key technologies of human-machine-environment states perception in mine Internet of things[J]. Journal on Communications, 2020, 41(2):1-12.
- 徐勇军, 李国权, 陈前斌, 等. 基于非正交多址接入异构携能网络稳健能效资源分配算法[J]. 通信学报, 2020, 41(2): 84-96.  
XU Y J, LI G Q, CHEN Q B, et al. Robust energy efficiency for SWIPT-enabled heterogeneous NOMA network[J]. Journal on Communications, 2020, 41(2): 84-96.
- 肖斌, 景如霞, 毕秀丽, 等. 基于分组 SIFT 的图像复制粘贴篡改快速检测算法[J]. 通信学报, 2020, 41(3): 62-70.  
XIAO B, JING R X, BI X L, et al. Fast copy-move forgery detection algorithm based on group SIFT[J]. Journal on Communications, 2020, 41(3): 62-70.
- 王雪, 金涛, 钱志鸿, 等. D2D 中继辅助通信的能效优化算法研究[J]. 通信学报, 2020, 41(3): 71-79.  
WANG X, JIN T, QIAN Z H, et al. Research on maximizing energy efficiency for relay-aided D2D communication[J]. Journal on Communications, 2020, 41(3): 71-79.
- 赵临东, 庄文芹, 陈建新, 等. 异构蜂窝网络中分层任务卸载: 建模与优化[J]. 通信学报, 2020, 41(4): 34-44.  
ZHAO L D, ZHUANG W Q, CHEN J X, et al. Hierarchical task offloading in heterogeneous cellular network: modeling and optimization[J]. Journal on Communications, 2020, 41(4): 34-44.
- 牛凯, 戴金晟, 朴璿楠. 面向 6G 的极化码与极化处理[J]. 通信学报, 2020, 41(5): 9-17.  
NIU K, DAI J C, PIAO J N. Polar codes and polar processing for 6G wireless systems[J]. Journal on Communications, 2020, 41(5): 9-17.
- 谢莎, 李浩然, 李玲香, 等. 太赫兹通信技术综述[J]. 通信学报, 2020, 41(5): 168-186.  
XIE S, LI H R, LI L X, et al. Survey of terahertz communication technology[J]. Journal on Communications, 2020, 41(5): 168-186.
- 张平, 李世林, 刘宜明, 等. 区块链赋能的边缘异构计算系统中资源调度研究[J]. 通信学报, 2020, 41(10): 1-14.  
ZHANG P, LI S L, LIU Y M, et al. Resource management in blockchain-enabled heterogeneous edge computing system[J]. Journal on Communications, 2020, 41(10): 1-14.
- 赵海涛, 张唐伟, 陈跃, 等. 基于 DQN 的车载边缘网络任务分发卸载算法[J]. 通信学报, 2020, 41(10): 172-178.  
ZHAO H T, ZHANG T W, CHEN Y, et al. Task distribution offloading algorithm of vehicle edge network based on DQN[J]. Journal on Communications, 2020, 41(10): 172-178.

# 通信学报

Journal on Communications



发行代号：  
国内2-676  
国外M395

2021年12月25日出版 定价：98.00元

ISSN 1000-436X



9 771000 436212