

职称申报材料附件

姓名： 陈鸿龙

单位： 控制科学与工程学院

2020 年 3 月
中国石油大学（华东）

目 录

1. 学历学位证书
2. 岗前培训合格证书
3. 国外学习经历证明材料
4. 班主任、学业导师工作经历证明材料
5. 论文首页
6. SCI、EI 收录证明
7. 专利授权书
8. 项目合同书、项目验收报告
9. 成果获奖证书
10. 校优毕业论文指导教师证书
11. 参与平台建设证明材料
12. 学术组织任职证明材料

普通高等学校

毕业证书



学生 陈鸿龙 性别 男，一九八四年九月十七日生，于二〇〇二年九月至二〇〇六年七月在本校 自动化 专业

肆 年制本科学习，修完教学计划规定的全部课程，成绩合格，准予毕业。

校 名：中国石油大学（华东）

校（院）长：



证书编号：104251200605002250

二〇〇六年七月一日



学士学位证书

(普通高等教育本科毕业生)

陈鸿龙，男，

1984年09月生。自2002

年09月至2006年07月



在 信息与控制工程学院

自动化

专业

完成了肆年制本科学历计划，业已毕业。
经审核符合《中华人民共和国学位条例》
的规定，授予 工 学学士学位。

中国石油大学（华东）

学位评定委员会主席

王兆岐

证书编号： 104254062250

二〇〇六年七月一日



硕士学位证书

陈鸿龙，男，1984年9月17日生。在

浙江大学

控制科学与工程

学科（专业）已通过硕士学位的课程

考试和论文答辩，成绩合格。根据《中华人民共和国学位条例》的规定，授予工学硕士学位。

浙 江 大 学

校 长

学位评定委员会主席

杨卫



证书编号：1033532608110343

二〇〇八年十二月三十日

浙江大学

硕士研究生

毕 业 证 书



编号:

103351200802110343

研究生 陈鸿龙 , 性别 男 ,

一九八四年 九 月 十七 日生, 于

二〇〇六年 九 月至二〇〇八年十二月在

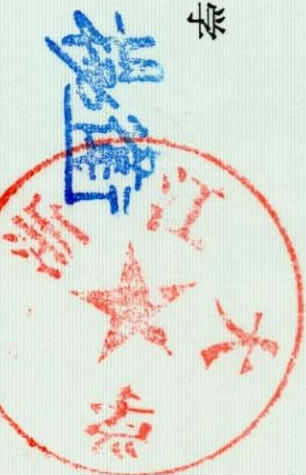
控制科学与工程 专业

学习, 修完硕士研究生培养计划规定的全部课程, 成绩合格, 毕业论文答辩通过, 准予毕业。

浙 江 大 学

校 长

二〇〇八年十二月三十日





THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

This is to certify that

CHEN Honglong

having satisfied the examiners
and having fulfilled all other requirements
has been awarded the degree of

DOCTOR OF PHILOSOPHY

二零一二年十月二十七日

此證

哲學博士

考試及格照章頒授

陈鸿龙

修業期滿

畢業證書

President

Chancellor

Academic Secretary



教務長 湯劉毓芬

校長 唐偉章

校監 梁振英

27 October 2012

01618





教育部留学服务中心

香港、澳门特别行政区 学历学位认证书

教留服认香港[2012]03686号

陈鸿龙，男，中国国籍，1984年9月17日生于福建省。

陈鸿龙2009年2月至2012年8月在香港理工大学(The Hong Kong Polytechnic University)计算学系从事研究，论文通过，于2012年10月获得香港理工大学颁发的毕业证书，并被授予哲学博士学位。

经核查，香港理工大学系中国香港特别行政区正规高等学校。陈鸿龙所获毕业证书经查无误。

香港特别行政区高等教育实行单证书制度。学生所获不同层次学位表明其具有相应的学历。

教育部留学服务中心
港澳台地区学历学位认证办公室
二〇一二年十二月二十四日

中国石油大学(华东)人事处

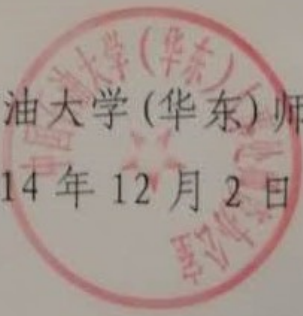
岗前培训合格证明

兹证明中国石油大学(华东)信息与控制工程学院**陈鸿龙**同志于2013年参加山东省组织的高等学校教师岗前培训并取得岗前培训合格证。

特此证明

中国石油大学(华东)师资办公室

2014年12月2日



留学回国人员证明

(2016) 洛 教(文) 证字 2119 号

兹证明 陈鸿龙 (男 ☒、女 ☐) 护照号码 G32556893) 系我国

在 美 国 亚利桑那州立大学 学校 (单位)

的高级研究学者 ☐、访问学者 ☐、博士后 ☒、博士研究生 ☐、硕士研究生 ☐、
本科生 ☐、大专生 ☐、其他留学人员 ☐

在我驻外使 (领) 馆报到日期 2015 年 11 月 28 日

注册入学日期 2015 年 11 月 28 日

毕 (结) 业日期 2016 年 11 月 24 日

拟回国日期 2016 年 11 月 24 日

毕 (结) 业证书名称 _____ 号码 _____

备注 (留学经历描述) _____

留学回国人员签字:

经办人签字:

负责人签字:

教育 (文化) 处 (组) 盖章

2016 年 09 月 14 日

第一联: 交留学回国人员

教育部国际合作与交流司 2012 年制表

注意事项

- 1、本证明只为学成回国工作的留学人员开具。
- 2、本证明由我驻外使 (领) 馆教育 (文化) 处 (组) 在留学人员回国时填写, 不得涂改。
- 3、本证明经使 (领) 馆教育 (文化) 处 (组) 经办人、负责人签字并在第一、第二联加盖公章方为有效。
- 4、第一联由留学人员保存, 其他单位可查验原件, 收存复印件, 不得收取原件。

控制科学与工程学院

班主任/学业导师任职经历及考核证明

陈鸿龙同志于 2013 年 9 月至 2016 年 6 月担任自动化专业 1303 班班主任，于 2017 年 9 月至 2019 年 12 月担任自动化专业 1703 班班主任，于 2019 年 9 月至 2019 年 12 月担任自动化专业 1903 班学业导师。于 2015 年 12 月参加学院的班主任考核，考核结果为优秀，于 2016 年 12 月参加学院的班主任考核，考核结果为合格，于 2017 年 12 月参加学院的班主任考核，考核结果为合格，于 2018 年 12 月参加学院的班主任考核，考核结果为合格，于 2019 年 12 月参加学院的班主任考核，考核结果为优秀，于 2019 年 12 月参加学院的学业导师考核，考核结果为合格。

特此证明！



优秀班主任 (100人)

地球科学与技术学院 (9人) :

吴会胜 曹丹平 曾 喆 李福来 杜庆军 杨国权 林腊梅
苏妮娜 裴仰文

石油工程学院 (11人) :

付帅师 刘德新 刘志慧 刘玉泉 史玉才 周 童 娄 敏
崔传智 徐加放 白 莉 黄维安

化学工程学院 (17人) :

丁传芹 刘会娥 吴文婷 吴萍萍 国亚东 孙 娟 张 兰
曲剑波 杨修洁 杨向平 段红玲 蒋文春 薄守石 钮根林
陈 坤 陈金庆 张 松

机电工程学院 (13人) :

王彦富 谢 静 李雨桐 殷晓康 张 辛 曹爱请 牛俊邦
张大磊 赵 明 刘恩洋 赵 严 崔运静 赵学进

信息与控制工程学院 (7人) :

仇志华 周 鹏 张 欣 王宇红 陈鸿龙 马文忠 魏晓媛



优秀班主任（100人）

地球科学与技术学院（5人）：

马存飞 李志娜 范宜仁 赵建华 曹文俊

石油工程学院（7人）：

王子振 孙永鹏 张亚 赵欣 娄敏 贾寒 郭胜来

化学工程学院（9人）：

王纯正 刘义 杨军卫 杨修洁 吴文婷 张金弘 孟亦飞
夏薇 覃正兴

机电工程学院（10人）：

马宁 孔得朋 石永军 闫怡飞 纪佳馨 杜洋 吴宝贵
陈敬凯 殷晓康 蔡宝平

储运与建筑工程学院（9人）：

毛宁 朱秀星 朱建鲁 刘翠伟 宋明 高伟 黄思凝
管友海 滕厚兴

材料科学与工程学院（6人）：

于思荣 李邵仁 宋玉强 黄万群 曹宁 甄玉花

新能源学院（13人）

马文忠 王宗明 左海强 巩志强 许伟伟 许康 李祥林
李斌 李强 张克舫 张丽霞 林日亿 徐海亮

海洋与空间信息学院（5人）

白永良 刘宝弟 刘建航 张爱竹 顾朝志

控制科学与工程学院（4人）：

陈鸿龙 季文海 周兰娟 廖明燕



Efficiently and Completely Identifying Missing Key Tags for Anonymous RFID Systems

Honglong Chen, *Member, IEEE*, Zhibo Wang, *Member, IEEE*,
Feng Xia, *Senior Member, IEEE*, Yanjun Li, and Leyi Shi

Abstract—Radio frequency identification (RFID) systems can be applied to efficiently identify the missing items by attaching them with tags. Prior missing tag identification protocols concentrated on identifying all of the tags. However, there may be some scenarios in which we just care about the *key tags* instead of all tags, making it inefficient to merely identify the missing key tags due to the interference of replies from the *ordinary tags* (i.e., nonkey tags). In this paper, we propose to investigate the problem of efficiently and completely identifying the missing key tags for anonymous RFID systems in which the tag privacy is required to be well protected. First, we propose a vector-based missing key tag identification protocol called VEKI. Then we propose an improved protocol called iVEKI, which consists of two phases: 1) ordinary tag deactivation and 2) missing key tag identification. The parameters of the proposed VEKI and iVEKI protocols are theoretically optimized to maximize the time efficiency. Finally, we conduct extensive simulations to evaluate the proposed VEKI and iVEKI protocols and the simulation results illustrate that they outperform other existing protocols in terms of execution time.

Index Terms—Anonymous radio frequency identification (RFID) systems, efficiently and completely, missing key tag identification, parameter optimization.

I. INTRODUCTION

WITH the recent rapid development of wireless sensor networks [3], [27]–[29] and Internet of Things [35], [36], radio frequency identification (RFID) has

been an emerging technology with wide industrial applications such as localization [5], object tracking [8], warehouse management [26], supply chain management [7], etc. A large-scale RFID system always consists of a back-end server, multiple readers and thousands of low-cost tags [20]. According to whether they are within the readers' interrogating regions or not, the tags can be classified into *present tags* and *missing tags* [6]. RFID systems can be applied to identify the missing items by using readers to identify the tags attached on the items. A recent report [25] illustrated that the U.S. retail industry lost about \$42 billion in 2013 due to shrink, including shoplifting, employee or supplier fraud, and administrative errors. Therefore, missing tag identification becomes severely significant and has attracted much attention from the research community.

Most of prior missing tag identification protocols concentrated on identifying all the tags of the system. However, there may be some scenarios in which we only care about the *key tags* [16] instead of all tags. For instance, in a large shopping mall, there are some expensive items such as jewelries and watches and the tags attached on them are considered as the key tags, while the tags attached to the other relatively cheap items are considered as the ordinary tags. In some situations, the clerk may just want to monitor the expensive items (or a particular set of items), which can be actualized by identifying the missing key tags. However, it is inefficient to adopt the prior protocols in identifying the missing key tags for the RFID system since the *ordinary tags*, i.e., nonkey tags, (with a larger population) will also reply to the reader's query and interfere with the missing key tag identification.

A potential solution for the missing key tag identification in RFID systems is to query the ID of each key tag and the one with no reply can be identified as missing. However, in this paper, we consider an anonymous RFID system, in which the tag ID should not be directly transmitted in the air to preserve the privacy [30]. Take the shopping mall for an example again, the key tag ID should be well protected since it would be risky to make the tag ID corresponding to some expensive item publicly known. The potential attackers may make use of this information to intrude into the system, such as launching a cloning attack [2]. Another example of the anonymous RFID system is a package of medicine purchased by someone from Amazon, since the package information may be closely related to the customer's privacy [14], the tag ID affixed on it should be well protected to keep private. Therefore, the ID-query protocol is inapplicable for the anonymous RFID system.

Manuscript received June 19, 2017; revised August 4, 2017; accepted September 5, 2017. Date of publication September 14, 2017; date of current version August 9, 2018. This work was supported in part by the NSFC under Grant 61772551, Grant 61502352, Grant 61572106, and Grant 61772472, in part by Shandong Provincial Key Program of Research and Development under Grant 2018GGX101035, in part by the Qingdao Fundamental Research Project under Grant 15-9-1-79-jch, in part by the Fundamental Research Funds for the Central Universities under Grant 18CX07003A, Grant 16CX02059A and Grant 413000035, in part by the Natural Science Foundation of Hubei Province under Grant 2017CFB503, in part by the Natural Science Foundation of Jiangsu Province under Grant BK20150383, and in part by the Natural Science Foundation of Zhejiang Province under Grant LY17F020020. (Corresponding author: Zhibo Wang.)

H. Chen is with the College of Information and Control Engineering, China University of Petroleum, Qingdao 266555, China (e-mail: chenhl@upc.edu.cn).

Z. Wang is with the School of Computer, Wuhan University, Wuhan 430072, China (e-mail: zbwang@whu.edu.cn).

F. Xia is with the School of Software, Dalian University of Technology, Dalian 116620, China (e-mail: f.xia@ieee.org).

Y. Li is with the College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310023, China (e-mail: yjli@zjut.edu.cn).

L. Shi is with the College of Computer and Communication Engineering, China University of Petroleum, Qingdao 266555, China (e-mail: shileiyi@upc.edu.cn).

Digital Object Identifier 10.1109/IIOT.2017.2752239

Efficient and Reliable Missing Tag Identification for Large-Scale RFID Systems With Unknown Tags

Honglong Chen, *Member, IEEE*, Guoliang Xue, *Fellow, IEEE*, and Zhibo Wang, *Member, IEEE*

Abstract—Radio frequency identification (RFID), which promotes the rapid development of Internet of Things (IoT), has been an emerging technology and widely deployed in various applications such as warehouse management, supply chain management, and social networks. In such applications, objects can be efficiently managed by attaching them with low-cost RFID tags and carefully monitoring them. The missing objects, therefore, can be identified by the readers in the RFID system. Most of prior missing tag identification protocols consider the ideal scenario that all the tags' IDs are known to the reader, which ignore that some tags with unknown IDs, called unknown tags, may be present in the system. In this paper, we investigate the problem of efficiently identifying the missing tags with a predefined reliability for large-scale RFID systems with unknown tags. We first propose a basic efficient and reliable missing tag identification protocol called B-ERMI. Then we propose an enhanced protocol called E-ERMI to further improve the efficiency. The parameters of our proposed ERMI protocols are optimized to minimize the execution time. We also conduct extensive simulations to evaluate the proposed ERMI protocols and the simulation results illustrate that the ERMI protocols outperform other existing ones.

Index Terms—Efficient and reliable protocols, missing tag identification, radio frequency identification (RFID) systems, unknown tags.

I. INTRODUCTION

RECENTLY radio frequency identification (RFID), which promotes the rapid development of Internet of Things (IoT) [1], [26], is becoming an emerging technology [3], [32], [37]. With careful considerations in security and privacy [5], [6], [28], [29], RFID can be widely deployed

in various applications such as warehouse management [25], supply chain management [17], and social networks [27] owing to its attractive features including low-cost, multiple simultaneous access, and nonline-of-sight reading. In general, an RFID system consists of a back-end server, multiple readers, and lots of low-cost tags (as cheap as 5 cents per tag [18]). In most applications, the deployed RFID systems can efficiently monitor the objects by attaching them with cheap tags, whose stored information can be interrogated by the reader. To stimulate its sustained applications in industry field and our daily life, RFID has attracted much attention from the research community on cardinality estimation [12], [31], missing tag detection [11], [16], tag collection [2], [20], and so on.

In a conventional shopping mall, the staff may need to laboriously check each item to verify whether it is missing or not. However, if the shopping mall has been equipped with an RFID system, this problem can be easily transformed into missing tag identification, which is much easier to actualize. According to a recent report [24], the U.S. retail industry lost about \$42 billion in 2013 due to shrink, including shoplifting, employee or supplier fraud, and administrative errors. Thus, there is a tremendous demand to deploy RFID systems with capacity of missing tag identification to reduce capital lost. Many protocols have been proposed for missing tag identification due to its importance [8], [11], [23], [35].

Intuitively, there are two typical solutions to identify the missing tags for RFID systems. The first one is sequentially querying the ID of each tag, during which the tags with no reply will be identified as missing. The advantage of the ID query protocol is that it can guarantee the complete identification of all the missing tags. Obviously, its disadvantage lies in low efficiency due to the time-consuming tag ID broadcast, making it severely slow, especially, for large-scale RFID systems. The other solution is collecting the response of each tag using a framed slotted Aloha protocol [8], [11], [22], [23], [35], in which the reader can identify the missing tags if there is no reply in their associated slots. Such existing protocols do not require the time-consuming ID broadcast. However, they failed to prevent the interference from the unknown tags in the RFID systems, resulting in either reducing the efficiency or sacrificing the identification reliability. For example, in a large warehouse, the frequent loading of new come goods will introduce unknown tags into the system, which will also reply to the reader's query.

In this paper, we concentrate on investigating the problem of efficiently and reliably identifying the missing tags for

Manuscript received November 18, 2016; revised December 27, 2016; accepted January 25, 2017. Date of publication February 6, 2017; date of current version June 15, 2017. This work was supported in part by NSFC Grant 61309023, NSF Grant 1457262, and Grant 1461886, NSFC Grant 61502352, National Basic Research Program of China Grant 2014CB340600, Shandong Provincial Key Program of Research and Development Grant 2015GGX101045, Qingdao Fundamental Research Project Grant 15-9-1-79-jch, the Fundamental Research Funds for the Central Universities of China Grant 16CX02059A, Natural Science Foundation of Hubei Province Grant 2015CFB203 and Natural Science Foundation of Jiangsu Province Grant BK20150383.

H. Chen is with the College of Information and Control Engineering, China University of Petroleum, Qingdao 266555, China (e-mail: chenhl@upc.edu.cn).

G. Xue is with the School of Computing, Informatics, and Decision Systems Engineering, Arizona State University, Tempe, AZ 85287 USA (e-mail: xue@asu.edu).

Z. Wang is with the School of Computer, Wuhan University, 430072 Wuhan, China (e-mail: zbwang@whu.edu.cn).

Digital Object Identifier 10.1109/IIOT.2017.2664810

MAC: Missing Tag Iceberg Queries for Multi-Category RFID Systems

Honglong Chen , *Member, IEEE*, Guolei Ma, Zhibo Wang , *Senior Member, IEEE*,
Qian Wang , *Member, IEEE*, and Jiguo Yu , *Senior Member, IEEE*

Abstract—Recently radio frequency identification (RFID) is promoting the rapid development of Internet of Things and has been widely applied in numerous industrial applications such as inventory management, object tracking and smart logistics, etc. Tags in some RFID applications can be classified into multiple categories according to the types of objects they are attached to. One of the important functionalities for the multi-category RFID systems is the missing tag cardinality estimation of each category. This paper focuses on solving the missing tag iceberg query problem for multi-category RFID systems, i.e., to determine a set of categories, whose missing tags are more than a threshold, with a required reliability. We firstly propose two basic missing tag iceberg query schemes called MAC-SZE and MAC-HZE, which adopt the singleton-zero estimator and homogeneous-zero estimator, respectively. To further improve the query efficiency, we then propose two segmented enhanced schemes called MAC-SSZE and MAC-SHZE, which eliminate the unnecessary slots in each frame. We conduct theoretical analysis to guarantee the required reliability is satisfied. The simulations are finally conducted and the results illustrate that the proposed missing tag iceberg query schemes greatly outperform other existing one.

Index Terms—Iceberg queries, missing tags, multi-category, RFID systems.

I. INTRODUCTION

AS ONE of the fundamental technologies of Internet of things (IoTs) [1], [9], [10], [24], [25], [33], [34], radio frequency identification (RFID) [15], [30] is promoting the rapid development of IoTs and has been widely applied in numerous industrial applications such as inventory management [22],

object tracking [4], [23] and smart logistics [7], [19], etc. Typically a large-scale RFID system comprises a powerful back-end server, one or multiple readers and a large amount of resource-limited and cheap tags. Although a UHF reader's interrogating range is limited (up to 10 m [29]), the tags locating in a large area can be cooperatively monitored by a certain number of readers. Therefore, a large-scale RFID system can contain up to tens of thousands of tags, the statistical information of which, such as cardinality or the number of missing tags, may be significant [6], [15].

In most of RFID-based applications, the tags may be attached on different objects such as merchandizes in a shopping mall, animals in a zoo or even a newborn baby in a hospital. The reader can monitor the tags' presence by interrogating them. According to the types of the carriers, the tags in the RFID system can be classified into multiple categories, which is termed as multi-category RFID system in this paper and has been studied in the fields of classification [12], [18], cardinality estimation [13], [29], missing tag detection [6] and identification [5], and so on. In this paper, we intend to study and solve the missing tag iceberg query problem for multi-category RFID systems, i.e., to determine a set of categories, whose missing tags are more than a threshold, with a required reliability. The missing tag iceberg query contributes to improving the inventory managing efficiency. For example, it can help the manager to realize which types of goods or products are often misplaced or stolen.

The missing tag iceberg query problem for the multi-category RFID systems can be achieved by sequentially querying the IDs of tags in each category until the number of un-replying tags exceeds the threshold. Obviously, such kind of approach is inefficient due to the time-consuming characteristic of the ID query process. Another potential solution is to estimate the cardinality of present tags in each category [29], since the cardinality of missing tags in each category equals the category's size minus its present tag cardinality. However, in most applications, the missing tags always occupy a small part of all the tags. In such scenarios, directly estimating present tag cardinality may result in a relatively large estimation variance, making it difficult to satisfy the required reliability, i.e., severely degrading the query efficiency. In this paper, we propose to solve the missing tag iceberg query problem by estimating the missing tag cardinality of each category based on each slot's state difference [6] in the executed frame, in which the framed slotted Aloha protocol is adopted.

Manuscript received June 26, 2018; accepted July 21, 2018. Date of publication August 6, 2018; date of current version October 15, 2018. This work was supported in part by the NSFC under Grants 61772551, 61502352, 61672321, 61373027, and 61771289, in part by the Shandong Provincial Key Program of Research and Development under Grant 2018GGX101035, in part by the Natural Science Foundation of Hubei Province under Grant 2017CFB503, and in part by the Fundamental Research Funds for the Central Universities (18CX07003A, 2042018gf0043, and 18CX02133A). The review of this paper was coordinated by Prof. C. Zhang. (*Corresponding author: Jiguo Yu.*)

H. Chen and G. Ma are with the College of Information and Control Engineering, China University of Petroleum (East China), Qingdao 266580, China (e-mail: honglongchen1984@gmail.com; 1610079407@qq.com).

Z. Wang and Q. Wang are with the School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China (e-mail: wzb.zju@gmail.com; qianwang@whu.edu.cn).

J. Yu is with the Qilu University of Technology (Shandong Academy of Sciences), Shandong Computer Science Center (National Supercomputer Center in Jinan), Jinan P. R. China and School of Information Science and Engineering, Qufu Normal University, Rizhao 276826, China (e-mail: jiguoYu@sina.com).

Color versions of one or more of the figures in this paper are available online at <http://ieeexplore.ieee.org>.

Digital Object Identifier 10.1109/TVT.2018.2863726

Probabilistic Detection of Missing Tags for Anonymous Multicategory RFID Systems

Honglong Chen¹, *Member, IEEE*, Guolei Ma, Zhibo Wang, *Member, IEEE*, Feng Xia², *Senior Member, IEEE*, and Jiguo Yu³, *Senior Member, IEEE*

Abstract—In many radio-frequency identification (RFID) applications, one of the essential systematic functionalities is to quickly detect missing-tag event in case of misplacement or other incorrect operations. In this paper, we focus on probabilistically detecting the missing tags for the anonymous multicategory RFID systems without revealing the tag privacy. The main objective is to minimize the detection time while satisfying the required detection reliability of each category. First, we propose to use a multihash technique to sequentially detect the missing tags category-by-category, called segmented sequential detection approach, in which the frame segmentation is adopted to reduce the detection time. Then, we propose an enhanced segmented sequential detection approach to further improve the detection efficiency by deactivating the identified existing tags. We conduct extensive simulations to illustrate the effectiveness of our proposed two missing tag detection approaches.

Index Terms—Anonymous, missing tag detection, multicategory radio-frequency identification (RFID) systems, probabilistic.

I. INTRODUCTION

SHRINK, including shoplifting, employee or supplier fraud and administrative errors have become the main cause of capital loss for retailers, which made the retail industry in U.S. lose about 42 billion dollars in 2013 [28]. Thus, it is essential to quickly detect missing items in a large warehouse. With the recent rapid development of wireless sensor networks [2], [32], [33] and Internet of things [39], [40], radio frequency identification (RFID) has been an emerging technology and RFID systems [9], [24], [35] can be deployed to monitor the products instead of human beings by attaching low-cost tags (e.g., as low

as 5 cents per tag [23]) to objects, which can communicate their stored information with the reader(s) when interrogated. In such kind of applications, the detection of missing items can be automatically simplified to detect whether any tags are absent by the reader via tag query. Therefore, efficient missing tag detection plays an important role in various RFID applications and has attracted a lot of research attention in recent years [12], [19], [25], [37].

Typically the missing tag detection protocols can be classified into two categories [19], [25]: probabilistic and deterministic. The probabilistic protocols [19], [21], [25], [29] try to detect a missing-tag event with a predefined probability without identifying which tags are missing. While the deterministic protocols [12], [14], [26], [37] need to exactly identify all the missing tags, which are therefore comparatively slower. Normally, the probabilistic and deterministic protocols are not independent to each other and should be used together [19]: a probabilistic protocol can be used to detect the missing-tag event and a deterministic protocol will be executed to identify all the missing tags once the missing-tag event is detected.

In this paper, we concentrate on the probabilistic detection of missing tags for the anonymous multi-category RFID systems. Firstly, the anonymous characteristic is essential in some privacy-sensitive applications such as the medicine tracking system [17], in which a patient may not want his/her medication to be publicly known. Therefore, in an anonymous RFID system, the tag privacy should be cautiously protected during the applications. Secondly, the tags in many RFID applications are categorized into multiple categories. For example, in an RFID-deployed medicine tracking system, the tags can be categorized [16], [27], [34] according to the types of items they are attached to. In such applications with multi-category RFID tags, it may be necessary to detect the missing-tag event for each category, since the department director may want to know which type of items is missing. Therefore, how to efficiently detect the missing tag of each category for the multi-category RFID systems with a certain predefined probability but not revealing the tag privacy becomes a challenging problem, which is our motivation in this paper to propose a series of missing tag detection approaches.

A straightforward solution for missing tag detection is to sequentially query the ID of each tag. However, there are two problems. On one hand, the ID of each tag is privacy-sensitive which can not be directly queried in the anonymous RFID systems. On the other hand, such kind of scheme is extraordinary

Manuscript received November 4, 2016; revised March 28, 2017; accepted June 14, 2017. Date of publication July 11, 2017; date of current version December 14, 2017. This work was supported in parts by NSFC under grants 61772551, 61502352, 61572106, 61672321, 61373027, and 61672198, Qingdao Fundamental Research Project (No. 15-9-1-79-jch), the Fundamental Research Funds for the Central Universities (No. 16CX02059A, No. 413000035), the Natural Science Foundation of Hubei Province (No. 2015CFB203), and the Natural Science Foundation of Jiangsu Province (No. BK20150383, No. BK20150854). The review of this paper was coordinated by Dr. P. Lin. (*Corresponding author: Jiguo Yu.*)

H. Chen and G. Ma are with the College of Information and Control Engineering, China University of Petroleum (East China), Qingdao 266580, China (e-mail: honglongchen1984@gmail.com; 1610079407@qq.com).

Z. Wang is with the School of Computer, Wuhan University, Wuhan 430072, China (e-mail: zbwang@whu.edu.cn).

F. Xia is with the School of Software, Dalian University of Technology, Dalian 116023, China (e-mail: f.xia@ieee.org).

J. Yu is with the School of Information Science and Engineering, Qufu Normal University, Rizhao 276826, China (e-mail: jiguo@qnu.edu.cn).

Color versions of one or more of the figures in this paper are available online at <http://ieeexplore.ieee.org>.

Digital Object Identifier 10.1109/TVT.2017.2726005

A Secure Credit-Based Incentive Mechanism for Message Forwarding in Noncooperative DTNs

Honglong Chen, *Member, IEEE*, Wei Lou, *Member, IEEE*, Zhibo Wang, *Member, IEEE*, and Qian Wang, *Member, IEEE*

Abstract—Delay-tolerant networks (DTNs) are an emergent communication paradigm characterized by intermittent connectivity. The nodes in DTNs can take advantage of their contact opportunities to forward messages. However, in noncooperative DTNs, the nodes may be selfish and reluctant to cooperate with each other in message forwarding. In such DTNs, stimulating cooperation among the nodes will be indispensable. Recently, many incentive mechanisms have been proposed to motivate nodes to cooperate in message forwarding. However, most of them cannot guarantee systematic security. To resolve the drawback of the previous incentive mechanisms, we first propose a credit-based rewarding scheme called the earliest path singular rewarding (EPSR) scheme to motivate the nodes to truthfully forward the messages during every contact opportunity. Then, we propose another credit-based rewarding scheme called the earliest path cumulative rewarding (EPCR) scheme by further considering that a node may get more contact information on others. We prove that both the EPSR and EPCR schemes are incentive compatible, and the payment for each delivered message is upper bounded. Furthermore, the proposed schemes can prevent selfish nodes having malicious behaviors. We have conducted real-trace-based simulations to illustrate the effectiveness of the proposed EPSR and EPCR schemes.

Index Terms—Cooperation, noncooperative delay-tolerant networks (DTNs), rewarding schemes, secure.

Manuscript received April 6, 2015; revised June 29, 2015; accepted August 18, 2015. Date of publication September 7, 2015; date of current version August 11, 2016. This paper was presented in part at the IEEE International Conference on Computer Communications and Networks. This work was supported in part by the National Natural Science Foundation of China under Grant 61309023, Grant 61272463, Grant 61373167, and Grant 61502352; by the Shandong Provincial Natural Science Foundation, China, under Grant ZR2013FQ032; by the Shandong Provincial Key Program of Research and Development under Grant 2015GGX101045; by the Hong Kong General Research Fund under Grant PolyU-524308 and Grant PolyU-521312; by The Hong Kong Polytechnic University under Grant A-PJ16, Grant A-PL84, Grant 1-VZ5N, and Grant 4-BCB6; by the Natural Science Foundation of Hubei Province under Grant 2013CFB297 and Grant 2015CFB203; by the Natural Science Foundation of Jiangsu Province under Grant BK20150383; and by the Wuhan Science and Technology Bureau under Grant 20150101010020. The review of this paper was coordinated by Prof. Y. Cheng.

H. Chen is with the College of Information and Control Engineering, China University of Petroleum, Qingdao 266580, China, and also with the Department of Computing, Hong Kong Polytechnic University, Kowloon, Hong Kong (e-mail: chenhl@upc.edu.cn).

W. Lou is with the Department of Computing, Hong Kong Polytechnic University, Kowloon, Hong Kong, and also with Hong Kong Polytechnic University Shenzhen Research Institute, Shenzhen 518057, China.

Z. Wang and Q. Wang are with the School of Computer, Wuhan University, Wuhan 430072, China.

Color versions of one or more of the figures in this paper are available online at <http://ieeexplore.ieee.org>.

Digital Object Identifier 10.1109/TVT.2015.2477164

I. INTRODUCTION

AS an emergent communication paradigm, delay-tolerant networks (DTNs) [1]–[3] are competent for many applications, such as vehicular networks [4]–[6], mobile social networks [7], [8], and pocket switched networks [9]. However, DTNs often experience intermittent connectivity due to the high mobility or sparse deployment of the nodes, in which there are generally no stable end-to-end delivery paths. Therefore, the traditional routing protocols are not applicable for the intermittently connected DTNs. Epidemic routing [10] is a simple but competitive DTN routing protocol, in which each node will fully make use of every contact opportunity to replicate the messages to its encounter. Although epidemic routing may introduce a high overhead, it can be easily implemented in applications and achieve satisfying performance [11], [12].

In noncooperative DTNs [29], the nodes may be managed by some rational individuals [13], such as human beings or other autonomous parties. Such nodes may be selfish [6], [11], [12], [14], [15], i.e., they only aim to maximize their individual utilities and will not be willing to cooperate with others to truthfully forward the messages if they can make no profit from message forwarding, or they may even conduct some malicious behaviors to get extra profit from message forwarding. Due to the distributed characteristic of DTNs, it is difficult to detect and prohibit the selfish behaviors conducted by the individual nodes. Therefore, it is necessary to have an efficient incentive mechanism for the noncooperative DTNs to stimulate cooperation among the selfish nodes in message forwarding.

Generally, the incentive mechanisms can be classified into three categories [15]: reputation-based, credit-based, and tit-for-tat-based (TFT-based) schemes. The reputation-based schemes require each node to monitor the traffic information of all its neighbors and keep track of their reputations, which should be propagated to all other nodes efficiently and effectively. The TFT-based schemes require each node to detect the misbehavior of its neighbors. It would be difficult to achieve direct traffic monitoring or misbehavior detection in intermittently connected DTNs. On the other hand, credit-based schemes use virtual credits to motivate selfish nodes to participate in the message forwarding, and the credits they earned from forwarding other nodes' messages can be used to pay for the delivery of their own messages. Furthermore, the rewarding process can be conducted by a central manager, the communication between which and the nodes is delay tolerant. The given characteristics of credit-based schemes make them suitable for DTNs. Therefore, we will adopt the credit-based incentive scheme in this paper to stimulate nodes' cooperation.

Received 7 January 2016; revised 16 May 2016; accepted 22 June 2016.
Date of publication 29 June 2016; date of current version 5 December 2018.

Digital Object Identifier 10.1109/TETC.2016.2586192

On Achieving Asynchronous Energy-Efficient Neighbor Discovery for Mobile Sensor Networks

HONGLONG CHEN^{ID}, (Member, IEEE), WEI LOU^{ID}, (Member, IEEE),
ZHIBO WANG^{ID}, (Member, IEEE), AND FENG XIA^{ID}, (Senior Member, IEEE)

H. Chen is with the College of Information and Control Engineering, China University of Petroleum,
Qingdao P. R. China and the Department of Computing, The Hong Kong Polytechnic University, Kowloon Hong Kong

W. Lou is with the Department of Computing, The Hong Kong Polytechnic University, Kowloon Hong Kong

Z. Wang is with the School of Computer, Wuhan University, Wuhan, Hubei 430072, P. R. China

F. Xia is with the School of Software, Dalian University of Technology, Dalian Liaoning 116620, P. R. China

CORRESPONDING AUTHOR: H. CHEN (honglongchen1984@gmail.com)

ABSTRACT Recent advances in mobile sensor networks (MSNs) lead to a wide demand of wireless communication based applications. However, due to the battery technology constraint, many MSNs-based applications are confined by the limited power resource capacity. Thus, discovering neighbors with minimal power consumption and latency becomes an indispensable characteristic to guarantee the feasibility of above applications. Most of previously proposed time-slotted-based neighbor discovery protocols excessively idealize the power consumption model, which ignores the power consumption and time duration of the transient state. In this paper, we propose a more practical model named enhanced power consumption model that considers the power consumption and time duration of the transient state. We then propose the asynchronous energy-efficient neighbor discovery protocols called Quick-Connect (*Q-Connect*) including *Q-Connect_A*, *Q-Connect_U* and *Q-Connect_{UI}* protocols, each of which can provide a strict upper bound on the discovery latency. We consider both the slot-aligned and slot-unaligned cases. For slot-aligned case, we propose the *Q-Connect_A* protocol, which can greatly reduce the worst-case discovery latency. For slot-unaligned case, we first propose the *Q-Connect_U* protocol, based on which we further propose an improved protocol called *Q-Connect_{UI}*. Finally, we conduct state-based simulations to illustrate the effectiveness of the proposed *Q-Connect* protocols.

INDEX TERMS Asynchronous, energy-efficient, mobile sensor networks, neighbor discovery protocol

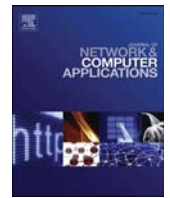
I. INTRODUCTION

The rapid development of micro-electronic devices such as smartphones, PDAs and sensor motes leads to the demand of wide variety of applications in Mobile Sensor Networks (MSNs) [1]–[6], such as industrial Internet of Things (IIoT) [7], underwater sensor networks [8], vehicular networks [9] and social networks [10]–[12], etc. MSNs, in which some of the nodes are mobile (e.g., they can be carried by vehicles), can be applied in the above scenarios for data collection from the deployed nodes. The implementation of such applications relies on the intermittent connectivity [13] based communications among the mobile nodes, a prerequisite of which is to realize neighbor discovery with a short enough latency.

Without considering the constraint of energy resource, it is uncomplicated to realize short-latency neighbor discovery since the nodes can search for their neighbors by incessantly broadcasting and receiving beacon messages. However, MSNs are usually composed of battery-driven nodes with limited energy resource [14]. The periodical broadcasting

and receiving is impracticable since the limited energy capacity cannot afford such a energy-consuming operation. Therefore, energy-efficiency [15] becomes an indispensable characteristic for neighbor discovery in MSNs.

Basically, neighbor discovery can be classified into two categories: synchronous and asynchronous protocols. Since it is difficult to achieve network-level clock synchronization, synchronous neighbor discovery protocols based on the assumption that nodes are synchronized are far away from real application scenarios. Consequently, asynchronous neighbor discovery protocols attract more attentions from researchers in recent years. In asynchronous neighbor discovery protocols, the nodes always work in a time-slotted [16] mode for power conservation, in which the time can be divided into a serial of slots [17]. Each node keeps active during specific slots and sleeps in other ones. During active slots, each node can search neighbors via beacon message broadcasting and receiving. There are at least two prerequisites for two nodes to successfully discover each other:



RMTS: A robust clock synchronization scheme for wireless sensor networks

Xuxin Zhang^a, Honglong Chen^{a,*}, Kai Lin^a, Zhibo Wang^{b,c}, Jiguo Yu^d, Leyi Shi^e

^a College of Information and Control Engineering, China University of Petroleum, Qingdao, PR China

^b School of Cyber Science and Engineering, Wuhan University, Wuhan, PR China

^c State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, PR China

^d Qilu University of Technology (Shandong Academy of Sciences), Shandong Computer Science Center (National Supercomputer Center in Jinan), Shandong Provincial Key Laboratory of Computer Networks, Jinan, PR China

^e College of Computer and Communication Engineering, China University of Petroleum, Qingdao, PR China

ARTICLE INFO

Keywords:

Bounded noises
Clock synchronization
Maximum consensus
Wireless sensor networks

ABSTRACT

In recent years, wireless sensor networks (WSNs) have attracted more and more attention, but some applications of WSNs are still restricted by various factors, one of which is the clock synchronization among nodes. It is difficult to estimate the noises caused by communication delay, clock drift and measurement errors, which makes it challenging to achieve accurate clock synchronization. In this paper, we consider a bounded noise model, which does not need to satisfy any fixed probability distribution, nor does it need to have a fixed mean or variance. Under this noise model, we propose a novel clock synchronization scheme based on maximum consensus, which is called Robust Maximum Time Synchronization (RMTS). The proposed RMTS scheme starts with the estimation of relative skew and offset. On the basis, software parameters are adjusted so that all the nodes in the network can have the same software skew and offset. We theoretically prove that the proposed scheme can guarantee the accuracy of clock synchronization. Simulations are conducted to validate the effectiveness of the proposed scheme. The performance comparison with the other two schemes demonstrates that the RMTS scheme outperforms the existing ones.

1. Introduction

With the recent advances in Internet of things (IoTs) (Al-Fuqaha et al., 2015; Wang et al., 2018, 2019) and radio frequency identification (RFID) (Chen et al., 2018b, 2018c), wireless sensor networks (WSNs) (Akyildiz et al., 2002; Huang et al., 2017) are widely applied to various fields such as smart home (Li and Lin, 2015), traffic control (Sinan et al., 2017) and environment monitoring (Chen and Lou, 2015). However, the applications of WSNs are restricted by some factors, such as the clock synchronization (Xie et al., 2018). For instance, each node is equipped with an oscillator to provide a hardware clock, and the different oscillator properties will lead to different hardware clocks among nodes (Chen et al., 2018a), which would affect the normal function of WSNs. And the fundamental task of clock synchronization is to make all nodes in the network keep the same time (Koivisto et al., 2017).

Actually, clock synchronization is a precondition for various applications of WSNs (Benzaida et al., 2017; Lamonaca et al., 2014; Wang et al., 2017b). In many of these applications, it is significant that all nodes

in the network refer to the common time. One of the typical applications is the target tracking (Chen and Lou, 2015). In this scenario, each node in WSN transmits the location and time of the target it detects to the center node of the network. On receiving the information, the center node processes the data with corresponding algorithms to make a decision on the moving information of the target, such as its direction and speed. If the time among nodes is inconsistent, the center node can not get the exact corresponding relationship between the time and position of the moving target, making it unable to conduct a reliable judgement. In addition, many other applications (Wang et al., 2017a) in WSNs, e.g., data compression and fusion, nodes cooperation and sensor scheduling are all based on the accomplishment of clock synchronization.

However, there are two main challenges to design an accurate and robust clock synchronization scheme for wireless sensor networks. The first one is the communication delay during the synchronization process. Since communication delay is caused by the time it takes to prepare data, send data and read data, it is difficult to eliminate the delay at hardware level, which introduces a fundamental restriction to clock

* Corresponding author.

E-mail addresses: chenhl@upc.edu.cn, honglongchen1984@outlook.com (H. Chen).

<https://doi.org/10.1016/j.jnca.2019.02.028>

Received 25 July 2018; Received in revised form 2 January 2019; Accepted 25 February 2019

Available online 4 March 2019

1084-8045/© 2019 Published by Elsevier Ltd.

Received April 28, 2019, accepted May 9, 2019, date of publication May 16, 2019, date of current version June 4, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2917257

Deformable Convolutional Matrix Factorization for Document Context-Aware Recommendation in Social Networks

HONGLONG CHEN¹, JINNAN FU¹, LEI ZHANG², SHUAI WANG², KAI LIN¹, LEYI SHI³, AND LIANHAI WANG^{4,5}

¹College of Information and Control Engineering, China University of Petroleum, Qingdao 102200, China

²Department of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing 210000, China

³College of Computer and Communication Engineering, China University of Petroleum, Qingdao 102200, China

⁴Shandong Academy of Sciences, Qilu University of Technology, Jinan 250300, China

⁵Shandong Provincial Key Laboratory of Computer Networks, Shandong Computer Science Center, National Supercomputer Center in Jinan, Jinan 250101, China

Corresponding author: Leyi Shi (shileiyi@upc.edu.cn)

This work was supported in part by the NSFC under Grant 61772551, Grant 21606256, and Grant 21606255, in part by the Shandong Provincial Key Program of Research and Development under Grant 2018GGX101035 and Grant 2018GGX101025, in part by the Natural Science Foundation of Shandong Province, China, under Grant ZR2019MF034, Grant ZR2016BQ14, and Grant ZR2016BQ16, in part by the Fundamental Research Funds for the Central Universities under Grant 18CX07003A, in part by the Open Research Fund from Shandong Provincial Key Laboratory of Computer Networks under Grant SDKLCN-2018-06, and in part by the Natural Science Foundation of Jiangsu Province under Grant BK20150854.

ABSTRACT The extreme sparsity of the rating data seriously affects the recommendation quality of the recommendation system. In order to alleviate the problem of data sparsity, some convolutional neural network (CNN)-based models make full use of text data to improve the recommendation accuracy. However, due to the inherent properties of the traditional convolutional network, it can only extract features in a fixed position, and rely on the primitive bounding box based feature extraction, thus ignoring the flexibility of the traditional convolution. In this paper, we adopt a flexible convolutional network called deformable convolutional network (DCN), which extends the convolution transformation model capability by adding an offset layer to the traditional convolution layer, and then propose a novel deformable convolutional network matrix factorization (DCNMF) recommendation model. Specifically, we combine the DCN with word embedding to deeply capture the contextual information of document and build a latent model, which is incorporated into the probabilistic matrix factorization (PMF) model to enhance the recommendation accuracy. We conduct extensive experiments on the real-world datasets, and the experimental results show that the DCNMF outperforms the compared benchmarks.

INDEX TERMS Collaborative filtering, contextual information, neural networks, recommendation system.

I. INTRODUCTION

With the wide applications of social networks [18], [25]–[27] and Internet of things (IoTs) [4], [5], [10], [23], [24], [29], the recommendation system is popular in people's daily lives recently, such as online shopping, article reading, and films, etc. For instance, the recommendation system can greatly help the customers by suggesting them the products or services with potential interest, based on their preferences, needs, and purchase histories. However, with the rapid development of Internet, the problem of information overload has become increasingly prominent. With the increase of online

shopping sites, the categories and quantities of products and services provided by the sellers have increased dramatically. Although it brings more choices for the customers, it becomes more and more difficult for them to handle the vast amount of information, making the rating data sparser and sparser. For example, some of the largest e-commerce platforms, such as Taobao, Ebay and Amazon, have a wealth of users and items. Intuitively, the sparseness of the rating data seriously affects the prediction accuracy of the rating in the recommendation system.

One of the techniques to solve the problem of rating data's sparseness is to use auxiliary text data (comments, abstracts or project description documents) to improve the accuracy of the recommendation system. Some researchers

The associate editor coordinating the review of this manuscript and approving it for publication was Chun-Wei Tsai.

Received August 30, 2018, accepted September 21, 2018, date of publication October 1, 2018, date of current version October 19, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2872543

Segmented Bloom Filter Based Missing Tag Detection for Large-Scale RFID Systems With Unknown Tags

KAI LIN¹, HONGLONG CHEN¹, (Member, IEEE), TIANJIAO DAI¹,
DENGHUI LIU², LU LIU¹, AND LEYI SHI³

¹College of Information and Control Engineering, China University of Petroleum, Qingdao 266580, China

²Everdisplay Optonics (Shanghai) Ltd., Shanghai 201506, China

³College of Computer and Communication Engineering, China University of Petroleum, Qingdao 266580, China

Corresponding author: Honglong Chen (honglongchen1984@gmail.com)

This work was supported in part by NSFC under Grant 61772551, Grant 21606255, and Grant 61872385, in part by the Shandong Provincial Key Program of Research and Development under Grant 2018GGX101035 and Grant 2018GGX101025, in part by the Fundamental Research Funds for the Central Universities under Grant 18CX07003A and Grant 18CX02133A, and in part by the Natural Science Foundation of Shandong Province, China, under Grant ZR2016BQ16.

ABSTRACT Radio frequency identification (RFID) is one of the key technologies of the Internet of Things, which has been widely applied to many scenarios, such as tracking, warehouse monitoring, and vehicular social network. In such applications, some of the objects are attached with low-cost tags, which need to be monitored carefully. Hence, the object monitoring can be achieved by missing tag detection in the RFID system. However, unknown tags, whose IDs are not known by the reader in prior, may exist in the system to interfere the missing tag detection and reduce the time efficiency. In this paper, we propose a segmented bloom filter-based missing tag detection scheme called SBFMD, which consists of two phases, i.e., deactivation phase and detection phase. The idea behind the proposed SBFMD scheme is to eliminate the useless slots away from the bloom filter-based frame to improve the detection efficiency. We theoretically optimize the parameters of the proposed SBFMD scheme to maximize the efficiency with a required reliability. Extensive simulations are conducted to evaluate the performance of the proposed SBFMD scheme, the results of which validate its effectiveness.

INDEX TERMS Missing tag detection, RFID, segmented bloom filter, unknown tags.

I. INTRODUCTION

A. BACKGROUND

Radio Frequency Identification (RFID) technology has made remarkable progress in recent years and is widely applied to many scenarios such as tracking [4], warehouse monitoring [25] and vehicular social network [9], [20], [28] due to its distinct characteristics including low cost, non-line-of-sight, long lifetime, etc. In most applications, an RFID system consists of one or multiple readers, a lot of RFID tags and a back-end server. Specially, the RFID reader equipped with antennas can collect information from the tags within its interrogated area. The back-end server provides computing capacity and storage space for the reader. Each tag equipped with a low-cost microchip has a unique serial number, i.e., tag ID. In general, there are two categories of tags: passive tags and active tags. Passive tags have no power source, which

can harvest the energy from the reader's electromagnetic waves. While the active tags are driven by their own internal power sources, making them be able to communicate with the reader directly.

B. PROBLEM AND INTENTION

The theft, supplier fraud and staff errors gave rise to 44 billion dollars in loss for U.S. retail industry in 2014 according to a recent study [18]. The emergence of RFID technology can greatly reduce the losses caused by the missing products through monitoring the products equipped with tags. Obviously, the missing products can be discovered by missing tag detection in the RFID system. In recent years, a large number of outstanding works have emerged for missing tag detection, and lots of protocols were proposed in these existing works. However, these protocols have some common defects.

Received August 28, 2018, accepted September 23, 2018, date of publication October 5, 2018, date of current version October 29, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2873669

On Using Sampling Bloom Filter for Unknown Tag Identification in Large-Scale RFID Systems

HONGLONG CHEN¹, (Member, IEEE), LU LIU¹, RONGJIE CHE²,
KAI LIN¹, XIN AI¹, AND YANJUN LI³

¹College of Information and Control Engineering, China University of Petroleum, Qingdao 257000, China

²Sinopec Petroleum Engineering Corporation, Dongying 257026, China

³School of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310023, China

Corresponding author: Honglong Chen (honglongchen1984@gmail.com)

This work was supported in part by NSFC under Grants 61772551, 61772472, 61872385, and 21606255, in part by the Shandong Provincial Key Program of Research and Development under Grants 2018GGX101035 and 2018GGX101025, in part by the Fundamental Research Funds for the Central Universities under Grant 18CX07003A and Grant 18CX02133A, in part by the Natural Science Foundation of Zhejiang Province under Grant LY17F020020, and in part by the Natural Science Foundation of Shandong Province, China, under Grant ZR2016BQ16.

ABSTRACT Radio Frequency Identification (RFID) is one of the key technologies for Internet of things. In RFID systems, the tags without registering in advance are called unknown tags, which usually appear in the scenarios, where the tag-attached objects are moved into or misplaced in the reader's interrogating area. Consequently, unknown tag identification is significant for RFID-based applications, which is the concentration of this paper. We first propose a basic efficient unknown tag identification protocol based on sampling Bloom filter called UTI-SBF, which consists of known tag deactivation phase and unknown tag identification phase. The idea behind the UTI-SBF protocol is to deactivate the known tags to counteract their interference on the unknown tag identification. Then, we propose an enhanced protocol called EUTI-SBF, which eliminates the non-homogeneous slots based on the UTI-SBF protocol to improve the time efficiency. The parameters of the two protocols are theoretically analyzed to maximize the efficiency. We conduct extensive simulations to evaluate the proposed UTI-SBF and EUTI-SBF protocols and the simulation results illustrate that the UTI-SBF and EUTI-SBF protocols outperform the BUIP protocol. In particular, the EUTI-SBF protocol only consumes about 70% of deactivation time compared with the BUIP protocol in the known tag deactivation phase.

INDEX TERMS Known tag deactivation, radio frequency identification (RFID) systems, time efficiency, unknown tag identification.

I. INTRODUCTION

Radio frequency identification (RFID), which has greatly promoted the development of Internet of things (IoTs) [1], [29], [30], [33], [39]–[41], is widely used in various industrial fields [9], [34], [43] after considering the security and privacy issues [28], [31], [32], [38]. RFID systems are usually composed of electronic tags, readers, and back-end server [12]. Electronic tags are used to identify objects, while the reader has a powerful capacity of computation and storage, which can communicate with the tags via radio frequency signal [22] without line-of-sight. The back-end server is the control center that stores and identifies information collected by the reader [11]. The specific characteristics of RFID, including the low cost of tags [21], non-line-of-sight reader-tag communications [22], and so on, lead to the

wide applications of RFID systems. In most of the RFID applications, the tags are attached to different objects, which can then be efficiently managed by interrogating the tags, conducted by the reader. Typically, RFID tags are divided into three categories: passive tags, active tags and semi-active tags. Passive tag is the most widely used one, which has no internal power supply and can be driven by electromagnetic waves sent by the reader, resulting in a relatively short communication range (generally 3 to 5 meters). The active tag has an internal power supply, which is more expensive than the passive tag and has a longer communication range. For the semi-active tag, it has an internal power supply for the information processing, while its communication is still driven by the reader's electromagnetic waves.



Efficient 3-dimensional localization for RFID systems using jumping probe

Honglong Chen^{a,*}, Guolei Ma^a, Zhibo Wang^b, Jiguo Yu^c, Leyi Shi^d,
Xiangyuan Jiang^a

^a College of Information and Control Engineering, China University of Petroleum, Qingdao, PR China

^b School of Computer, Wuhan University, Wuhan, PR China

^c School of Information Science and Engineering, Qufu Normal University, Rizhao, PR China

^d College of Computer and Communication Engineering, China University of Petroleum, Qingdao, PR China

ARTICLE INFO

Article history:

Available online 8 December 2016

Keywords:

Jumping probe

Localization efficiency

RFID

3-dimensional localization

ABSTRACT

Radio Frequency Identification (RFID) technology manifests its potential in widespread applications, such as warehouse management, library maintenance and product tracking, etc. One of the most important characteristics for RFID-based applications is their 3-Dimensional localizability. Recently, researchers have proposed some 3-Dimensional RFID-based localization schemes, but most of them suffer from low efficiency. In this paper, we target at improving the efficiency of RFID-based localization, including energy efficiency and time efficiency, without sacrificing localization accuracy. The main idea is to adopt a “jumping probe” in distance estimation, based on which we propose the 3-Dimensional RFID-based localization schemes called JumpLoc, including a passive scheme two active schemes. In the passive JumpLoc scheme, a target tag will be located based on the estimated distances between itself and some reference readers. While the active schemes include basic and enhanced active JumpLoc schemes to locate a target reader. We numerically analyze the localization efficiency improvement of the proposed JumpLoc schemes. We also conduct simulations to validate their effectiveness, the results of which show that the passive JumpLoc scheme can improve the energy efficiency and time efficiency by at least 56% and 34% respectively, and the active JumpLoc schemes can improve the energy efficiency and time efficiency by at least 82% and 83% respectively.

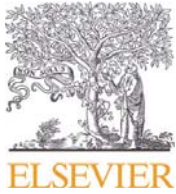
© 2016 Elsevier B.V. All rights reserved.

1. Introduction

Radio Frequency Identification (RFID) [1–3], as an emerging technology, has gained increasingly widespread applications in industry [4,5], especially with the explosive development of Wireless Sensor Networks (WSNs) [6–11] and Internet of Things (IoTs) [12]. An RFID system typically consists of two basic components—reader and tag, the communication between which does not rely on line-of-sight. Moreover, RFID tag becomes smaller and smaller with a very low price. The above features make the large-scale RFID applications [3] possible, and many applications, such as health monitoring [13], library maintenance [14] and product tracking [15] can greatly benefit from utilization of RFID systems with security and privacy [16–18] considerations.

* Corresponding author.

E-mail address: chenhl@upc.edu.cn (H. Chen).



Contact expectation based routing for delay tolerant networks



Honglong Chen^{a,b,c,*}, Wei Lou^{b,c}

^a College of Information and Control Engineering, China University of Petroleum, PR China

^b Department of Computing, The Hong Kong Polytechnic University, Kowloon, Hong Kong

^c The Hong Kong Polytechnic University Shenzhen Research Institute, Shenzhen, PR China

ARTICLE INFO

Article history:

Received 23 January 2015

Revised 20 July 2015

Accepted 28 July 2015

Available online 7 August 2015

Keywords:

Buffer management

Community aware

Delay tolerant networks

Expected encounter

Routing protocols

ABSTRACT

In conventional networks, routing problem can be modeled as the design of an efficient source-to-destination route based on persistent end-to-end paths. However, in a delay tolerant network (DTN), nodes are intermittently connected and thus, the end-to-end paths will not always exist, in which routing is a challenging issue. Previous DTN routing protocols tend to make routing decision based on the nodes' contact information. In this paper, we observe that considering both the nodes' contact information and message property such as the time-to-live (TTL) would help to improve the performance. Embedded this idea, we first propose an expected encounter based routing protocol (EER) which distributes multiple replicas of a message proportionally between two encounters according to their expected encounter values. In case of a single replica of a message, EER makes the routing decision by comparing two encountering nodes' minimum expected meeting delays to destination. We further propose a community aware routing protocol (CAR) which takes advantages of the high contact frequency property of the nodes within the same community. We also propose the buffer management strategies corresponding for the two protocols. We conduct simulations to evaluate our proposed protocols and some existing ones on three metrics: delivery ratio, latency and goodput. The simulation results illustrate that our proposed EER and CAR protocols outperform other existing ones.

© 2015 Elsevier B.V. All rights reserved.

1. Introduction

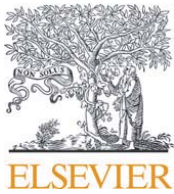
Delay tolerant networks (DTNs) [1,2] are an emergent communication paradigm, which can be applied to many applications such as delay tolerant event collection [3], pocket switch networks [4] and social networks [5–7], etc. In typical DTNs, nodes are always mobile, making the conventional routing protocols based on persistent end-to-end paths not still applicable since they do not always exist. Due to the mobile characteristic of nodes in DTNs, the link between each pair of encountering nodes will be intermittent, thus the network topology will change over time. Therefore, it is difficult

to design an efficient routing protocol for DTNs based on the intermittently connected links.

Store-carry-and-forward mechanism is widely adopted to deliver messages in DTNs. It will be relatively easier for a node to make an optimal routing decision if it is aware of global network connectivity. However, it is hard for a node to obtain the global network connectivity as it is time-varying. Fig. 1 shows a simple network with six mobile nodes which are intermittently connected. The network topology varies from time t_1 to t_4 . For instance, if node A wants to send a message to node D at t_1 , according to the global network connectivity, the optimal delivery path for this message is from node A to node E at t_2 , then from node E to node F at t_3 and finally from node F to node D at t_4 . However, node A may apply the best effort strategy to deliver message to node B at t_1 since it meets node B first, resulting in its failing to

* Corresponding author. Tel.: +86- 13573861376.

E-mail addresses: honglongchen1984@gmail.com, chenhl@upc.edu.cn (H. Chen), csweilou@comp.polyu.edu.hk (W. Lou).



On protecting end-to-end location privacy against local eavesdropper in Wireless Sensor Networks



Honglong Chen^{a,b,*}, Wei Lou^{b,c}

^a College of Information and Control Engineering, China University of Petroleum, Qingdao, PR China

^b Department of Computing, The Hong Kong Polytechnic University, Kowloon, Hong Kong

^c The Hong Kong Polytechnic University Shenzhen Research Institute, Shenzhen, PR China

ARTICLE INFO

Article history:

Received 11 March 2013

Received in revised form 13 January 2014

Accepted 21 January 2014

Available online 28 January 2014

Keywords:

Local eavesdropper

Location privacy

Wireless sensor networks

ABSTRACT

Wireless Sensor Networks (WSNs) are often deployed in hostile environments to detect and collect interested events such as the appearance of a rare animal, which is called event collection system. However, due to the open characteristic of wireless communications, an adversary can detect the location of a source or sink and eventually capture them by eavesdropping on the sensor nodes' transmissions and tracing the packets' trajectories in the networks. Thus the location privacy of both the source and sink becomes a critical issue in WSNs. Previous research only focuses on the location privacy of the source or sink independently. In this paper, we address the importance of location privacy of both the source and sink and propose four schemes called forward random walk (FRW), bidirectional tree (BT), dynamic bidirectional tree (DBT) and zigzag bidirectional tree (ZBT) respectively to deliver messages from source to sink, which can protect the end-to-end location privacy against local eavesdropper. Simulation results illustrate the effectiveness of the proposed location privacy protection schemes.

© 2014 Elsevier B.V. All rights reserved.

1. Introduction

Recent advancement in wireless communications and Micro-Electro-Mechanical Systems (MEMS) has enabled the development of low-cost Wireless Sensor Networks (WSNs), which are made up of a number of sensor nodes that are self-organized for various applications, such as mobile target detection [1], earthquake monitoring [2], and habitat monitoring [3]. In these applications, sensor nodes are deployed to detect the existence of an interested event, such as the appearance of a rare animal. The sensor nodes that detect the occurrence of the interested event will send the detection information to a sink (or base station) by multi-hop wireless communications. Such kind of systems is called event collection system [4], which is one of the important applications in WSNs.

Due to the open characteristic of wireless communications, it is not difficult to attack wireless sensor networks with the goal of either obtaining confidential data or simply disrupting the normal operations of the WSN applications [5–7]. In either case, they may involve threats to one of the following two types of WSN privacy, *content* privacy and *contextual* privacy [8]. The former refers to the confidentiality of the content of the packets passing between the nodes in the network. This is usually guaranteed by using methods of encryption and authentication [9]. The latter refers to the confidentiality of information about traffic patterns in the network, which may be used by adversaries to disrupt the network. The location privacy, i.e., the confidentiality of the location of either source, sink, or both, is a kind of contextual privacy.

* Corresponding author at: College of Information and Control Engineering, China University of Petroleum, Qingdao, PR China. Tel.: +86 13573861376.
E-mail addresses: honglongchen1984@gmail.com, chenhl@upc.edu.cn (H. Chen), csweilou@comp.polyu.edu.hk (W. Lou).

RESEARCH ARTICLE

On providing wormhole-attack-resistant localization using conflicting sets

Honglong Chen^{1*}, Wei Lou^{2,3} and Zhi Wang⁴¹ College of Information and Control Engineering, China University of Petroleum, Qingdao, China² Department of Computing, The Hong Kong Polytechnic University, Kowloon, Hong Kong³ Shenzhen Research Institute, The Hong Kong Polytechnic University, Shenzhen, China⁴ State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou, China

ABSTRACT

Wormhole attack is a severe attack that can be easily mounted on a wide range of wireless networks without compromising any cryptographic entity or network node. In the wormhole attack, an attacker sniffs packets at one point in the network and tunnels them through the wormhole link to another point. Such kind of attack can deteriorate the localization procedure in wireless sensor networks. In this paper, we first analyze the impacts of the wormhole attack on the localization procedure. Then, we propose a secure localization scheme against the wormhole attacks called SLAW including three phases: wormhole attack detection, neighboring locators differentiation, and secure localization. The main idea of the SLAW is to build a so-called conflicting set for each locator based on the abnormalities during the message exchanges, which can be used to differentiate the dubious locators to achieve secure localization. We first consider the simplified system model in which there is no packet loss and all the nodes have the same transmission range. We further consider the general system model where the packet loss exists and different types of nodes have different transmission radii. We conduct the simulations to illustrate the effectiveness of the proposed secure localization scheme and compare it with the existing schemes under different network parameters. Copyright © 2014 John Wiley & Sons, Ltd.

KEYWORDS

secure localization; wormhole attacks; wireless sensor networks; conflicting set

*Correspondence

Honglong Chen, College of Information and Control Engineering, China University of Petroleum, Qingdao, China.

E-mail: chenhl@upc.edu.cn

1. INTRODUCTION

In many wireless sensor network (WSN) applications, such as the emergency response systems, military field operations, and environment monitoring systems, the inaction of measurement data without location information makes the self-localization capability a highly desirable characteristic for the nodes in the networks. Most of the localization algorithms for WSNs estimate the positions of location-unknown nodes on the basis of the position information of a set of nodes (*locators*) and the inter-node measurements. Generally, the localization techniques can be classified into two categories: *range-based* and *range-free* schemes. The range-based localization schemes assume that the distances between sensors and locators can be estimated using different measurements, such as time of arrival [1], time difference of arrival [2,3], angle of arrival [4], or received signal strength indicator (RSSI [5]). In contrast, the range-free localization schemes rely on other features of the network,

such as hop count [6], centroid [7], Approximate-Point-In-Triangulation (APIT) [8], amorphous computation [9], directional antenna [10], signal fingerprinting [11], LAND-MARC [12], and so on.

Because of the natural vulnerability of the wireless communications, that is, it is easy for a malicious node to sniff packets from or inject packets into the wireless networks, security becomes a challenging issue in WSNs [13]. Despite the recent advances of localization in WSNs, most of the existing localization systems are vulnerable under the adversarial scenario where malicious attacks can disturb the localization process. For example, a compromise attack [14] may induce the node to get incorrect distance measurements, leading to the malfunction of the range-based localization technique. Therefore, security is a necessary characteristic of the localization process in the hostile wireless networks.

Attackers, which can threaten the localization of nodes in a hostile WSN, can generally be classified into two

针对虫洞攻击的无线传感器网络安全定位方法

陈鸿龙¹, 王志波², 王智³, 许江铭⁴, 李燕君⁵, 刘丽萍⁶

(1. 中国石油大学(华东) 信息与控制工程学院, 山东 青岛 266580; 2. 武汉大学 计算机学院, 湖北 武汉 430072;
3. 浙江大学 工业控制技术国家重点实验室, 浙江 杭州 310027; 4. 中国石油塔里木油田公司, 新疆 库尔勒 841000;
5. 浙江工业大学 计算机科学与技术学院, 浙江 杭州 310014; 6. 天津大学 电气与自动化工程学院, 天津 300072)

摘 要: 节点定位技术是无线传感器网络的关键技术之一, 是很多基于无线传感器网络的应用的基础。然而, 无线传感器网络通常部署在无人值守的敌对环境中, 攻击节点能够很容易地破坏网络中节点的定位过程。针对无线传感器网络中距离无关的定位技术, 分析了虫洞攻击对 DV-Hop 定位过程的影响, 提出了一种无线传感器网络中抵御虫洞攻击的 DV-Hop 安全定位方法。仿真结果表明, 所提出的安全定位方法能够有效降低虫洞攻击对 DV-Hop 定位过程的影响, 验证了该方法的有效性。

关键词: 无线传感器网络; 虫洞攻击; 安全定位; DV-Hop 定位

中图分类号: TP393

文献标识码: A

Secure localization scheme against wormhole attack for wireless sensor networks

CHEN Hong-long¹, WANG Zhi-bo², WANG Zhi³, XU Jiang-ming⁴, LI Yan-jun⁵, LIU Li-ping⁶

(1. College of Information and Control Engineering, China University of Petroleum, Qingdao 266580, China;
2. Computer School, Wuhan University, Wuhan 430072, China; 3. State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou 310027, China; 4. China Petro Tarim Oilfield Company, Kurla 841000, China;
5. College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310014, China;
6. School of Electrical Engineering and Automation, Tianjin University, Tianjin 300072, China)

Abstract: As one of the key technologies in wireless sensor networks (WSN), localization is the basis of many WSN-based applications. However, WSNs are often deployed in the hostile environment, in which the attackers can easily disrupt the localization procedure of the nodes. The effects of wormhole attack on the DV-Hop localization procedure are analyzed firstly, after which a secure localization scheme against the wormhole attack is proposed. The simulation results illustrate that the proposed secure localization scheme can efficiently reduce the effects of the wormhole attack on the DV-Hop localization, which validates the effectiveness of the proposed scheme.

Key words: wireless sensor networks; wormhole attack; secure localization; DV-Hop localization

1 引言

近年来, 微机电系统 (MEMS, micro-electro-mechanical systems) 以及无线通信等技术的迅猛发展, 使无线传感器网络 (WSN, wireless sensor

networks) 的研究^[1]得到越来越多的研究机构 and 学者们的支持。目前, 无线传感器网络有着极其广泛的应用, 包括军事领域的目标定位和追踪, 民用领域的森林火警监测、医疗监护和智能家居等。然而, 许多无线传感器网络的应用是基于节点位置信息

收稿日期: 2013-10-08; 修回日期: 2013-12-09

基金项目: 国家自然科学基金资助项目(61309023, 61273079, 61104208); 山东省自然科学基金资助项目(ZR2013FQ032); 中央高校基本科研业务费专项基金资助项目(13CX02100A); 浙江省可视媒体智能处理技术研究重点实验室开放课题基金资助项目(2012008)

Foundation Items: The National Natural Science Foundation of China (61309023, 61273079, 61104208); The Natural Science Foundation of Shandong Province (ZR2013FQ032); The Fundamental Research Funds for the Central Universities (13CX02100A); The Open Project of Zhejiang Provincial Key Lab of Intelligent Processing Research of Visual Media (2012008)

基于 RFID 反向散射的标签定位实验平台

陈鸿龙, 李宪敏, 代天骄, 孙 良

(中国石油大学(华东)信息与控制工程学院, 山东 青岛 266580)

摘 要:介绍了基于测距定位方法的基本工作原理,设计了一套基于射频识别反向散射的标签定位实验平台。该实验平台包括 1 个后端服务器、1 台英频杰阅读器、多个 RFID 天线和 1 个标签。RFID 天线的位置已知,作为信标节点并由阅读器控制,标签位置未知。由天线发送射频信号,信号到达标签后经反向散射返回天线,阅读器测得射频信号经由传输路径的相位变化,基于射频信号的传输模型估计天线和标签之间的距离,并结合天线的位置信息,利用极大似然估计方法估计标签的位置信息。该实验平台涵盖了射频通信、信号分析和处理以及定位算法等内容,有助于学生深入学习和理解基于 RFID 定位方法的原理和应用,能够培养和提高学生针对复杂工程问题的创新能力和工程实践能力。

关键词: 射频识别; 反向散射; 相位; 极大似然估计

中图分类号: TN925 **文献标识码:** A **文章编号:** 1002-4956(2019)10-0092-03

Experimental platform for label location based on RFID backscattering

CHEN Honglong, LI Xianmin, DAI Tianjiao, SUN Liang

(College of Information and Control Engineering, China University of Petroleum, Qingdao 266580, China)

Abstract: This paper introduces the basic working principle of the ranging and positioning method and designs a label positioning experimental platform based on radio frequency identification backscattering. The experimental platform includes a back-end server, an English band reader, multiple RFID antennas and a tag. The location of the RFID antenna is known. As the beacon node and as controlled by the reader, the location of the tag is unknown. The radio frequency signal is transmitted from the antenna and returned to the antenna by backscattering after arriving at the tag. The reader measures the phase change of the radio frequency signal through the transmission path, and estimates the distance between the antenna and the tag based on the transmission model of the radio frequency signal. Combined with the position information of antenna, the position information of tag is estimated by maximum likelihood estimation method. The experimental platform covers radio frequency communication, signal analysis and processing, and location algorithm. It is helpful for students to deeply understand the principle and application of location method based on RFID, and it can also cultivate and improve students' innovative ability and engineering practice ability for complex engineering problems.

Key words: radio frequency identification; backscatter; phase; maximum likelihood estimation

物联网^[1-2]是指通过信息传感设备,按照约定的协议,把物品和互联网连接起来,进行信息交换和通信,实现智能化识别、定位、跟踪、监控和管理的一种网络。近年来物联网技术的发展日新月异,取得了许多

重大突破并得到广泛应用^[3-4]。射频识别(RFID)^[5]技术作为物联网的关键核心技术之一,目前已经被广泛应用于石油石化、仓储管理和物流追踪等领域,并取得巨大的经济效益。例如,将 RFID 系统应用于高校实验室的实验设备管理^[6],通过实现对 RFID 标签的监测即可实现对实验设备的快速的、高效的以及可靠的自动化管理,大大提高实验室的运行效率。

在物联网的应用中,感知层中的节点通过传感器采集相关感知信息,并经过传输层将感知信息传输到应用层,进行数据处理、分析和应用。但是,在许多

收稿日期: 2019-03-07

基金项目: 国家自然科学基金面上项目(61772551);山东省重点研发计划(2018GGX101035);中国石油大学(华东)校级教改项目(JY-B201833)

作者简介: 陈鸿龙(1984—):男,福建泉州,副教授,博士生导师,计算机科学博士,研究方向为物联网。

E-mail: chenhl@upc.edu.cn

基于物联网的抽油机群远程监控实验平台

陈鸿龙¹, 杨玉斌², 田力丹¹, 马国蕾¹, 李晓辉¹

- (1. 中国石油大学(华东) 信息与控制工程学院, 山东 青岛 266580;
2. 中国电子科技集团公司第四十一研究所, 山东 青岛 266580)

摘 要: 设计了一套基于物联网的抽油机群远程监控实验平台。该实验平台基于自行设计的 ZigBee 节点、施耐德电气公司的可编程控制器(PLC)Modicon M340 和 GPRS 网络, 实现了对抽油机群工作状态的远程监控。该实验平台涵盖了抽油机的信息采集、信息传输(包括有线和无线)、信息存储和信息处理等实验教学内容, 有助于学生深入学习和理解物联网技术在石油开采领域中的设计方法和应用, 培养和提高学生的创新能力和工程实践能力。

关键词: 抽油机群; 远程监控; 物联网; ZigBee 节点; GPRS 网络

中图分类号: TE933; TP277 **文献标志码:** A **文章编号:** 1002-4956(2016)2-0114-03

An experimental platform for remote monitoring of pumping unit group based on Internet of things

Chen Honglong¹, Yang Yubin², Tian Lidan¹, Ma Guolei¹, Li Xiaohui¹

- (1. College of Information and Control Engineering, China University of Petroleum, Qingdao 266580, China;
2. The 41st Institute of China Electronics Technology Group Corporation, Qingdao 266580, China)

Abstract: The basic working principles of the beam-pumping units are firstly briefly introduced and then an experimental platform for remote monitoring of pumping unit group based on Internet of things is designed. The designed experimental platform is based on the self-designed ZigBee node, the PLC of Schneider Electric (Modicon M340) and the GPRS network. In the experimental platform, the contents of information collection of the pumping unit, information transmission (including wired and wireless communications), information storage and information processing are covered. The designed experimental platform will help the experimenters learn and understand the design methods and applications of the Internet of things technology in the petroleum field, cultivate and improve their innovation capacity and engineering practice capacity.

Key words: pumping unit group; remote monitoring; internet of things; ZigBee node; GPRS network

物联网技术利用局部网络或互联网等通信手段, 把传感器、控制器、机器、人员和物等通过新的方式联系在一起, 形成人与物、物与物相联, 实现信息化、远程管理控制和智能化的网络^[1-3]。近年来, 物联网技术的研

究得到了国内学者的高度重视并取得了许多研究成果^[4-6]。物联网以其感知半径大、感知范围广、方便部署、长期自主运行、低功耗、低成本等诸多优势在石油石化生产过程监测^[7]、生态环境监控^[8]和战场监视^[9]等诸多领域得到广泛应用, 被称为继计算机、互联网之后世界信息产业发展的第三次浪潮。

抽油机是陆地油田广泛使用的石油开采设备之一, 主要是通过加压的办法使石油出井^[10]。抽油机的正常运转是保障原油稳定生产的前提条件之一。然而, 抽油机通常分布在野外环境中, 其运行状态的远程监控比较复杂, 需要将抽油机的运行参数实时地远程传输至中央服务器。因此, 对抽油机(尤其是抽油机群)运行状态的远程监控面临很多困难。

收稿日期: 2015-07-29

基金项目: 中国石油大学(华东) 校级青年教改项目; 国家自然科学基金项目(61309023); 山东省自然科学基金项目(ZR2013FQ032); 山东省重点研发计划项目(2015GGX101045); 青岛市科技计划项目(15-9-1-79-jch)

作者简介: 陈鸿龙(1984—), 男, 福建泉州, 博士, 副教授, 硕士生导师, 研究方向为无线传感网络、容迟网络和移动自组织网络。

E-mail: chenhl@upc.edu.cn

Dynamic Distributed Honeypot Based on Blockchain

LEYI SHI¹, YANG LI¹, TIANXU LIU¹, JIA LIU¹, BAOWING SHAN¹, AND HONGLONG CHEN^{1,2} 

¹College of Computer and Communication Engineering, China University of Petroleum, Qingdao 257067, China

²College of Information and Control Engineering, China University of Petroleum, Qingdao 257067, China

Corresponding author: Honglong Chen (honglongchen1984@gmail.com)

This work was supported in part by the Shandong Provincial Natural Science Foundation under Project ZR2019MF034, in part by the National Natural Science Foundation of China under Grant 61772551, in part by the Shandong Provincial Key Program of Research and Development under Grant 2018GGX101035, in part by the Fundamental Research Funds for the Central Universities under Grant 18CX07003A, in part by the Open Research Fund from Shandong Provincial Key Laboratory of Computer Networks under Grant SDKLCN-2018-06.

ABSTRACT Honeypot technology can be applied to efficiently attract attackers and exhaust their resources. However, the traditional static honeypot is easy to be recognized by anti-honeypot technology. By contrast, most of the dynamic honeypots can simulate the real system in time, thus interacting with an intruder in disguise. In this paper, we employ the dynamic property of honeypot in four kinds of services of our system. However, this dynamic property shows up in a location and identification, indicating that genuine or fake services (honeypots) are changeable in different hosts. Thus, the dynamic property of our system differs from the dynamic honeypot aforementioned. Besides, we adopt the blockchain platform (Ethereum) to decentralize our system and store the port access data by delivering a private chain. To illustrate the effectiveness of our scheme in theory and practice, security analysis, eavesdropping attack, scanning attack, and DoS attack experiments are conducted. The results show that our scheme is valid in safeguarding against network attack.

INDEX TERMS Honeypot, blockchain, security analysis, network security.

I. INTRODUCTION

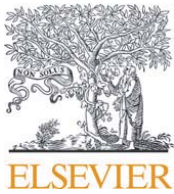
As a proactive defense mechanism, a honeypot is becoming an indispensable tool for providing network security in wide applications such as Internet of Things (IoT) [1]–[4], wireless sensor networks (WSNs) [5], [6] and vehicular networks [7], etc. With proactivity and inveiglement, a honeypot can attract an attacker to interact with the fake system resources, which prevents valuable resources from being attacked. Generally speaking, honeypots are traps that imitate actual systems and monitor intruders in physical or virtual formalization. Compared with traditional methods, including but not restricted to Firewall and Intrusion Detection System (IDS), honeypots completely overthrow passiveness in network defense domain. Consequently, honeypots have gained widespread attention among cyber-security forces.

Honeypots can be classified into two categories in terms of variation attribute: static and dynamic honeypots. Static honeypots are designed to deceive attackers by imitating

some system characteristics. However, because of the fixed configuration and response, they are prone to be detected by attackers, who further escape the meaningless traps and launch an attack towards real system. The changeable property in dynamic honeypots improves the weakness of the former. Due to the changeable configuration, the pseudo system (i.e., dynamic honeypot [8]) is capable of cheating intruders and of learning their attacking modes.

There are some typical works about dynamic honeypots. By integrating and analyzing data collected with passive and active tools, a dynamically configuration scheme [8] can be generated and implemented in Local Area Network (LAN) and enterprise network deployment. Both the real and fake systems simultaneously take effect during runtime. As described in [9], the flow identified as legitimate or aggressive serves as measurement criteria for generating dynamic honeypots. According to the network load, the detail numerical result about honeypots and servers is derived. The result is carried out in actual deployment. Besides, a honeynet management framework [10] can be used to generate dynamic configuration approach. However, the dynamic

The associate editor coordinating the review of this manuscript and approving it for publication was Marco Anisetti.



Securing DV-Hop localization against wormhole attacks in wireless sensor networks



Honglong Chen^{a,b}, Wei Lou^{c,d}, Zhi Wang^{a,*}, Junfeng Wu^e, Zhibo Wang^a, Aihua Xia^a

^a State Key Lab of Industrial Control Technology, Zhejiang University, Hangzhou, PR China

^b College of Information and Control Engineering, China University of Petroleum, Qingdao, PR China

^c Department of Computing, The Hong Kong Polytechnic University, Hong Kong

^d The Hong Kong Polytechnic University Shenzhen Research Institute, Shenzhen, PR China

^e Department of Electronic and Computer Engineering, The Hong Kong University of Science and Technology, Hong Kong

ARTICLE INFO

Article history:

Received 8 May 2013

Received in revised form 27 December 2013

Accepted 17 January 2014

Available online 30 January 2014

Keywords:

DV-Hop localization

Wireless sensor networks

Wormhole attack

ABSTRACT

Node localization becomes an important issue in the wireless sensor network as its wide applications in environment monitoring, emergency rescue and battlefield surveillance, etc. Basically, the DV-Hop localization scheme can work well with the assistance of beacon nodes that have the capability of self-positioning. However, if the network is invaded by a wormhole attack, the attacker can tunnel the packets via the wormhole link to severely disrupt the DV-Hop localization process. The distance-vector propagation phase during the DV-Hop localization can even aggravate the positioning error, compared to the localization schemes without wormhole attacks. In this paper, we analyze the impacts of wormhole attack on the DV-Hop localization scheme, based on which we propose a label-based DV-Hop secure localization scheme to defend against the wormhole attack. We further theoretically prove the correctness of the proposed scheme. Simulation results illustrate the effectiveness of the proposed label-based DV-Hop secure localization scheme.

© 2014 Elsevier B.V. All rights reserved.

1. Introduction

With the advantages of low cost, large scale, densely distributed deployment and self-configuration, Wireless Sensor Networks (WSNs) have been applied in many fields to monitor and control the physical world [1]. In WSNs, sensed data will make no sense without the nodes' position information. Hence, nodes are required to locate themselves in many WSN applications, such as environment monitoring, emergency rescue and battlefield surveillance, etc.

Many protocols and algorithms are proposed to solve the node's localization problem, which can be classified into two categories: range-based and range-free [2] schemes. Range-based schemes calculate the location using the point-to-point distance (or angle) estimates. Though range-based schemes are able to obtain relatively accurate results, they can be applied only when nodes are equipped with sophisticated hardware for the distance measurement. Range-free schemes do not rely on the availability of range (or angle) estimates, thus they need no expensive hardware. Considering that the hardware requirement of range-based schemes is inappropriate for the resource-constrained WSNs, researchers are pursuing range-free localization techniques as a cost-effective alternative [2].

The DV-Hop [3] localization, as a range-free localization scheme, is applied with the assumption of isotropic networks. First, beacons (or anchors), as location-known nodes, flood their positions through the network so that all the nodes can

* Corresponding author. Tel.: +86 18658100255.

E-mail addresses: wangzhizju@gmail.com, wangzhi@iipc.zju.edu.cn (Z. Wang).

Privacy-Preserving Crowd-Sourced Statistical Data Publishing with An Untrusted Server

Zhibo Wang¹, Senior Member, IEEE, Xiaoyi Pang, Yahong Chen, Huajie Shao, Member, IEEE, Qian Wang², Member, IEEE, Libing Wu, Member, IEEE, Honglong Chen³, Member, IEEE, and Hairong Qi, Fellow, IEEE

Abstract—The continuous publication of aggregate statistics over crowd-sourced data to the public has enabled many data mining applications (e.g., real-time traffic analysis). Existing systems usually rely on a trusted server to aggregate the spatio-temporal crowd-sourced data and then apply differential privacy mechanism to perturb the aggregate statistics before publishing to provide strong privacy guarantee. However, the privacy of users will be exposed once the server is hacked or cannot be trusted. In this paper, we study the problem of real-time crowd-sourced statistical data publishing with strong privacy protection under an untrusted server. We propose a novel distributed agent-based privacy-preserving framework, called DADP, that introduces a new level of multiple agents between the users and the untrusted server. Instead of directly uploading the check-in information to the untrusted server, a user can randomly select one agent and upload the check-in information to it with the anonymous connection technology. Each agent aggregates the received crowd-sourced data and perturbs the aggregated statistics locally with Laplace mechanism. The perturbed statistics from all the agents are further combined together to form the entire perturbed statistics for publication. In particular, we propose a distributed budget allocation mechanism and an agent-based dynamic grouping mechanism to realize global w -event ϵ -differential privacy in a distributed way. We prove that DADP can provide w -event ϵ -differential privacy for real-time crowd-sourced statistical data publishing under the untrusted server. Extensive experiments on real-world datasets demonstrate the effectiveness of DADP.

Index Terms—Mobile crowdsensing, data publishing, untrusted server, differential privacy, privacy-preserving

1 INTRODUCTION

WITH the rapid development of networking and mobile devices, we are facing an explosive increase of crowd-sourced data (e.g., check-in data at Foursquare [1], real-time traffic at Waze [2], air quality at SensorMap [3] and commonSense [4]) from millions of users. These crowd-sourced data can be aggregated in real-time and mined by machine learning technologies to discover valuable information and further benefit our life (e.g., popular restaurants recommendation [5], real-time traffic analysis and navigation [6]). Recently more and more agencies (e.g., governments and companies) are publishing the crowd-sourced data to the public for data mining purposes. However, the

promising advantages of data publishing and mining are at the risk of disclosing sensitive information to data miners. A recent study [7] showed that with some outside information, the human mobility data obtained from users can be linked back to an individual. With the increasing concern of privacy leakage, private data publishing mechanisms are urgently required to protect the sensitive information of individuals while not affecting the utility of crowd-sourced data published for data mining purposes.

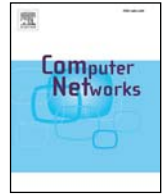
Differential privacy [8], which can provide privacy for data publishing with strong theoretical guarantee, has emerged as a compelling privacy model. [9], [10], [11], [12] realizes differentially private data publishing, which provides ϵ -differential privacy for “one-time” release of statistical data. In order to further provide strong privacy guarantee for real-time data, a new privacy model called “ w -event privacy” [13] has been proposed, which protects any event sequence occurring in w successive time instants. Several effective approaches, such as BD [13], BA [13], and RescueDP [14], have been proposed to realize w -event privacy for real-time data publishing under the trusted server.

Despite the successful privacy-protection of applying differential privacy to data publishing, most of existing systems rely on a trusted server to aggregate the crowd-sourced data and perturb the true aggregated statistics prior to their publishing. Fig. 1a shows the traditional architecture of data collection and statistics publishing under a trusted server, where users upload data directly to the trusted server which then performs statistic calculation and

- Z. Wang, X. Pang, Y. Chen, and Q. Wang are with the Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan, Hubei 430072, P.R. China. E-mail: {zwbwang, xypang, yahchen, qianwang}@whu.edu.cn.
- H. Shao is with the Department of Computer Science, University of Illinois Urbana-Champaign, Urbana, IL 61801. E-mail: hshao5@illinois.edu.
- L. Wu is with the School of Computer Science, Wuhan University, Wuhan, Hubei 430072, P.R. China. E-mail: wu@whu.edu.cn.
- H. Chen is with the College of Information and Control Science, China University of Petroleum, Beijing 266580, P. R. China. E-mail: honglongchen1984@gmail.com.
- H. Qi is with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996. E-mail: hqi@utk.edu.

Manuscript received 14 Apr. 2018; revised 28 June 2018; accepted 27 July 2018. Date of publication 31 July 2018; date of current version 2 May 2019. (Corresponding author: Libing Wu.)

For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below. Digital Object Identifier no. 10.1109/TMC.2018.2861765



Achieving location error tolerant barrier coverage for wireless sensor networks



Zhibo Wang^a, Honglong Chen^b, Qing Cao^c, Hairong Qi^c, Zhi Wang^d, Qian Wang^{a,*}

^a State Key Lab of Software Engineering, School of Computer, Wuhan University, China

^b Information and Control Engineering, China University of Petroleum, Qingdao, China

^c Electrical Engineering and Computer Science, University of Tennessee, Knoxville, USA

^d State Key Laboratory of Industrial Control Technology, Hangzhou, China

ARTICLE INFO

Article history:

Received 8 July 2016

Revised 16 November 2016

Accepted 17 November 2016

Available online 24 November 2016

Keywords:

Barrier coverage

Location error

Fault tolerance

Sensor networks

ABSTRACT

Barrier coverage is a critical issue in wireless sensor networks deployed in security applications (e.g., border protection), whose performance strongly depends on the locations of sensor nodes. Existing works on barrier coverage typically assume that sensor nodes have accurate location information, which is not reasonable or practical for many real sensor networks. In this paper, we study the barrier coverage problem when sensor nodes have location errors and deploy mobile sensor nodes to improve barrier coverage if the network is not barrier-covered after initial deployment. We analyze the effects of location errors for barrier coverage and propose a fault-tolerant weighted barrier graph to model the barrier coverage formation problem. Based on the graph, we prove that the minimum number of mobile sensor nodes needed to achieve barrier coverage with a guarantee is the length of the shortest path on the graph. Furthermore, we improve the computational efficiency of the fault-tolerant barrier coverage formation algorithm by removing unnecessary edges on the graph. Experimental results validate the correctness of our analysis and the proposed algorithms.

© 2016 Elsevier B.V. All rights reserved.

1. Introduction

Wireless sensor networks (WSNs) have been widely used as an effective surveillance tool for security applications, such as battle-field surveillance, border protection, and airport intruder detection. To detect intruders who penetrate the region of interest (ROI), we need to deploy a set of sensor nodes that can provide coverage of the ROI, a problem that is often referred to as *barrier coverage* [1], where sensor nodes form *barriers* for intruders.

Deterministic and random deployment are the two most popular ways of deploying sensor nodes in the ROIs. For ROIs within friendly environments, a deterministic deployment can be used to deploy sensor nodes to specific locations. However, in general, the ROIs are within harsh environments that are difficult for humans to reach, which makes random deployment (e.g., dropping by aircraft) the only practical way to deploy nodes. When only stationary sensor nodes are used, after the initial random deployment, it is highly possible that sensor nodes could not form a barrier due to the gaps in their coverage, which would allow intruders to cross

the ROIs without being detected. Therefore, it is necessary to deploy more sensor nodes to form a barrier. In fact, it is difficult, if possible at all, to improve barrier coverage for sensor networks consisting of only stationary nodes¹. Fortunately, with recent technological advances, practical mobile nodes (e.g., Robomote [2] and Packbot [3]) have been developed, which provides us a way to improve barrier coverage performance after sensor networks have been deployed.

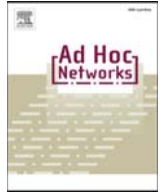
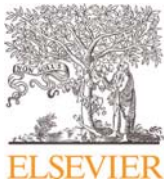
The location information of nodes provides the basis of many applications, such as navigation and target tracking. However, it is costly to equip each node with GPS receivers. Therefore, the locations of nodes are unknown when they are randomly deployed. To obtain the location of each node, a lot of localization algorithms have been proposed, including range-based (e.g., TOA [4], TDOA [5], and RSSI [6]) and range-free (e.g., DV-HOP [7,8], and APIT [9]) localization algorithms. However, none of them can provide accurate locations, which inevitably introduces location errors.

The existence of location errors can significantly affect the quality of barrier coverage provided by sensor networks. In reality, we can only know the measured locations instead of the true locations of sensor nodes. As shown in Fig. 1(a), although nodes *a* and

* Corresponding author.

E-mail addresses: zbwang@whu.edu.cn (Z. Wang), qianwang@whu.edu.cn (Q. Wang).

¹ We use “sensor nodes” or “nodes” interchangeably in this paper.



Cost-effective barrier coverage formation in heterogeneous wireless sensor networks



Zhibo Wang^{a,b}, Qing Cao^b, Hairong Qi^b, Honglong Chen^c, Qian Wang^{a,d,*}

^aState Key Lab of Software Engineering, School of Computer, Wuhan University, China

^bElectrical Engineering and Computer Science, University of Tennessee, Knoxville, USA

^cInformation and Control Engineering, China University of Petroleum, Qingdao, China

^dKey Lab of Aerospace Information Security and Trusted Computing, Wuhan University, China

ARTICLE INFO

Article history:

Received 28 December 2016

Revised 19 April 2017

Accepted 19 June 2017

Available online 20 June 2017

Keywords:

Wireless sensor networks

Barrier coverage

Heterogeneous sensors

Mobile sensors

ABSTRACT

Barrier coverage is a critical issue in wireless sensor networks (WSNs) for security applications, which however cannot be guaranteed to be formed after initial random deployment of sensors. Existing work on barrier coverage mainly focus on homogeneous WSNs, while little effort has been made on exploiting barrier coverage formation in heterogeneous WSNs where different types of sensors are deployed with different sensing models and costs. In this paper, we study how to efficiently form barrier coverage by leveraging multiple types of mobile sensors to fill in gaps between pre-deployed stationary sensors in heterogeneous WSNs. The stationary sensors are grouped into clusters and a cluster-based directional barrier graph is proposed to model the barrier coverage formation problem. We prove that the minimum cost of mobile sensors required to form a barrier with stationary sensors is the length of the shortest path on the graph. Moreover, we propose a greedy movement algorithm for heterogeneous WSNs to efficiently schedule different types of mobile sensors to different gaps while minimizing the total moving cost. In particular, we formulate the movement problem for homogeneous WSNs as a minimum cost bipartite assignment problem, and solve it in polynomial time using the Hungarian algorithm. Extensively experimental results on homogeneous and heterogeneous WSNs demonstrate the effectiveness of the proposed algorithms.

© 2017 Elsevier B.V. All rights reserved.

1. Introduction

Wireless sensor networks (WSNs) have been widely used as an effective surveillance tool for security applications, such as battlefield surveillance, border protection, and airport intruder detection. To detect intruders who penetrate the regions of interest (ROI), we need to deploy a set of sensor nodes that can provide coverage of the ROI, a problem that is often referred to as *barrier coverage* [1], where sensors form a *barrier* to prevent intruders from crossing the ROI. When only stationary sensors are used, however, after the initial random deployment, it is possible that sensors could not form a barrier due to gaps in their coverage, which would allow intruders to cross the ROI without being detected. In fact, it is difficult if possible at all to improve barrier coverage for sensor networks consisting of only stationary sensors. Fortunately, with recent technical advances, practical mobile sensors (e.g., Robomote

[2], Packbot [3]) have been developed, which provides us a way to improve barrier coverage performance after sensor networks have been deployed.

An intruder detection system could consist of only one type of sensors where all sensors have the same sensing range and angle. This kind of sensor network is often refereed as a *homogeneous WSN*. Cameras probably are the most widely used sensors for security applications. For example, the FREEDOM system [4], deployed on the border between Mexico and United States, uses cameras to detect illegal intruders. However, in reality, a system may consist of different types of sensors where they have different sensing ranges, sensing angles and costs. This kind of sensor network is often refereed as a *heterogeneous WSN*. For example, The SBInet project [5] supported by US government uses cameras, radars and ground sensors to construct a virtual fence to detect illegal intruders (e.g., drug dealers and illegal immigrants). In this paper, we mainly focus on barrier coverage in heterogeneous WSNs and consider the homogeneous WSN as a special case of the heterogeneous WSN.

* Corresponding author.

E-mail addresses: zbwang@whu.edu.cn (Z. Wang), qianwang@whu.edu.cn (Q. Wang).

报告编号: 202000187

论文检索报告

被检索人单位: 控制科学与工程学院

被检索人: 陈鸿龙

检索数据库: SCIE (SCI)

检索结果: 收录 19 篇。

特此证明, 详见附件。

注:

1. 该报告检索论文均由被检索人提交并得到被检索人确认。
2. 不排除姓名相同、姓名拼写相同的情况。

中国石油大学(华东)图书馆

2020 年 1 月 8 日



报告编号: 202000187

附件1

1

Efficiently and Completely Identifying Missing Key Tags for Anonymous RFID Systems

作者: Chen, HL(Chen, Honglong);Wang, ZB(Wang, Zhibo);Xia, F(Xia, Feng);Li, YJ(Li, Yanjun);Shi, LY(Shi, Leyi);

来源出版物: IEEE INTERNET OF THINGS JOURNAL 卷: 5 期: 4,SI 页码范围: 2915-2926 出版年: 2018

通讯作者地址: Wang, ZB (reprint author), Wuhan Univ, Sch Comp, Wuhan 430072, Hubei, Peoples R China.

地址: 1. [Chen, Honglong]China Univ Petr, Coll Informat & Control Engr, Qingdao 266555, Peoples R China.

2. [Wang, Zhibo]Wuhan Univ, Sch Comp, Wuhan 430072, Hubei, Peoples R China.

3. [Xia, Feng]Dalian Univ Technol, Sch Software, Dalian 116620, Peoples R China.

4. [Li, Yanjun]Zhejiang Univ Technol, Coll Comp Sci & Technol, Hangzhou 310023, Zhejiang, Peoples R China.

5. [Shi, Leyi]China Univ Petr, Coll Comp & Commun Engr, Qingdao 266555, Peoples R China.

IDS 号: GQ1VD

在“Web of Science”核心合集中的被引频次: 12

在中的被引频次: 0 (他引0次, 自引0次)

ISSN: 2327-4662

入藏号: WOS:000441428700062

影响因子: 9.515000

JCR学科: ENGINEERING, ELECTRICAL & ELECTRONIC 期刊分区: Q1

JCR学科: COMPUTER SCIENCE, INFORMATION SYSTEMS 期刊分区: Q1

JCR学科: TELECOMMUNICATIONS 期刊分区: Q1

中科院一级学科: 工程技术 一级学科分区: 1区; 二级学科: COMPUTER SCIENCE, INFORMATION SYSTEMS计算机: 信息系统 二级学科分区: 1区

中科院一级学科: 工程技术 一级学科分区: 1区; 二级学科: ENGINEERING, ELECTRICAL & ELECTRONIC工程: 电子与电气 二级学科分区: 1区

中科院一级学科: 工程技术 一级学科分区: 1区; 二级学科: TELECOMMUNICATIONS电信学 二级学科分区: 1区

2

Efficient and Reliable Missing Tag Identification for Large-Scale RFID Systems With Unknown Tags

作者: Chen, HL(Chen, Honglong);Xue, GL(Xue, Guoliang);Wang, ZB(Wang, Zhibo);

来源出版物: IEEE INTERNET OF THINGS JOURNAL 卷: 4 期: 3 页码范围: 736-748 出版年: 2017

通讯作者地址: Chen, HL (reprint author), China Univ Petr, Coll Informat &

Control Engn, Qingdao 266555, Peoples R China.

地址: 1. [Chen, Honglong]China Univ Petr, Coll Informat & Control Engn, Qingdao 266555, Peoples R China.

2. [Xue, Guoliang]Arizona State Univ, Sch Comp Informat & Decis Syst Engn, Tempe, AZ 85287 USA.

3. [Wang, Zhibo]Wuhan Univ, Sch Comp, Wuhan 430072, Peoples R China.

IDS 号: EY2RE

在“Web of Science”核心合集中的被引频次: 14

在中的被引频次: 0 (他引0次, 自引0次)

ISSN: 2327-4662

入藏号: WOS:000403816300011

影响因子: 5.863000

JCR学科: ENGINEERING, ELECTRICAL & ELECTRONIC 期刊分区: Q1

JCR学科: COMPUTER SCIENCE, INFORMATION SYSTEMS 期刊分区: Q1

JCR学科: TELECOMMUNICATIONS 期刊分区: Q1

中科院一级学科: 工程技术 一级学科分区: 1区; 二级学科: COMPUTER SCIENCE, INFORMATION SYSTEMS 计算机: 信息系统 二级学科分区: 1区

中科院一级学科: 工程技术 一级学科分区: 1区; 二级学科: ENGINEERING, ELECTRICAL & ELECTRONIC 工程: 电子与电气 二级学科分区: 1区

中科院一级学科: 工程技术 一级学科分区: 1区; 二级学科: TELECOMMUNICATIONS 电信学 二级学科分区: 1区

3

MAC: Missing Tag Iceberg Queries for Multi-Category RFID Systems

作者: Chen, HL (Chen, Honglong); Ma, GL (Ma, Guolei); Wang, ZB (Wang, Zhibo); Wang, Q (Wang, Qian); Yu, J (Yu, Jiguo);

来源出版物: IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY 卷: 67 期: 10 页码范围: 9947-9958 出版年: 2018

通讯作者地址: Yu, J (reprint author), Qilu Univ Technol, Shandong Comp Sci Ctr, Shandong Acad Sci, Natl Supercomp Ctr Jinan, Jinan, Shandong, Peoples R China.; Yu, J (reprint author), Qufu Normal Univ, Sch Informat Sci & Engn, Rizhao 276826, Peoples R China.

地址: 1. [Chen, Honglong]China Univ Petr East China, Coll Informat & Control Engn, Qingdao 266580, Peoples R China.

2. [Ma, Guolei]China Univ Petr East China, Coll Informat & Control Engn, Qingdao 266580, Peoples R China.

3. [Wang, Zhibo]Wuhan Univ, Sch Cyber Sci & Engn, Wuhan 430072, Hubei, Peoples R China.

4. [Wang, Qian]Wuhan Univ, Sch Cyber Sci & Engn, Wuhan 430072, Hubei, Peoples R China.

5. [Yu, Jiguo]Qilu Univ Technol, Shandong Comp Sci Ctr, Shandong Acad Sci, Natl Supercomp Ctr Jinan, Jinan, Shandong, Peoples R China., Qufu Normal Univ, Sch Informat Sci & Engn, Rizhao 276826, Peoples R China.

IDS 号: GX6FC

在“Web of Science”核心合集中的被引频次：7

在中的被引频次：0（他引0次，自引0次）

ISSN: 0018-9545

入藏号: WOS:000447853300071

影响因子: 5.339000

JCR学科: ENGINEERING, ELECTRICAL & ELECTRONIC 期刊分区: Q1

JCR学科: TELECOMMUNICATIONS 期刊分区: Q1

JCR学科: TRANSPORTATION SCIENCE & TECHNOLOGY 期刊分区: Q1

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: ENGINEERING, ELECTRICAL & ELECTRONIC工程: 电子与电气 二级学科分区: 2区

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: TELECOMMUNICATIONS电信学 二级学科分区: 2区

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: TRANSPORTATION SCIENCE & TECHNOLOGY运输科技 二级学科分区: 2区

4

On Achieving Asynchronous Energy-Efficient Neighbor Discovery for Mobile Sensor Networks

作者: Chen, HL (Chen, Honglong); Lou, W (Lou, Wei); Wang, ZB (Wang, Zhibo); Xia, F (Xia, Feng);

来源出版物: IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING 卷: 6 期: 4 页码范围: 553-565 出版年: 2018

通讯作者地址: Chen, HL (reprint author), China Univ Petr, Coll Informat & Control Engn, Qingdao, Peoples R China.; Chen, HL (reprint author), Hong Kong Polytech Univ, Dept Comp, Kowloon, Hong Kong, Peoples R China.

地址: 1. [Chen, Honglong]China Univ Petr, Coll Informat & Control Engn, Qingdao, Peoples R China.

2. Hong Kong Polytech Univ, Dept Comp, Kowloon, Hong Kong, Peoples R China.

3. [Lou, Wei]Hong Kong Polytech Univ, Dept Comp, Kowloon, Hong Kong, Peoples R China.

4. [Wang, Zhibo]Wuhan Univ, Sch Comp, Wuhan 430072, Hubei, Peoples R China.

5. [Xia, Feng]Dalian Univ Technol, Sch Software, Dalian 116620, Liaoning, Peoples R China.

IDS 号: HD4RI

在“Web of Science”核心合集中的被引频次：7

在中的被引频次：0（他引0次，自引0次）

ISSN: 2168-6750

入藏号: WOS:000452515100011

影响因子: 4.989000

JCR学科: COMPUTER SCIENCE, INFORMATION SYSTEMS 期刊分区: Q1

JCR学科: TELECOMMUNICATIONS 期刊分区: Q1

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: COMPUTER SCIENCE, INFORMATION SYSTEMS计算机: 信息系统 二级学科分区: 2区

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: TELECOMMUNICATIONS电信学

二级学科分区: 2区

5

Probabilistic Detection of Missing Tags for Anonymous Multicategory RFID Systems

作者: Chen, HL(Chen, Honglong);Ma, GL(Ma, Guolei);Wang, ZB(Wang, Zhibo);Xia, F(Xia, Feng);Yu, JG(Yu, Jiguo);

来源出版物: IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY 卷: 66 期: 12 页码范围: 11295-11305 出版年: 2017

通讯作者地址: Yu, JG (reprint author), Qufu Normal Univ, Sch Informat Sci & Engn, Rizhao 276826, Peoples R China.

地址: 1. [Chen, Honglong]China Univ Petr East China, Coll Informat & Control Engn, Qingdao 266580, Peoples R China.

2. [Ma, Guolei]China Univ Petr East China, Coll Informat & Control Engn, Qingdao 266580, Peoples R China.

3. [Wang, Zhibo]Wuhan Univ, Sch Comp, Wuhan 430072, Hubei, Peoples R China.

4. [Xia, Feng]Dalian Univ Technol, Sch Software, Dalian 116023, Peoples R China.

5. [Yu, Jiguo]Qufu Normal Univ, Sch Informat Sci & Engn, Rizhao 276826, Peoples R China.

IDS 号: FQ5KP

在“Web of Science”核心合集中的被引频次: 10

在中的被引频次: 0 (他引0次, 自引0次)

ISSN: 0018-9545

入藏号: WOS:000418399000053

影响因子: 4.432000

JCR学科: ENGINEERING, ELECTRICAL & ELECTRONIC 期刊分区: Q1

JCR学科: TELECOMMUNICATIONS 期刊分区: Q1

JCR学科: TRANSPORTATION SCIENCE & TECHNOLOGY 期刊分区: Q1

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: ENGINEERING, ELECTRICAL & ELECTRONIC工程: 电子与电气 二级学科分区: 2区

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: TELECOMMUNICATIONS电信学 二级学科分区: 2区

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: TRANSPORTATION SCIENCE & TECHNOLOGY运输科技 二级学科分区: 2区

6

A Secure Credit-Based Incentive Mechanism for Message Forwarding in Noncooperative DTNs

作者: Chen, HL(Chen, Honglong);Lou, W(Lou, Wei);Wang, ZB(Wang, Zhibo);Wang, Q(Wang, Qian);

来源出版物: IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY 卷: 65 期: 8 页码范围: 6377-6388 出版年: 2016

通讯作者地址: Chen, HL (reprint author), China Univ Petr, Coll Informat & Control Engn, Qingdao 266580, Peoples R China.

地址: 1. [Chen, Honglong]China Univ Petr, Coll Informat & Control Engn, Qingdao 266580, Peoples R China.

2. Hong Kong Polytech Univ, Dept Comp, Kowloon, Hong Kong, Peoples R China.

3. [Lou, Wei]Hong Kong Polytech Univ, Dept Comp, Kowloon, Hong Kong, Peoples R China.

4. Hong Kong Polytech Univ, Shenzhen Res Inst, Shenzhen 518057, Peoples R China.

5. [Wang, Zhibo]Wuhan Univ, Sch Comp, Wuhan 430072, Peoples R China.

6. [Wang, Qian]Wuhan Univ, Sch Comp, Wuhan 430072, Peoples R China.

IDS 号: DT4J0

在“Web of Science”核心合集中的被引频次: 12

在中的被引频次: 0 (他引0次, 自引0次)

ISSN: 0018-9545

入藏号: WOS:000381446200041

影响因子: 4.066000

JCR学科: ENGINEERING, ELECTRICAL & ELECTRONIC 期刊分区: Q1

JCR学科: TELECOMMUNICATIONS 期刊分区: Q1

JCR学科: TRANSPORTATION SCIENCE & TECHNOLOGY 期刊分区: Q1

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: ENGINEERING, ELECTRICAL & ELECTRONIC工程: 电子与电气 二级学科分区: 2区

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: TELECOMMUNICATIONS电信学 二级学科分区: 2区

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: TRANSPORTATION SCIENCE & TECHNOLOGY运输科技 二级学科分区: 3区

7

RMTS: A robust clock synchronization scheme for wireless sensor networks

作者: Zhang, XX(Zhang, Xuxin);Chen, HL(Chen, Honglong);Lin, K(Lin, Kai);Wang, ZB(Wang, Zhibo);Yu, JG(Yu, Jiguo);Shi, LY(Shi, Leyi);

来源出版物: JOURNAL OF NETWORK AND COMPUTER APPLICATIONS 卷: 135 页码范围: 1-10 出版年: 2019

通讯作者地址: Chen, HL (reprint author), China Univ Petr, Coll Informat & Control Engn, Qingdao, Shandong, Peoples R China.

地址: 1. [Zhang, Xuxin]China Univ Petr, Coll Informat & Control Engn, Qingdao, Shandong, Peoples R China.

2. [Chen, Honglong]China Univ Petr, Coll Informat & Control Engn, Qingdao, Shandong, Peoples R China.

3. [Lin, Kai]China Univ Petr, Coll Informat & Control Engn, Qingdao, Shandong, Peoples R China.

4. [Wang, Zhibo]Wuhan Univ, Sch Cyber Sci & Engn, Wuhan, Hubei, Peoples R China.,Nanjing Univ, State Key Lab Novel Software Technol, Nanjing, Jiangsu, Peoples R China.

5. [Yu, Jiguo]Qilu Univ Technol, Shandong Acad Sci, Shandong Comp Sci Ctr, Natl Supercomp Ctr Jinan,Shandong Prov Key Lab Co, Jinan, Shandong, Peoples R China.

6. [Shi, Leyi]China Univ Petr, Coll Comp & Commun Engn, Qingdao, Shandong,

Peoples R China.

IDS 号: HV8TX

在“Web of Science”核心合集中的被引频次: 4

在中的被引频次: 0 (他引0次, 自引0次)

ISSN: 1084-8045

入藏号: WOS:000466258100001

影响因子: 5.273000

JCR学科: COMPUTER SCIENCE, SOFTWARE ENGINEERING 期刊分区: Q1

JCR学科: COMPUTER SCIENCE, HARDWARE & ARCHITECTURE 期刊分区: Q1

JCR学科: COMPUTER SCIENCE, INTERDISCIPLINARY APPLICATIONS 期刊分区: Q1

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: COMPUTER SCIENCE, HARDWARE & ARCHITECTURE 计算机: 硬件 二级学科分区: 2区

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: COMPUTER SCIENCE, INTERDISCIPLINARY APPLICATIONS 计算机: 跨学科应用 二级学科分区: 2区

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: COMPUTER SCIENCE, SOFTWARE ENGINEERING 计算机: 软件工程 二级学科分区: 1区

8

Deformable Convolutional Matrix Factorization for Document Context-Aware Recommendation in Social Networks

作者: Chen, HL (Chen, Honglong); Fu, JN (Fu, Jinnan); Zhang, L (Zhang, Lei); Wang, S (Wang, Shuai); Lin, K (Lin, Kai); Shi, LY (Shi, Leyi); Wang, LH (Wang, Lianhai);

来源出版物: IEEE ACCESS 卷: 7 页码范围: 66347-66357 出版年: 2019

通讯作者地址: Shi, LY (reprint author), China Univ Petr, Coll Comp & Commun Engrn, Qingdao 102200, Shandong, Peoples R China.

地址: 1. [Chen, Honglong]China Univ Petr, Coll Informat & Control Engrn, Qingdao 102200, Shandong, Peoples R China.

2. [Fu, Jinnan]China Univ Petr, Coll Informat & Control Engrn, Qingdao 102200, Shandong, Peoples R China.

3. [Zhang, Lei]Nanjing Univ Posts & Telecommun, Dept Internet Things, Nanjing 210000, Jiangsu, Peoples R China.

4. [Wang, Shuai]Nanjing Univ Posts & Telecommun, Dept Internet Things, Nanjing 210000, Jiangsu, Peoples R China.

5. [Lin, Kai]China Univ Petr, Coll Informat & Control Engrn, Qingdao 102200, Shandong, Peoples R China.

6. [Shi, Leyi]China Univ Petr, Coll Comp & Commun Engrn, Qingdao 102200, Shandong, Peoples R China.

7. [Wang, Lianhai]Qilu Univ Technol, Shandong Acad Sci, Jinan 250300, Shandong, Peoples R China., Natl Supercomp Ctr Jinan, Shandong Comp Sci Ctr, Shandong Prov Key Lab Comp Networks, Jinan 250101, Shandong, Peoples R China.

IDS 号: IC6AL

在“Web of Science”核心合集中的被引频次: 0

在中的被引频次: 0 (他引0次, 自引0次)

ISSN: 2169-3536

入藏号: WOS:000471050600001

影响因子: 4.098000

JCR学科: ENGINEERING, ELECTRICAL & ELECTRONIC 期刊分区: Q1

JCR学科: COMPUTER SCIENCE, INFORMATION SYSTEMS 期刊分区: Q1

JCR学科: TELECOMMUNICATIONS 期刊分区: Q1

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: COMPUTER SCIENCE, INFORMATION SYSTEMS 计算机: 信息系统 二级学科分区: 2区

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: ENGINEERING, ELECTRICAL & ELECTRONIC 工程: 电子与电气 二级学科分区: 3区

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: TELECOMMUNICATIONS 电信学 二级学科分区: 3区

9

On Using Sampling Bloom Filter for Unknown Tag Identification in Large-Scale RFID Systems

作者: Chen, HL (Chen, Honglong); Liu, L (Liu, Lu); Che, RJ (Che, Rongjie); Lin, K (Lin, Kai); Ai, X (Ai, Xin); Li, YJ (Li, Yanjun);

来源出版物: IEEE ACCESS 卷: 6 页码范围: 57095-57104 出版年: 2018

通讯作者地址: Chen, HL (reprint author), China Univ Petr, Coll Informat & Control Engn, Qingdao 257000, Peoples R China.

地址: 1. [Chen, Honglong] China Univ Petr, Coll Informat & Control Engn, Qingdao 257000, Peoples R China.

2. [Liu, Lu] China Univ Petr, Coll Informat & Control Engn, Qingdao 257000, Peoples R China.

3. [Che, Rongjie] Sinopec Petr Engr Corp, Dongying 257026, Peoples R China.

4. [Lin, Kai] China Univ Petr, Coll Informat & Control Engn, Qingdao 257000, Peoples R China.

5. [Ai, Xin] China Univ Petr, Coll Informat & Control Engn, Qingdao 257000, Peoples R China.

6. [Li, Yanjun] Zhejiang Univ Technol, Sch Comp Sci & Technol, Hangzhou 310023, Zhejiang, Peoples R China.

IDS 号: GY8XA

在“Web of Science”核心合集中的被引频次: 0

在中的被引频次: 0 (他引0次, 自引0次)

ISSN: 2169-3536

入藏号: WOS:000448921400001

影响因子: 4.098000

JCR学科: ENGINEERING, ELECTRICAL & ELECTRONIC 期刊分区: Q1

JCR学科: COMPUTER SCIENCE, INFORMATION SYSTEMS 期刊分区: Q1

JCR学科: TELECOMMUNICATIONS 期刊分区: Q1

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: COMPUTER SCIENCE, INFORMATION SYSTEMS 计算机: 信息系统 二级学科分区: 2区

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: ENGINEERING, ELECTRICAL & ELECTRONIC 工程: 电子与电气 二级学科分区: 3区

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: TELECOMMUNICATIONS电信学
二级学科分区: 3区

10

Segmented Bloom Filter Based Missing Tag Detection for Large-Scale RFID Systems With Unknown Tags

作者: Lin, K(Lin, Kai);Chen, HL(Chen, Honglong);Dai, TJ(Dai, Tianjiao);Liu, DH(Liu, Denghui);Liu, L(Liu, Lu);Shi, LY(Shi, Leyi);

来源出版物: IEEE ACCESS 卷: 6 页码范围: 54435-54446 出版年: 2018

通讯作者地址: Chen, HL (reprint author), China Univ Petr, Coll Informat & Control Engn, Qingdao 266580, Peoples R China.

地址: 1. [Lin, Kai]China Univ Petr, Coll Informat & Control Engn, Qingdao 266580, Peoples R China.

2. [Chen, Honglong]China Univ Petr, Coll Informat & Control Engn, Qingdao 266580, Peoples R China.

3. [Dai, Tianjiao]China Univ Petr, Coll Informat & Control Engn, Qingdao 266580, Peoples R China.

4. [Liu, Denghui]Everdisplay Optron Shanghai Ltd, Shanghai 201506, Peoples R China.

5. [Liu, Lu]China Univ Petr, Coll Informat & Control Engn, Qingdao 266580, Peoples R China.

6. [Shi, Leyi]China Univ Petr, Coll Com & Control Engn, Qingdao 266580, Peoples R China.

IDS 号: GX8VE

在“Web of Science”核心合集中的被引频次: 0

在中的被引频次: 0 (他引0次, 自引0次)

ISSN: 2169-3536

入藏号: WOS:000448071500001

影响因子: 4.098000

JCR学科: ENGINEERING, ELECTRICAL & ELECTRONIC 期刊分区: Q1

JCR学科: COMPUTER SCIENCE, INFORMATION SYSTEMS 期刊分区: Q1

JCR学科: TELECOMMUNICATIONS 期刊分区: Q1

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: COMPUTER SCIENCE, INFORMATION SYSTEMS计算机: 信息系统 二级学科分区: 2区

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: ENGINEERING, ELECTRICAL & ELECTRONIC工程: 电子与电气 二级学科分区: 3区

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: TELECOMMUNICATIONS电信学
二级学科分区: 3区

11

Efficient 3-dimensional localization for RFID systems using jumping probe

作者: Chen, HL(Chen, Honglong);Ma, GL(Ma, Guolei);Wang, ZB(Wang, Zhibo);Yu, JG(Yu, Jiguo);Shi, LY(Shi, Leyi);Jiang, XY(Jiang, Xiangyuan);

来源出版物: PERVASIVE AND MOBILE COMPUTING 卷: 41 页码范围: 300-318 出版年:

2017

通讯作者地址: Chen, HL (reprint author), China Univ Petr, Coll Informat & Control Engn, Qingdao, Peoples R China.

地址: 1. [Chen, Honglong]China Univ Petr, Coll Informat & Control Engn, Qingdao, Peoples R China.

2. [Ma, Guolei]China Univ Petr, Coll Informat & Control Engn, Qingdao, Peoples R China.

3. [Wang, Zhibo]Wuhan Univ, Sch Comp, Wuhan, Hubei, Peoples R China.

4. [Yu, Jiguo]Qufu Normal Univ, Sch Informat Sci & Engn, Rizhao, Peoples R China.

5. [Shi, Leyi]China Univ Petr, Coll Comp & Commun Engn, Qingdao, Peoples R China.

6. [Jiang, Xiangyuan]China Univ Petr, Coll Informat & Control Engn, Qingdao, Peoples R China.

IDS 号: FK8UM

在“Web of Science”核心合集集中的被引频次: 5

在中的被引频次: 0 (他引0次, 自引0次)

ISSN: 1574-1192

入藏号: WOS:000413784800019

12

Contact expectation based routing for delay tolerant networks

作者: Chen, HL(Chen, Honglong); Lou, W(Lou, Wei);

来源出版物: AD HOC NETWORKS 卷: 36 页码范围: 244-257 出版年: 2016

通讯作者地址: Chen, HL (reprint author), China Univ Petr, Coll Informat & Control Engn, Beijing, Peoples R China.

地址: 1. [Chen, Honglong]China Univ Petr, Coll Informat & Control Engn, Beijing, Peoples R China.

2. Hong Kong Polytech Univ, Dept Comp, Kowloon, Hong Kong, Peoples R China., Hong Kong Polytech Univ, Shenzhen Res Inst, Shenzhen, Peoples R China.

3. [Lou, Wei]Hong Kong Polytech Univ, Dept Comp, Kowloon, Hong Kong, Peoples R China., Hong Kong Polytech Univ, Shenzhen Res Inst, Shenzhen, Peoples R China.

IDS 号: CZ0DG

在“Web of Science”核心合集集中的被引频次: 18

在中的被引频次: 0 (他引0次, 自引0次)

ISSN: 1570-8705

入藏号: WOS:000366774700016

13

On protecting end-to-end location privacy against local eavesdropper in Wireless Sensor Networks

作者: Chen, HL(Chen, Honglong); Lou, W(Lou, Wei);

来源出版物: PERSASIVE AND MOBILE COMPUTING 卷: 16 页码范围: 36-50 出版年: 2015

通讯作者地址: Chen, HL (reprint author), China Univ Petr, Coll Informat & Control Engn, Qingdao, Peoples R China.

地址: 1. [Chen, Honglong]China Univ Petr, Coll Informat & Control Engn, Qingdao, Peoples R China.

2. Hong Kong Polytech Univ, Dept Comp, Kowloon, Hong Kong, Peoples R China.

3. [Lou, Wei]Hong Kong Polytech Univ, Dept Comp, Kowloon, Hong Kong, Peoples R China.

4. Hong Kong Polytech Univ, Shenzhen Res Inst, Shenzhen, Peoples R China.

IDS 号: AZ1XG

在“Web of Science”核心合集集中的被引频次: 34

在中的被引频次: 0 (他引0次, 自引0次)

ISSN: 1574-1192

入藏号: WOS:000348027800004

14

On providing wormhole-attack-resistant localization using conflicting sets

作者: Chen, HL(Chen, Honglong);Lou, W(Lou, Wei);Wang, Z(Wang, Zhi);

来源出版物: WIRELESS COMMUNICATIONS & MOBILE COMPUTING 卷: 15 期: 15 页码范围: 1865-1881 出版年: 2015

通讯作者地址: Chen, HL (reprint author), China Univ Petr, Coll Informat & Control Engn, Qingdao, Peoples R China.

地址: 1. [Chen, Honglong]China Univ Petr, Coll Informat & Control Engn, Qingdao, Peoples R China.

2. [Lou, Wei]Hong Kong Polytech Univ, Dept Comp, Kowloon, Hong Kong, Peoples R China., Hong Kong Polytech Univ, Shenzhen Res Inst, Shenzhen, Peoples R China.

3. [Wang, Zhi]Zhejiang Univ, State Key Lab Ind Control Technol, Hangzhou 310003, Zhejiang, Peoples R China.

IDS 号: CT30V

在“Web of Science”核心合集集中的被引频次: 3

在中的被引频次: 0 (他引0次, 自引0次)

ISSN: 1530-8669

入藏号: WOS:000362717200001

15

Securing DV-Hop localization against wormhole attacks in wireless sensor networks

作者: Chen, HL(Chen, Honglong);Lou, W(Lou, Wei);Wang, Z(Wang, Zhi);Wu, JF(Wu, Junfeng);Wang, ZB(Wang, Zhibo);Xia, AH(Xia, Aihua);

来源出版物: PERVASIVE AND MOBILE COMPUTING 卷: 16 页码范围: 22-35 出版年: 2015

通讯作者地址: Wang, Z (reprint author), Zhejiang Univ, State Key Lab Ind Control Technol, Hangzhou 310003, Zhejiang, Peoples R China.

地址: 1. [Chen, Honglong]Zhejiang Univ, State Key Lab Ind Control Technol, Hangzhou 310003, Zhejiang, Peoples R China.

2. China Univ Petr, Coll Informat & Control Engn, Qingdao, Peoples R China.
3. [Lou, Wei]Hong Kong Polytech Univ, Dept Comp, Hong Kong, Hong Kong, Peoples R China., Hong Kong Polytech Univ, Shenzhen Res Inst, Shenzhen, Peoples R China.
4. [Wang, Zhi]Zhejiang Univ, State Key Lab Ind Control Technol, Hangzhou 310003, Zhejiang, Peoples R China.
5. [Wu, Junfeng]Hong Kong Univ Sci & Technol, Dept Elect & Comp Engn, Hong Kong, Hong Kong, Peoples R China.
6. [Wang, Zhibo]Zhejiang Univ, State Key Lab Ind Control Technol, Hangzhou 310003, Zhejiang, Peoples R China.
7. [Xia, Aihua]Zhejiang Univ, State Key Lab Ind Control Technol, Hangzhou 310003, Zhejiang, Peoples R China.

IDS 号: AZ1XG

在“Web of Science”核心合集集中的被引频次: 22

在中的被引频次: 0 (他引0次, 自引0次)

ISSN: 1574-1192

入藏号: WOS:000348027800003

16

Privacy-Preserving Crowd-Sourced Statistical Data Publishing with An Untrusted Server

作者: Wang, ZB(Wang, Zhibo);Pang, XY(Pang, Xiaoyi);Chen, YH(Chen, Yahong);Shao, HJ(Shao, Huajie);Wang, Q(Wang, Qian);Wu, LB(Wu, Libing);Chen, HL(Chen, Honglong);Qi, HR(Qi, Hairong)

来源出版物: IEEE TRANSACTIONS ON MOBILE COMPUTING 卷: 18 期: 6 页码范围: 1356-1367 出版年: 2019

通讯作者地址: Wu, LB (reprint author), Wuhan Univ, Sch Comp Sci, Wuhan 430072, Hubei, Peoples R China.

地址: 1. [Wang, Zhibo]Wuhan Univ, Sch Cyber Sci & Engn, Key Lab Aerosp Informat Secur & Trusted Comp, Minist Educ, Wuhan 430072, Hubei, Peoples R China.

2. [Pang, Xiaoyi]Wuhan Univ, Sch Cyber Sci & Engn, Key Lab Aerosp Informat Secur & Trusted Comp, Minist Educ, Wuhan 430072, Hubei, Peoples R China.

3. [Chen, Yahong]Wuhan Univ, Sch Cyber Sci & Engn, Key Lab Aerosp Informat Secur & Trusted Comp, Minist Educ, Wuhan 430072, Hubei, Peoples R China.

4. [Shao, Huajie]Univ Illinois, Dept Comp Sci, Urbana, IL 61801 USA.

5. [Wang, Qian]Wuhan Univ, Sch Cyber Sci & Engn, Key Lab Aerosp Informat Secur & Trusted Comp, Minist Educ, Wuhan 430072, Hubei, Peoples R China.

6. [Wu, Libing]Wuhan Univ, Sch Comp Sci, Wuhan 430072, Hubei, Peoples R China.

7. [Chen, Honglong]China Univ Petr, Coll Informat & Control Sci, Beijing 266580, Peoples R China.

8. [Qi, Hairong]Univ Tennessee, Dept Elect Engn & Comp Sci, Knoxville, TN 37996 USA.

IDS 号: HX0ID

在“Web of Science”核心合集集中的被引频次: 18

在中的被引频次: 0 (他引0次, 自引0次)

ISSN: 1536-1233

入藏号: WOS:000467071900010

影响因子: 4.474000

JCR学科: COMPUTER SCIENCE, INFORMATION SYSTEMS 期刊分区: Q1

JCR学科: TELECOMMUNICATIONS 期刊分区: Q1

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: COMPUTER SCIENCE, INFORMATION SYSTEMS 计算机: 信息系统 二级学科分区: 2区

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: TELECOMMUNICATIONS 电信学 二级学科分区: 2区

17

Cost-effective barrier coverage formation in heterogeneous wireless sensor networks

作者: Wang, ZB(Wang, Zhibo);Cao, Q(Cao, Qing);Qi, HR(Qi, Hairong);Chen, HL(Chen, Honglong);Wang, Q(Wang, Qian);

来源出版物: AD HOC NETWORKS 卷: 64 页码范围: 65-79 出版年: 2017

通讯作者地址: Wang, Q (reprint author), Wuhan Univ, Sch Comp, State Key Lab Software Engn, Wuhan, Hubei, Peoples R China.; Wang, Q (reprint author), Wuhan Univ, Key Lab Aerosp Informat Secur & Trusted Comp, Wuhan, Hubei, Peoples R China.

地址: 1. [Wang, Zhibo]Wuhan Univ, Sch Comp, State Key Lab Software Engn, Wuhan, Hubei, Peoples R China.

2. Univ Tennessee, Elect Engr & Comp Sci, Knoxville, TN USA.

3. [Cao, Qing]Univ Tennessee, Elect Engr & Comp Sci, Knoxville, TN USA.

4. [Qi, Hairong]Univ Tennessee, Elect Engr & Comp Sci, Knoxville, TN USA.

5. [Chen, Honglong]China Univ Petr, Informat & Control Engr, Qingdao, Peoples R China.

6. [Wang, Qian]Wuhan Univ, Sch Comp, State Key Lab Software Engn, Wuhan, Hubei, Peoples R China.

7. Wuhan Univ, Key Lab Aerosp Informat Secur & Trusted Comp, Wuhan, Hubei, Peoples R China.

IDS 号: FD3BM

在“Web of Science”核心合集集中的被引频次: 30

在中的被引频次: 0 (他引0次, 自引0次)

ISSN: 1570-8705

入藏号: WOS:000407408500006

18

Achieving location error tolerant barrier coverage for wireless sensor networks

作者: Wang, ZB(Wang, Zhibo);Chen, HL(Chen, Honglong);Cao, Q(Cao, Qing);Qi, HR(Qi, Hairong);Wang, Z(Wang, Zhi);Wang, Q(Wang, Qian);

来源出版物: COMPUTER NETWORKS 卷: 112 页码范围: 314-328 出版年: 2017

通讯作者地址: Wang, Q (reprint author), Wuhan Univ, Sch Comp, State Key Lab

Software Engn, Wuhan, Hubei, Peoples R China.

地址: 1. [Wang, Zhibo]Wuhan Univ, Sch Comp, State Key Lab Software Engn, Wuhan, Hubei, Peoples R China.

2. [Chen, Honglong]China Univ Petr, Informat & Control Engn, Qingdao, Peoples R China.

3. [Cao, Qing]Univ Tennessee, Elect Engn & Comp Sci, Knoxville, TN USA.

4. [Qi, Hairong]Univ Tennessee, Elect Engn & Comp Sci, Knoxville, TN USA.

5. [Wang, Zhi]Wuhan Univ, Sch Comp, State Key Lab Software Engn, Wuhan, Hubei, Peoples R China.

6. State Key Lab Ind Control Technol, Hangzhou, Zhejiang, Peoples R China.

7. [Wang, Qian]Wuhan Univ, Sch Comp, State Key Lab Software Engn, Wuhan, Hubei, Peoples R China.

IDS 号: EI8TU

在“Web of Science”核心合集中的被引频次: 34

在中的被引频次: 0 (他引0次, 自引0次)

ISSN: 1389-1286

入藏号: WOS:000392781800021

影响因子: 2.522000

JCR学科: COMPUTER SCIENCE, HARDWARE & ARCHITECTURE 期刊分区: Q1

JCR学科: COMPUTER SCIENCE, INFORMATION SYSTEMS 期刊分区: Q2

JCR学科: ENGINEERING, ELECTRICAL & ELECTRONIC 期刊分区: Q2

JCR学科: TELECOMMUNICATIONS 期刊分区: Q2

中科院一级学科: 工程技术 一级学科分区: 3区; 二级学科: COMPUTER SCIENCE, HARDWARE & ARCHITECTURE 计算机: 硬件 二级学科分区: 3区

中科院一级学科: 工程技术 一级学科分区: 3区; 二级学科: COMPUTER SCIENCE, INFORMATION SYSTEMS 计算机: 信息系统 二级学科分区: 3区

中科院一级学科: 工程技术 一级学科分区: 3区; 二级学科: ENGINEERING, ELECTRICAL & ELECTRONIC 工程: 电子与电气 二级学科分区: 3区

中科院一级学科: 工程技术 一级学科分区: 3区; 二级学科: TELECOMMUNICATIONS 电信学 二级学科分区: 3区

19

Dynamic Distributed Honeypot Based on Blockchain

作者: Shi, LY(Shi, Leyi); Li, Y(Li, Yang); Liu, TX(Liu, Tianxu); Liu, J(Liu, Jia); Shan, BY(Shan, Baoying); Chen, HL(Chen, Honglong);

来源出版物: IEEE ACCESS 卷: 7 页码范围: 72234-72246 出版年: 2019

通讯作者地址: Chen, HL (reprint author), China Univ Petr, Coll Informat & Control Engn, Qingdao 257067, Shandong, Peoples R China.

地址: 1. [Shi, Leyi]China Univ Petr, Coll Comp & Commun Engn, Qingdao 257067, Shandong, Peoples R China.

2. [Li, Yang]China Univ Petr, Coll Comp & Commun Engn, Qingdao 257067, Shandong, Peoples R China.

3. [Liu, Tianxu]China Univ Petr, Coll Comp & Commun Engn, Qingdao 257067, Shandong, Peoples R China.

4. [Liu, Jia]China Univ Petr, Coll Comp & Commun Engn, Qingdao 257067, Shandong, Peoples R China.

5. [Shan, Baoying]China Univ Petr, Coll Comp & Commun Engn, Qingdao 257067, Shandong, Peoples R China.

6. [Chen, Honglong]China Univ Petr, Coll Informat & Control Engn, Qingdao 257067, Shandong, Peoples R China.

IDS 号: IE2AA

在“Web of Science”核心合集中的被引频次: 0

在中的被引频次: 0 (他引0次, 自引0次)

ISSN: 2169-3536

入藏号: WOS:000472185700001

影响因子: 4.098000

JCR学科: ENGINEERING, ELECTRICAL & ELECTRONIC 期刊分区: Q1

JCR学科: COMPUTER SCIENCE, INFORMATION SYSTEMS 期刊分区: Q1

JCR学科: TELECOMMUNICATIONS 期刊分区: Q1

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: COMPUTER SCIENCE, INFORMATION SYSTEMS 计算机: 信息系统 二级学科分区: 2区

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: ENGINEERING, ELECTRICAL & ELECTRONIC 工程: 电子与电气 二级学科分区: 3区

中科院一级学科: 工程技术 一级学科分区: 2区; 二级学科: TELECOMMUNICATIONS 电信学 二级学科分区: 3区

报告编号: 202000187



报告编号: 202000188

论文检索报告

被检索人单位: 控制科学与工程学院

被检索人: 陈鸿龙

检索数据库: EI (EI)

检索结果: 收录 1 篇。

特此证明, 详见附件。

注:

1. 该报告检索论文均由被检索人提交并得到被检索人确认。
2. 不排除姓名相同、姓名拼写相同的情况。

中国石油大学(华东)图书馆

2020 年 1 月 8 日



报告编号: 202000188

附件1

1

Accession number:20151800797086

Title:Secure localization scheme against wormhole attack for wireless sensor networks

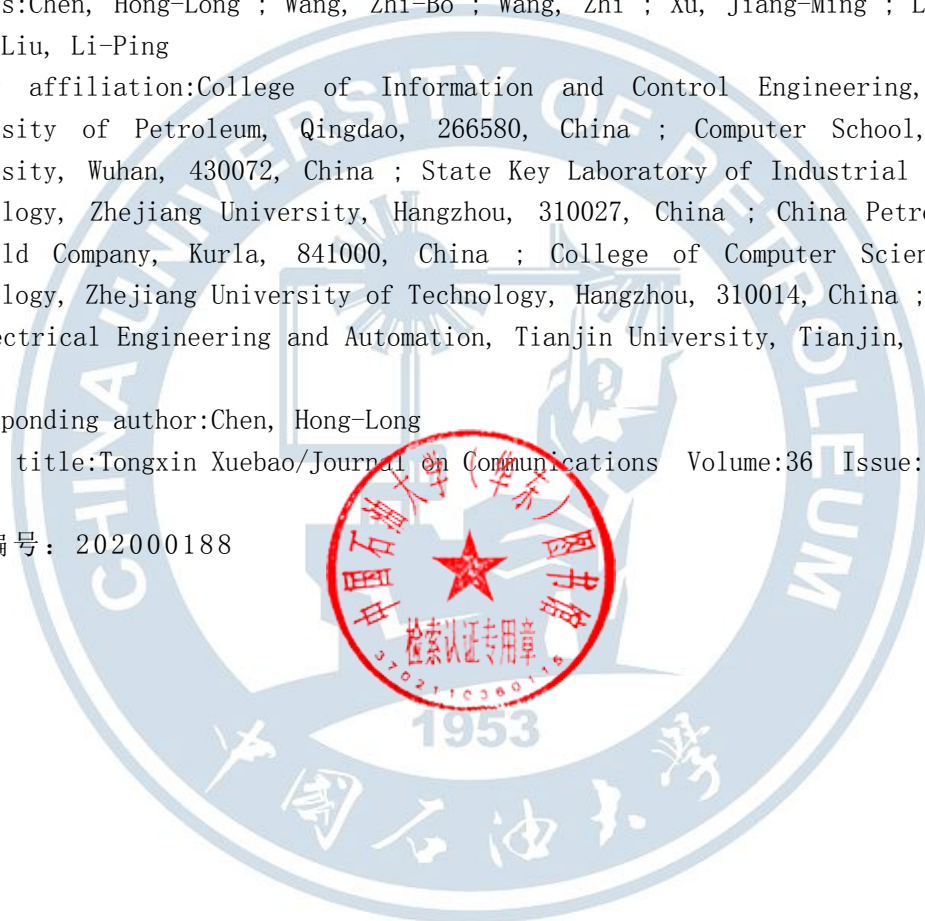
Authors:Chen, Hong-Long ; Wang, Zhi-Bo ; Wang, Zhi ; Xu, Jiang-Ming ; Li, Yan-Jun ; Liu, Li-Ping

Author affiliation:College of Information and Control Engineering, China University of Petroleum, Qingdao, 266580, China ; Computer School, Wuhan University, Wuhan, 430072, China ; State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou, 310027, China ; China Petro Tarim Qilfield Company, Kurla, 841000, China ; College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou, 310014, China ; School of Electrical Engineering and Automation, Tianjin University, Tianjin, 300072, China

Corresponding author:Chen, Hong-Long

Source title:Tongxin Xuebao/Journal on Communications Volume:36 Issue:3 2015

报告编号: 202000188



证书号第2061994号



发明专利证书

发明名称：容迟网络中基于期望会面节点数的路由方法

发明人：陈鸿龙；田力丹；王志波；马国蕾；连雪

专利号：ZL 2015 1 0560533.X

专利申请日：2015年09月06日

专利权人：中国石油大学（华东）；武汉大学苏州研究院

授权公告日：2016年05月11日

本发明经过本局依照中华人民共和国专利法进行审查，决定授予专利权，颁发本证书并在专利登记簿上予以登记。专利权自授权公告之日起生效。

本专利的专利权期限为二十年，自申请日起算。专利权人应当依照专利法及其实施细则规定缴纳年费。本专利的年费应当在每年09月06日前缴纳。未按照规定缴纳年费的，专利权自应当缴纳年费期满之日起终止。

专利证书记载专利权登记时的法律状况。专利权的转移、质押、无效、终止、恢复和专利权人的姓名或名称、国籍、地址变更等事项记载在专利登记簿上。



局长
申长雨

申长雨



证书号第2210039号



发明专利证书

发明名称：一种基于跳跃式查询的被动式三维射频识别定位方法

发明人：陈鸿龙；马国蕾；李晓辉；田力丹

专利号：ZL 2015 1 0319895.X

专利申请日：2015年06月11日

专利权人：中国石油大学（华东）

授权公告日：2016年08月24日

本发明经过本局依照中华人民共和国专利法进行审查，决定授予专利权，颁发本证书并在专利登记簿上予以登记。专利权自授权公告之日起生效。

本专利的专利权期限为二十年，自申请日起算。专利权人应当依照专利法及其实施细则规定缴纳年费。本专利的年费应当在每年06月11日前缴纳。未按照规定缴纳年费的，专利权自应当缴纳年费期满之日起终止。

专利证书记载专利权登记时的法律状况。专利权的转移、质押、无效、终止、恢复和专利权人的姓名或名称、国籍、地址变更等事项记载在专利登记簿上。



局长
申长雨

申长雨



证书号第2449186号



发明专利证书

发明名称：无线传感器网络移动信标节点的虫洞攻击检测及定位方法

发明人：陈鸿龙;王志波;王智

专利号：ZL 2014 1 0030021.8

专利申请日：2014年01月22日

专利权人：中国石油大学（华东）

授权公告日：2017年04月12日

本发明经过本局依照中华人民共和国专利法进行审查，决定授予专利权，颁发本证书并在专利登记簿上予以登记。专利权自授权公告之日起生效。

本专利的专利权期限为二十年，自申请日起算。专利权人应当依照专利法及其实施细则规定缴纳年费。本专利的年费应当在每年01月22日前缴纳。未按照规定缴纳年费的，专利权自应当缴纳年费期满之日起终止。

专利证书记载专利权登记时的法律状况。专利权的转移、质押、无效、终止、恢复和专利权人的姓名或名称、国籍、地址变更等事项记载在专利登记簿上。



局长
申长雨

申长雨



证书号第2946321号



发明专利证书

发明名称：匿名射频识别系统基于向量的丢失关键标签的识别方法

发明人：陈鸿龙；付金楠；丁鑫旺；刘璐；林凯；王志波；石乐义

专利号：ZL 2017 1 0991315.0

专利申请日：2017年10月23日

专利权人：中国石油大学（华东）

地址：266580 山东省青岛市开发区长江西路66号

授权公告日：2018年06月01日

授权公告号：CN 107644185 B

本发明经过本局依照中华人民共和国专利法进行审查，决定授予专利权，颁发本证书并在专利登记簿上予以登记。专利权自授权公告之日起生效。

本专利的专利权期限为二十年，自申请日起算。专利权人应当依照专利法及其实施细则规定缴纳年费。本专利的年费应当在每年10月23日前缴纳。未按照规定缴纳年费的，专利权自应当缴纳年费期满之日起终止。

专利证书记载专利权登记时的法律状况。专利权的转移、质押、无效、终止、恢复和专利权人的姓名或名称、国籍、地址变更等事项记载在专利登记簿上。



局长
申长雨

申长雨



证书号第2909867号



发明专利证书

发明名称：含有未知标签的射频识别系统的丢失标签识别方法

发明人：陈鸿龙;林凯;刘璐;付金楠;丁鑫旺;石乐义

专利号：ZL 2017 1 0311783.9

专利申请日：2017年05月05日

专利权人：中国石油大学(华东)

地址：266580 山东省青岛市黄岛区长江西路66号

授权公告日：2018年05月01日

授权公告号：CN 107145807 B

本发明经过本局依照中华人民共和国专利法进行审查，决定授予专利权，颁发本证书并在专利登记簿上予以登记。专利权自授权公告之日起生效。

本专利的专利权期限为二十年，自申请日起算。专利权人应当依照专利法及其实施细则规定缴纳年费。本专利的年费应当在每年05月05日前缴纳。未按照规定缴纳年费的，专利权自应当缴纳年费期满之日起终止。

专利证书记载专利权登记时的法律状况。专利权的转移、质押、无效、终止、恢复和专利权人的姓名或名称、国籍、地址变更等事项记载在专利登记簿上。



局长

申长雨

申长雨



证书号第 2933250 号



发明专利证书

发明名称：匿名多组射频识别系统的丢失标签非确定性并行检测方法

发明人：陈鸿龙；杨黎鹏；车荣杰；丁鑫旺；付金楠；林凯；刘璐
石乐义

专利号：ZL 2017 1 0296555.9

专利申请日：2017 年 04 月 28 日

专利权人：中国石油大学（华东）；中石化石油工程设计有限公司

地址：266580 山东省青岛市经济技术开发区长江西路 66 号

授权公告日：2018 年 05 月 22 日

授权公告号：CN 107038398 B

本发明经过本局依照中华人民共和国专利法进行审查，决定授予专利权，颁发本证书并在专利登记簿上予以登记。专利权自授权公告之日起生效。

本专利的专利权期限为二十年，自申请日起算。专利权人应当依照专利法及其实施细则规定缴纳年费。本专利的年费应当在每年 04 月 28 日前缴纳。未按照规定缴纳年费的，专利权自应当缴纳年费期满之日起终止。

专利证书记载专利权登记时的法律状况。专利权的转移、质押、无效、终止、恢复和专利权人的姓名或名称、国籍、地址变更等事项记载在专利登记簿上。



局长
申长雨

申长雨



证书号第2960783号



发明专利证书

发明名称：匿名分组 RFID 系统的丢失标签检测方法

发明人：陈鸿龙;马国蕾;丁鑫旺;林凯;刘璐;石乐义

专利号：ZL 2016 1 0909384.8

专利申请日：2016 年 10 月 19 日

专利权人：中国石油大学(华东)

地址：266580 山东省青岛市黄岛区长江西路 66 号

授权公告日：2018 年 06 月 15 日

授权公告号：CN 106503759 B

本发明经过本局依照中华人民共和国专利法进行审查，决定授予专利权，颁发本证书并在专利登记簿上予以登记。专利权自授权公告之日起生效。

本专利的专利权期限为二十年，自申请日起算。专利权人应当依照专利法及其实施细则规定缴纳年费。本专利的年费应当在每年 10 月 19 日前缴纳。未按照规定缴纳年费的，专利权自应当缴纳年费期满之日起终止。

专利证书记载专利权登记时的法律状况。专利权的转移、质押、无效、终止、恢复和专利权人的姓名或名称、国籍、地址变更等事项记载在专利登记簿上。



局长
申长雨

申长雨



证书号第 3459223 号



发明专利证书

发明名称：基于 SHZE 的大规模分组 RFID 系统的丢失标签冰山查询方法

发明人：艾欣;陈鸿龙;林凯;代天骄;王志波;石乐义

专利号：ZL 2018 1 1139682.9

专利申请日：2018 年 09 月 28 日

专利权人：中国石油大学（华东）

地址：266580 山东省青岛市黄岛区长江西路 66 号

授权公告日：2019 年 07 月 16 日

授权公告号：CN 109255275 B

国家知识产权局依照中华人民共和国专利法进行审查，决定授予专利权，颁发发明专利证书并在专利登记簿上予以登记。专利权自授权公告之日起生效。专利权期限为二十年，自申请日起算。

专利证书记载专利权登记时的法律状况。专利权的转移、质押、无效、终止、恢复和专利权人的姓名或名称、国籍、地址变更等事项记载在专利登记簿上。



局长
申长雨

申长雨



证书号第 3459223 号



专利权人应当依照专利法及其实施细则规定缴纳年费。本专利的年费应当在每年 09 月 28 日前缴纳。未按照规定缴纳年费的，专利权自应当缴纳年费期满之日起终止。

申请日时本专利记载的申请人、发明人信息如下：

申请人：

中国石油大学（华东）

发明人：

陈鸿龙；艾欣；林凯；代天骄；王志波；石乐义



项目批准号	61772551
申请代码	F020809
归口管理部门	
依托单位代码	25706108A1489-2710



617725511004552

国家自然科学基金委员会 资助项目计划书

资助类别：面上项目

亚类说明：

附注说明：常规面上项目

项目名称：面向大规模RFID系统的标签安全监测关键技术研究

直接费用：63万元 执行年限：2018.01-2021.12

负责人：陈鸿龙

通讯地址：山东省青岛市黄岛区长江西路66号

邮政编码：266580 电 话：053286981335

电子邮件：chenhl@upc.edu.cn

依托单位：中国石油大学（华东）

联系人：谭树成 电 话：053286981837

填表日期：2017年09月01日

国家自然科学基金委员会制



国家自然科学基金委员会资助项目计划书填报说明

- 一、项目负责人收到《关于国家自然科学基金资助项目批准及有关事项的通知》（以下简称《批准通知》）后，请认真阅读本填报说明，参照国家自然科学基金相关项目管理办法及《国家自然科学基金资助项目资金管理办法》（请查阅国家自然科学基金委员会官方网站首页“政策法规”-“管理办法”栏目），按《批准通知》的要求认真填写和提交《国家自然科学基金委员会资助项目计划书》（以下简称《计划书》）。
- 二、填写《计划书》时要求科学严谨、实事求是、表述清晰、准确。《计划书》经国家自然科学基金委员会相关项目管理部门审核批准后，将作为项目研究计划执行和检查、验收的依据。
- 三、《计划书》各部分填写要求如下：
 - （一）简表：由系统自动生成。
 - （二）摘要及关键词：各类获资助项目都必须填写中、英文摘要及关键词。
 - （三）项目组主要成员：计划书中列出姓名的项目组主要成员由系统自动生成，与申请书原成员保持一致，不可随意调整。如果批准通知中“项目评审意见及修改意见表”中“对研究方案的修改意见”栏目有调整项目组成员相关要求的，待项目开始执行后，按照项目成员变更程序另行办理。
 - （四）资金预算表：按批准资助的直接费用填报资金预算表和预算说明书，其中的劳务费、专家咨询费金额不应高于申请书中相应金额。国家重大科研仪器研制项目、重大项目还应按照预算评审后批复的直接费用各科目金额填报资金预算表、预算说明书及相应的预算明细表。
 - （五）正文：
 1. 面上项目、青年科学基金项目、地区科学基金项目：如果《批准通知》中没有修改要求的，只需选择“研究内容和研究目标按照申请书执行”即可；如果《批准通知》中“项目评审意见及修改意见表”中“对研究方案的修改意见”栏目明确要求调整研究期限和研究内容等的，须选择“根据研究方案修改意见更改”并填报相关修改内容。
 2. 重点项目、重点国际（地区）合作研究项目、重大项目、国家重大科研仪器研制项目：须选择“根据研究方案修改意见更改”，根据《批准通知》的要求填写研究（研制）内容，不得自行降低、更改研究目标（或仪器研制的技术性能与主要技术指标以及验收技术指标）或缩减研究（研制）内容。此外，还要突出以下几点：
 - （1）研究的难点和在实施过程中可能遇到的问题（或仪器研制风险），拟采用的研究（研制）方案和技术路线；
 - （2）项目主要参与者分工，合作研究单位之间的关系与分工，重大项目还需说明课题之间的关联；
 - （3）详细的年度研究（研制）计划。



3. 国家杰出青年科学基金、优秀青年科学基金和海外及港澳学者合作研究基金项目：须选择“根据研究方案修改意见更改”，按下列提纲撰写：
 - (1) 研究方向；
 - (2) 结合国内外研究现状，说明研究工作的学术思想和科学意义（限两个页面）；
 - (3) 研究内容、研究方案及预期目标（限两个页面）；
 - (4) 年度研究计划；
 - (5) 研究队伍的组成情况。
4. 国家自然科学基金基础科学中心项目：须选择“根据研究方案修改意见更改”，应当根据评审委员会和现场考察专家组的意见和建议，进一步完善并细化研究计划，作为评估和验收的依据。按下列提纲撰写：
 - (1) 五年拟开展的研究工作（包括主要研究方向、关键科学问题与研究内容）；
 - (2) 研究方案（包括骨干成员之间的分工及合作方式、学科交叉融合研究计划等）；
 - (3) 年度研究计划；
 - (4) 五年预期目标和可能取得的重大突破等；
 - (5) 研究队伍的组成情况。
5. 对于其他类型项目，参照面上项目的方式进行选择和填写。



简表

申请者信息	姓 名	陈鸿龙	性 别	男	出生年月	1984年09月	民 族	汉族
	学 位	博士			职称	副教授		
	电 话	053286981335		电子邮件	chenhl@upc.edu.cn			
	传 真			个人网页				
	工 作 单 位	中国石油大学（华东）						
	所 在 院 系 所	信息与控制工程学院						
依托单位信息	名 称	中国石油大学（华东）					代码	25706108A1489
	联 系 人	谭树成		电子邮件	tsc1980@upc.edu.cn			
	电 话	053286981837		网站地址	http://www.upc.edu.cn/			
合作单位信息	单 位 名 称							代 码
项目基本信息	项 目 名 称	面向大规模RFID系统的标签安全监测关键技术研究						
	资 助 类 别	面上项目			亚 类 说 明			
	附 注 说 明	常规面上项目						
	申 请 代 码	F020809:传感网络协议与计算			F020805:网络安全			
	基 地 类 别							
	执 行 年 限	2018.01-2021.12						
	直 接 费 用	63万元						



项目摘要

中文摘要(500字以内):

射频识别(RFID)系统的标签监测包括标签数目估算、丢失标签检测和丢失标签识别等,是RFID的关键技术之一。目前大规模RFID系统的标签监测面临着效率低、干扰复杂、易受攻击以及隐私泄露等诸多亟待解决的问题,对RFID技术的发展提出了严峻挑战。本项目以大规模RFID系统为对象,以对阅读器与标签间信息交互效率影响因素的分析为基础,以提高帧时隙利用率、抑制标签监测干扰、优化监测性能等方法为主要技术手段,开展标签安全监测研究,重点解决以下科学问题:1)分组RFID系统的小组丢失标签估算效率及精度保障问题;2)分组RFID系统的小组丢失标签高效检测及可靠度问题;3)含未知标签的RFID系统丢失标签高效识别及关键丢失标签完全识别问题;4)标签监测过程的阻塞攻击检测及其标签ID信息隐私保护问题。最后,本项目将基于仿真与实验平台开展方法有效性验证。本项目的研究成果将为RFID的应用提供理论基础与方法支撑。

关键词: 大规模射频识别系统; 标签数目估算; 丢失标签检测; 丢失标签识别; 安全与隐私保护

Abstract(limited to 4000 words):

Tag monitoring in Radio Frequency Identification (RFID) systems, including tag cardinality estimation, missing tag detection and missing tag identification, etc, has been one of the key techniques of RFID. However, there are several problems to be solved in the tag monitoring such as low monitoring efficiency, multiple interference sources, vulnerability in security and privacy, making it be one of the challenging issues for RFID. This project intends to study on the secure tag monitoring for large-scale RFID systems based on the influence analysis of the communication efficiency between the reader and tags. The main techniques to be used in the research of this project include improving utilization of the framed slots, deactivating the interference in tag monitoring, and optimizing the monitoring performance, and so on. This project focuses on solving the following key scientific problems: 1) efficient missing tag cardinality estimation of each category for the multi-category RFID systems with accuracy guarantee, 2) efficient and reliable missing tag detection of each category for the multi-category RFID systems, 3) efficient missing tag identification for RFID systems with unknown tags and the complete missing key tag identification, 4) jamming attack detection and the tag ID privacy protection during the tag monitoring in RFID systems. Finally, this project will validate the effectiveness of the proposed schemes based on the simulation and experimental platform. The research results of this project will provide the theoretical foundation and methodology support for the further applications of RFID.

Keywords: Large-Scale Radio Frequency Identification Systems; Tag Cardinality Estimation; Missing Tag Detection; Missing Tag Identification; Security and Privacy Protection



项目组主要成员

编号	姓名	出生年月	性别	职称	学位	单位名称	电话	证件号码	项目分工	每年工 作时间 (月)				
1	陈鸿龙	1984. 09	男	副教授	博士	中国石油大学（华东）	053286981335	350583198409173113	项目负责人	8				
2	石乐义	1975. 09	男	教授	博士	中国石油大学(华东)	053286980615	370502197509143211	攻击检测	4				
3	刘昕	1974. 10	女	副教授	博士	中国石油大学(华东)	15853273273	370702197410011324	隐私保护	4				
4	黄庭培	1980. 04	女	讲师	博士	中国石油大学(华东)	15589843379	422822198004061045	RFID模型分析	5				
5	姜向远	1983. 03	男	讲师	博士	中国石油大学(华东)	15166687206	370281198303112616	丢失标签检测方法研究	5				
6	尚林源	1989. 01	男	博士生	硕士	中国石油大学(华东)	18954217608	370983198901256151	模型构建与分析	6				
7	张汉元	1991. 05	男	博士生	学士	中国石油大学(华东)	18353268494	370827199105061810	参数优化	6				
8	马国蕾	1992. 03	男	硕士生	学士	中国石油大学(华东)	18353244669	370523199203012412	丢失标签识别方法研究	10				
9	丁鑫旺	1992. 10	男	硕士生	学士	中国石油大学(华东)	13012457179	362522199210011518	算法仿真研究	10				
10	付金楠	1991. 03	男	硕士生	学士	中国石油大学(华东)	17853290843	370684199103181815	性能分析	10				
总人数			高级		中级		初级		博士后		博士生		硕士生	
10			3		2						2		3	



国家自然科学基金项目直接费用预算表（定额补助）

项目批准号：61772551

项目负责人：陈鸿龙

金额单位：万元

序号	科目名称	金额
1	一、项目直接费用	63.0000
2	1、设备费	4.0000
3	(1)设备购置费	4.0000
4	(2)设备试制费	0.00
5	(3)设备改造与租赁费	0.00
6	2、材料费	10.0000
7	3、测试化验加工费	0.00
8	4、燃料动力费	0.00
9	5、差旅/会议/国际合作与交流费	20.0000
10	6、出版/文献/信息传播/知识产权事务费	10.0000
11	7、劳务费	17.76
12	8、专家咨询费	1.2400
13	9、其他支出	0.00
14	二、自筹资金	0.00



预算说明书（定额补助）

（请按《国家自然科学基金项目资金预算表编制说明》中的要求，对各项支出的主要用途和测算理由及合作研究外拨资金，单价 ≥ 10 万元的设备等内容进行详细说明，可根据需要另加附页。）

一、直接费用 **63.0000 万元**

1、设备费： **4.0000 万元**

（1）设备购置费： **4.0000 万元**

RFID 开发套件：2 万元/套 $\times 1$ 套，传感器节点 Imote2：0.1 万元/个 $\times 10$ 个，调试版 MIB520：0.2 万元/个 $\times 5$ 个，合计：4 万元。

（2）设备试制费： **0.0000 万元**

（3）设备改造与租赁费： **0.0000 万元**

2、材料费： **10.0000 万元**

电子元件、电脑配件、打印纸和硒鼓等耗材费用：2.5 万元/年 $\times 4$ 年，合计：10 万元。

3、测试化验加工费： **0.0000 万元**

4、燃料动力费： **0.0000 万元**

5、差旅/会议/国际合作与交流费： **20.0000 万元**

差旅费：用于项目执行过程中业务调研、学术交流等工作所发生的外埠差旅费、市内交通费等：0.5 万元/人次 $\times 5$ 人次/年 $\times 4$ 年=10 万元。

会议费：承办一次课题研究相关小型学术会议：2 万元/次 $\times 1$ 次=2 万元。

国际合作与交流费：课题组成员出国参加顶级国际会议：1.5 万元/次 $\times 4$ 次=6 万元，邀请境外专家来华合作交流：1 万元/次 $\times 2$ 次=2 万元。

合计：20 万元。

6、出版/文献/信息传播/知识产权事务费： **10.0000 万元**

学术论文版面费：0.8 万元/篇 $\times 6$ 篇，国家发明专利代理费：0.8 万元/项 $\times 4$ 项，查新费：0.25 万元/次 $\times 4$ 次，购置图书费：1.0 万元。合计：10 万元。

7、劳务费 **17.7600 万元**

博士生：1200 元/人月 $\times 2$ 人 $\times 6$ 月/年 $\times 4$ 年=5.76 万元，硕士生：1000 元/人月 $\times 3$ 人 $\times 10$ 月/年 $\times 4$ 年=12.00 万元。合计：17.76 万元。

8、专家咨询费 **1.2400 万元**

用于邀请国内专家、教授做学术报告与学术交流：0.31 万元 /年 $\times 4$ 年，合计 1.24 万元。

9、其他支出 **0.0000 万元**

二、自筹资金 **0.0000 万元**

项目负责人签字：

科研部门公章：

财务部门公章：



报告正文

研究内容和研究目标按照申请书执行。



国家自然科学基金资助项目签批审核表

	<p>我接受国家自然科学基金的资助，将按照申请书、项目批准意见和计划书负责实施本项目（批准号：61772551），严格遵守国家自然科学基金委员会关于资助项目管理、财务等各项规定，切实保证研究工作时间，认真开展研究工作，按时报送有关材料，及时报告重大情况变动，对资助项目发表的论著和取得的研究成果按规定进行标注。</p> <p>项目负责人（签章）： 年 月 日</p>	<p>我单位同意承担上述国家自然科学基金项目，将保证项目负责人及其研究队伍的稳定和研究项目实施所需的条件，严格遵守国家自然科学基金委员会有关资助项目管理、财务等各项规定，并督促实施。</p> <p>依托单位（公章） 年 月 日</p>					
本栏目由基金委填写	<p>科学处审查意见：</p>						
	<p>建议年度拨款计划（本栏目为自动生成，单位：万元）：</p>						
	年度	总额	第一年	第二年	第三年	第四年	第五年
	金额						
	<p>科学部审查意见：</p> <p>负责人（签章）： 年 月 日</p>						
本栏目主要用于重大项目等	<p>相关局室审核意见：</p> <p>负责人（签章）： 年 月 日</p>						
	<p>委领导审批意见：</p> <p>委领导（签章）： 年 月 日</p>						

山东省科技计划项目验收证书

项 目 编 号：2015GGX101045

项 目 名 称：物联网跨层信息安全与隐私保护研究

完 成 单 位：中国石油大学（华东）信息与控制工程学院（盖章）

参 加 单 位：武汉大学计算机学院

验收组织部门：中国石油大学（华东）

验 收 日 期：2017 年 5 月 25 日

山东省科学技术厅

二〇一一年制

建成新装置	0 (套)	新工艺	0 (项)
-------	-------	-----	-------

2. 项目负责人情况

姓 名	性别	出生年月	专 业	学 历	职 称	联系电话
陈鸿龙	男	1984 年 9 月	计 算 机 科 学	博 士 研 究 生	副教授	13573861376

3. 项目研发人员情况

单位：人

项目研发人员总数	8
其中:博士	4
硕士	0
其中:高级职称	3
中级职称	1
其中:在校研究生	4

4. 项目实际到位经费情况

单位：万元

项 目 总经费	国 家 拨 款	省科技厅 拨款	市 县 拨 款	部 门 拨 款	自 筹 (含贷款)	其 它
20	0	20	0	0	0	0

5. 省拨经费支出情况

单位：万元

合 计	17.909723	5. 资料印刷费	5.054213
1. 仪器设备购置及维修费	4.000000	6. 调研差旅费	1.556450
2. 能源及材料消耗费	5.999060	7. 鉴定验收费	0.300000
3. 场地租赁费	0.000000	8. 管理费	1.000000
4. 试验外协费	0.000000	9. 其它费用	0.000000

二、目标任务完成情况

1. 主要解决的关键技术与创新点

- 节点利用时间槽片段 (fractional time slot) 广播 Beacon 数据包发现邻节点, 结合相应的休眠调度方法, 有效降低时延和能耗, 实现快速、节能的邻节点发现;
- 利用多哈希运算技术, 在保护标签信息隐私条件下有效实现对匿名多组 RFID 系统的小组标签选定, 进一步在丢失标签检测过程中利用片段化 (segmentation) 技术有效提高检测效率, 并通过参数优化实现效率最大化;
- 将节点携带数据包的时间长度作为节点数据包转发激励机制的报酬分配依据, 有效解决激励机制中存在的安全问题, 使之能够抵御伪造转发攻击、隐藏转发攻击和数据篡改攻击, 同时保障激励机制中的激励相容性和报酬有界性, 使其能够有效激发物联网中节点的数据包转发;
- 利用节点间信息交互过程的特性, 基于移动信标节点检测虫洞攻击的存在, 并利用节点的邻居信息在虫洞攻击下出现的异常, 建立相应的节点冲突集, 利用相应的特性实现对虫洞攻击节点的定位。

2. 技术指标

本项目执行期间, 累计发表和录用国内外期刊论文 11 篇, 其中 SCI 检索 5 篇(包括 SCI 二区 1 篇, SCI 三区 3 篇), EI 检索 4 篇, 核心期刊 2 篇, 申请国家发明专利 8 项, 其中已授权 3 项, 实审 3 项。

3. 经济指标

有助于推动物联网产业的进一步发展。

4. 社会效益

推动物联网服务于社会的同时, 一定程度上有效保护用户的信息安全与隐私。

三、验收意见

2017年5月25日，受省科技厅委托，中国石油大学（华东）组织有关专家，对中国石油大学（华东）承担的山东省科技计划项目“物联网跨层信息安全与隐私保护研究”进行验收。专家委员会通过资料审查、听取汇报、质询和讨论，形成如下验收意见：

1. 验收资料齐全规范，数据翔实，符合验收要求。
2. 该项目针对物联网跨层信息安全与隐私保护问题，提出了一种高效的邻节点发现方法、检出各组标签中的丢失标签事件的方法、一种促使激励相容的安全激励机制和虫洞攻击节点的检测及定位方法。
3. 发表学术论文 11 篇，SCI 收录 5 篇，申请发明专利 8 项，其中已授权 3 项。
4. 项目经费使用规范合理，做到了专款专用。

验收委员会认为：该项目完成了合同规定的各项指标，同意通过验收。

验收专家组组长：韩定坤 副组长：邵延军

2017 年 5 月 25 日

四、项目主要参加人员名单

姓 名	性别	出生年月	技术职称	学历	工作单位	承担的主要研究任务	本人签名
陈鸿龙	男	1984-09	副教授	博士研究生	中国石油大学(华东)信息与控制工程学院	项目负责人	陈鸿龙
石乐义	男	1975-09	教授	博士研究生	中国石油大学(华东)计算机与通信工程学院	加密算法设计	石乐义
王志波	男	1984-05	副教授	博士研究生	武汉大学计算机学院	调度算法设计	王志波
姜向远	男	1983-03	讲师	博士研究生	中国石油大学(华东)信息与控制工程学院	虫洞攻击检测方法设计	姜向远
邵伟明	男	1986-09	博士生	本科	中国石油大学(华东)信息与控制工程学院	模型构建	邵伟明
张汉元	男	1991-05	博士生	本科	中国石油大学(华东)信息与控制工程学院	算法优化	张汉元
杨玉斌	男	1990-06	硕士生	本科	中国石油大学(华东)信息与控制工程学院	算法仿真与性能分析	杨玉斌
阮宏镁	女	1989-09	硕士生	本科	中国石油大学(华东)信息与控制工程学院	算法仿真与性能分析	阮宏镁

五、验收专家组名单

姓 名	工 作 单 位	所学专业	现从事专业	职务/职称	本人签名
韩宝坤	山东科技大学	机械电子工程	机械电子工程	机电学院副院长/教授	韩宝坤
郭建章	青岛科技大学	过程控制与装备	过程控制与装备	机电学院副院长/教授	郭建章
黄鹤松	山东科技大学	控制理论与控制工程	检测技术与自动化装置	副院长/教授	黄鹤松
撒占友	青岛理工大学	安全技术及工程	安全工程	安全科学与工程系主任/教授	撒占友
尚尔东	青岛茂生会计师事务所	会计学	会计审计	高级会计师	尚尔东

六、项目管理部门意见

项目主管部门意见

同意通过验收。



单位负责人审签：



(盖章)



2017年5月27日

省科技厅意见

新通发展公司

主管业务处、单位负责人审签：

(部门盖章)



年 月 日



山东省重点研发计划 项目任务书

项目编号：2018GGX101035

项目名称：基于帧时隙ALOHA的大规模RFID系统标签监测及其安全与隐私保护研究

项目主管部门（甲方）：中国石油大学（华东）

项目承担单位（乙方）：中国石油大学（华东）信息与控制工程学院

项目协作单位：武汉大学计算机学院

项目负责人：陈鸿龙

联系电话：13573861376

起止时间：2018 年01 月至 2019 年12 月

山东省科学技术厅

二〇一七年制

填 写 说 明

1. 本任务书系省科技厅为组织山东省重点研发计划项目研究而设计，任务书甲方为科技发展计划项目主管部门，乙方为项目承担单位。

2. 本任务书部分内容由山东省科技计划管理信息系统自动生成，承担单位可根据项目实际情况进行补充修改。

3. 本任务书需用 A4 纸打印，一式四份，项目主管部门一份，项目承担单位一份；省科技厅两份。

一、项目基本信息表

单位名称	中国石油大学（华东）信息与控制工程学院			主管部门	中国石油大学（华东）	
单位类型	[01]	01.高等院校 02.科研院所 03.国有企业 04.集体企业 05.私营企业 06.有限责任公司 07.股份有限公司 08.股份合作企业 09.联营企业 10.其它				
通讯地址	山东省青岛市黄岛区长江西路66号			邮政编码	266580	
项目负责人	姓名	性别	出生年月	身份证号码		联系电话
	陈鸿龙	男	1984-09-17	350583198409173113		13573861376
	传真		手机	E-mail		
	0532-86981335		13573861376	chenhl@upc.edu.cn		
职工总数	3385	人	大专以上人员	3125	人	研究开发人员 1659 人
项目起始时间		2018-01-01		计划完成时间		2019-12-31
技术领域	[01]	01. 电子信息 02.新材料 03. 先进制造 04. 新能源与高效节能 05. 交通运输 06. 现代服务业 07. 化工及建材 08. 轻工纺织 09.农业高技术 10. 农业生产 11. 农业设施装备 12. 农业现代产业 13. 新农村建设 14. 海洋科技 15. 资源与节约 16. 环境与可持续发展 17. 人口与健康 18. 中医药现代化 19. 公共安全 20. 生物技术 21.城镇发展与其他社会事业 22. 高新技术创新服务				
项目类别	[1] 1.科研 2.中试 3.新产品开发					
研究方式	[1] 1.本单位独立完成 2.产学研结合 3.引进消化再创新					
主要优势	[6][1][3](按优势大小选择三项) 1.重大理论突破 2.技术工艺创新突出 3.市场前景广阔 4.经济效益显著 5.社会效益显著 6.形成自主知识产权 7. 其它					
项目完成时 预期成果走向	知识产权 情况	专利	其中发明专利	技术标准	著作权	动植物新品种
		4	4	0	4	0
	科技报告 (篇)	立项报告	进展报告	专题报告	最终(技术)报告	合计
		1	1	0	1	3
	技术水平	[02] 1.国际领先 2.国际先进 3.国内领先 4.国内先进 5.省内领先 6.省内先进				
	市场前景	[03] 1.出口创汇 2.替代进口 3.填补国内空白 4.填补省内空白				
产业化后 经济效益	年增销售收入(万元)		年增税收(万元)	年增利润(万元)	创汇(万美元)	
	0.00		0.00	0.00	0.00	

二、主要研究内容

本项目面向大规模 RFID 系统，将对标签监测及其安全与隐私保护问题进行系统研究。如图 1 所示，本项目的研究内容如下：1) RFID 标签数目估算问题；2) RFID 丢失标签检测问题；3) RFID 丢失标签识别问题；4) RFID 安全与隐私保护问题。

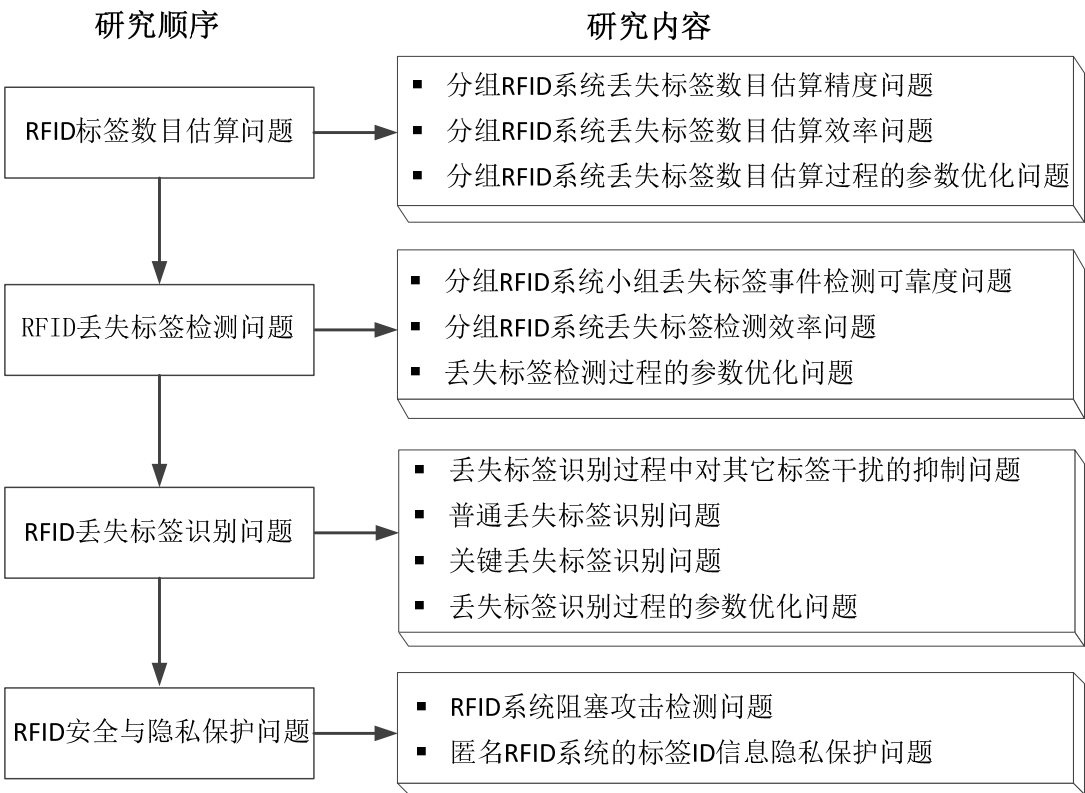


图 1 主要研究内容

1. RFID 标签数目估算问题

最直接的标签数目估算方法是由阅读器逐一广播每个标签 ID，每个标签接收到自己 ID 信息后返回应答信号，以实现零误差的标签个数统计。但是，这种估算方法效率太低，不适用于大规模 RFID 系统。因此，可以采用基于帧时隙 ALOHA (Framed Slotted Aloha) 协议的方法，由阅读器广播帧长度和随机种子 (Random seed)，每个标签根据接收到的帧长度和随机种子以及自身 ID，经过 Hash 计算得到其返回应答信号的时隙编号。对于每个时隙，若没有标签选择它作为应答时隙，则称为空时隙 (Empty slot)，若有且仅有一个标签选择它作为应答时隙，则称为 Singleton 时隙 (Singleton slot)，若至少两个标签选择它作为应答时隙，则称为冲突时隙 (Collision slot)。阅读器通过对应答帧每个时隙的状态检测，即可估算出系统中标签的数目。但是，针对大规模分组 RFID 系统，阅读器不仅需要估算出系统的标签总数目，还需要对每组的标签数目进行估算，而不同小组标签之间会互相干扰，严重影响估算精度和估算效率。本项目将针对大规模分组 RFID 系统提出准确高效的小组丢失标签数目估算方法，分析不同小组标签之间干扰对估算精度和估算效率的影响，研究标签数目估算的精度和效率问题，在估算精度满足系统要求的前提条件下，对网络参数，如帧长度和帧的个数等，进行优化，实现准确、高效的小组丢失标签数目估算。

2. RFID 丢失标签检测问题

RFID 系统中已知标签 ID 信息一般是预存在后端服务器，因此阅读器能够实时获取。为实现丢失标签事件检测，阅读器在广播帧长度和随机种子后，提前计算每个时隙返回应答信息的标签集合，并预测每个时隙的状态，待标签返回应答信息后，阅读器检测每个时隙的实际状态。由于标签丢失可能会改变某些时隙的状态，阅读器通过观测实际时隙状态和预期时隙状态之间的不同来检测丢失标签事件。然而，在大规模分组 RFID

系统中，在某一小组已经被检测出丢失标签事件之后，该小组的标签仍然会参与后续的丢失标签检测过程，降低帧时隙的利用率，因此，其检测效率不高。此外，在检测过程中如何同时满足每个小组丢失标签的检测可靠度要求，即：对于标签丢失个数超过一定阈值的小组，如何确保每组的丢失标签检测成功率都不低于给定的要求这一问题将成为一大难点。本项目将针对大规模分组 RFID 系统，分析和构建多组丢失标签检测可靠度和丢失标签个数、帧长度、检测轮次之间的数学模型关系，提出一种可靠度高的丢失标签检测方法，分析该检测方法中制约检测效率的关键因素，研究丢失标签检测效率问题，并构建出检测时间和帧长度、检测轮次之间的数学模型关系，在保证检测可靠度的前提条件下，优化检测时间，实现高效的小组丢失标签检测。

3. RFID 丢失标签识别问题

RFID 系统标签的丢失可能会导致某些时隙的状态发生变化，即由非空时隙（Non-empty slot）变成空时隙（Empty slot），阅读器可以通过检测这一变化来识别系统中丢失的标签 ID 信息。但是，若 RFID 系统中存在部分未知标签，则这些未知标签同样会基于阅读器广播的帧长度和随机种子，计算其返回应答信息的时隙编号，并在相应的时隙发送应答信息，使得原本由于丢失标签而由非空状态变成空状态的时隙，可能会被未知标签选做应答时隙而又变为非空时隙，严重影响丢失标签的识别。本项目针对含未知标签的大规模 RFID 系统，分析未知标签的应答对丢失标签识别过程的干扰，将提出一种能够有效抑制未知标签干扰的丢失标签识别方法，解决抑制未知标签和识别效率之间的矛盾，在保障丢失标签识别可靠度满足系统要求的前提下，通过参数优化，有效降低丢失标签识别时间，最大化识别效率。此外，本项目进一步将 RFID 系统中的标签分为普通标签和关键标签，分析普通标签对关键丢失标签识别过程的干扰，提出相应的关键丢失标签识别方法，实现对关键丢失标签的完全识别，并通过构建关键丢失标签识别时间和帧长度等网络参数之间的模型关系，实现性能优化，提高识别效率。

4. RFID 安全与隐私保护问题

RFID 系统中的阻塞攻击（Jamming attack）能够随机挑选特定的时隙发送信息，影响阅读器对其他标签应答信息的接收。阻塞攻击的应答会使原本为空的时隙变成 Singleton 时隙，而原本为 Singleton 的时隙变为冲突时隙，降低标签数目估算精度、丢失标签检测率和丢失标签识别准确度。本项目针对大规模 RFID 系统的标签监测过程，将提出一种阻塞攻击检测方法，能够及时有效地检测阻塞攻击，并且在保障攻击检测成功率的前提下，优化检测速率。此外，匿名 RFID 系统中的攻击节点能够监听系统中广播的标签 ID 信息，泄露标签的信息隐私，破坏 RFID 的系统功能。本项目针对匿名 RFID 系统，将着力解决标签监测过程中的标签 ID 信息隐私保护问题，提出面向分组 RFID 系统的小组标签选定方法，在小组选定过程中避免小组 ID 信息的广播，有效防止攻击节点对 ID 信息的监听，实现对标签信息隐私的有效保护。

三、主要技术指标

本项目拟实现以下技术指标：

1. 提出精确高效的分组 RFID 系统小组丢失标签数目估算方法，申请国家发明专利 1 项并投稿论文 1 篇；
2. 提出分组 RFID 系统中小组丢失标签并行检测和顺序检测方法，申请国家发明专利 1 项并投稿论文 1 篇；
3. 提出 RFID 系统中能够有效抑制未知标签的丢失标签识别方法，申请国家发明专利 1 项并投稿论文 1 篇；
4. 提出 RFID 系统中阻塞攻击检测方法及带隐私保护的小组标签选定方法，申请国家发明专利 1 项并投稿论文 1 篇。

四、主要创新点及先进性

本项目的创新点主要包括以下几点：

1. 利用帧时隙状态的变化，通过数学模型关系转换，准确估算分组 RFID 系统的小组丢失标签数目，在估算过程中标识出已识别的丢失标签，有效降低待估算的标签规模，提高估算效率；
2. 通过检测时隙状态的变化快速有效地检测分组 RFID 系统的小组丢失标签事件，建立丢失标签检测可靠度与帧长度、检测次数等参数之间的关系，从理论上同时保障多组标签的丢失标签检测可靠度要求，在检测过程中抑制已确认的未丢失标签，有效提高检测效率；
3. 针对含未知标签的 RFID 系统丢失标签识别，实现对未知标签的快速有效抑制，并在丢失标签识别过程中进一步抑制剩余未知标签，最小化未知标签的影响，以满足系统的识别可靠度要求。同时，对普通标签进行有效抑制，降低其对关键丢失标签识别过程的干扰，实现关键丢失标签的快速完全识别；
4. 快速有效地检测 RFID 系统的阻塞攻击，克服其对标签监测过程的干扰，并有效解决分组 RFID 系统中对小组标签选定过程的标签 ID 信息隐私保护问题，有效保障标签监测过程的安全性。

五、项目经费预算

项目计划总投资		20.00 万元		其中已完成投资		0.00 万元	
计划新增投资来源	单位自筹		0.00 万元				
	金融贷款		0.00 万元				
	财政 拨款	20.00 万元	其中:国家财政拨款		0.00 万元		
			省科技经费		20.00 万元		
			地方政府配套		0.00 万元		
	其它		0.00 万元				
新增投资中省科技 经费支出预算	直接经费		设备费		2.90 万元		
			材料费		3.00 万元		
			测试化验加工费		0.00 万元		
			燃料动力费		0.00 万元		
			差旅会议国际合作与交流费		3.00 万元		
			出版/文献/信息传 播/知识产权事务费		2.00 万元		
			劳务费		5.00 万元		
			专家咨询费		1.25 万元		
			其它费用		0.00 万元		
	间接费用		承担单位为项目研究提供的房屋占用，日常水、电、气、暖消耗		0.00 万元		
			有关管理费用的补助支出		1.40 万元		
			激励科研人员的绩效支出		1.45 万元		
			其它费用		0.00 万元		

六、项目进度安排

计划进度	开始时间	截止时间	完成的主要指标(要可考核)
	2018-01-01	2018-06-30	申请国家发明专利1项，投稿论文1篇
	2018-07-01	2018-12-31	申请国家发明专利1项，投稿论文1篇
	2019-01-01	2019-06-30	申请国家发明专利1项，投稿论文1篇
	2019-07-01	2019-12-31	申请国家发明专利1项，投稿论文1篇

七、项目课题组成员

姓名	性别	出生年月	职称/职务	工作单位	项目中分工	参加月/年
陈鸿龙	男	1984-09-17	副教授	中国石油大学（华东）	项目负责人	8
石乐义	男	1975-09-14	教授	中国石油大学（华东）	标签数目估算方法设计	4
王志波	男	1984-05-10	副教授	武汉大学	标签隐私保护方法设计	4
姜向远	男	1983-03-11	讲师	中国石油大学（华东）	丢失标签检测方法设计	6
林凯	男	1992-03-27	硕士研究生	中国石油大学（华东）	丢失标签识别方法设计	10
刘璐	女	1992-03-21	硕士研究生	中国石油大学（华东）	攻击检测研究	10
丁鑫旺	男	1992-10-01	硕士研究生	中国石油大学（华东）	性能分析	10
付金楠	男	1991-03-18	硕士研究生	中国石油大学（华东）	算法仿真研究	10
王帅	男	1995-02-21	硕士研究生	中国石油大学（华东）	实验平台搭建	10
秦雨婷	女	1995-03-28	硕士研究生	中国石油大学（华东）	实验测试	10

八、任务书签订各方意见

项目主管部门（甲方）

（公 章）

负责人（签字）

年 月 日

项目承担单位（乙方）

项目负责人（签字）

财务负责人（盖章）

（公 章）

年 月 日

省科技厅主管处、单位

（公 章）

负责人（签字）

年 月 日

九、共同条款

1. 乙方必须按要求编报年度计划执行情况、下一年度经费预算和有关统计报表，交甲方汇总后，及时上报省科技厅。逾期不报，省科技厅有权暂停拨款。

2. 任务书执行过程中，乙方如需调整任务，向甲方提出变更内容及其理由的申请报告，经甲方审核后报省科技厅审定后实施。未接到正式批准书以前，双方须按原任务书履行，否则后果由自行调整的一方负责。

3. 乙方因某种原因（如：与项目申请书内容有出入、挪用经费、技术措施或某些条件不落实）致使计划无法执行，而要求中止，应视不同情况，部分、全部退还所拨经费；如乙方没有提出中止任务书的要求，甲方可根据调查情况有权提出中止的处理建议，报省科技厅审核批准后执行。

4. 甲方根据应用技术研发资金开支的规定，监督经费的使用情况。凡不符合规定的开支，甲方负责提出调整意见。必要时，省科技厅有权直接提出调整或撤销意见。

5. 乙方应严格按照规定提交相应的科技报告：立项下达后、任务书签署前，应呈交立项报告；项目执行中，年度或中期审核前应呈交进展报告；专题报告[指实验（试验）报告、调研报告、工程报告、测试报告、评估报告等蕴含科研活动细节及基础数据的报告]根据项目执行情况据实呈交；项目完成后三个月内、申请验收前，须呈交最终（技术）报告。对未提交相应科技报告或者科技报告质量达不到合格标准的项目，按不通过验收或不予结题处理。

6. 本任务书签订各方均负有相应的责任。若有争议或纠纷时，按山东省重点研发计划管理办法有关条款处理。

项目编号： 15-9-1-79-jch

青岛市应用基础研究计划项目任务书
(青年专项)

项目名称 面向资源受限移动感知网络的信息安全与隐私保护研究

项目类别 自主创新计划（应用研究专项—青年应用基础研究）

起止年限 2015-09 至 2017-09

项目负责人 陈鸿龙 电话及手机 13573861376

项目联系人 裴红艳 电话及手机 0532-86981837

承担单位 中国石油大学（华东） (盖章)

参与单位 (盖章)

承担单位地址 山东省青岛市黄岛区长江西路66号 邮编 266580

青岛市科技局

二〇一四年制

一、研究内容、研究方案及技术路线

（研究内容应围绕项目目标，分层次、有条理地叙述，突出所解决的关键科学问题、关键技、研究特色和创新点；研究方案与技术路线应突出实现课题预期目标的总体研究思路、工作安排以及技术路线的创新性、可行性。）

1. 项目目标：针对资源受限移动感知网络的信息安全与隐私保护，首先提出一种能量高效的安全邻节点发现方法；其次提出一种数据包转发安全激励机制，并通过设计数据包传输的路由方式，有效保护端到端位置隐私；最后提出抵御虫洞攻击的安全定位方法。
2. 研究内容：高效、安全邻节点发现问题；数据包转发安全激励问题；端到端位置隐私保护问题；安全定位问题。
3. 主要技术难题及创新点：利用时间槽片段广播Beacon数据包，结合相应的休眠调度方法，有效降低时延和能耗，并基于Beacon信息的一致性，保障邻节点发现过程的安全性，实现高效、安全的邻节点发现；将节点携带数据包时间长度作为转发激励机制的报酬分配依据，有效解决激励机制中存在的安全问题，使之能够抵御常见攻击，同时保障激励相容性和报酬有界性；在感知数据包收集过程中，节点主动生成并转发无效数据包，使得网络中有效数据包和无效数据包的传输路径形成树状结构，防止攻击节点发现源节点和目的节点；在节点定位过程中，利用节点间信息交互过程的特性，建立相应的节点冲突集，利用节点测距信息一致性与节点冲突集之间的关系，有效辨识被虫洞攻击影响的测距信息，实现安全定位过程。

二、预期目标

（预期目标必须说明项目期内研究所要达到的指标、理论上在哪些方面可能取得何种程度的突破；应用前景及对解决经济和社会发展面临的问题可能做出的贡献；论文著作发表情况、知识产权情况、获奖情况、获得其它计划支持进一步研究的可能等。预期目标应提出具体、明确的可考核的指标，避免目标空泛。）

- 1. 在移动感知网络、分布式计算、物联网等相关领域的国内外主流学术期刊、国际知名会议上发表与本项目相关的高质量学术论文（SCI或EI检索）4-5篇；
- 2. 申请国家发明专利3-4项；
- 3. 培养硕士研究生2人，协助培养博士研究生1人；
- 4. 参加和组织关于移动感知网络和分布式计算领域的国内、国际会议，并举办小型的专题讨论会。

三、年度计划

(年度计划分研究内容和预期目标分别阐述,研究内容要具体说明当年需完成的研究任务以便于项目中期检查;预期目标要说明当年所能解决的问题、课题研究的进展程度和指标、文章、专利等情况,对预期目标要有较为具体的描述。)

年 度	研究内容	预期目标
第一年	1. 分析邻节点发现过程中需要解决的能耗、时延和安全问题; 2. 提出能量高效的安全邻节点发现方法,从理论上分析邻节点发现方法的性能; 3. 通过仿真和实验验证所提出的安全邻节点发现方法的有效性。	解决邻节点发现的能耗、时延和安全问题,发表学术论文1篇,申请发明专利1个。
第二年	1. 分析数据包转发激励机制过程中需要解决的激励相容问题、报酬有界问题和安全问题; 2. 提出利用节点携带数据包时间长度来分配报酬的数据包转发安全激励机制; 3. 仿真实现所提出的安全激励机制,验证其有效性; 4. 分析数据包收集过程中的源节点和目的节点的位置隐私保护问题; 5. 提出一种基于树状结构的数据包传输方式,有效降低数据包传输的能耗和时延,并保护端到端的位置信息隐私; 6. 仿真实现所提出的位置隐私保护方法。	解决数据包转发激励问题和数据包收集过程中的位置隐私问题,发表学术论文2篇,申请发明专利1-2个。
第三年	1. 分析移动感知网络中虫洞攻击对节点定位过程的影响; 2. 提出能够有效抵御虫洞攻击的安全定位方法,并从理论上证明其安全性; 3. 通过仿真验证所提出的安全定位方法的有效性。	解决移动感知网络中的安全定位问题,发表学术论文1篇,申请发明专利1个。

 青岛市科技计划项目任务书

 青岛市科技计划项目任务书

 青岛市科技计划项目任务书

四、项目承担单位、参加单位及主要研究开发人员

项目负责人：							
姓名	性别	年龄	职称/职务	从事专业	在本项目中承担的主要工作	是否有工资性收入	所在单位
陈鸿龙	男	31	副教授	计算机	项目负责人	是	中国石油大学（华东）信息与控制工程学院
主要研究开发人员：							
姜向远	男	32	讲师	自动化	调度算法设计	是	中国石油大学（华东）信息与控制工程学院
研究生：							
马国蕾	男	22	硕士研究生	控制理论与控制工程	位置隐私保护研究	否	中国石油大学（华东）信息与控制工程学院
邵伟明	男	29	博士研究生	控制理论与控制工程	模型构建	否	中国石油大学（华东）信息与控制工程学院
张汉元	男	24	博士研究生	控制理论与控制工程	算法优化	否	中国石油大学（华东）信息与控制工程学院
阮宏镁	女	26	硕士研究生	控制理论与控制工程	算法仿真与性能测试	否	中国石油大学（华东）信息与控制工程学院

五、项目资金预算

经费单位：万元

序号	预算科目名称	金额
	市科技专项资金	
1	(一) 直接费用	4.65
2	1. 设备费	0
3	(1) 购置设备费	0
4	(2) 试制设备费	0
5	(3) 设备改造与租赁费	0
6	2. 材料费	1
7	3. 测试化验加工费	0
8	4. 燃料动力费	0
9	5. 差旅费	1.4
10	6. 会议费	0
11	7. 国际合作与交流费	0
12	8. 出版/文献/信息传播/知识产权事务费	1.5
13	9. 劳务费	0.75
14	10. 专家咨询费	0
15	11. 其他支出	详情查看下方附：任务书其他支出表
16	(二) 间接费用	0.35
	合计	5

附：任务书其他支出表

合计	专项资金	自筹资金

附：需附购置设备明细表

序号	设备名称	规格	购置时间	产地	数量	单价	总价	备注
1								

六、任务书各方签章

甲方：

青岛市科学技术局

法定代表人或委托代理人（签字）

许辉

项目主管处室负责人（签字）

李欣

项目主管处室经办人（签字）

李坚



乙方：

法定代表人或委托代理人（签字）

红山印红

项目负责人（签字）

陈鸿飞

开户银行、账号

中国银行股份有限公司青岛经济技术
开发支行 25604391524



丙方：

法定代表人或委托代理人（签字）

红山印红

项目负责人（签字）

开户银行、账号



七、共同条款

任务各方共同遵守《青岛市科技计划项目管理办法》（青科字（2013）8号）（以下简称《办法》）：

1、乙方必须按要求编报年度计划执行情况和有关统计报表，逾期不报，市科技局有权暂停拨款。

2、任务执行过程中，乙方如需调整任务，应根据《办法》中有关规定，向甲方提出变更内容及其理由的申请报告，经甲方审核后实施。未经接到正式批准书以前，双方须按原任务书履行，否则后果由自行调整的一方负责。

3、乙方因某种原因（如：与可行性研究内容有出入、挪用经费、技术措施或某些条件不落实）致使计划无法执行，而要求中止任务，应视不同情况，部分、全部退还所拨经费；如乙方没有提出中止任务的要求，甲方可根据调查情况有权提出中止任务的处理建议。

4、乙方承担任务所需市科技经费按《青岛市财政局 青岛市科技局关于印发〈青岛市科学技术专项资金管理暂行办法〉的通知》（青财文〔2008〕65号）管理和使用。

5、甲方根据市科技计划经费开支的规定，监督经费的使用情况。凡不符合规定的开支，甲方负责提出调整意见。必要时，市科技局有权直接提出调整或撤销意见。

6、任务执行过程中，甲方无故中止任务时，所拨经费、物资不得追回，并承担善后处理所发生的费用。甲方提出变更任务书有关内容时，按《青岛市科技局关于印发〈青岛市科技计划项目变更规程〉的通知》（青科计字〔2013〕12号）有关条款办理。

7、本任务书签订各方均负有相应的责任。若有争议或纠纷时，按《办法》有关条款处理。

项目批准号：

中国石油大学（华东）

自主创新科研计划项目 计划任务书

项目名称： 大规模物联网关键技术研究

项目类型： 青年基金 项目亚类： 优青培育

研究期限： 2018 年 1 月至 2020 年 12 月

负 责 人： 陈鸿龙 联系电话： 13573861376

电子邮箱： chenhl@upc.edu.cn

依托院部： 信息与控制工程学院

2018 年 3 月 6 日填

计划任务书编制说明

1. 凡列入中国石油大学（华东）自主创新科研计划的项目都应编制此计划任务书。
2. 封面“项目批准号”由学校统一编定。
3. 各项内容要认真填写，文字表达明确、严谨、扼要。文字叙述部分用宋体小4号字。
4. 书面材料均用A4纸双面打印，于左侧胶装成册，封面统一为白色。并提交与纸质材料内容一致的电子版。
5. 该项目的《申请书》作为附件附在后面一起装订。
6. 此计划任务书作为项目中期进度检查和结题验收的依据。
7. 其它有关要求，可参阅《中国石油大学（华东）自主创新科研计划项目管理办法》。

一、基本信息

负责人信息	姓 名	陈鸿龙	性 别	男	出生年月	1984 年 9 月
	最后学位	博士	授予时间	2012 年 10 月	职 称	副教授
	主要研究方向	物联网				
	所属科研机构	信息与控制工程学院				
承担单位		信息与控制工程学院		合作单位		
项目信息	项目名称	大规模物联网关键技术研究				
	隶属学科	控制理论与控制工程			批准金额(万元)	20
	项目类型	A	A.青年基金 B.科技专项 C.研究生创新基金			
	起止时间	2018 年 1 月 至 2020 年 12 月				
	主题词(3 个)	物联网、射频识别系统、移动社交网络				
	预期成果	<input checked="" type="checkbox"/> 专著、论文 <input checked="" type="checkbox"/> 专利 <input type="checkbox"/> 软件 <input type="checkbox"/> 样机、样品 <input type="checkbox"/> 其它				
项目组成员	姓名	所在单位	职称	本项目中承担的任务	签字	
	马国蕾	信息与控制工程学院	硕士研究生	标签数量估计		
	丁鑫旺	信息与控制工程学院	硕士研究生	工控系统安全		
	付金楠	信息与控制工程学院	硕士研究生	移动社交网络推荐		
	林凯	信息与控制工程学院	硕士研究生	丢失标签检测		
	刘璐	信息与控制工程学院	硕士研究生	未知标签检测		
<p>项目摘要(限 400 字以内):</p> <p>近年来物联网的发展日新月异,已被广泛应用于石油石化、智能家居、车联网和供应链管理等诸多领域并取得巨大的经济效益。然而,物联网技术的进一步发展受到从感知层、网络层到应用层的诸多因素制约。本项目的前期研究工作分别围绕物联网感知层的邻节点发现和射频识别(RFID)标签监测,网络层的路由、缓存管理和数据包转发激励,应用层的安全定位和位置信息隐私保护等方面展开深入研究,并取得了一些重要的成果,对物联网的技术发展起到一定的推动作用。然而,物联网的发展仍然面临诸多挑战。本项目将继续围绕大规模物联网关键技术展开深入研究,包括邻节点发现、未知标签数目估计和识别、丢失标签数目估计、检测和识别、RFID 系统的安全与隐私保护、移动社交网络推荐、工控物联网安全、无人机远程控制与安全认证等问题。本项目的研究具有重要的理论意义和广泛的应用前景,相关研究成果必将助力于提高我国物联网研究领域的理论层面与技术层面的原始创新能力。</p>						

注: 1. “承担单位”、“合作单位”填写负责人所在院部等二级单位; 2. 项目“隶属学科”填二级或以下学科; 3. 项目组成员“所在单位”填写所在院部等二级单位。4.若为“研究生

创新项目”，则项目组成员中第一位应为其导师。

二、研究目标、主要研究内容

1. 研究目标

邻节点发现：实现邻节点间的快速发现，保障邻节点发现时延的有界以及实现邻节点发现过程的能量高效性。

未知标签数目估计和识别：对 RFID 系统中的未知标签的数目进行估算，使估算精度满足系统要求，并对未知标签进行识别，收集所有未知标签的 ID 信息。

丢失标签数目估计、检测和识别：实现分组 RFID 系统中丢失标签个数的精确估算，对系统中是否存在丢失标签这一事件实现高效检测，并有效识别丢失标签的 ID 信息。

RFID 系统的安全与隐私保护：有效检测 RFID 系统中的典型攻击，包括克隆攻击和阻塞攻击等，并且在标签监测过程中有效保护标签 ID 信息的隐私。

移动社交网络推荐：解决移动社交网络中信息过载条件下的精准推荐，克服推荐系统中用户到项目评级数据的稀疏性。

工控物联网安全问题：从攻/防两方面研究工控物联网的安全问题，包括从攻击方角度的攻击调度策略问题和从防守方的攻击检测问题。

无人机远程控制和认证问题：实现智能手机对无人机的远程控制，通过实时的位置更新，控制无人机的目的地，并且通过有效的安全认证避免无人机被恶意捕获。

2. 主要研究内容

邻节点发现：进一步考虑节点数据包传输的稳定性，即：节点广播的 Beacon 信息可能会产生冲突。首先分析节点广播 Beacon 信息的频率对数据包冲突率和发现时延的关系，设计相应的休眠调度和 Beacon 信息广播策略，解决数据包冲突和发现时延之间的矛盾，通过理论分析和参数优化，保障邻节点发现时延的有界以及实现邻节点发现过程的能量高效性。

未知标签数目估计和识别：阅读器知晓所有已知标签的 ID，可以利用该信息、随机数种子、以及帧长度估计每个时隙的状态，通过检测每个时隙的实际状态和预期状态的变化，构建未知标签个数期望值与相应参数的数学模型关系，实现对未知标签的数量估计。同时，利用采样布鲁姆过滤器（Sampling Bloom Filter）对每个标签进行时隙选择，利用已知标签所选的时隙，对已知标签进行失活，降低其对未知标签识别过程的干扰。当所有已知标签均被失活后，即可对未知标签进行逐一识别。

丢失标签数目估计、检测和识别：利用丢失标签引起的时隙状态的变化，构建

丢失标签个数期望值和相应参数的数学模型关系,通过对状态发生变化的时隙个数的测量实现对丢失标签的个数估计,进一步利用时隙状态的变化,对丢失标签进行检测和识别,并利用片段化技术提高检测和识别效率。

RFID 系统的安全与隐私保护: 分析 RFID 系统中的典型攻击,如克隆攻击和阻塞攻击对时隙状态的影响,通过检测时隙的实际状态和期望状态的区别,实现对攻击的检测。通过合理的标签选择方法设计,避免在标签监测过程中广播标签的 ID,实现标签 ID 信息的隐私保护。

移动社交网络推荐: 为了解决评级矩阵稀疏性的问题,利用将可变卷积神经网络与概率矩阵分解相结合的情景感知推荐系统来获取上下问信息,该方法主要是利用可变卷积提取用户以及项目的情景信息,并为用户和项目建立潜在模型,将用户和项目的潜在模型合并到概率矩阵分解模型中,以此来提高推荐精度。

工控物联网安全问题: 攻击方:当传感器通过物联网发送数据给远端估计器时,存在攻击者恶意破坏通信信道,如拒绝服务攻击(DoS),通过堵塞无线信道来降低估计器的精度,影响系统性能。考虑到攻击者能量受限,攻击者可以发起三种攻击模式,即:不攻击、低能耗和高能耗攻击。在攻击者能量约束条件下,实现对攻击者攻击调度的优化配置,通过建立马尔科夫链模型,把最优问题转化为状态转移概率,再运用马尔科夫的极限概率分布,通过理论推导和实验证明,得到在动态调度下的最优攻击策略。防守方:当有窃听者偷听物联网中的隐私数据,利用收集到的数据推断系统状态或者个人隐私。主要方法为利用差分隐私保护方法,通过对数据进行差异处理,使得变化后的数据与之前无隐私保护的数据相似,但又不会泄漏关键数据。从而能达到对数据隐私的保护。

无人机远程控制和认证: 基于 STM32 芯片,并通过 GSM 模块实现与用户手机之间的远程通信,然后通过 STM32 芯片对接收到的用户数据经过处理后通过一定的通信方式与挂载无人机实现数据传输,从而实现对于无人机的远程控制。给无人机发送目的地位置信息的同时,采集目的地周围 WiFi 热点的 SSID 的信号强度作为指纹信息,一并发送给无人机,无人机在飞抵目的地降落之前,首先进行相应的 SSID 指纹采集,并与用户发送的指纹信息进行匹配,实现安全认证。

三、预期成果及考核指标（预期成果及考核指标应切实可行，须量化可考核）

本项目拟在三年的研究过程中，形成面向大规模物联网关键技术的研究体系，研究成果将以学术论文、发明专利、学术合作、人才培养和学生培养等形式体现，具体包括：

- 在国内外著名学术期刊和会议上发表高水平论文（SCI/EI 检索）5-7 篇，其中 SCI 二区以上至少 3 篇；
- 申请国家发明专利 4-5 项；
- 组织和参加物联网相关领域的国内外学术会议；
- 结合本项目的研究成果，申报国家优秀青年基金项目；
- 结合本项目的研究，培养硕士研究生 4-5 名。

四、项目研究进度计划

1) 2018 年度：

- 分析现有邻节点发现方法不足，研究邻节点的快速、高效发现方法，保障邻节点发现时延的有界性，提高邻节点发现的能量有效性；
- 研究 RFID 系统中的未知标签的数目估算问题，使估算精度满足系统要求，并对未知标签进行识别，收集所有未知标签的 ID 信息；
- 研究分组 RFID 系统中丢失标签个数的精确估算，对系统中是否存在丢失标签这一事件实现高效检测，并有效识别丢失标签的 ID 信息。

2) 2019 年度：

- 研究 RFID 系统中的典型攻击的检测方法，包括克隆攻击和阻塞攻击等，并且在标签监测过程中有效保护标签 ID 信息的隐私；
- 研究移动社交网络中信息过载条件下的精准推荐问题，克服推荐系统中用户到项目评级数据的稀疏性。

3) 2020 年度：

- 从攻/防两方面研究工控物联网的安全问题，包括从攻击方角度的攻击调度策略问题和从防守方的攻击检测问题；
- 研究无人机的远程控制问题，通过实时的位置更新，控制无人机的目的地，并且通过有效的安全认证避免无人机被恶意捕获。

五、经费预算表

经费预算表

(金额单位: 万元)

科目名称	申请经费	计算依据与说明(必填)
1、仪器设备费	1.5	
(1) 购置	1.5	RFID 开发套件: 1.5 万元/套×1 套, 合计: 1.5 万元。
(2) 试制	0.0	
(3) 维修、租赁	0.0	
2、实验材料费	3.6	购置无线通信实验用的电子元件、传感器等: 1.2 万元/年×3 年=3.6 万元。
3、测试化验加工费	0.0	
4、差旅费	2.4	用于项目执行过程中业务调研、学术交流等工作所发生的外埠差旅费、市内交通费等: 0.2 万元/人次×4 人次/年×3 年=2.4 万元。
5、会议费	0.0	
6、国际合作与交流费	0.0	
7、出版物/文献/信息传播费/知识产权事物费	3.0	学术论文版面费: 0.5 万元/篇×2 篇, 国家发明专利代理费: 0.5 万元/项×4 项。合计: 3.0 万元。
8、劳务费	9.0	研究生劳务费: 500 元/人/月×5 人×12 月/年×3 年=9.0 万元。
9、专家咨询费	0.5	邀请国内外教授来校交流: 0.25 万元/人次×2 人次=0.5 万元。
10、其它	0.0	
合 计	20.0	

注: 资助经费不得购置常规性办公耗材或用品, 不得购置通用性办公设备(如计算机、打印机等)。

六、计划任务书各方签约

1. 项目负责人承诺

本人确认本计划任务书及附件内容真实、准确。将严格按照《中国石油大学（华东）自主创新科研计划项目管理办法（试行）》与本计划任务书的规定，认真履行项目负责人职责，积极组织开展研究工作，合理安排研究经费，按时报送有关材料并接受检查。若在项目执行过程中违反有关规定，本人将承担全部责任。

负责人（签字）：

年 月 日

2. 承担单位及合作单位承诺

（1）承担单位

已经按照学校有关规定与项目申报要求对计划任务书内容进行了审核。我单位将根据项目研究内容，落实项目研究所需条件；认真履行项目承担单位的管理职责。

负责人（签字）：

（公章）

年 月 日

（2）合作单位

同意参加合作研究，将按照学校有关规定，认真履行项目合作单位的管理职责。

负责人（签字）：

（公章）

年 月 日

3. 科技处审核意见

负责人（签章）：

（公章）

年 月 日

4. 学校自主创新科研计划领导小组审批意见

负责人（签章）：

年 月 日

七、附件

1. 《中国石油大学（华东）自主创新科研计划项目申请书》
2. 导师推荐书（仅研究生创新基金需要）

项目批准号：16CX02059A

中国石油大学（华东）

自主创新科研计划项目 计划任务书

项目名称：基于非加密技术的资源受限物联网安全问题研究

项目类型：青年基金延续资助项目

所属学科：控制理论与控制工程

负责人：陈鸿龙 联系电话：13573861376

电子邮件：chenhl@upc.edu.cn

依托单位：信息与控制工程学院

研究期限：2016 年 1 月 至 2018 年 12 月

2016 年 5 月 3 日填

计划任务书编制说明

1. 凡列入中国石油大学（华东）自主创新科研计划的项目都应编制此计划任务书。
2. 封面“项目批准号”由学校统一编定。
3. 各项内容要认真填写，文字表达明确、严谨、扼要。文字叙述部分用宋体小4号字。
4. 书面材料均用A4纸双面打印，于左侧胶装成册，封面统一为白色。并提交与纸质材料内容一致的电子版。
5. 该项目的《申请书》作为附件附在后面一起装订。
6. 此计划任务书作为项目中期进度检查和结题验收的依据。
7. 其它有关要求，可参阅《中国石油大学（华东）自主创新科研计划项目管理办法》。

一、基本信息

负责人信息	姓 名	陈鸿龙	性 别	男	出生年月	1984 年 9 月
	最后学位	博士	授予时间	2012 年 10 月	职 称	副教授
	主要研究方向	物联网				
	所属科研机构	信息与控制工程学院				
承担单位		信息与控制工程学院		合作单位		
项目信息	项目名称	基于非加密技术的资源受限物联网安全问题研究				
	隶属学科	控制理论与控制工程			批准金额(万元)	6
	项目类型	A	A.青年基金 B.科技专项 C..研究生创新基金			
	起止时间	2016 年 1 月 至 2018 年 12 月				
	主题词(3 个)	非加密、资源受限、物联网安全				
	预期成果	<input checked="" type="checkbox"/> 专著、论文 <input checked="" type="checkbox"/> 专利 <input type="checkbox"/> 软件 <input type="checkbox"/> 样机、样品 <input type="checkbox"/> 其它				
项目组成员	姓名	所在单位	职称	本项目中承担的任务	签字	
	陈鸿龙	信息与控制工程学院	副教授	项目负责人		
	马国蕾	信息与控制工程学院	硕士研究生	算法仿真与性能验证		
项目摘要(限 400 字以内): 近年来物联网技术的发展日新月异,已被广泛应用于石油石化、智能家居和物流管理等诸多领域,并取得了重大经济效益。然而,随着物联网应用的逐渐深入,网络信息安全与隐私泄露问题日趋严重,极大制约着物联网技术的进一步发展和推广。本项目针对资源受限的物联网,拟利用非加密技术解决从感知层到应用层的安全邻节点发现、RFID 标签安全识别、端到端位置隐私保护和安全定位等安全问题,具体包括:针对感知层的邻节点发现,提出一种能量高效的能够抵御 Sybil 攻击的安全邻节点发现方法;针对感知层的 RFID 标签识别,提出一种能够抵御 Jamming 攻击的标签高效安全识别方法;针对网络层,提出一种能量高效、低延时的数据包传输方法,有效保护端到端的位置隐私;针对应用层,提出一种能够有效抵御虫洞攻击的安全定位方法。本项目将有效解决物联网的安全问题,完善物联网的理论研究,为基于物联网的广泛应用提供理论基础与方法支撑。						

注: 1. “承担单位”、“合作单位”填写负责人所在院部等二级单位; 2. 项目“隶属学科”填二级或以下学科; 3. 项目组成员“所在单位”填写所在院部等二级单位。4.若为“研究生创新项目”,则项目组成员中第一位应为其导师。

二、研究目标、主要研究内容

1. 研究目标

本项目以资源受限物联网安全问题为研究对象，在全面分析物联网节点在带宽、能量和处理能力等资源受限的条件下，研究其从感知层到网络层，再到应用层的信息安全与隐私保护问题，拟实现以下研究目标：

- (1) 提出能量高效、安全的邻节点发现方法，通过网络参数优化配置，有效降低邻节点发现时延和节点能耗，降低最坏情况下的发现时延，利用邻节点发现信息的一致性有效抵御 Sybil 攻击的影响；
- (2) 提出 RFID 系统中 Jamming 攻击检测方法，实现 RFID 标签的快速、安全识别，通过对 Frame 长度、轮次和标签应答概率等网络参数的优化，最大化标签识别效率；
- (3) 提出有效的端到端节点位置信息隐私保护机制，在降低数据包传输时延和节点能耗的同时，增加源节点和汇聚节点的安全周期，有效保护端到端的位置隐私；
- (4) 提出适用于复杂网络通信模型下的安全定位方法，利用网络中节点间信息交互特性，构建节点冲突集，有效辨识并剔除受到虫洞攻击影响的测距信息和节点跳数信息，实现抵御虫洞攻击的安全定位；
- (5) 通过性能仿真和实验测试相结合的方式，验证所提出的信息安全与隐私保护方法的有效性。

2. 主要研究内容

物联网的体系结构可以划分为三个层次：感知层、网络层和应用层。随着物联网的大力发展和广泛应用，信息安全与隐私泄漏问题日趋严重，网络中的恶意攻击节点能够轻易地从上述各层渗透到物联网中，给物联网应用的信息安全与隐私保护带来极大的挑战。本项目面向资源受限的物联网，分别针对其感知层、网络层和应用层，深入研究其安全问题。如图 1 所示，本项目的主要研究内容如下：1) 安全邻节点发现问题；2) RFID 标签安全识别问题；3) 端到端位置隐私保护问题；4) 安全定位问题。

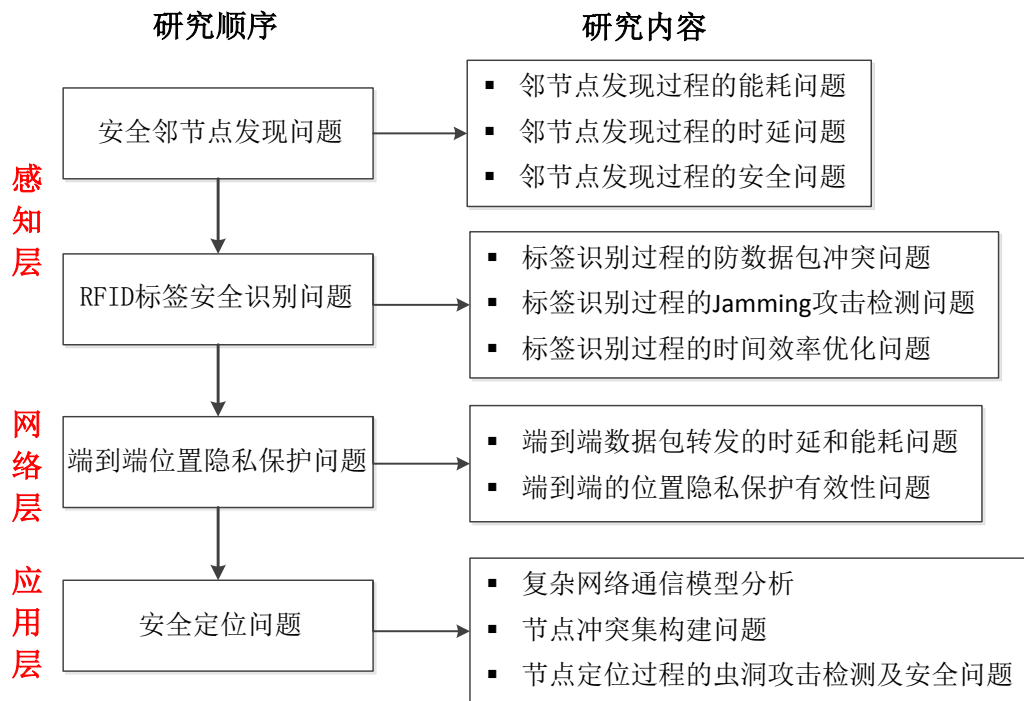


图 1 主要研究内容

三、预期成果及考核指标（预期成果及考核指标应切实可行，须量化可考核）

- 在国内外著名学术期刊和会议上发表高水平论文 4-5 篇，其中 SCI/SCIE 检索至少 3 篇；
- 申请国家发明专利 1-2 项；
- 组织和参加物联网相关领域的国内外学术会议；
- 结合本项目的研究，培养硕士研究生 1-2 名。

四、项目研究进度计划

1) 2016.01-2016.09

- 深入分析现有邻节点发现方法的特点及不足，归纳邻节点发现过程中需要解决的发现时延、节点能耗与安全特性问题；
- 分别提出基于时间槽对齐的和基于时间槽非对齐的能量高效的邻节点发现方法，建立相关数学模型，从理论上分析所提出的邻节点发现方法的时延和节点能耗等性能；
- 提出基于邻节点信息一致性的 Sybil 攻击检测方法，结合邻节点发现方法，综合分析发现时延、节点能耗和安全特性，实现参数的优化配置；
- 仿真实现所提出的安全邻节点发现方法，进行相应的性能分析与比较。

2) 2016.10-2017.06

- 构建 RFID 系统中的标签识别过程的数据包冲突模型，分析数据包冲突对标签识别过程的影响；
- 提出带性能保障的 Jamming 攻击检测方法，有效检测出 RFID 标签识别过程中存在的 Jamming 攻击；
- 提出 RFID 标签快速识别方法，通过理论分析与参数优化，实现标签识别效率的最大化；
- 对所提出的标签安全识别方法进行仿真与实验验证。

3) 2017.07-2018.03

- 构建事件监测系统网络模型关系，分析源节点和汇聚节点的位置隐私重要性；
- 提出真实数据包的传输路径设计方法，有效保护端到端位置隐私的安全性；
- 提出影子数据包的生成和传输机制，有效诱使攻击节点偏离真实数据包的传输路径，进一步提高端到端的位置隐私安全性；
- 分析数据包传输时延、节点能耗以及源节点和汇聚节点位置隐私安全性的模型关系，实现网络参数的优化配置；
- 仿真验证所提出的端到端位置隐私保护方法的有效性。

4) 2018.04-2018.12

- 深入分析复杂网络通信模型下的节点间信息交互特性，提出信标节点的冲突集构建方法；
 - 分析虫洞攻击对节点定位的影响，提出相应的虫洞攻击检测方法；
 - 利用节点间信息交互特性和信标节点的冲突集，提出相应的测距信息和跳数信息的辨识方法，实现安全定位；
 - 对所提出的安全定位方法进行仿真分析和实验验证；
- 汇总以上各阶段研究成果，撰写并提交项目总结研究报告，做好项目验收工作。

五、经费预算表

项目负责人：陈鸿龙

项目批准号：16CX02059A

项目名称：基于非加密技术的资源受限物联网安全问题研究

(金额单位：万元)

科目名称	金额	计算依据与说明
一.研究经费	5.4	
1.科研业务费	3	
(1) 测试/化验/加工费		
(2) 会议费/差旅费	1	项目执行过程中学术交流等工作所发生的外埠差旅费、市内交通费等
(3) 出版物/文献/信息传播费/知识产权事物费	2	购置图书费、打印复印费、版面费、专利代理费等
(4) 其它(说明列应具体阐述)		
2.实验材料费	1.4	以下材料费科目应详细列明需购置材料的名称
(1) 原材料 / 试剂 / 药品购置费		
(2) 其它	1.4	购置无线通信模块、传感器等电子元器件等费用
3.仪器设备费(小型)	1	
(1) 购置	1	购买无线传感器节点等实验设备
(2) 试制		
(3) 维修、租赁		
二.国际合作与交流费		
三.劳务费(详细说明)	0.6	不得超过资助经费的 10%
四.专家咨询费		
合 计	6	

六、计划任务书各方签约

1. 项目负责人承诺

本人确认本计划任务书及附件内容真实、准确。将严格按照《中国石油大学（华东）自主创新科研计划项目管理办法（试行）》与本计划任务书的规定，认真履行项目负责人职责，积极组织开展研究工作，合理安排研究经费，按时报送有关材料并接受检查。若在项目执行过程中违反有关规定，本人将承担全部责任。

负责人（签字）：

年 月 日

2. 承担单位及合作单位承诺

（1）承担单位

已经按照学校有关规定与项目申报要求对计划任务书内容进行了审核。我单位将根据项目研究内容，落实项目研究所需条件；认真履行项目承担单位的管理职责。

负责人（签字）：

（公章）

年 月 日

（2）合作单位

同意参加合作研究，将按照学校有关规定，认真履行项目合作单位的管理职责。

负责人（签字）：

（公章）

年 月 日

3. 科技处审核意见

负责人（签章）：

（公章）

年 月 日

4. 学校自主创新科研计划领导小组审批意见

负责人（签章）：

年 月 日

七、附件

1. 《中国石油大学（华东）自主创新科研计划项目申请书》
2. 导师推荐书（仅研究生创新基金需要）



项目批准号	61872385
申请代码	F020710
归口管理部门	
依托单位代码	25706108A1489-2710



国家自然科学基金委员会 资助项目计划书

资助类别：面上项目

亚类说明：

附注说明：

项目名称：无源物联网中组网关键技术研究

直接费用：64万元 执行年限：2019.01-2022.12

负责人：黄庭培

通讯地址：山东省青岛市黄岛区长江西路66号

邮政编码：266580 电 话：053286980620

电子邮件：huangtingpei@upc.edu.cn

依托单位：中国石油大学（华东）

联系人：谭树成 电 话：053286981837

填表日期：2018年08月17日

国家自然科学基金委员会制



国家自然科学基金委员会资助项目计划书填报说明

- 一、项目负责人收到《关于国家自然科学基金资助项目批准及有关事项的通知》（以下简称《批准通知》）后，请认真阅读本填报说明，参照国家自然科学基金相关项目管理办法及《国家自然科学基金资助项目资金管理办法》（请查阅国家自然科学基金委员会官方网站首页“政策法规”栏目），按《批准通知》的要求认真填写和提交《国家自然科学基金委员会资助项目计划书》（以下简称《计划书》）。
- 二、填写《计划书》时要求科学严谨、实事求是、表述清晰、准确。《计划书》经国家自然科学基金委员会相关项目管理部门审核批准后，将作为项目研究计划执行和检查、验收的依据。
- 三、《计划书》各部分填写要求如下：
 - （一）简表：由系统自动生成。
 - （二）摘要及关键词：各类获资助项目都必须填写中、英文摘要及关键词。
 - （三）项目组主要成员：计划书中列出姓名的项目组主要成员由系统自动生成，与申请书原成员保持一致，不可随意调整。如果批准通知中“项目评审意见及修改意见表”中“对研究方案的修改意见”栏目有调整项目组成员相关要求的，待项目开始执行后，按照项目成员变更程序另行办理。
 - （四）资金预算表：根据批准资助的直接费用，按照《国家自然科学基金项目预算表编制说明》填报资金预算表和预算说明书。国家重大科研仪器研制项目、重大项目还应按照预算评审后批复的直接费用各科目金额填报资金预算表、预算说明书及相应的预算明细表。
 - （五）正文：
 1. 面上项目、青年科学基金项目、地区科学基金项目：如果《批准通知》中没有修改要求的，只需选择“研究内容和研究目标按照申请书执行”即可；如果《批准通知》中“项目评审意见及修改意见表”中“对研究方案的修改意见”栏目明确要求调整研究期限和研究内容等的，须选择“根据研究方案修改意见更改”并填报相关修改内容。
 2. 重点项目、重点国际（地区）合作研究项目、重大项目、国家重大科研仪器研制项目：须选择“根据研究方案修改意见更改”，根据《批准通知》的要求填写研究（研制）内容，不得自行降低、更改研究目标（或仪器研制的技术性能与主要技术指标以及验收技术指标）或缩减研究（研制）内容。此外，还要突出以下几点：
 - （1）研究的难点和在实施过程中可能遇到的问题（或仪器研制风险），拟采用的研究（研制）方案和技术路线；
 - （2）项目主要参与者分工，合作研究单位之间的关系与分工，重大项目还需说明课题之间的关联；
 - （3）详细的年度研究（研制）计划。



3. 国家杰出青年科学基金、优秀青年科学基金和海外及港澳学者合作研究基金项目：须选择“根据研究方案修改意见更改”，按下列提纲撰写：
 - (1) 研究方向；
 - (2) 结合国内外研究现状，说明研究工作的学术思想和科学意义（限两个页面）；
 - (3) 研究内容、研究方案及预期目标（限两个页面）；
 - (4) 年度研究计划；
 - (5) 研究队伍的组成情况。
4. 国家自然科学基金基础科学中心项目：须选择“根据研究方案修改意见更改”，应当根据评审委员会和现场考察专家组的意见和建议，进一步完善并细化研究计划，作为评估和验收的依据。按下列提纲撰写：
 - (1) 五年拟开展的研究工作（包括主要研究方向、关键科学问题与研究内容）；
 - (2) 研究方案（包括骨干成员之间的分工及合作方式、学科交叉融合研究计划等）；
 - (3) 年度研究计划；
 - (4) 五年预期目标和可能取得的重大突破等；
 - (5) 研究队伍的组成情况。
5. 对于其他类型项目，参照面上项目的方式进行选择和填写。



简表

申请者信息	姓 名	黄庭培	性 别	女	出生年月	1980年04月	民 族	土家族
	学 位	博士			职称	讲师		
	是否在站博士后	否			电子邮件	huangtingpei@upc.edu.cn		
	电 话	053286980620			个人网页			
	工 作 单 位	中国石油大学（华东）						
	所 在 院 系 所	计算机与通信工程学院						
依托单位信息	名 称	中国石油大学（华东）					代码	25706108A1489
	联 系 人	谭树成			电子邮件	tsc1980@upc.edu.cn		
	电 话	053286981837			网站地址	http://www.upc.edu.cn/		
合作单位信息	单 位 名 称							
项目基本信息	项 目 名 称	无源物联网中组网关键技术研究						
	资 助 类 别	面上项目				亚 类 说 明		
	附 注 说 明							
	申 请 代 码	F020710:物联网				F020709:新型感知计算及网络		
	基 地 类 别							
	执 行 年 限	2019.01-2022.12						
	直 接 费 用	64万元						



项目摘要

中文摘要:

随着散射通信技术与能量收集技术的不断发展,在未来物联网中,网络节点可以是无源的(Battery-Free),即节点自身不配备或不主要依赖电池等电源设备,而是从环境中获取能量,支撑数据的感知、传输和分布式计算。我们将这种主要由无源设备构成的物联网称为无源物联网。由于通过能量收集获取到的能量不可控、反向散射通信内在的不对称、低功耗、短距离等特性,导致无源物联网在单跳和多跳组网中面临新的挑战。

本申请项目拟以无源物联网中的组网问题为研究对象,对单跳多址接入问题、分布式全双工无源物联网中的干扰问题、多跳无源物联网中的路由问题展开深入研究。拟重点解决以下科学问题:1)能量收集对组网协议的影响问题;2)分布式全双工无源物联网中的干扰再生问题;3)多跳无源物联网中的路由问题。最后,本项目将基于仿真与实验平台相结合的方式开展方法有效性验证。本项目的研究成果将为未来无源物联网的应用提供理论基础与方法支撑。

Abstract:

With the development of backscatter communication and energy-harvesting technologies, in the future Internet of Things, nodes in the network are battery-free. That is, the nodes do not have battery or not mainly rely on battery and other power equipment, and they harvest energy from the environment to perform sensing, communication and distributed computing. We refer to the Internet of Things, which is mainly composed of battery-free devices, as the passive Internet of Things. Because the energy harvested from the environment is uncontrollable, and the internal asymmetry, low power consumption, and short communication distance of backscattering communication, the networking problem in single-hop and multi-hop battery-free Internet of Things faces new challenges.

This project intends to study on the networking problem in passive Internet of Things, including the multi-access problem in single-hop passive Internet of Things, the interference problem in the distributed full-duplex battery-free Internet of Things and the routing problem in the multi-hop battery-free Internet of Things. This project focuses on solving the following key scientific problems: 1) the influence of energy harvesting on the networking protocol; 2) the interference regeneration problem in the distributed full-duplex battery-free Internet of Things; 3) the routing problem in the multi-hop battery-free Internet of Things. Finally, this project will validate the effectiveness of the proposed schemes based on the simulation and experimental platform. The research results of this project will provide the theoretical foundation and methodology support for the further applications of battery-free Internet of Things.

关键词(用分号分开): 无源物联网; 组网; 反向散射通信; 能量收集; 群智感知

Keywords(用分号分开): Battery-Free Internet of Things; Networking Protocol; Backscatter Communications; Energy Harvesting; Crowdsensing



项目组主要成员

编号	姓名	出生年月	性别	职称	学位	单位名称	电话	证件号码	项目分工	每年工 作时间 (月)				
1	黄庭培	1980.04	女	讲师	博士	中国石油大学（华东）	053286980620	422822198004061045	项目负责人	8				
2	陈鸿龙	1984.09	男	副教授	博士	中国石油大学(华东)	0532-86981335	350583198409173113	问题建模、协议设计	4				
3	李世宝	1978.12	男	副教授	硕士	中国石油大学(华东)	15966883535	370727197812294870	网络建模	4				
4	张红霞	1981.07	女	副教授	博士	中国石油大学(华东)	18562056627	650105198107220025	网络建模研究	4				
5	陈海华	1983.06	男	讲师	博士	中国石油大学(华东)	0532-86981969	420983198306250016	调制、编码技术研究	4				
6	马诗源	1995.04	男	硕士生	学士	中国石油大学(华东)	13061410059	210682199504231513	算法、协议实现	8				
7	张宁	1994.01	女	硕士生	学士	中国石油大学(华东)	18724710575	14262319940105612X	算法、协议性能分析与评价	8				
8	姜忠泰	1993.10	男	硕士生	学士	中国石油大学(华东)	18561768190	370687199310110015	算法、协议实现	8				
9	李大伟	1994.12	男	硕士生	学士	中国石油大学(华东)	15763949485	370112199412088017	算法实现	8				
10	董轩江	1994.06	男	硕士生	学士	中国石油大学(华东)	18300231305	142601199406261319	多址接入算法实现	8				
总人数			高级		中级		初级		博士后		博士生		硕士生	
10			3		2		0		0		0		5	



国家自然科学基金项目直接费用预算表（定额补助）

项目批准号：61872385

项目负责人：黄庭培

金额单位：万元

序号	科目名称	金额
1	项目直接费用合计	64.0000
2	1、设备费	4.0000
3	(1)设备购置费	4.0000
4	(2)设备试制费	0.00
5	(3)设备升级改造与租赁费	0.00
6	2、材料费	14.0000
7	3、测试化验加工费	0.00
8	4、燃料动力费	0.00
9	5、差旅/会议/国际合作与交流费	15.0000
10	6、出版/文献/信息传播/知识产权事务费	15.8000
11	7、劳务费	12.8000
12	8、专家咨询费	2.4000
13	9、其他支出	0.0000



预算说明书（定额补助）

（请按《国家自然科学基金项目资金预算表编制说明》中的要求，对各项支出的主要用途和测算理由及合作研究外拨资金、单价≥10万元的设备费等内容进行详细说明，可根据需要另加附页。）

一、直接费用	64.00 万元
1、设备费：	4.00 万元
（1）设备购置费：	4.00 万元
WISP5 开发套件：0.5万元/套×4套，Imote2传感器节点：0.15 万元/个×10 个，调试版MIB520：0.1万元/个×5 个，合计：4.00 万元。	
（2）设备试制费：	0.00 万元
（3）设备改造与租赁费：	0.00 万元
2、材料费：	14.00 万元
无源RFID电子标签、电子元器件、传感器模块、电脑配件、打印纸和硒鼓等耗材费用：3.5 万元/年×4 年，合计：14.00 万元。	
3、测试化验加工费：	0.00 万元
4、燃料动力费：	0.00 万元
5、差旅/会议/国际合作与交流费：	15.00 万元
差旅费：用于项目执行过程中开展科学实验、科学考察、业务调研、学术交流等工作所发生的外埠差旅费、市内交通费等：0.5 万元/人次×4人次/年×4 年=8.00 万元。	
国际合作与交流费：课题组成员出国参加顶级国际会议：1.5 万元/次×2 次=3万元，邀请境外专家来华合作交流：2 万元/次×2 次=4.00 万元。	
合计：15.00万元。	
6、出版/文献/信息传播/知识产权事务费：	15.80 万元
学术论文出版费：0.8 万元/篇×10 篇，专利申请费：0.5 万元/项×4 项，文献检索费：0.25万元/次×8 次，图书购置及打印复印装订等费：3.8 万元，合计：15.80 万元。	
7、劳务费	12.80 万元
硕士生：800 元/人月×5人×8 月/年×4 年=12.80 万元。	
8、专家咨询费	2.40 万元
用于邀请国内专家、教授做学术报告与学术交流：0.2 万元/次×3 次/年×4 年，合计2.40 万元。	
9、其他支出	0.00 万元

项目负责人签字：

科研部门公章：

财务部门公章：



报告正文

研究内容和研究目标按照申请书执行。



国家自然科学基金资助项目签批审核表

	<p>我接受国家自然科学基金的资助，将按照申请书、项目批准意见和计划书负责实施本项目（批准号：61872385），严格遵守国家自然科学基金委员会关于资助项目管理、财务等各项规定，切实保证研究工作时间，认真开展研究工作，按时报送有关材料，及时报告重大情况变动，对资助项目发表的论著和取得的研究成果按规定进行标注。</p> <p>项目负责人（签章）： 年 月 日</p>	<p>我单位同意承担上述国家自然科学基金项目，将保证项目负责人及其研究队伍的稳定和研究项目实施所需的条件，严格遵守国家自然科学基金委员会有关资助项目管理、财务等各项规定，并督促实施。</p> <p>依托单位（公章） 年 月 日</p>					
本栏目由基金委填写	<p>科学处审查意见：</p>						
	<p>建议年度拨款计划（本栏目为自动生成，单位：万元）：</p>						
	年度	总额	第一年	第二年	第三年	第四年	第五年
	金额						
	<p>科学部审查意见：</p> <p>负责人（签章）： 年 月 日</p>						
本栏目主要用于重大项目等	<p>相关局室审核意见：</p> <p>负责人（签章）： 年 月 日</p>						
	<p>委领导审批意见：</p> <p>委领导（签章）： 年 月 日</p>						

资助项目立项任务书

项目基本信息	项目名称	基于拟态安全的空间数据系统安全防护策略研究				
	立项编号	ZR2019MF034		项目类别	面上项目	
	执行期限	2019-07至2022-06		资助经费	20.00万元	
	学科分类	系统安全		学科代码	F020605	
项目承担人信息	姓名	石乐义	性别	男	身份证号	370502197509143211
	电子邮箱	shileyi@upc.edu.cn			联系电话	15192702617
	单位名称	中国石油大学（华东）			专业技术职务	教授
	所在单位(院系)	计算机与通信工程学院			主管部门	中国石油大学（华东）
	所在省级以上重点实验室		无			
项目组成员（与申请书一致，不包含主持人）						
姓名	职称	工作单位	任务分工	每年工作时间（月）	签名	
程子敬	研究员	北京卫星信息工程研究所	CCSDS协议研究	3	程子敬	
陈鸿龙	副教授	中国石油大学（华东）	拟态变换方法研究	5	陈鸿龙	
赵俊楠	在读博士生	中国石油大学（华东）	防护有效机理研究	8	赵俊楠	
郭宏彬	在读硕士生	中国石油大学（华东）	系统攻击测试	8	郭宏彬	
刘娜	在读硕士生	中国石油大学（华东）	系统软切换机制研究	8	刘娜	
马猛飞	在读硕士生	中国石油大学（华东）	系统仿真设计	8	马猛飞	
朱红强	在读硕士生	中国石油大学（华东）	系统攻击测试	8	朱红强	
需呈交科技报告（篇）						
年度进展报告			最终(技术)报告(必须填，一般为1)			
1			1			
注：严格按照科技报告的有关规定呈交科技报告。项目执行中，年度或中期审核前应呈交进展报告；项目完成后三个月内、开展验收前，须呈交最终（技术）报告。未完成科技报告任务的，项目不予结题。						

资助经费预算表 (单位: 万元)

科目	预算经费	备注(计算依据与说明)
项目资助总额	20.00	
一、项目直接费用	17.00	
1、设备费	2.00	
(1)设备购置费	2.00	购置计算服务器1台
(2)设备试制费	0.00	
(3)设备改造与租赁费	0.00	
2、材料费	2.00	U盘、存储条卡、光盘、打印硒鼓等材料
3、测试化验加工费	0.00	
4、燃料动力费	0.00	
5、差旅/会议/国际合作与交流费	2.00	参加国内召开的学术交流会议3次, 参加境外学术交流1次
6、出版/文献/信息传播/知识产权事务费	6.50	发表SCI/EI检索高水平学术论文4-6篇, 申请国家发明专利2-4项
7、劳务费	4.50	参加课题的研究生劳务费
8、专家咨询费	0.00	
9、其他支出	0.00	
二、项目间接经费 (比例:20%)	3.00	
1、绩效支出	2.00	用于课题组成员绩效支出
2、管理费	1.00	5%科研管理费
3、房屋占用/日常水电气暖消耗	0.00	
三、自筹资金	0.00	

项目负责人承诺: 本人接受山东省自然科学基金的资助, 并将严格遵守山东省自然科学基金委员会关于资助项目管理和财务管理的各项规定, 认真开展研究工作, 按照项目申请书中的内容完成各项指标。按时报送有关材料, 及时报告重大变动情况, 对资助项目发表的论著和取得的研究成果按规定进行标注。

项目负责人签字:

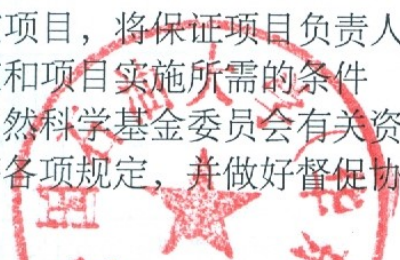
R. Gai

2019 年 5 月 10 日

依托单位审核意见

山东省自然科学基金委员会办公室审查意见

我单位同意承担该项目, 将保证项目负责人及其研究队伍的稳定和项目实施所需的条件, 严格遵守山东省自然科学基金委员会有关资助项目管理、财务等各项规定, 并做好督促协调工作。



依托单位 (公章)

2019 年 5 月 22 日



(公章)

年 月 日

学校教学成果获奖证书

获奖成果：面向智能信息技术需求 培养自动化工程创新人才

主要完成人：刘 宝 王宇红 陈鸿龙 张晓东 张 欣 华陈权 邓晓刚 孙 良 王 钊
盛 立 郝志丹 邢兰昌 陈卫红 王树斌 孟令雅 丛 琳 齐玉娟

获奖等级：二等奖

主要完成单位：控制科学与工程学院

中国石油大学（华东）

二〇一九年十二月

2017年学校优秀教学成果获奖证书

成果名称：自动化专业拔尖创新人才培养计划研究与实践

获奖等级：二等奖

主要完成人：华陈权 王宇红 康忠健 刘 宝 邓晓刚
邢兰昌 邬志丹 孙 良 王 钊 陈鸿龙

中国石油大学（华东）
二〇一七年十一月

2017年学校优秀教学成果获奖证书

成果名称：面向新世纪人才需求 自动化国家特色&教育认证专业协同建设与改革

获奖等级：一等奖

主要完成人：刘 宝 王宇红 华陈权 邓晓刚 孙 良
王 钊 邬志丹 陈鸿龙 邢兰昌 陈卫红
王树斌 孟令雅 盛 立 丛 琳

中国石油大学（华东）

二〇一七年十一月

第二届全国高校自动化类专业
青年教师实验设备设计“创客大赛”

银 奖

所属单位：中国石油大学（华东）

参赛作品：自动化仿真实验系统

参赛教师：陈鸿龙 孙良 王钊 杨明辉 张晓东

主办方

教育部高等学校自动化类专业教学指导委员会
(清华大学代章)

2019年8月

编号：CKDS-2019-12



陈鸿龙

控制科学与工程学院

优秀 教师

中共中国石油大学（华东）委员会

二〇一九年九月

研究生优秀学位论文证书

证书编号: S2019030

学位论文题目: 含未知标签的大规模 RFID 系统中丢失标签检测方法研究

学科专业名称: 控制工程

论文作者姓名: 林 凯

指导教师姓名: 陈鸿龙

学位论文等级: 2019年中国石油大学优秀硕士学位论文论文

中国石油大学(华东)

2019年9月11日

中国石油大学 (华东)

CHINA UNIVERSITY OF PETROLEUM

优秀本科毕业设计 (论文) 证书

学生姓名: 黄杨

论文题目: 移动群智感知系统中面向任务的员工招募方法研究

专业名称: 自动化

指导教师: 陈鸿龙

中国石油大学 (华东)

2019 年 6 月

中国石油大学 (华东)

CHINA UNIVERSITY OF PETROLEUM

优秀本科毕业设计 (论文) 证书

学生姓名: 夏斯港

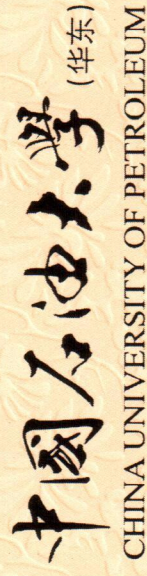
论文题目: 基于 FPGA 的相对延时脉冲发生器设计

专业名称: 自动化

指导教师: 陈鸿龙

中国石油大学 (华东)

2019 年 6 月



优秀本科毕业设计 (论文) 证书

学生姓名: 张绪新

论文题目: 无线传感器网络中的时钟同步技术研究

专业名称: 自动化

指导教师: 陈鸿龙



教育部办公厅

教高厅函〔2019〕46号

教育部办公厅关于公布 2019 年度国家级和 省级一流本科专业建设点名单的通知

各省、自治区、直辖市教育厅(教委),新疆生产建设兵团教育局,有关部门(单位)教育司(局),部属各高等学校、部省合建各高等学校:

为深入贯彻落实全国教育大会精神,贯彻落实新时代全国高校本科教育工作会议精神 and 《教育部关于加快建设高水平本科教育 全面提高人才培养能力的意见》、“六卓越一拔尖”计划 2.0 系列文件等要求,全面振兴本科教育,提高高校人才培养能力,实现高等教育内涵式发展,根据《教育部办公厅关于实施一流本科专业建设“双万计划”的通知》(教高厅函〔2019〕18号),经各高校网上申报、高校主管部门审核,教育部高等学校教学指导委员会评议、投票,我部认定了首批 4054 个国家级一流本科专业建设点,其中中央赛道 1691 个、地方赛道 2363 个(名单见附件 1)。同时,经各省

级教育行政部门审核、推荐,确定了 6210 个省级一流本科专业建设点(名单见附件 2)。现将 2019 年度国家级和省级一流本科专业建设点名单予以公布。各地各高校要持续努力,认真实施好一流专业建设“双万计划”。

一、完善专业建设规划。各地各高校要按照一流专业建设条件,完善本科专业建设三年规划,统筹实施好国家级和省级一流本科专业建设计划。要健全专业动态调整机制,做好专业优化、调整、升级、换代和新建工作,加快国家急需专业建设,持续改进专业布局结构。

二、持续提升专业水平。对首批入选的专业建设点,各地各高校要完善支持措施,持续加强建设,不断夯实基础、改善条件。要坚持需求导向、标准导向、特色导向,以社会需求为前提,以一流专业标准为参照,强化专业特色,持续提升专业内涵和建设水平。要以专业认证促进专业高质量发展,落实“学生中心、产出导向、持续改进”的理念,建强用好基层教学组织,形成以提高人才培养水平为核心的质量文化。

三、发挥示范领跑作用。一流专业建设点要以新思想、新理念、新技术、新方法、新标准、新体系为引领,建设一批新工科、新医科、新农科、新文科示范性本科专业,建设一批适应创新型、复合型、应用型人才培养需要的一流本科课程,在专业改革创新、师资队伍、教学资源、质量保障体系等各方面发挥示范辐射作用。

附件:1. 2019 年度国家级一流本科专业建设点名单

2. 2019 年度省级一流本科专业建设点名单



Editorial Leadership and Staff

Editor-in-Chief

Editorial Board [A-F](#) [G-K](#) [L-Q](#) [S-Z](#)

Associate Editors

Staff

Associate Editors

[Outstanding Associate Editors](#)

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)



Thank you to our Outstanding Associate Editors of 2018 for their outstanding contributions to IEEE Access throughout 2018.

[View our Outstanding Associate Editors of 2018](#)

The IEEE Access Associate Editors are responsible for ensuring that the publication maintains the highest quality while adhering to the publication policies and procedures of IEEE.

To apply or recommend a colleague for an Associate Editor position at IEEE Access, please [complete the nomination form](#).

A

Khalid Mahmood Aamir
University of Sargodha, Pakistan

Andrea Abate
University of Salerno, Italy

Haider Abbas
National University of Sciences & Technology, Pakistan

Qammer Abbasi
University of Glasgow, UK

Derek Abbott
University of Adelaide, Australia

Berdakh Abibullaev
Nazarbayev University, Kazakhstan

[Back to top of list](#)

At a Glance

- Journal: IEEE Access
- Format: Open Access
- Frequency: Continuous
- Submission to publication: 4-6 weeks (typical)
- Topics: All topics in IEEE
- Model: Binary Peer Review
- Impact factor: 4.098
- Article processing charge: US \$1,750

[Learn More](#)

Featured Articles

- [Printed Circuit Board Implementation of Wideband Radial Power Combiner](#)
- [User Grouping for Hybrid VLC/RF Networks With NOMA: A Coalitional Game Approach](#)
- [On the Automated Management of Security Incidents in Smart Spaces](#)
- [An Experimental-Based Review of Image Enhancement and Image Restoration Methods for Underwater Imaging](#)

[View All](#)

Submit an Article

Learn about article acceptance requirements, who is eligible to publish, types of submissions encouraged, and tools to help you submit.

[Learn More](#)

Announcements

- [IEEE Access: Now Over 25,000 Articles Published](#)
- [IEEE Access welcomes new Managing Editor, Jenny Mahoney](#)
- [IEEE Access: Now Over 20,000 Articles Published](#)
- [IEEE Access Impact Factor Increases to 4.098](#)

Sudipta Chattopadhyay

Mizoram University, India

Periklis Chatzimisios

Alexander TEI of Thessaloniki, Greece

Raghvendra Chaudhary

Indian Institute of Technology (ISM), India

Kuan Chee

University of Nottingham, UK

Hongbin Chen

Guilin University of Electronic Technology, China

Yang Chen

Fudan University, China

Wen Chen

The Hong Kong Polytechnic University, Hong Kong

Zheng Chen

Zhejiang University, China

Honglong Chen

China University of Petroleum, China

Mu-Yen Chen

National Taichung University of Science and Technology, Taiwan

Zhiyong Chen

Shanghai Jiao Tong University, China

Fei Chen

Northeastern University, China

Yanbo Chen

North China Electric Power University, China

Liang-Bi Chen

Southern Taiwan University of Science and Technology, Taiwan

Chi-Yuan Chen

National Ilan University, Taiwan

Poki Chen

National Taiwan University of Science and Technology, China

Xue-wen Chen

Wayne State University, USA

Wen Chen

Shanghai Jiao Tong University, China

Xu Chen

Sun Yat-Sen University, Guangzhou, China

Huiling Chen

Wenzhou University, China

Yu-Chi Chen

Yuan Ze University, Taiwan

Baile Chen

Shanghai Tech University, China

Kang Chen

Southern Illinois University Carbondale, USA

Yanjiao Chen

Wuhan University, China

Xiang Chen

Nantong University, China

Qingchun Chen

Southwest Jiaotong University, China

Chao-Yang Chen

Hunan University of Science & Technology, China

Xun Chen