

ICCNS 2021

2021 the 11th International Conference on Communication and Network Security

Beijing Jiaotong University, Weihai, China
December 3-5, 2021

Conference Program

Co-sponsored by



北京交通大学(威海)
Beijing Jiaotong University, Weihai

Published by



The image shows the entrance of Beijing University of Aeronautics and Astronautics (Beihang University). The golden Chinese characters '北京交通大学' and the English name 'BEIJING UNIVERSITY OF AERONAUTICS AND ASTRONAUTICS' are visible on the building's facade. In the foreground, there are yellow flowers and a fence. The word 'CONTENT' is written in large blue letters with a white arrow pointing to the right.

CONTENT ▶

1 Welcome Message

2 Conference Committees

3 Keynote Speakers

4 Instruction of Online Conference

5 Daily Schedule

6 Authors Presentation

WELCOME MESSAGE

On behalf of Conference Committees, we welcome you to attend 2021 the 11th International Conference on Communication and Network Security during December 3-5, 2021, online, hosted by Beijing Jiaotong University, Weihai, China.

It is a great pity that we cannot communicate face to face due to the outbreak of the COVID-19. Thereby, we have to hold this conference online. From a practical perspective, there are some benefits for holding the online conferences. It mainly allows attendees to avoid crowd contact and effectively prevent virus infection. We believe that the online conference can also provide a unique experience for all participants. We hope all is well with you and your family. Meanwhile, we would sincerely appreciate for your understanding and cooperation.

It's the 11th year of ICCNS conference, but it will witness the development of the field in communication and network security. ICCNS will keep working on itself as an event whose aim is to provide this chance and platform for the researchers from academia, industry, and government institutions to exchange and present the novel research on communication and network security.

Many members of the organizing team worked very hard to turn our initial visions for this conference into reality, we would like to warmly thank all organizing committee members for their dedication before and after this unique event. Your expertise, enthusiasm, and time commitment enabled us to prepare the final program. Our Final thanks would go to the authors, thanks for your support to our conferences.

We hope that all participants and other interested readers benefit from and enjoy the presentations and proceedings and also find it stimulating in this process. We pursue higher and better international conference, your suggestions and comments are welcome.

Conference Organizing Committees

CONFERENCE COMMITTEES

Honorary Chair

Zhongliang Guan, Vice-president, Beijing Jiaotong University, Weihai, China

Conference Chairs

Ying Liu, Beijing Jiaotong University, Weihai, China

Masahiro Fujita, The University of Tokyo, Japan

Conference Co-chair

Yanlei Bai, Beijing Jiaotong University, Weihai, China

Program Chair

Masayuki Arai, Teikyo University, Japan

Huifang Chen, Zhejiang University, China

Publicity Co-chairs

Zhibin Chen, Kunming University of Science and Technology, China

Jie Yu, Beijing Jiaotong University, Weihai, China

Local Organizing Committee

Guangzhi Liu, Beijing Jiaotong University, Weihai, China

Min Zhang, Beijing Jiaotong University, Weihai, China

Jingwei He, Beijing Jiaotong University, Weihai, China

Finance Chair

Xin Zhang, Beijing Jiaotong University, Weihai, China

Technical Committee

Heqing Huang, IBM TJ Watson, USA

YOGESH B. GURAV, Zeal College of Engineering and Research, India

Declan Delaney, University College Dublin, Ireland

Wenye Li, The Chinese University of Hong Kong, China

Dr. Diane Gan, University of Greenwich, UK

Arash Habibi Lashkari, University of New Brunswick, Canada

Gaurav Varshney, IIT Jammu, India

Erdogan Dogdu, Computer Science at Angelo State University, USA

Richa Sharma, JK Lakshmipat University, India

Kocsis Gergely, University of Debrecen, Hungary

Dimitris Kanellopoulos, University of Patras, Greece

Bobby Barua, Ahsanullah University of Science and Technology, Bangladesh

KHALDI Amine, Universite Kasdi Merbah Ouargla, Algeria

Jyh-haw Yeh, Boise State University, USA

Richa Sharma, K Lakshmipat University, India

Yan Wang, Temple University, USA

Harbin Engineering University, China

Jain-Shing Liu, Providence University, Taiwan, China

Xiaoming Hu, Shanghai Polytechnic University, China

Chungen Xu, Nanjing University of Science and Technology, China

Jilong Bian, Northeast Forestry University, China

E. Prince Edward, Sri Krishna Polytechnic College, Coimbatore, India

Zhongyuan Qin, Southeast University, China

Meiryani, Bina Nusantara University, Indonesia



Prof. Zhu Han

University of Houston, USA

Bio: Zhu Han received the B.S. degree in electronic engineering from Tsinghua University, in 1997, and the M.S. and Ph.D. degrees in electrical engineering from the University of Maryland, College Park, in 1999 and 2003, respectively. From 2000 to 2002, he was an R&D Engineer of JDSU, Germantown, Maryland. From 2003 to 2006, he was a Research Associate at the University of Maryland. From 2006 to 2008, he was an assistant professor in Boise State University, Idaho. Currently, he is a John and Rebecca Moores Professor in Electrical and Computer Engineering Department as well as Computer Science Department at University of Houston, Texas. His research interests include security, wireless resource allocation and management, wireless communication and networking, game theory, and wireless multimedia. Dr. Han is an NSF CAREER award recipient 2010. Dr. Han has several IEEE conference best paper awards, and winner of 2011 IEEE Fred W. Ellersick Prize, 2015 EURASIP Best Paper Award for the Journal on Advances in Signal Processing and 2016 IEEE Leonard G. Abraham Prize in the field of Communication Systems (Best Paper Award for IEEE Journal on Selected Areas on Communications). Dr. Han is the winner 2021 IEEE Kiyo Tomiyasu Award. He has been IEEE fellow since 2014, AAAS fellow since 2020 and IEEE Distinguished Lecturer from 2015 to 2018. Dr. Han is 1% highly cited researcher according to Web of Science since 2017.

Federated Learning and Analysis in Mobile Edge Computing

Abstract: In recent years, mobile devices are equipped with increasingly advanced computing capabilities, which opens up countless possibilities for meaningful applications, e.g., for augmented reality, Internet of Things, and vehicular networks. Traditional cloud-based Machine Learning (ML) approaches require the data to be centralized in a cloud server or data center. However, this results in critical issues related to unacceptable latency and communication inefficiency. To this end, Mobile edge computing (MEC) has been proposed to bring intelligence closer to the edge, where data is originally generated. However, conventional edge ML technologies still require personal data to be shared with edge servers. Recently, in light of increasingly privacy concerns, the concept of Federated Learning (FL) has been introduced. In FL, end devices use their local data to train a local ML model required by the server. The end devices then send the local model updates instead of raw data to the server for aggregation. FL can serve as an enabling technology in mobile edge networks since it enables the collaborative training of an ML model and also enables ML for mobile edge network optimization. However, in a large-scale and complex mobile edge network, FL still faces the implementation challenges with regard to communication costs and resource allocation. In this talk, we begin with an introduction to the background and fundamentals of FL. Then, we discuss several potential challenges for FL implementation. In addition, we study the extension to federated analysis.



Prof. Yonghui Li

The University of Sydney, Australia

Bio: Yonghui Li is a Professor and Director of Wireless Engineering Laboratory, in School of Electrical and Information Engineering, the University of Sydney. He is the recipient of the prestigious Australian Research Council (ARC) Queen Elizabeth II Fellowship in 2008 and ARC Future Fellowship in 2012. His current research interests are in the area of wireless communications, Internet of Things, Wireless networks, 5G and wireless AI. He participated in \$500million Australian national Smart Grid Smart City project, the world first large-scale demonstration project. He has published more than 300 papers in IEEE journals and conferences. Several of his journal papers have been included in ESI highly cited papers. According to google scholar, his research works have been cited more than 10000 times. He is now an editor for IEEE Transactions on Communications, and IEEE Transactions on Vehicular Technology. He also served as a guest editor for several special issues of IEEE journals, such as IEEE JSAC special issue on Millimeter Wave Communications, IEEE Communications Magazine on Wireless AI, IEEE IoT Journal, IEEE Transactions on Industrial Informatics, IEEE Access. He received several best paper awards from IEEE International Conference on Communications (ICC) 2014, IEEE PIMRC 2017 and IEEE Wireless Days Conferences (WD) 2014.

5G Ultra Reliable and Low Latency Networks

Abstract: The world is currently witnessing the rise of many mission critical applications such as tele-surgery, intelligent transportation, industry automation, virtual reality and augmented reality, vehicular communications, etc. Guaranteeing these stringent reliability and end-to-end latency requirements continues to prove to be quite challenging, due to the significant shift in paradigms required in both theoretical fundamentals of wireless communications as well as design principles. For instance, the fourth generation of cellular networks (4G) currently provide an unpredictable latency that can range from 50ms to several seconds, with block error rates as high as 10^{-1} . On the other hand, industry is demanding URLLC provide 1 ms end-to-end latency and overall packet loss probabilities as low as 10^{-5} - 10^{-7} . Motivated by the above, in this talk, I will present the challenges and potential solutions for 5G and beyond 5G to support ultra reliable and low latency communications (URLLC) from physical layer up to network layer.



Prof. Junhui Zhao

**Beijing Jiaotong University, East
China Jiaotong University, China**

Bio: Junhui Zhao is a Professor of Beijing Jiaotong University and East China Jiaotong University. He is also the dean of the Information Engineering School and Artificial Intelligence School in East China Jiaotong University. His research interest includes vehicular networks, wireless communications, and mobile communications. He is a Fellow of China Institute of Communications, a Fellow of IET, a Distinguished Member of CCF, and a Senior Member of IEEE. He is the Secretary General of Jiangxi Artificial Intelligence Society, and the Standing Director of Jiangxi Institute of Communications and Jiangxi Institute of Electronics. He also serves as a Deputy Director of Automobile Committee of China Association of Productivity Promotion Centers and Computer Application Committee of CCF.

Prof. Zhao received the Best Paper Award at WICON 2015, WCSP 2017, IEEE/CIC ICC 2018, APCC 2018, IEEE GLOBECOM 2019. He hosts several programs supported by NSFC, including 1 key program. He also hosts 2 sub-programs of the National Key Research and Development Program. He won the honorary titles of New Century Excellent Talents of the Ministry of Education, Long-term Leading Talents of Double Thousand Program of Jiangxi Province, Excellent Scientific and Technological Worker of Chinese Electronics Society, Excellent Worker of Chinese Artificial Intelligence Society and so on.

5G Vehicular Networks: The Fusion of Computation and Communication

Abstract: The vehicles are developing rapidly in the direction of electronization, network-connection and intelligentization. Vehicular networks are visioned as the key application of intelligent transportation system (ITS). With the development of 5G and 5G beyond techniques, the challenges and problems of the communication rate and latency in vehicular networks will be further solved. 5G vehicular networks have been viewed as the hot topic to build the practical deployment for ITS.

In this talk, we firstly introduce the essential concept and the recent advances of 5G vehicular networks. Then we show our latest contributions including vehicle-to-everything (V2X), platoon intelligence, edge intelligence, UAV-aided vehicular communication, blockchain-based vehicular resource management, dynamic offloading for vehicular resource allocation and security in the domain of vehicular networks. We also explain the research models and corresponding performance analysis of our proposed solutions. We finally present some applications for 5G vehicular networks. Several university-industry collaborations reveal how our theoretical researches on 5G vehicular networks are applied to the real systems.

We humbly hope this talk will shed light for forthcoming researchers to explore the uncharted part of the future vehicular networks.








PRESENTATION TIPS

Zoom Link: <https://zoom.us/j/91785403130>
Password:120305

Date	Arrangement
December 3, 2021	Zoom Test
December 4, 2021	Opening Ceremony & Keynote Speech Session 1
December 5, 2021	Session 2 Keynote Speech Reply

Rename Your Screen Name	Example
Authors: Paper ID-Name	R0001-San Zhang
Listener: Listener Number-Name	Listener- San Zhang
Keynote Speaker: Keynote-Name	Keynote- San Zhang
Committee Member: Position-Name	Committee- San Zhang

Note

-  **Enter the room 10-15 minutes in advance.**
-  Prepare the PPT file of your presentation on your laptop in advance.
-  **Duration of each Presentation:** about **17 Minutes of Presentation** and **3 Minutes of Q&A.**
-  **Questions:** During the conference, if you have any question, please contact “Assistant” privately, you’ll get assisted immediately.
-  **Duration of Oral Presentation:** 20 Minutes of Presentation including Q&A.
-  **Dress Code:** All participants are required to dress formally. Casual wear is unacceptable. National formal dress is acceptable.
-  **Note:** The regular oral presentation time arrangement is for reference only. In case any absence or some presentations are less than 20 minutes, please join your session before it starts.

Online Platform Download Instruction



国内作者Zoom下载链接 (For China)

点击下方按钮下载电脑Zoom客户端

Click button to download Zoom Computer Client

下载

点击下方按钮下载Zoom移动应用

Click button to download Zoom mobile application



Zoom Download Link (For Oversea)

Click button to download Zoom Computer Client

Download

Click button to download Zoom mobile application



•Read Zoom using instruction here: [Click](#). Please do join Zoom Test on December 3, we will guide how to use ZOOM to make presentation one by one.

DAILY SCHEDULE

➤ **December 3, 2021** | GMT+8, Beijing Time **Zoom Test**

Zoom Link: <https://zoom.us/j/91785403130> **Password:120305**

Test Session

Test Time

Conference Committee Test

10:00-17:00 (Breakout Room)

Session 1

Communication and Information Security

NS1002 NS1003 NS1010 NS1011 NS1006 NS1012

10:00-12:00

Session 2

Advanced Information Technology and Management

NS0002 NS0003 NS1008 NS1009 NS1004

14:00-16:00

DAILY SCHEDULE

➤ **December 4, 2021** | GMT+8, Beijing Time

Zoom Link: <https://zoom.us/j/91785403130> **Password:**120305

Conference Host: Prof. Ying Liu, Beijing Jiaotong University, Weihai, China

09:00-09:15	Opening Ceremony
09:00-09:05	Welcome Message Prof. Zhongliang Guan, Beijing Jiaotong University, China
09:05-09:10	Opening Remarks Prof. Masahiro Fujita, The University of Tokyo, Japan
09:10-09:15	Group Photo
09:15-11:45	Keynote Speech Session
09:15-10:00	Keynote Speech I Prof. Zhu Han, University of Houston, USA Topic: Federated Learning and Analysis in Mobile Edge Computing
10:00-10:45	Keynote Speech II Prof. Yonghui Li, The University of Sydney, Australia Topic: 5G Ultra Reliable and Low Latency Networks
10:45-11:00	Break Time
11:00-11:45	Keynote Speech III Prof. Junhui Zhao, Beijing Jiaotong University, East China Jiaotong University, China Topic: 5G Vehicular Networks: The Fusion of Computation and Communication
11:45-14:00	Lunch Time

DAILY SCHEDULE

➤ **December 4, 2021** | GMT+8, Beijing Time

Zoom Link: <https://zoom.us/j/91785403130> **Password:120305**

11:45-14:00	Lunch Time
14:00-16:00	Session 1 Session Topic: Communication and Information Security Session Chair: Dr. Richa Sharma, JK Lakshmipat University, Jaipur, India NS1002 NS1003 NS1010 NS1011 NS1006 NS1012

DAILY SCHEDULE

➤ **December 5, 2021** | GMT+8, Beijing Time

Zoom Link: <https://zoom.us/j/91785403130> **Password:**120305

10:00-11:40	Session 2 Session Topic: Advanced Information Technology and Management Session Chair: Prof. Chungen Xu, Nanjing University of Science and Technology, China NS0002 NS0003 NS1008 NS1009 NS1004
-------------	---

12:00-14:00	Lunch Time
-------------	------------

14:00-14:30	Closing Ceremony
-------------	------------------

14:30-16:30	Keynote Session Replay
-------------	------------------------

Authors Presentation — Session 1

Zoom Link: <https://zoom.us/j/91785403130>
Password: 120305

Communication and Information Security

Session Chair

Dr. Richa Sharma, JK Lakshmipat University, Jaipur, India

Session Time: 14:00-16:00, December 4, 2021, GMT+8, Beijing Time

Papers: NS1002 NS1003 NS1010 NS1011 NS1006 NS1012

Research on Topology Evolution of Autonomous System Network

Yue Zhang, Guozheng Yang, Zhihao Luo, Shicheng Zhou

Presenter: Yue Zhang, National University of Defense Technology, China

Abstract: After investigating the study about autonomous system level networks, we found that the latest data analysis used is open data provided in 2013. Thus, based on the open-source network BGP routing information provided by RouteViews from 2000 to 2020, this paper designs the calculation and analysis methods of the topological characteristic parameters of autonomous system level network combing the research theories and methods of Complex Network. Using these methods, the scale and topological characteristic parameters of the autonomous system-level network are calculated monthly from the global level and the national levels. And the evolution of the network scale and topological characteristics in the past 21 years are analyzed. Through analyzing the evolution of the number of connections, the number of network segments, the number of IP addresses, the number of nodes, the number of cores, the number of betweenness, and the average length of the path, and so on. Some regularities of network evolution are summarized. Firstly, some characteristics of the network are strongly correlated with each other. Since 2012, this kind of node has resumed its main part in the network whose number of degrees is 1, because the nodes of countries with late network development have gradually increased their influence. The evolution of the national autonomous system network characteristics is self-similar to the global network, but there are certain differences in different countries. These conclusions provide method support for the macro-level understanding of the Internet's topological characteristics and further inference of its evolutionary trend.

NS1002
14:00-14:20

<p>NS1003 14:20-14:40</p>	<p>The Side-Channel Vulnerability in Network Protocol Kaiqi Ru, Yanning Zheng, Xuewei Feng, Dongxia Wang Presenter: Kaiqi Ru, Institute of System Engineering AMS PLA, China</p> <p>Abstract: Some recent studies have found that there are some side-channel vulnerabilities in the operating system. Attackers would exploit the side-channel vulnerability for malicious purpose, such as hijack connections, denial of service attacks, etc. Currently, most attacks are detected manually. In this paper, we found that the reason for the existence of network protocol side-channel vulnerability is the use of shared resources. Since the state of shared resource affects all connections, when a connection uses a shared resource, information about that connection can be inferred by observing the usage of the shared resource. In order to find the shared resources, we implemented a tool called TASR which is a method of static analysis. The first is to find out what shared resources are available by the definition of shared resources in static analysis. Then, the data packet is used as the taint source to search the tainted shared resources. The second step is to analyze the taint-transmission-path according to the acquired tainted shared variable. Then it can find the side-channel vulnerability. By using this method on TCP, UDP and ICMP protocols, we find the following four shared variables: challenge_count, tcp_memory_allocated, tcp_memory_pressure, sysctl_icmp_msg_per_sec. It is difficult for tcp_memory allocated and tcp_memory pressure to exploit, because they will go through multiple strict checks. Using challenge_count can hijack the connection and inject malicious packets. Using sysctl_icmp_msg_per_sec can assist in DNS cache poisoning attack.</p>
<p>NS1010 14:40-15:00</p>	<p>Optimization of Spectrum Efficiency in UAV Cognitive Communication Network Based on Trajectory Planning Yilong GU, Yangchao Huang, Yuetong Zhang, Qi An, Huizhu Han, Youbin Fu, Yanhui Zhang Presenter: Yilong GU, Air Force Engineering University, China</p> <p>Abstract: In order to solve the shortage of spectrum resources and improve the spectrum efficiency (SE) in unmanned aerial vehicle (UAV) cognitive communication network, this paper optimizes the sensing radian and UAV's real-time trajectory from the perspective of time and space resource allocation. Firstly, the sensing radian is optimized to maximize throughput. Secondly, under the constraints of the primary user (PU) interference threshold, the maximum speed of UAV, the initial and terminal positions of UAV, the flight trajectory of UAV is optimized in real time by iteration algorithm to maximize the throughput. Finally, the SE optimization algorithm based on sensing radian allocation and trajectory planning for UAV cognitive communication is proposed. Simulation results show that the proposed algorithm is effective and better than existing schemes.</p>

<p>NS1011 15:00-15:20</p>	<p>Security Analysis of Embedded SIM Remote Provisioning Protocol Using SPIN Zhonglin Ding, Yang Hu, Wei Luo, Zhongming Huang, Lei Zhang, Zhongyuan Qin Presenter: Lei Zhang, Southeast University, China</p> <p>Abstract: With the advent of the 5G era, embedded SIM (eSIM) technology has been created to meet the needs of M2M technology. In earlier years, the GSMA provided a detailed description of the architecture and configuration protocol of the eSIM over-the-air writing technology. The remote configuration protocol of eSIM cards is divided into the processes of configuration file download, installation, activation, de-activation, and deletion. In this protocol, there are attacks such as identity impersonation threats, tampering threats, denial of service and eavesdropping threats, etc. This paper analyzes the security of key session establishment during the download and the installation of configuration files. And it uses a four-channel parallel method to simulate the session establishment process. The attacker is modeled based on the Dolev-Yao model. Through the test of the SPIN model detection tool, it is found that the attacker can intercept information from eSIM and SM-DP during the establishment of the key session. However, because the attacker lacks the key, he cannot obtain valid information from the obtained ciphertext. Therefore, the attacker cannot forge or modify the message. Our work proves the security of the eSIM system.</p>
<p>NS1006 15:20-15:40</p>	<p>Strengthening the Security of Deniable Authentication Scheme Using Zero-Knowledge Proof Asep Rizal Nurjaman and Ari Moesriami Barmawi Presenter: Asep Rizal Nurjaman, School of Computing Telkom University Bandung, Indonesia</p> <p>Abstract: In an electronic voting system, authentication is used to ensure that the voter is legitimate without knowing his/her identity, while the vote collectors verify the data is received from a legitimate user without knowing the identity of the voter. One of the authentication schemes that fulfilled this requirement is called a deniable authentication scheme, where the receiver can prove the source of the message while another party cannot identify the source of the message. In 2013, Li-Takagi et al. proposed a deniable authentication scheme. However, Li-Takagi's scheme has weaknesses if the receiver fully cooperates with the third party. In this case, the third party can identify the source of a given message. In the proposed method, zero-knowledge proof is introduced to preserve the anonymity of the deniable authentication scheme when the receiver fully cooperates with the third party. Based on the analysis, the proposed scheme fulfills the requirement of the deniable authentication scheme when the receiver fully cooperates with the third party. However, the proposed scheme has additional computation costs for securing the shared secret key. Two attack schemes that are carried out on both Li-Takagi and the proposed scheme are the MITM attack and the impersonation attack. The probability of breaking the proposed scheme using an MITM attack is higher than when using Li-Takagi's scheme, but the probability of breaking the proposed scheme using an impersonation attack is the same as Li-Takagi's scheme.</p>

Bidirectional Underwater Blue-green Laser Communication Based on OFDM Modulation

Lanjun Sun, Shaojun Zhang, Zhenshan Fu, Yuehong Gong, Yanchao Zhang

Presenter: Lanjun Sun, Shandong Jiaotong University, China

NS1012
15:40-16:00

Abstract: An underwater bidirectional laser wireless communication system based on orthogonal frequency division multiplexing (OFDM) is designed. High-power semiconductor lasers with 450nm and 520nm are employed as the light sources and APD is selected as the detector. Underwater wireless laser LAN communication based on IPV4 protocol is implemented, the communication rate of which can be up to 50Mbps. The blue-green laser communication system has the characteristics of fast transmission rate, high bandwidth, strong secrecy and small volume, which can realize LAN networking and internet connection. It has a good application prospect and practical value in the field of autonomous underwater vehicle and underwater sensor network.

Authors Presentation — Session 2

Zoom Link: <https://zoom.us/j/91785403130>

Password:120305

Advanced Information Technology and Management

Session Chair

Prof. Chungen Xu, Nanjing University of Science and Technology, China

Session Time: 10:00-11:40, December 5, 2021, GMT+8, Beijing Time

Papers: NS0002 NS0003 NS1008 NS1009 NS1004

The Role of Financial Technology for Development of Micro, Small and Medium Enterprises (Msmes) in Indonesia
Meiryani, Noviyanti Hanna Uli Pakpahan, Dianka Wahyuningtias, ZAIDI MAT DAUD, Suryadiputra Liawatimena
Presenter: Noviyanti Hanna Uli Pakpahan, Bina Nusantara University, Indonesia

NS0002
10:00-10:20

Abstract: The rapid development has made financial technology/financial technology's innovations more diverse according to the needs and financial problems that arise. With the existence of financial technology (financial technology) it can also make the financial service process faster, more effective and easier. Because of the development in the field of financial technology with the various solutions offered, this study aims to examine the role of financial technology for the development of MSMEs (Micro and Medium Enterprises), this research also includes aspects of the role of financial inclusion for the development of MSMEs to be able to see how much public knowledge is about financial service products and risk knowledge. The case study in this research is MSMEs in the Tangerang area using quantitative methods. The results of research using multiple linear regression analysis found that the role of financial financial technology for the development of MSMEs has a significant positive effect. Meanwhile, financial inclusion for the development of MSMEs has a positive and insignificant effect on the dependent variable. This study concludes that the use of financial technology for MSME businesses, as well as the high reference to financial products, are important factors in encouraging the development of MSMEs.

<p>NS0003 10:20-10:40</p>	<p>Analysis of Software Accounting Effectiveness on Data Sales in Bliss Kitchen Meiryani, Hanny Franciska, Suryadiputra Liawatimena, Zaidi Mat Daud, Hana Ulinnuha Presenter: Hanny Franciska, Bina Nusantara University, Indonesia</p> <p>Abstract: The development of the increasingly advanced business world will certainly always be related to technological developments, especially in the current 4.0 era. In Indonesia, there are various types of companies such as services, manufacturing, food, and others. The development of the company will cause more and more complex transactions. It is very unlikely that the company has to record all forms of operations with a manual system, especially for large companies with so much data that they need a system to help process data quickly so that all transactions can be processed into reliable information. complete and accurate so that the company's goals can be realized. The purpose of this study was to determine the effectiveness of accurate accounting software for recording sales reports in one of the companies that engaged in food & beverage, namely Bliss Kitchen. The research that the writer did used is a quantitative approach with a survey method. This study finds that Accurate software that applied in Bliss kitchen is effective. Evidence shows the results of the questionnaire from Bliss Kitchen employees is positive about Accurate.</p>
<p>NS1008 11:00-11:20</p>	<p>Mission-Oriented Networks Robustness Based on Cascade Model Tao Ma, Fang Yang, Chao Chang, Jun Huang Presenter: Fang Yang, National University of Defense Technology, China</p> <p>Abstract: In network science, network connectivity is usually used to evaluate network performance, but this does not represent the services that network systems can provide. Therefore, the robustness of the mission when the network is damaged represents the service survivability of the network. This article introduces missions into the network system and constructs a mission-oriented network model. In this model, the execution of each mission requires resources. When resources are insufficient, the mission is completed by mutual communication and cooperation between nodes. Due to the damage of some nodes in the network system, the allocation of mission resources and the communication path will be changed. This may cause other nodes to fail due to congestion or overload. We build a cascading failure model to describe this process. This paper compares different attack strategies through simulation experiments, it is found that node resources will play a critical role in robustness.</p>

<p>NS1009 10:40-11:00</p>	<p>Lightweight Hybrid Data Exfiltration using DNS based on Machine Learning Samaneh Mahdavifar, Amgad Hanafy Salem, Princy Victor, Miguel Garzon, Amir H. Razavi, Natasha Hellberg, Arash Habibi Lashkari Presenter: Samaneh Mahdavifar, UNB, Canada</p> <p>Abstract: Domain Name System (DNS) is a popular way to steal sensitive information from enterprise networks and maintain a covert tunnel for command and control communications with a malicious server. Due to the significant role of DNS services, enterprises often set the firewalls to let DNS traffic in, which encourages the adversaries to exfiltrate encoded data to a compromised server controlled by them. To detect low and slow data exfiltration and tunneling over DNS, in this paper, we develop a two-layered hybrid approach that uses a set of well-defined features. Because of the lightweight nature of the model in incorporating both stateless and stateful features, the proposed approach can be applied to resource-limited devices. Furthermore, our proposed model could be embedded into existing stateless-based detection systems to extend their capabilities in identifying advanced attacks. We generate and release CIC-Bell-DNSEXF-2021, a large dataset of 270.8 MB DNS traffic generated by exfiltrating various file types ranging from small to large sizes. We leverage our developed feature extractor to extract 30 features from the DNS packets, resulting in a final structured dataset of 323,698 heavy attack samples, 53,978 light attack samples, and 641,642 distinct benign samples. The experimental analysis of utilizing several Machine Learning (ML) algorithms on our dataset shows the effectiveness of our hybrid detection system even in the existence of light DNS traffic.</p>
<p>NS1004 11:20-11:40</p>	<p>SDNHive: A Proof-of-Concept SDN and Honeygot System for Defending Against Internal Threats Meatasit Karakate, Hiroshi Esaki, and Hideya Ochiai Presenter: Meatasit Karakate, The University of Tokyo, Japan</p> <p>Abstract: Nowadays, ransomware attacks are becoming more popular because they allow attackers to receive ransom payments from their victims. While older ransomware used to spread using social engineering means, modern ransomware tends to also be equipped with worm-like features. This allows it to propagate from the initially infected device to other computers in the same network. Those attacks motivated us to propose SDNHive, a proof-of-concept SDN and Honeygot-based protection system that can protect clean devices from being attacked by ransomware-infected devices in the same network. For intrusion protection, SDNHive implements address blacklisting, connection blocking, and transparent traffic rerouting inside the controller. These functions are called by the honeygot through our custom API once malicious activities are detected. Therefore, the honeygot in our system is not simply a decoy host, but a real intrusion detection device that can detect SMB and ARP scans. Our system is unique since state-of-the-art systems use only the SDN controller for both detection and protection. Still, we also implement the SMB and ARP scan detection functions inside the SDN controller as well in order to compare both SDN-only and SDN+Honeygot approaches. To demonstrate the performance of SDNHive, we create a Virtual Malware Testbed that simulates a real-life network with the ONOS SDN controller, the honeygot, and a mix of Linux and Windows virtual machines.</p>

We evaluate our system by using it to prevent WannaCry, a well-known SMB ransomware, from propagating to other hosts inside our testbed. Additionally, we also monitor CPU usage for each of the functions inside the system. When using only the SDN controller, our system is able to detect WannaCry within 20 seconds from the start of the propagation. The CPU usage stays at about 20 percent. However, when we make both the SDN controller and the honeypot work together, WannaCry is detected in only 2.5 seconds, and the CPU load is negligible. This proves that our SDN+Honeypot approach is better than the current SDN-only solutions.

➤ Beijing Jiaotong University, Weihai, China



Beijing Jiaotong University is a national key university under the direct administration of the Ministry of Education and now is jointly supported by the Ministry of Education, the China Railway Corporation and Beijing Municipal Government. Weihai campus is invited by Weihai Municipal People's government. In order to adapt to the development of National Blue Economic Zone and the need of further building a perfect regional national education system, it carries out high-level and international education in Nanhai New Area of Weihai with the mode of “building a nest to attract Phoenix”.



Beijing Jiaotong University attaches great importance to the development and construction of Weihai campus, taking Weihai campus as the main position of Sino foreign cooperation in running schools, the training base for international teaching staff, the experimental area for comprehensive reform of the University and the demonstration area for serving the local economic and social development. Weihai campus is characterized by Sino foreign cooperation in running schools.

The multicultural atmosphere, collegiate system and association construction in campus ensure the education mechanism of all staff involving, and guarantee the inheritance and innovation of school motto “Knowing & Doing”. “Think of the source while drinking the water, love the country and honor the alma mater.” Now, adhering to the university motto of “knowing and doing”, Weihai Campus shoulders a new mission and is serving the development of Weihai’s international “exquisite city” with a more pioneering spirit and the construction goal of “world-class university with distinctive characteristics”.



Address:

No.69, Xiandai Road,
Nanhai New Area, Weihai
City, Shandong Province,
China



ICCNS

Communication and Network Security

***Thank you for
attending ICCNS 2021***



北京交通大学(威海)
Beijing Jiaotong University, Weihai