佐证材料清单

1. 成员身份证明

2. 相关学术论文

3. 相关专利

4. 教改论文

5. 教育部就业育人项目

6. 校教改项目

7. “本科课程思政优秀教学案例”一等奖

项目主持人情况证明

项目主持人，**彭景惠**，**女**，30 岁，讲师，目前是广东技术师范大学网络空间安全学院在职人员（青年教师）。

项目组成员情况表

姓名	性别	年龄	职称	工作单位	分工	人员类别
张瑜	男	48	教授	广东技术师范大学	理论指导	普通教师
罗建桢	男	39	副教授	广东技术师范大学	实践指导	中层干部
陈桂宏	女	40	副教授	广东技术师范大学	线上课程	普通教师
欧阳佳	男	37	讲师	广东技术师范大学	线上平台	普通教师
陈兵	男	37	讲师	广东技术师范大学	技术指导	普通教师

特此证明！

教务处盖章：

广东技术师范大学 教务处 4401060069133

2023年7月6日

检索证明

根据委托人提供的论文材料，委托人**中国地质大学计算机学院/ 西伦敦大学彭景惠Jinghui Peng**3篇论文收录情况如下表。

序号	论文名称	发表刊物及发表的年月卷期/页码等	作者排名	作者文中单位	收录情况	影响因子	中科院大类分区
1	Security of Streaming Media Communications with Logistic Map and Self-Adaptive Detection-Based Steganography	IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING 出版年：2020 卷期：　页码：- 文献类型：	第一作者	School of Computer Science, China University of Geosciences	已在线发表，暂未被SCI收录	IF2-year=6.864 IF5-year=5.9 (2019)	工程技术　2区 Top期刊：是 (2019)
2	Information retrieval of mass encrypted data over multimedia networking with N-level vector model-based relevancy ranking	MULTIMEDIA TOOLS AND APPLICATIONS 出版年：2017　JAN 卷期：76　2 页码：2569-2589 文献类型：Article	第一作者	School of Computer Science, China University of Geosciences	SCI	IF2-year=1.541 IF5-year=1.471 (2017)	工程技术　4区 Top期刊：否 (2017)
3	Covert Communication over VoIP Streaming Media with Dynamic Key Distribution and Authentication	IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING 出版年：2020 卷期：　页码：- 文献类型：	第一作者	University of West London	已在线发表，暂未被SCI收录	IF2-year=6.864 IF5-year=5.9 (2019)	工程技术　2区 Top期刊：是 (2019)

检索员：田成
华南农业大学图书馆
2020-07-17

Security of Streaming Media Communications with Logistic Map and Self-Adaptive Detection-Based Steganography

Jinghui Peng, Yijing Jiang, Shanyu Tang, and Farid Meziane, *Fellow, BCS*

Abstract—Voice over IP (VoIP) is finding its way into several applications, but its security concerns still remain. This paper shows how a new self-adaptive steganographic method can ensure the security of covert VoIP communications over the Internet. In this study an Active Voice Period Detection algorithm is devised for PCM codec to detect whether a VoIP packet carries active or inactive voice data, and the data embedding location in a VoIP stream is chosen randomly according to random sequences generated from a logistic chaotic map. The initial parameters of the chaotic map and the selection of where to embed the message are negotiated between the communicating parties. Steganography experiments on active and inactive voice periods were carried out using a VoIP communications system. Performance evaluation and security analysis indicates that the proposed VoIP steganographic scheme can withstand statistical detection, and achieve secure real-time covert communications with high speech quality and negligible signal distortion.

Index Terms— Security, VoIP, streaming communications, steganography

1 Introduction

With the development of the Internet, text messaging alone is hard to meet people's demands for multimedia communications. Internet users need more direct and vivid modern ways of communication, such as audio or video communications. Voice over Internet Protocol (VoIP) is one of the most popular audio communications services on the Internet. VoIP is finding its way into several applications, and it is expected to become a service like electricity or water.

The Internet enables VoIP to provide reliable, global, low-cost and/or even free services, so many users communicate with each other daily using VoIP products, leading to increasing traffic of VoIP streams transmitted over the Internet. Due to the highly redundant representation in VoIP streams, VoIP is considered to be a dynamic cover object for steganography compared with static cover objects such as text, image and audio files [1-2]. As an interesting subject in the field of information security, steganography or covert communication (channel) works by hiding messages in inconspicuous cover objects (e.g. VoIP streams) that are then sent to the intended recipient [1]. Steganography can provide an additional layer of security in addition to encryption by embedding the encrypted message into steganographic carriers, which helps individuals or organisations protect sensitive information. For example, a message can be steganographically embedded into the least significant bits of frames on a CD. Covert steganographic channels can be used to bypass the censorship in a hostile environment. The covert channel can also be used by the adversary as a possible means of information exchange. A message can be concealed before distribution by splicing it to the end of a copy of a normal audio or video. A disgruntled employee may use steganography to ship out the most commercially sensitive information.

VoIP provides real-time audio communication services over the Internet, and VoIP packets are discarded immediately on arrival. That means that attackers do not normally have sufficient time to detect whether VoIP dynamic streams contain the hidden message or not. The real-time character of VoIP is useful in protecting the message hidden in their streams; however, the real-time requirements make it hard to perform necessary operations to embed the message into the streams without causing signal distortion.

VoIP communications consist of two phases: signalling phase and conversation phase. The signalling phase sets up and negotiates VoIP session parameters between the communicating parties. The most popular signalling protocol is called Session Initiation Protocol (SIP). As mutual authentication is a cryptographic scheme used to convince parties of each other's identity and to exchange session keys, it is typically used only when an extra level of security is needed, especially in VoIP communications [3]. Some key agreement protocols and authentication

- *J. Peng is with the School of Computer Science, China University of Geosciences, Wuhan, China. E-mail: 826625501@qq.com; University of West London, London W5 5RF, UK. E-mail: 21368391@student.uwl.ac.uk.*
- *Y. Jiang is with the School of Computer Science, China University of Geosciences, Wuhan, China. E-mail: yijingjiang2012@gmail.com.*
- *Prof. S. Tang is with the School of Computing and Engineering, University of West London, London W5 5RF, UK. E-mail: Shanyu.Tang@uwl.ac.uk.*
- *Prof. F. Meziane is with the School of Computing, Science and Engineering, University of Salford, Salford M5 4WT, UK. E-mail: F.Meziane@salford.ac.uk.*

Covert Communication over VoIP Streaming Media with Dynamic Key Distribution and Authentication

Jinghui Peng, Shanyu Tang, *FBCS*

***Abstract*—Voice over Internet Protocol (VoIP) is widely embedded into commercial and industrial applications. VoIP streams can be used as innocuous cover objects to hide secret data in steganographic systems. The security offered by VoIP signalling protocols is likely to be compromised due to a sharp increase in computing power. This paper describes a theoretical and experimental investigation of covert steganographic communications over VoIP streaming media. A new information theoretical model of secure covert VoIP communications was constructed to depict the security scenarios in steganographic systems against passive attacks. A one way accumulation-based steganographic algorithm was devised to integrate dynamic key updating and exchange with data embedding and extraction, so as to protect steganographic systems from adversary attacks. Theoretical analysis of steganographic security using information theory proves that the proposed model for covert VoIP communications is secure against a passive adversary. The effectiveness of the steganographic algorithm for covert VoIP communications was examined by means of performance and robustness measurements. The results reveal that the algorithm has no or little impact on real-time VoIP communications in terms of imperceptibility, speech quality and signal distortion, and is more secure and effective at improving the security of covert VoIP communications than other related algorithms with comparable data embedding rates.**

***Index Terms*—Authentication, covert communication, key distribution, steganography, VoIP.**

I. Introduction

THE past decade has witnessed the rapid development of embedded Voice over Internet Protocol (VoIP) for commercial and industrial applications. Widening access to the Internet greatly facilitates the use of multimedia applications in people's daily lives. Evolving network technology such as streaming has enjoyed a rise in popularity. However, security measures are struggling to keep up with the pace of change in attack tactics.

Encryption and decryption technologies are normally used to address data security and privacy issues. There are symmetric encryption and public-key encryption that enable the translation of a plaintext message into ciphertext. However, an increase in computing power has led to decryption of several encryption algorithms, such as MD5 [1], DES [2] and SHA-1 [3], indicating possible vulnerabilities in the encryption primitives. It is generally recognised that encrypted messages are obvious, and when intercepted, it is clear that the communicating parties are communicating secretly.

As a sub-branch, digital steganography is defined as 'the art of concealed communication by hiding messages in seemingly innocuous objects' and 'the very existence of a steganographic message is secret' [4]. Steganography in static cover objects, such as text, BMP or JPEG images, and WAV or MP3 audio files, has been explored extensively [5]-[7]. Network protocols and streaming media [8], such as VoIP, are also used to realise covert steganographic communications.

There has been a large body of research into steganographic algorithms for covert communications over streaming media, but the key distribution problem in covert steganographic communications has been sidestepped. In fact, the successfulness of steganographic algorithms for covert communications relies largely on the transmission of secret keys between the communicating parties. Security in transmission of secret keys is more crucial for covert VoIP communications because of the timing and loss of packets, i.e. covert VoIP communications require continuous embedding and necessary synchronization between the communicating parties. So far there are no reliable and secure key transmission schemes that could be put into use for covert VoIP communications. Thus, secure key transmission for covert steganographic communications is worth studying apart from designing effective steganographic algorithms for them.

The main purpose of this study is to explore the potential of one way accumulation-based dynamic key updating and transmission for innovative applications in the field of covert

Manuscript received July 30, 2019; revised October 14, 2019; accepted February 26, 2020. This work was supported in part by various industrial sponsors under Grant 28801.

J. Peng and S. Tang are with the University's Centre for Cybersecurity and Criminology, University of West London, London, W5 5RF, UK (e-mail: jinghui.peng0826@gmail.com; corresponding author: S. Tang; phone: +44 (0)20 8231 2948; e-mail: shanyu.tang@uwl.ac.uk).

Multimed Tools Appl (2017) 76:2569–2589
DOI 10.1007/s11042-015-3224-y

Information retrieval of mass encrypted data over multimedia networking with N-level vector model-based relevancy ranking

Jinghui Peng[1] · Shanyu Tang[1,2] · Liping Zhang[1] · Ran Liu[1]

Received: 17 July 2015 / Revised: 4 December 2015 / Accepted: 29 December 2015 /
Published online: 18 January 2016

Abstract With an explosive growth in the deployment of networked applications over the Internet, searching the encrypted information that the user needs becomes increasingly important. However, the information search precision is quite low when using Vector space model for mass information retrieval, because long documents having poor similarity values are poorly represented in the vector space model and the order in which the terms appear in the document is lost in the vector space representation with intuitive weighting. To address the problems, this study proposed an N-level vector model (NVM)-based relevancy ranking scheme with an introduction of a new formula of the term weighting, taking into account the location of the feature term in the document to describe the content of the document properly, investigated into ways of ranking the encrypted documents using the proposed scheme, and conducted realistic simulation of information retrieval of mass encrypted data over multimedia networking. Results indicated that the timing of the index building, the most costing part of the relevancy ranking scheme, increased with the increase in both the document size and the multimedia content of the document being searched, which is in agreement with the expected. Performance evaluation demonstrated that our specially designed NVM-based encrypted information retrieval system is effective in ranking the encrypted documents transmitted over multimedia networks with large recall ratio and great retrieval precision.

Keywords Encrypted data retrieval · N-level vector model · Relevancy ranking · Multimedia security

✉ Shanyu Tang
shanyu.tang@gmail.com

[1] School of Computer Science, China University of Geosciences, 388 Lumo Road, Wuhan, Hubei Province 430074, Peoples Republic of China

[2] University of Salford, Salford M5 4WT, UK

World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:13, No:7, 2019

Fast Fourier Transform-Based Steganalysis of Covert Communications over Streaming Media

Jinghui Peng, Shanyu Tang, Jia Li

Open Science Index, Computer and Information Engineering Vol:13, No:7, 2019 waset.org/Publication/10010544

Abstract**—**Steganalysis seeks to detect the presence of secret data embedded in cover objects, and there is an imminent demand to detect hidden messages in streaming media. This paper shows how a steganalysis algorithm based on Fast Fourier Transform (FFT) can be used to detect the existence of secret data embedded in streaming media. The proposed algorithm uses machine parameter characteristics and a network sniffer to determine whether the Internet traffic contains streaming channels. The detected streaming data is then transferred from the time domain to the frequency domain through FFT. The distributions of power spectra in the frequency domain between original VoIP streams and stego VoIP streams are compared in turn using t-test, achieving the p-value of 7.5686E-176 which is below the threshold. The results indicate that the proposed FFT-based steganalysis algorithm is effective in detecting the secret data embedded in VoIP streaming media.

Keywords**—**Steganalysis, security, fast Fourier transform, streaming media.

I. Introduction

COVERT communication can be used to transmit confidential information on mobile telecommunications. There are three main ways to implement it: secure channel, encryption technology and information hiding. The secure channel is a private communications path established by the communicating parties, which is not accessible for others. It has high security but high cost and poor extensibility. Encryption technology largely depends on the length of the key used for encryption and decryption. As computer processing capabilities increase rapidly, it becomes less reliable to increase system security by increasing the key length. Digital steganography has drawn people’s attention in the field of information hiding. Based on encryption technology, it embeds confidential information into seemingly innocuous transmissions, that is, the encrypted confidential information is “invisible”, which is unlikely to be detected by attackers, thus reducing the probability of confidential information being attacked. From the perspective of information transmission security, steganography is one of the most advanced information hiding technologies.

A new generation of mobile telecommunications has emerged as a result of advances in wireless communications and mobile terminal technology. The third generation of mobile telecommunications technology (referred to as 3G) adopts the IMT-2000 international standard, which offers voice service, higher data transfer rates (200 kbps), broadband multimedia communications, and wireless access to the Internet. The fourth generation of mobile telecommunications (referred to as 4G), using OFDMA and MIMO (TD-LTE), is designed to provide high-speed (100 Mbps) data transmission services such as VoIP and IP Multimedia Subsystem (IMS), with a fibre broadband experience similar to a fixed-line network. With the advent of the era of 3G and 4G, streaming media such as VoIP has been widely used on the mobile Internet, providing a new dynamic cover object for information hiding, especially steganography.

Streaming media steganography has attracted the attention of information security experts all over the world. On the one hand, streaming media contain plenty of redundancy, which can be used to hide confidential information. Compared with image, audio, text and other multimedia files and network channels, streaming media are better cover objects. On the other hand, the widespread use of streaming media on mobile telecommunications networks has portrayed a variety of new mobile Internet services: mobile instant messaging, mobile TV, mobile content sharing, mobile E-reading, mobile social, mobile advertising and so on. Therefore, steganography in streaming media has broad application prospects in the field of mobile Internet.

Steganalysis, the countermeasure technology of covert communication in the field of information hiding, is developing rapidly with the strong demand of investigation into covert communication. Steganographic technology is very likely to be exploited by hostile agents, terrorists and evil forces. By hiding their secret information in streaming media, they intend to avoid content scrutinising and tracing, and use it to organise crimes and terrorist activities, and steal military and commercial information. It would endanger national and public security, and undermine social stability. Therefore, with the rapid development of mobile Internet, it is imminent to develop steganalysis technology for mobile networks, especially steganalysis of streaming media steganography. At present, research in streaming media steganalysis on the mobile Internet is at an early stage, and few preliminary results have been published.

This study was aimed to devise a steganalysis method for streaming media that are ubiquitous on the mobile Internet and explore ways of universal and real-time detection and countermeasure of steganography in streaming media on the mobile Internet.

J. Peng and S. Tang are with the School of Computing and Engineering, University of West London, London, UK (e-mail: 21368391@student.uwl.ac.uk, shanyu.tang@ uwl.ac.uk).

J. Li is with the Freelance Consultancy, Merton, London, UK (e-mail: lily.jjl@gmail.com).

Engineering Applications of Artificial Intelligence ∎ (∎∎∎∎) ∎∎∎–∎∎∎

Contents lists available at ScienceDirect

Engineering Applications of Artificial Intelligence

journal homepage: www.elsevier.com/locate/engappai

Multiple-negative survey method for enhancing the accuracy of negative survey-based cloud data privacy: Applications and extensions☆

Ran Liu [a,b], Jinghui Peng [a], Shanyu Tang [a,b,*]

[a] School of Computer Science, China University of Geoscience, Wuhan, Hubei 430074, China
[b] Hubei Key Laboratory of Intelligent Geo-Information Processing, China University of Geosciences, Wuhan 430074, China

ARTICLE INFO

Article history:
Received 9 January 2016
Received in revised form
10 May 2016
Accepted 6 June 2016

Keywords:
Artificial immune system
Cloud data privacy
Multiple-negative survey
Confidence level
Bayes method
Anonymity vote model

ABSTRACT

Cloud computing brings convenience to people's lives because of its high efficiency, usability, accessibility and affordability. But the privacy of cloud data faces severe challenges. Although negative survey, which is inspired by Artificial Immune System (AIS), can protect users' privacy data with high efficiency and degree of privacy protection, its accuracy is influenced by the number of client terminals, and insufficient client terminals may lead to large errors. This study focuses on a multiple-negative survey method of remedying this weakness. Compared with the traditional negative survey method, the multiple-negative survey method collects each user's multiple different negative categories rather than only one negative category. Two key scientific problems (accuracy and confidence level) are analyzed, and an application (anonymity vote model) is then proposed based on the multiple-negative survey method.

1. Introduction

Inspired by negative selection principle (Hofmeyr and Forrest, 2000), which is an essential mechanism of Artificial Immune System (AIS), the negative selection algorithm (Forrest et al., 1994) has been proposed and used in network security and virus detection. The negative selection algorithm can generate a set of detectors unmatched by itself. If a sample is matched by a detector, the sample is marked as “nonself”, otherwise it is marked as “self”. Negative representation (Esponda, 2008), which is inspired by the negative selection algorithm and Artificial Immune System (AIS), is a new kind of information representation. Different from the general information representation, negative representation stores the contents not consistent with the real information. Existing work (Esponda et al., 2004, 2005, 2007) showed that reversing a negative representation (such as negative databases) to get the original information equals to solve a SAT formula. Based on this kind of property, negative representation can be used for information security (Esponda et al., 2007). As shown in Zhao et al., negative representation can be used for iris recognition.

In recent years, users face cloud data privacy protection problems with the advent of cloud computing and intelligent computing techniques. Cloud data privacy protection affects the high efficiency of cloud computing to a certain degree. So reducing the amount of background calculations to the cloud data privacy protection in client terminal is an urgent issue. Negative survey (Esponda, 2006; Esponda and Guerrero, 2009), which is inspired by the negative representation of information, could protect the privacy of participants effectively while collecting information. In Horey et al. (2007), negative survey is used for anonymous collection of traffic behavior. Furthermore, negative survey method (Esponda et al., 2016) allows each participant to select different number of negative categories to customize its own privacy degree. Negative surveys only collect parts of the negative categories, so this method can increase operating speeds by saving the tedious encryption process. Meanwhile, how to enhance the accuracy (Bao et al., 2013) of converting negative survey results into positive survey results is one of the key issues in negative surveys.

The main research (Esponda and Guerrero, 2009; Horey et al., 2007; Bao et al., 2013, 2014; Xie et al., 2011; Lu et al., 2014; Liu et al., 2015) of present work focuses on the traditional negative survey (symbolized as 1-NS). Only limited work (Esponda et al., 2016; Bao et al., 2014) discusses the multiple-negative survey. In consequence, the content of this study is enhancing the accuracy of negative survey-based cloud data privacy by multiple-negative survey, i.e. each participant selects multiple different negative

☆An earlier abbreviated version of this paper was presented as the ICSI3 2015, Taormina, Italy, 17–18 July 2015.

*Corresponding author at: School of Computer Science, China University of Geoscience, Wuhan, Hubei 430074, China.
E-mail address: shanyu.tang@gmail.com (S. Tang).

http://dx.doi.org/10.1016/j.engappai.2016.06.002
0952-1976/© 2016 Elsevier Ltd. All rights reserved.

Please cite this article as: Liu, R., et al., Multiple-negative survey method for enhancing the accuracy of negative survey-based cloud data privacy: Applications and extensions. Eng. Appl. Artif. Intel. (2016), http://dx.doi.org/10.1016/j.engappai.2016.06.002

Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2015, Article ID 958154, 9 pages
http://dx.doi.org/10.1155/2015/958154

Research Article

An Efficient Approximation Method for Calculating Confidence Level of Negative Survey

Ran Liu, Jinghui Peng, and Shanyu Tang

School of Computer Science, China University of Geosciences, Wuhan, China

Correspondence should be addressed to Shanyu Tang; shanyu.tang@gmail.com

Received 27 April 2015; Revised 23 July 2015; Accepted 2 September 2015

Academic Editor: Ofer Hadar

The confidence level of negative survey is one of the key scientific problems. The present work uses generation function to analyse the confidence level and uses a greedy algorithm to calculate that, which is used to evaluate the dependable level of negative survey. However, the present method is of low efficiency and complex. This study focuses on an efficient approximation method for calculating the confidence level of negative survey. This approximation method based on central limit theorem and Bayesian method can get the results efficiently.

1. Introduction

Artificial immune system simulates the mechanism of biology immune system to model and design effective algorithm for solving some complex issues. Negative selection principle [1] is one of the unique mechanisms of biology immune system, and the implication of negative selection principle is that the immaturity T cell dies if it *matches* with itself as it grows, and it survives if it *mismatches* with itself. Inspired by negative selection principle, the negative selection algorithm [2] is proposed and can be used for network security, virus detection [3, 4], and anomaly detection [5].

Similarly, the negative survey [6], which is inspired by negative selection principle, is a novel and promising indirect question method for information security and enhancing privacy in collecting sensitive data and individual privacy [7]. Negative surveys consist of a question and c $(c \geq 3)$ categories for the interviewees to select from. In contrast to traditional surveys, the participants are required to select a category that does *not* agree with the fact [6, 8]; that is, randomly select a category from the other $c-1$ unreal categories. For convenience, it defines *positive category* as the category that agrees with the fact, while it defines *negative category* as the other $c-1$ categories that do *not* agree with the fact [6].

The negative survey method can attain privacy protection with lower power and higher degree and boost participants' confidence. The main calculation of collecting sensitive data with negative survey is reconstructing the corresponding positive survey in the central processor. The privacy preserving properties of negative survey do not rely on anonymity, cryptography, or any legal contracts, but rather participants not revealing their own privacy information. And the negative survey method is applicable to collecting data at a high speed in low-powered mobile devices such as smart phones and tablets [9].

The positive survey can be reconstructed from a result of negative survey. For a survey consisting of a question and c $(c \geq 3)$ categories for n interviewees to select from, a negative survey result is $R = (r_1, r_2, \ldots, r_c)$, where r_i is the results of category i in negative survey. Meanwhile, the original positive survey is $T = (t_1, t_2, \ldots, t_c)$, where t_i is the number of interviewees belonging to category i. Define $v_{i,j}$ as the probability that category i is chosen given that a respondent positively belongs to category j, where $\sum_{i=1}^{c} v_{i,j} = 1$ and $v_{i,i} = 0$. Define the probability matrix as V as Formula (1), and $R = TV$ and $T = RV^{-1}$. In consequence, the positive survey T can be reconstructed from a negative survey R:

$$V = \begin{bmatrix} 0 & v_{1,2} & \cdots & v_{1,c} \\ v_{2,1} & 0 & \cdots & v_{2,c} \\ \vdots & \vdots & \ddots & \vdots \\ v_{c,1} & v_{c,2} & \cdots & 0 \end{bmatrix}. \quad (1)$$

Security Issues of Cognitive Radio Communications Technology

Jinghui Peng[1], Li Pan[2], Shanyu Tang[1]

[1] School of Computing and Engineering, University of West London, St Mary’s Road,
London W5 5RF, UK. E: shanyu.tang@uwl.ac.uk
[2] School of Computer Science, China University of Geosciences, 388 Lumo Road,
Wuhan, 430074, China

Abstract

As a communication technology, Cognitive Radio (CR) systems are vulnerable to various malicious attacks, both traditional wireless attacks and some new classes of security threats. Thus, it is essential to strengthen its security to make CR viable and reliable for creative industrial applications. Primary User Emulation attacks are one of the most detrimental attacks on CR networks. If a malicious or selfish node apes the signal characteristics of a Primary User (PU), it will impair both a PU and a Second User (SU) by meddling with the former and thwarting the latter from accessing communication channels. This study discusses existing measures against cyber attacks, analyses deficiencies in these solutions, and then proposes a new security scheme, which is based on Trust Authentication Centre (TAC), using a Hash function and Public Key Cryptosystem (PKC) to distinguish between attacks and PUs. Security analysis and experimental results show that the proposed scheme reduced the execution time and memory space of SUs.

Keywords:
Cognitive radio; Spectrum sensing; Primary User Emulation attack; Sora

Introduction

With the rapid development of communication technologies, spectrum resources become more and more scarce. Previous studies have indicated that the shortage of radio spectral resource is getting serious day by day because the spectrum allocation policy is not adequate. To improve the utilisation of spectrum allocation, Joseph Mitola proposed the concept of Cognitive Radio (CR) in 1999, which has attracted much attention in the international communication community. The basic idea of CR is to make wireless terminals have the ability to detect ‘spectrum holes’ and to take full advantage of them without affecting other primary users.

As a communication technology, Cognitive Radio systems are vulnerable to various malicious attacks, both traditional wireless attacks and some new classes of security threats. Thus, it is essential to strengthen its security to make CR viable and reliable for creative industrial applications.

This study is devoted to analysing the security issues of CR communication technology and proposing a new algorithm and security solution. The main work includes two aspects: research into spectrum sensing technology applicable to a Sora platform; and protection of CR networks in the event of a Primary User Emulation

Steganography with AES encryption for secure real-time VoIP covert communications

TANG Shanyu[1*], Peng Jinghui[1], ZHANG Liping[1] & ZHOU Zhangbing[2]

[1] *School of Computer Science, China University of Geosciences, Wuhan 430074, China*
[2] *School of Information Engineering, China University of Geosciences, Beijing 100083, China*

Abstract As a popular real-time service on the Internet, Voice over Internet Protocol (VoIP) communication attracts more and more attention from the researchers in the information security field. In this study, we proposed a VoIP steganographic algorithm with variable embedding capacities, incorporating AES and key distribution, to realize a real-time covert VoIP communication. The covert communication system was implemented by embedding a secret message encrypted with symmetric cryptography AES-128 into audio signals encoded by PCM codec. At the beginning of each VoIP call, a symmetric session key (SK) was assigned to the receiver with a Session Initiation Protocol-based authentication method. The secret message was encrypted and then embedded into audio packets with different embedding algorithms before sending them, so as to meet the real-time requirements of VoIP communications. For each audio packet, the embedding capacity was calculated according to the specific embedding algorithm used. The encryption and embedding processes were almost synchronized. The time cost of encryption was so short that it could be ignored. As a result of AES-based steganography, observers could not detect the hidden message using simple statistical analysis. At the receiving end, the corresponding algorithm along with the SK was employed to retrieve the original secret message from the audio signals. Performance evaluation with state-of-the-art network equipment and security tests conducted using the Mann-Whitney-Wilcoxon method indicated that the proposed steganographic algorithm is secure, effective, and robust.

Keywords VoIP, steganography, AES, covert communication, Mann-Whitney-Wilcoxon

1 Introduction

Voice over Internet Protocol (VoIP) communication is one of the most popular real-time services on the Internet. VoIP has more advantages than traditional telephony, since the Internet allows VoIP to provide low-cost, high-reliability, and global services. VoIP streams often have a highly redundant representation, which usually permits the addition of significantly large amount of secret data by means of simple and subtle modifications that preserve the perceptual content of the underlying cover object. With the increasing percentage of VoIP streams in all of the Internet traffic, VoIP is considered to be a better cover object for information hiding compared with “static” cover objects such as text files, image files, and audio files. Besides, VoIP connection is usually very short, and so it is unlikely for attackers to detect the hidden data within VoIP streams. Their real-time characteristics may be used to improve the security of the hidden data embedded in VoIP “dynamic” streams.

Steganography is a method of embedding secret data into a cover object, which should not cause unacceptable distortion and arouse observers’ attention. Both steganography and encryption technology keep the confidentiality of the secret data, but there are significant differences in many aspects between them. Encryption technology only protects the content of the secret data, making them unreadable. Thus, unauthorized users can know the existence, except the specific details about the secret data. Steganography hides the existence of the secret data, such that unauthorized users know neither the existence of the secret data nor the details of it.

Steganography is one of the most important areas of information security, becoming more and more flourishing to apply in various fields. For example, military communication systems usually need to be at higher security levels. They require not only encrypting the messages exchanged, but also hiding the existence of the messages, which means attackers even cannot perceive the existence of the messages. For protecting the intellectual property of digital products, merchants often embed their trade mark or unique logo into digital products with steganography. There are also some other applications of steganography.

In early steganography literature, steganography was widely used in image [1-3], audio [4-5], and video [6] files. For image steganography, the common method was to modify the least significant bit (LSB) of pixels in an image using

*Corresponding author (email: shanyu.tang@gmail.com)

SECURE COVERT COMMUNICATIONS OVER STREAMING MEDIA USING DYNAMIC STEGANOGRAPHY

Jinghui Peng

***Abstract*—Streaming technologies such as VoIP are widely embedded into commercial and industrial applications, so it is imperative to address data security issues before the problems get really serious. This thesis describes a theoretical and experimental investigation of secure covert communications over streaming media using dynamic steganography. A covert VoIP communications system was developed in C++ to enable the work being carried out. A new information theoretical model of secure covert communications over streaming media was constructed to depict the security scenarios in streaming media-based steganographic systems with passive attacks.The model involves a stochastic process that models an information source for covert VoIP communications and the theory of hypothesis testing that analyses the adversary's detection performance.The potential of hardware-based true random key generation and chaotic logistic map for innovative applications in covert VoIP communications was explored. Using the read time stamp counter of CPU as an entropy source was designed to generate true random numbers as secret keys for streaming media steganography. A novel interval selection algorithm was devised to choose randomly data embedding locations in VoIP streams using random sequences generated from a logistic chaotic map.**

***Index Terms*—Covert communications, hardware random key, key distribution, steganography, VoIP**

I. Introduction

VOICE over IP (VoIP) communication systems have been embedded into an increasing number of industrial applications such as smart transportation systems and intelligent healthcare systems. When implementing VoIP applications in building systems or developing innovative smart products to assist people, security issues need to be addressed urgently due to ever evolving cyber threats in recent years.

VoIP can be achieved on any networks based on an internet protocol (IP), such as the Internet, Intranet, local area networks (LANs) and wireless networks. VoIP applications include Personal Computer (PC) to PC connection, PC to Public Switched Telephone Network (PSTN) or PSTN to PC connection, and PSTN to PSTN connection. The main services include voice services and real-time fax services over IP-based networks, interactive voice response (IVR) services implemented on the Web, and a variety of communication services such as E-mail and real-time telephone. VoIP services operate on an Internet protocol to transmit compressed voice samples as frames and messages as a group of bytes over an IP data network. In VoIP applications, voice from end-user equipment is converted into a signal level, digitised, compressed as voice payload and sent as IP packets.

VoIP transmits voice information over an IP network to realise real-time voice communication. The basic transmission process of VoIP includes collecting the original sender's voice, converting the original voice signal into a digital signal by analogue-to-digital conversion, compressing and encoding the digital signal through a voice compression algorithm, encapsulating the compressed voice data according to the standard of TCP/IP, and sending the encapsulated IP packets to the receiver over an IP network. The receiver decodes and decompresses the received voice data packets to obtain the original analogue voice signal, so as to realise the real-time communication of voice information on the network.

VoIP media streams are the dynamic flow of voice data packets which can be used as cover objects to build real-time steganographic systems with embedded VoIP for industrial applications such as new healthcare products to assist our aging population [1]. Cryptography and steganography are expected to complement each other to improve the security of steganographic systems. As a steganographic message is embedded in VoIP media streams after encryption, a strong key is essential to ensure that the message it protects remains absolutely secure. However, the key used for encryption and decryption of the message is normally a pseudorandom number, which is not secure enough because the key is subject to compromise. Given enough time and computational powers, the key would be unencrypted by attackers: if multiple PCs work in parallel, the time is drastically shortened, and today's supercomputers should be able to find a pseudorandom key in about an hour [2]. A true random number based on hardware is a perfect seed for a strong key which can guarantee the security of steganographic systems.

A number of research have been conducted on the basic techniques of real-time steganographic systems with embedded VoIP, but the security of keys used for the systems has not received the attention it deserves. If the keys are broken, the systems become unsecured, an eavesdropper can distinguish between the ordinary objects and the stego objects that contain the secret message, which means the secret

Self-adaptive steganographic scheme with chaotic map for secure covert VoIP communications

Author: **Name** **Jinghui Peng**
School School of Computing and Engineering

Supervisors: **Name of principal supervisor** **Shanyu Tang**
School School of Computing and Engineering
Name of second supervisors **Graham Brooks**
School School of Law and Criminology
Anastasia Sofroniou
School School of Computing and Engineering

Abstract

Steganography is finding ways to achieve covert communications over streaming media, which have increasing applications in Information and Communications Technology (ICT) industries, but the security of the steganographic system is subject to compromise. This paper shows how a self-adaptive audio steganographic scheme can realise secure real-time covert VoIP communications over the Internet. In this study an Active Voice Period Detection (AVPD) algorithm is devised for PCM codec to detect whether a VoIP packet carries active voice data or silence, and the data embedding location in a VoIP stream is chosen randomly according to random sequences generated from a logistic chaotic map. At the signalling phase, the initial parameters of the chaotic map and the selection of where to embed secret data are negotiated between the communicating parties. Steganography experiments on active and inactive voice periods were carried out on a VoIP communications platform, respectively. Performance evaluation and security analysis indicates that the proposed self-adaptive VoIP steganographic scheme can withstand statistical detection, and achieve secure real-time covert communications with high speech quality and negligible signal distortion.

FFT-based Steganalysis of Covert Communications over Streaming Media

Jinghui Peng, Shanyu Tang, Jia Li

***Abstract*—**Steganalysis seeks to detect the presence of secret data embedded in cover objects, and there is an imminent demand to detect hidden messages in streaming media. This paper shows how a new steganalysis algorithm based on Fast Fourier Transform (FFT) can be used to detect the existence of secret data embedded in streaming media. The proposed algorithm uses machine parameter characteristics and a network sniffer to determine whether the Internet traffic contains streaming channels. The detected streaming data is then transferred from the time domain to the frequency domain through FFT. The distributions of power spectra in the frequency domain between original VoIP streams and stego VoIP streams are compared in turn using t-test, achieving the p-value of 7.5686E-176 which is below the threshold. The results indicate that the proposed FFT-based steganalysis algorithm is effective in detecting the secret data embedded in VoIP streaming media.

***Keywords*—**Steganalysis, Security, Fast Fourier Transform (FFT), Streaming media

I. Introduction

COVERT communication can be used to transmit confidential information on mobile telecommunications. There are three main ways to implement it: secure channel, encryption technology and information hiding. The secure channel is a private communications path established by the communicating parties, which is not accessible for others. It has high security but high cost and poor extensibility. Encryption technology largely depends on the length of the key used for encryption and decryption. As computer processing capabilities increase rapidly, it becomes less reliable to increase system security by increasing the key length. Digital steganography has drawn people's attention in the field of information hiding. Based on encryption technology, it embeds confidential information into seemingly innocuous transmissions, that is, the encrypted confidential information is "invisible", which is unlikely to be detected by attackers, thus reducing the probability of confidential information being attacked. From the perspective of information transmission security, steganography is one of the most advanced information hiding technologies.

A new generation of mobile telecommunications has emerged as a result of advances in wireless communications and mobile terminal technology. The third generation of mobile telecommunications technology (referred to as 3G) adopts the IMT-2000 international standard, which offers voice service, higher data transfer rates (200 kbps), broadband multimedia communications, and wireless access to the Internet. The fourth generation of mobile telecommunications (referred to as 4G), using OFDMA and MIMO (TD-LTE), is designed to provide high-speed (100 Mbps) data transmission services such as VoIP and IP Multimedia Subsystem (IMS), with a fibre broadband experience similar to a fixed-line network. With the advent of the era of 3G and 4G, streaming media such as VoIP has been widely used on the mobile Internet, providing a new dynamic cover object for information hiding, especially steganography.

Streaming media steganography has attracted the attention of information security experts all over the world. On the one hand, streaming media contain plenty of redundancy, which can be used to hide confidential information. Compared with image, audio, text and other multimedia files and network channels, streaming media are better cover objects. On the other hand, the widespread use of streaming media on mobile telecommunications networks has portrayed a variety of new mobile Internet services: mobile instant messaging, mobile TV, mobile content sharing, mobile E-reading, mobile social, mobile advertising and so on. Therefore, steganography in streaming media has broad application prospects in the field of mobile Internet.

Steganalysis, the countermeasure technology of covert communication in the field of information hiding, is developing rapidly with the strong demand of investigation into covert communication. Steganographic technology is very likely to be exploited by hostile agents, terrorists and evil forces. By hiding their secret information in streaming media, they intend to avoid content scrutinising and tracing, and use it to organise crimes and terrorist activities, and steal military and commercial information. It would endanger national and public security, and undermine social stability. Therefore, with the rapid development of mobile Internet, it is imminent to develop steganalysis technology for mobile networks, especially steganalysis of streaming media steganography. At present, research in streaming media steganalysis on the mobile Internet is at an early stage, and few preliminary results have been published.

This study was aimed to devise a new steganalysis method for streaming media that are ubiquitous on the mobile Internet and explore ways of universal and real-time detection and countermeasure of steganography in streaming media on the mobile Internet.

J. Peng is with the School of Computing and Engineering, University of West London, London, UK (e-mail: 21368391@student.uwl.ac.uk).

S. Tang is with the School of Computing and Engineering, University of West London, London, UK (e-mail: shanyu.tang@ uwl.ac.uk).

J. Li is with the Freelance Consultancy, Merton, London, UK (e-mail: lily.jjl@gmail.com).

国 家 知 识 产 权 局

100176 北京市昌平区回龙观镇建材城西路9号院7号楼三层318 北京高航知识产权代理有限公司 王庞(010-57031488)	发文日： 2022年11月28日

申请号或专利号：**202210821106.2**　　　　发文序号：**2022112300660230**

申请人或专利权人： 广东技术师范大学

发明创造名称： 一种无线物联网数据安全智能传输系统以及加密方法

发明专利申请公布及进入实质审查阶段通知书

上述专利申请，经初步审查，符合专利法实施细则第44条的规定。根据专利法第34条的规定，该申请在38卷4701期2022年11月22日专利公报上予以公布。

根据申请人提出的实质审查请求，经审查，符合专利法第35条及实施细则第96条的规定，该专利申请进入实质审查阶段。

提示：

1. 根据专利法实施细则第51条第1款的规定，发明专利申请人自收到本通知书之日起3个月内，可以对发明专利申请主动提出修改。

2. 申请人可以访问国家知识产权局政府网站（www.cnipa.gov.cn）,在专利检索栏目中查询公布文本。如果申请人需要纸件申请公布单行本的纸件，可向国家知识产权局请求获取。

3. 申请文件修改格式要求：

对权利要求修改的应当提交相应的权利要求替换项，涉及权利要求引用关系时，则需要将相应权项一起替换补正。如果申请人需要删除部分权项，申请人应该提交整理后连续编号的部分权利要求书。

对说明书修改的应当提交相应的说明书替换段，不得增加和删除段号，仅只能对有修改部分段进行整段替换。如果要增加内容，则只能增加在某一段中；如果需要删除一个整段内容，应该保留该段号，并在此段号后注明：“此段删除”字样。段号以国家知识产权局回传的或公布/授权公告的说明书段号为准。

对说明书附图、摘要、摘要附图修改的应当提交相应的说明书附图、摘要、摘要附图替换页。

同时，申请人应当在补正书或意见陈述书中标明修改涉及的权项、段号、页。

审　查　员：自动审查　　　　审查部门：专利局初审及流程管理部

联系电话：010-62356655

纸件申请，回函请寄：100088 北京市海淀区蓟门桥西土城路6号　国家知识产权局专利局受理处收
电子申请，应当通过电子专利申请系统以电子文件形式提交相关文件。除另有规定外，以纸件等其他形式提交的文件视为未提交。

国家知识产权局

100176

北京市昌平区回龙观镇建材城西路 9 号院 7 号楼三层 318 北京高航
知识产权代理有限公司
王艳(17724210594)

发文日：

2023 年 06 月 05 日

申请号：**202310648780.X** 发文序号：2023060501437240

专利申请受理通知书

根据专利法第 28 条及其实施细则第 38 条、第 39 条的规定，申请人提出的专利申请已由国家知识产权局受理。现将确定的申请号、申请日等信息通知如下：

申请号：202310648780X
申请日：2023 年 06 月 01 日
申请人：广东技术师范大学
发明人：彭景惠,廖艺,蔡君,肖茵茵,易称福,陈桂宏,朱铮宇,闫骥爽
发明创造名称：一种基于认证中心的认知无线电防 PUE 攻击解决方法
经核实，国家知识产权局确认收到文件如下：
权利要求书 1 份 2 页,权利要求项数 ： 4 项
说明书 1 份 8 页
说明书附图 1 份 1 页
说明书摘要 1 份 1 页
专利代理委托书 1 份 2 页
发明专利请求书 1 份 5 页
向外国申请专利保密审查请求书 文件份数：1 份
实质审查请求书 文件份数：1 份
申请方案卷号：A2376203GZ

提示：

1.申请人收到专利申请受理通知书之后，认为其记载的内容与申请人所提交的相应内容不一致时，可以向国家知识产权局请求更正。

2.申请人收到专利申请受理通知书之后，再向国家知识产权局办理各种手续时，均应当准确、清晰地写明申请号。

3.国家知识产权局收到向外国申请专利保密审查请求书后，依据专利法实施细则第 9 条予以审查。

审 查 员：周晓鸣
联系电话：010-62356655

审查部门：初审及流程管理部

国家知识产权局
专利审查业务章
1101081359734

200101 纸件申请，回函请寄：100088 北京市海淀区蓟门桥西土城路 6 号 国家知识产权局专利局受理处收
2022.10 电子申请，应当通过专利业务办理系统以电子文件形式提交相关文件。除另有规定外，以纸件等其他形式提交的文件视为未提交。

《计算机教育》杂志稿件录用函

尊敬的**彭景惠**老师：

您的稿件**《项目式的应用密码学 OMO 混合式教学探索》**通过专家审阅，拟刊登在《计算机教育》杂志 2023 年 11 月第 11 期（请您一定到投稿平台上核实您的刊期，以避免我们误操作给您带来损失），并会在见刊两月后于《计算机教育》杂志网站上刊登。版面费共计 3000 元。

此致！

近祺！

《计算机教育》杂志社有限公司

2023/6/5

《计算机教育》杂志社有限公司
91110108754683063C
发票专用章
110108101190346

地址：北京市海淀区双清路学研大厦 B 座 908

邮编：100084

网址：http://www.jsjjy.com

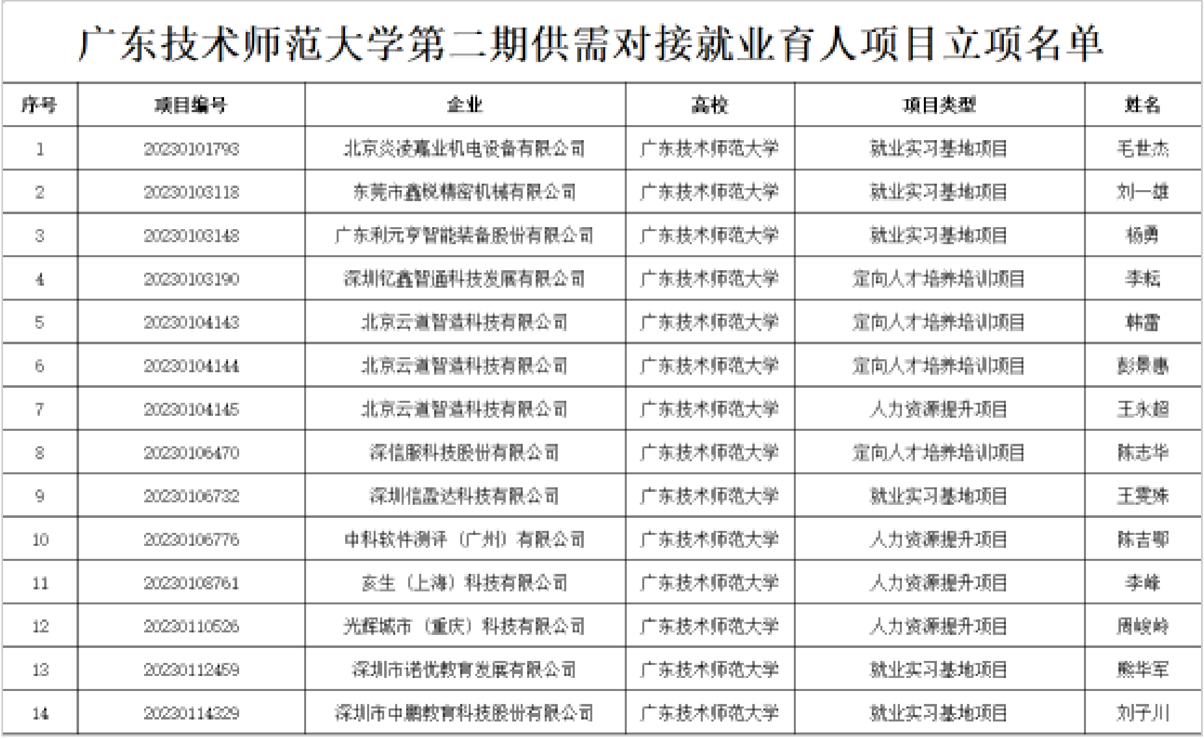
电话：（010）83470487、83470489、83470503

搜索 jsjjyzz 微信也精彩

我校14项就业育人项目获教育部立项

发布日期：2023-04-14　　浏览：　422

4月6日，教育部公布了第二期供需对接就业育人项目立项名单，根据《教育部高校学生司关于公布第二期供需对接就业育人项目立项名单的通知》（教学司函〔2023〕6号），我校毛世杰、刘一雄、杨勇、李耘等14位老师负责的项目顺利通过审批获得立项，立项数量较第一期增长了近200%。



广东技术师范大学第二期供需对接就业育人项目立项名单

序号	项目编号	企业	高校	项目类型	姓名
1	20230101793	北京炎凌嘉业机电设备有限公司	广东技术师范大学	就业实习基地项目	毛世杰
2	20230103118	东莞市鑫锐精密机械有限公司	广东技术师范大学	就业实习基地项目	刘一雄
3	20230103148	广东利元亨智能装备股份有限公司	广东技术师范大学	就业实习基地项目	杨勇
4	20230103190	深圳亿鑫智通科技发展有限公司	广东技术师范大学	定向人才培养培训项目	李耘
5	20230104143	北京云道智造科技有限公司	广东技术师范大学	定向人才培养培训项目	韩雷
6	20230104144	北京云道智造科技有限公司	广东技术师范大学	定向人才培养培训项目	彭景惠
7	20230104145	北京云道智造科技有限公司	广东技术师范大学	人力资源提升项目	王永超
8	20230106470	深信服科技股份有限公司	广东技术师范大学	定向人才培养培训项目	陈志华
9	20230106732	深圳信盈达科技有限公司	广东技术师范大学	就业实习基地项目	王雯姝
10	20230106776	中科软件测评（广州）有限公司	广东技术师范大学	人力资源提升项目	陈吉鄂
11	20230108761	亥生（上海）科技有限公司	广东技术师范大学	人力资源提升项目	李峰
12	20230110526	光辉城市（重庆）科技有限公司	广东技术师范大学	人力资源提升项目	周峻岭
13	20230112459	深圳市诺优教育发展有限公司	广东技术师范大学	就业实习基地项目	熊华军
14	20230114329	深圳市中鹏教育科技股份有限公司	广东技术师范大学	就业实习基地项目	刘子川

就业育人立项数量的大幅增长，既是对我校长期以来深入开展校企融合、校企合作工作成绩的肯定，也为我校进一步拓展人才培养思路提供了“路线图”，学校将结合“访企拓岗专项行动”，坚持以社会需求为导向，深入了解

北京云道

第二期供需对接就业育人项目
校企合作协议

云道智造
Internet Based Engineering

广东技术师范学院
GUANGDONG POLYTECHNIC NORMAL UNIVERSITY (GPNU)
1957

二零二二年十一月

协议

为充分发挥高等学校人才培养、科学研究和服务社会的功能，同时借助企业在资金及实践方面的优势，甲方拟通过教育部供需对接就业育人项目的实施，实现高校人才培养与企业发展的合作共赢。甲乙双方本着互利互惠的原则，经友好协商，建立合作伙伴关系，实施“定向人才培养培训项目-广东技术师范大学网络空间安全产教融合人才培养探索与实践项目”。现双方就该项目的实施签署如下协议：

第一条 合作内容及合作期限

甲乙双方就“定向人才培养培训项目-广东技术师范大学网络空间安全产教融合人才培养探索与实践项目”（以下简称：《广师大网安产教融合人才培养项目》）建立合作关系，并将以《广师大网安产教融合人才培养项目》申请教育部供需对接就业育人项目，合作期限为二年，自本协议签署并生效之日起计算。

第二条 项目经费及支付

2.1 经甲乙双方协商一致，在受本协议约束的前提下，甲方同意向乙方提供本项目经费人民币10000元（大写：壹万元整）。公司将依照本协议的规定支付该笔资金。

2.2 项目经费支付时间如下：

（1）甲方按照本协议第5.2条约定，经验收合格并收到乙方按本协议第2.4条要求开具的真实有效的等额增值税发票后30日内一次性全额支付项目经费。

（2）本协议约定期限届满，按照本协议第5.2条约定，本项目未能通过甲方验收，甲方有权不予支付本项目的项目经费。

2.3 甲方应按照前述约定将项目经费支付至乙方指定的以下银行账户：

单位名称：广东技术师范大学

开户银行：中国建设银行广州天河工业园支行

银行账号：44001470513050317023

2.4 乙方应在甲方付款前按甲方要求开具真实有效的增值税专用发票或增值税普通发票。甲方开票信息如下：

单位名称：北京云道智造科技有限公司

纳税人识别号：911101080933369842B

注册地址：北京市海淀区永泰庄北路1号天地邻枫5号楼一层106

电话号码：010-82363065

开户银行：中国银行股份有限公司北京清华园支行

银行账号：320762142329

第三条 甲方的权利和义务

3.1 在本协议约定的期限内，《广东技术师范大学网络空间安全产教融合人才培养探索与实践项目》研究期间，甲方有义务为乙方的教师及在校学生提供Simdroid软件的使用权限、必要的技术支持和学习资源支持。

3.2 经乙方同意，甲方有权在日常经营活动包括但不限于甲方其他教学活动、市场宣传、用户培训等活动中合理使用乙方基于《广东技术师范大学网络空间安全产教融合人才培养探索与实践项目》提供的教学内容和项目研究成果。

3.3 在本协议约定的期限内，甲方有权对乙方《广东技术师范大学网络空间安全产教融合人才培养探索与实践项目》的实施进展、Simdroid软件的使用情况进行随机抽查，如果发现乙方未按照本协议约定执行，甲方有权解除本协议，并将抽查结果上报教育部进行执行结果通报。

第四条 乙方的权利和义务

4.1 自本协议签订并生效之日起，乙方委派彭景惠（原则上为本协议关联就业育人项目负责人）为《广东技术师范大学网络空间安全产教融合人才培养探索与实践项目》的项目负责人，专门负责本项目的执行。

4.2 在本协议约定期限内，乙方对甲方提供的Simdroid软件仅可用于《广东技术师范大学网络空间安全产教融合人才培养探索与实践项目》研究及教学使用，不得对前述软件进行销售、许可使用、转让等盈利活动。

4.3 乙方应在本协议签署前，将《广东技术师范大学网络空间安全产教融合人才培养探索与实践项目》的项目申请书等提交甲方，在本协议约定期限内，乙方有义务根据甲方提出要求后7日内，向甲方提供《广东技术师范大学网络空间安全产教融合人才培养探索与实践项目》进展情况，包括但不限于《广东技术师范大学网络空间安全产教融合人才培养探索与实践项目》的年中及年末的项目执行报告、研究成果等。

4.4 乙方应于《广东技术师范大学网络空间安全产教融合人才培养探索与实践项目》结题前7日内，将项目执行情况及项目执行过程中所涉及的教育教学资源以书面形式提交给甲方。

4.5 乙方有权使用《广东技术师范大学网络空间安全产教融合人才培养探索与实践项目》的成果申报各类奖项和进行本校各专业的教育教学。

第五条 考核标准与项目验收

5.1 乙方基于甲方提供的Simdroid软件开展的教学课程及软件学习使用应达到如下考核标准：

（1）乙方根据用人企业需求，联合设立“仿真（CAE）软件特色班”，实施学科交叉融合，培养复合型人才，并提供详细教学计划及

课程大纲。

（2）面向在校学生，乙方与甲方联合制定培训计划，通过线上或线下、直播或录播的形式，配合企业开展仿真技术理论与实操、Simdroid仿真（CAE）软件平台使用、仿真APP开发、云仿真平台Simcapsule使用等课程培训。关于培训课时、作业要求、日程安排设置、学生学习督导等方面由甲乙双方根据具体需求共同商定。学生完成课程学习并提交作业后，甲乙双方协商为学生配发相应证明/证书。

（3）项目执行期间，乙方需确保不少于200名在校学生完成Simapps网站（https://www.simapps.com）注册及Simdroid软件下载。项目执行期间，乙方需培养总计200名仿真（CAE）应用工程师，每人至少产出并提交1个合格的仿真APP或工程文件（以该仿真APP或工程文件通过甲方审核或在其平台推广作为合格的标准）。

5.2 项目验收

（1）本协议签署后至本协议约定的合作期限届满之日的期间内，如乙方完成本协议第5.1条约定的考核标准，可随时向甲方提交验收相关资料，并发起结题流程，甲方配合完成项目验收及结题工作，经验收通过，甲方按照本协议第2.2条约定支付项目经费。

（2）如乙方按照前述第（1）项约定提起验收未通过，且仍在本协议约定的合作期限内的，乙方可继续履行本协议，待本协议约定的合作期限届满后再次提交验收，经甲方验收通过，甲方按照本协议第2.2条约定支付项目经费。

第六条 知识产权

乙方基于甲方提供的Simdroid软件就《广东技术师范大学网络空间安全产教融合人才培养探索与实践项目》及教学使用而研发的新的应用软件的著作权归乙方所有，甲方对前述新研发的应用软件具有

8.3 如乙方未按照本协议第4.3条、第4.4条约定向甲方提交相关文件资料，甲方有权暂时停止履行其在本协议项下的义务，待相关违约情形消除或违约责任得到履行后恢复履行，甲方根据此款规定暂停履行义务不构成甲方的违约。

8.4 本条所述的经济损失包括守约方因主张权利而支出的诉讼费/仲裁费、保全费、保全担保费、公证费、执行费、律师费等合理支出。

第九条 通知

9.1 本协议要求的或根据本协议做出的任何通知、请求、要求和其他通信往来应以书面形式按照本协议签署页提供的有效通讯地址和电子送达地址予以邮寄送达或电子方式通知（送达），其中电子送达地址是指签署页各方所确认的传真、电子邮箱、电话号码接收地址。

9.2 以上各方可以通过书面通知其他各方的形式修改上述信息，任何对上述信息的修改自该等书面通知送达其他各方时生效。

9.3 若本协议各方的联系方式、通讯地址等发生变更，应自变更之日起二个工作日内书面通知其他方，否则由未通知方承担由此引起的相关法律责任。

9.4 本协议要求的或根据本协议做出的任何通知、请求、要求和其他通信往来若以挂号信函方式发出，在投邮三(3)天后视为送达；若以特快专递方式发出，在投邮后48小时视为送达；若以传真方式发出，送达日以发件方完整的传真报告为准；若以电子邮件方式发送的，则一经发出即视为送达；若当面递交，一经面交即视为送达。若实际送达时间早于前述约定时间，以实际送达时间为准。

9.5 本协议各方在签署页确认的有效送达地址及联系方式，可以作为发生纠纷时人民法院或仲裁机构送达起诉书、证据、判决书、裁定书等诉讼文书的确认送达地址。

（本行以下无正文，为本协议之签字盖章页）

甲方：北京云道智造科技有限公司

（公章）

北京云道智造科技有限公司 合同专用章

法定代表人或授权代表签字：胡国峰

有效通讯地址：北京市海淀区永泰庄北路1号中关村东升国际科学园1号楼C单元2层

电子邮箱：guofeng.hu@ibe.cn

联系电话：18911150027

联系人：胡国峰

日期：2022年12月1日

乙方：广东技术师范大学

（公章）

广东技术师范大学 合同专用章 44010600069105

法定代表人或授权代表签字：彭景惠

有效通讯地址：**广东省广州市天河区中山大道293号**

电子邮箱：826625501@qq.com

联系电话：13026161858

联系人：彭景惠

日期：2022年11月14日

附件：

广东技术师范大学2022年校级教学改革研究项目拟立项名单

序号	所在单位	项目名称	项目负责人	项目类别
1	外国语学院	基于OBE“学训赛创四位一体”的商务英语人才培养模式构建	王永建	重点项目
2	汽车与交通工程学院	新工科背景下智能网联及新能源汽车现代产业学院人才培养模式探索	孔春玉	重点项目
3	电子与信息学院	基于结构方程模型的课程思政实施成效评价研究	许清媛	重点项目
4	文学与传媒学院	创新、创意、服务于一体的传媒类专业应用人才培养改革与实践	刘光磊	重点项目
5	计算机科学学院	信创牵引 产教融合——数据科学与大数据技术专业人才培养模式研究	李辉辉	重点项目
6	音乐学院	新文科视阈下高校公共音乐课跨学科育人的一体化实验研究	唐文滔	重点项目
7	计算机科学学院	应用型人才培养机制下《计算机组成原理》实验课程体系建设	张磊	重点项目
8	音乐学院	新文科视域下视唱练耳课程改革实践研究	王晓燕	重点项目
9	美术学院	新文科建设目标下的艺术设计专业跨学科T型人才培养模式改革研究与实践	杨璇	重点项目
10	机电学院	基于OBE理念的新时代中职师资教学能力培养研究——以机电类师范生“教学学习和实习”为例	陈飞昕	重点项目
11	光电工程学院	基于Flash技术辅助高中物理模型教学的研究	熊良斌	重点项目
12	广东工业实训中心	基于产教融合的职教师资能力标准及专业素质提升研究	赵先美	重点项目

28	体育与健康学院	广东技术师范大学学生体质特征及体育教学模式取向研究	黄善球	一般项目
29	光电工程学院	基于混合式教学模式的《大学物理》课程多元化考核评价体系研究	万巍	一般项目
30	外国语学院	以思维进阶式的问题设计训练提升英语师范生教学素养的探索与实践	张彦琳	一般项目
31	音乐学院	反思与重构：“双线混融教学”模式之于高校舞蹈教学改革研究	余畅	一般项目
32	教育科学与技术学院	基于混合式教学模式的高校学前教育专业课程思政建设路径研究——以《学前心理学》为例	张晓洁	一般项目
33	马克思主义学院	一流本科课程建设背景下《思想道德与法治》课程混合式教学改革研究	陈吉鄂	一般项目
34	法学与知识产权学院	法理学“双师同堂”专题教学改革探索	万娟娟	一般项目
35	外国语学院	基于CBL模式的商务英语教学模型构建	谭雯婷	一般项目
36	文学与传媒学院	新文科建设背景下影视评论课程“三位一体”教学体系改革与实践	温立红	一般项目
37	美术学院	新文科视野下设计专业跨学科教学模式研究与实践	窦潇	一般项目
38	汽车与交通工程学院	面向三全育人的《工程制图》课程思政教学改革研究	张小帆	一般项目
39	美术学院	“新师范”背景下美育融入 教师教育课程建设的路径探索	吕欣欣	一般项目
40	网络空间安全学院	基于项目式的《应用密码学》OMO混合式教学研究与实践	彭景惠	一般项目
41	学生处	高校职业发展与生涯规划课课程思政教学策略研究	黄曼琳	一般项目
42	机电学院	基于产教融合面向CAM的机械类人才培养探索与实践	李冬梅	一般项目

广东技术师范大学

教学改革研究项目申请书

项目名称：基于项目式的《应用密码学》OMO 混合式教学研究与实践

项目类别：□重点项目　☑一般项目

项目主持人：彭景惠

单位名称：广东技术师范大学网络空间安全学院

联系电话：13026161858

电子信箱：826625501@qq.com

填表日期：2022 年 6 月

广东技术师范大学教务处制

二〇二二年

一、简介

项目简况	项目名称	基于项目式的《应用密码学》OMO 混合式教学研究与实践			
	经费来源	学校资助经费	0.3 万元	起止年月	2022 年 7 月至 2024 年 7 月 （从申报年份开始计算， 研究时间 2 年）
		其他经费	万元		
项目学科分类		计算机类	预期成果形式	研究报告、课程方案、教改论文等	

项目主持人	姓 名	彭景惠	性别	女	出生年月	1993 年 7 月
	专业技术职务	校聘副教授	最终学位/授予 国家	中国/英国		

近二年教学工作简历	时 间	项 目 名 称	授课对象	学时	所 在 单 位
	2020. 09-2020.12	信息检索与知识产权	电子信息	32	广东技术师范大学网络空间安全学院
	2020.12-2021.01	信息安全实训	网络工程	32	广东技术师范大学网络空间安全学院
	2021.03-2021.06	高级网络技术	电子信息	36	广东技术师范大学网络空间安全学院
	2021.09-2022.01	专业英语	电子网安	32	广东技术师范大学网络空间安全学院
	2021.09-2022.01	应用密码学	网安	96	广东技术师范大学网络空间安全学院
	2022.02-	学术论文写作指导	电子网安	32	广东技术师范大学网络空间安全学院

教学改革研究和科学研究工作简况	时 间	项目名称（校、省、国家级项目）	概况（在研、结题、获奖）
	2022.01-2023.12	“基于同态理论的可认证组密钥协商与大数据加密检索安全研究”，广东省普通高校特色创新项目(排名第一)，9 万元	在研
	2021.01-2024.12	“VoIP 流媒体隐密通信研究”，广东技术师范大学人才引进项目，35 万元	在研

项目课题组主要成员简况（不含主持人）	总人数	高级职称人数	中级职称人数	初级职称人数	博士	硕 士	学士
	5	4	1	0	5		

姓 名	出生年月	专业技术职务	工 作 单 位	项目中的分工	签 名
张瑜	1975.08	教授	广东技术师范大学	理论指导	
罗建桢	1984.	副教授	广东技术师范大学	实践指导、教研合作	
陈桂宏	1983.	副教授	广东技术师范大学	参与教学改革	
欧阳佳	1986.5	讲师	广东技术师范大学	技术指导	

2、已具备的教学研究基础和环境，学校对课题的支持情况（含有关政策、经费支持及其使用管理机制、保障条件等），尚缺少的条件和拟解决的途径（300字以内）

五、经费预算

支出项目	金额（元）	依据及理由
差旅费	500	调查走访企业，案例收集等交通差旅支出
论文版面费	1000	教改论文发表
复印费	500	相关资料复印及打印
劳务费	1000	课程助教学生补助发放
合计	3000	

六、推荐、评审意见

学院审核意见 负责人签字：　　　　单位（盖　章） 年　　月　　日
学校审核意见 负责人签字：　　　　（盖　　　章） 年　　月　　日

附件

广东技术师范大学第三批课程思政优秀案例评选拟获奖名单

序号	所在学院	案例名称	作者姓名
1	自动化学院	《建筑节能技术》课程思政教学案例	操瑞兵
2	汽车与交通工程学院	面向三全育人的《工程制图》课程思政教学实践	张小帆
3	数学与系统科学学院	敬畏生命，追寻价值——《大学生心理健康教育》课程思政行与思	李玉佳、王婷婷
4	汽车与交通工程学院	“一推二融三进”的思政教学模式-自动控制原理课程	武威
5	机电学院	《材料成形工艺学》课程思政育人路径探索——以史为鉴，让材料成形制造的力量薪火相承	高吉祥
6	财经学院	厚于德、诚于信、敏于行——将“广东精神”融入《财务管理案例分析》课程教学	欧阳莹
7	文学与传媒学院	光影中国讲“四史”——《影视评论与写作》课程思政教学探索与实践	温立红
8	美术学院	以史为鉴培根铸魂，文化自信润物无声	周峻岭
9	职业教育教师学院	疫情隔离期间《木兰诗》单元主题教学：在线项目式教学的实践	张晓梅
10	财经学院	“谷贱伤农”怎么办？——需求弹性理论与价格支持政策的分析	郑旭芸
11	计算机科学学院	数据强国梦——《数据可视化技术》课程思政教学案例	杨阿庆
12	计算机科学学院	以信创为舟，思政为帆，畅游知识海洋——《软件测试》课程思政教学案例	盘茂杰
13	计算机科学学院	思政筑基育人：《操作系统原理》，融入“自主设计操作系统”的人才培养、教育实践	郑志硕
14	电子与信息学院	科技强国，使命光荣	阮剑亮
15	计算机科学学院	水到渠成的知识讲授，润物无声的思政教育——《数据挖掘与机器学习》课程思政教学案例	刘伟莉
16	招生就业办公室	澄清个人职业价值观——《职业生涯与发展规划》课程思政教学案例	黄曼琳、梁冬、林庆
17	外国语学院	思维文化融入《英汉语言对比》	宋伟奇

18	机电学院	基于 OBE 理念的《专业概论》课程思政育人路径探索——系好专业课程思政的第一粒扣子，成就有底色的专业人才	刘一雄
19	教育科学与技术学院	“一中心、二结合、三位一体、四步进阶”《教育心理学》课程思政的理念与实践	陈丽君
20	创新创业学院	课程思政的“听进去”与“行出来”——以《创新与创业基础》为例	吴凤池
21	国际教育学院	在来华留学生汉语教学中传播中华文化“天人合一”自然观	陈津津
22	法学与知识产权学院	解构民事权利义务，厚植经世济民情怀——《民法总论》课程思政探索	朱省志
23	体育与健康学院	建党百年中国羽毛球发展史理论课程融入思政元素之探索	向丽萍
24	机电学院	“铸魂・润心・笃行”：将培养责任意识和家国情怀融入《职业生涯与发展规划》课程教学	李晓敏
25	创新创业学院	“想百姓之所想”——将“为人民服务”刻入创新创业教育	张广珍
26	文学与传媒学院	新时代主流媒体的舆论引导	杨欣
27	法学与知识产权学院	厚植诚信土壤，建设品牌强国 ——《商标法》 课程思政探索	罗玥
28	汽车与交通工程学院	激发学生自驱力，培养大国工匠——《工程测量》课程思政教学案例分享	李薇
29	管理学院	融古通今，学贯中西，强化认同，坚定自信——《行政思想史》课程思政教学案例	蔡永宁
30	文学与传媒学院	思政融入课堂，让《电视新闻现场报道》更生动	孔涵
31	外国语学院	梦想、追求与人生——“The Pursuit of Dreams”	刘星莹
32	电子与信息学院	让课程思政与《C语言程序设计》课程同向同行	张子龙
33	法学与知识产权学院	“四个自信”筑牢法治根基，“分论教学”塑造刑法逻辑	吴岳樯
34	网络空间安全学院	基于项目式OMO混合教学的《应用密码学》多维度课程思政实践	彭景惠
35	汽车与交通工程学院	培植大国工匠，厚植家国情怀，助力创新型人才培养	王彦鹍
36	法学与知识产权学院	以公平正义为使命，育德法兼修法律人——《民事诉讼法学》课程思政探索	徐进静
37	文学与传媒学院	红色经典的范本意义：《剧作基础训练》课程对红色经典电影作品的选取与利用	秦凤华