## 1. Web Service Category Recommendation with Feature Word Semantic Enhancement and tag Co-occurrence

**Accession number:** 20234715078004
**Authors:** Guoqing, Pan (1); Yuan, Chang (1); Haoquan, Qi (1); Qiang, Hu (1)
**Author affiliation:** (1) College of Information Science and Technology, Qingdao University of Science and Technology, Qingdao, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 686-689
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** The generation quality of service function vectors in the existing Web category recommendation methods is not high. Most methods lack the consideration of label association. It may lead to inaccurate classification. To solve the above problems, this paper proposes a Web service category recommendation method with keyword semantic enhancement and label co-occurrence. TextRank is used to extract the keywords in the service description. The keyword vector and the service description vector generated by Bert are concatenated to enhance the semantic features of the service function vectors. With the help of the co-occurrence relationship of labels, a label co-occurrence graph is constructed, and Node2Vec is used for node embedding representation. The rationality of multi-label classification combination is improved by incorporating the co-occurrence degree of label combination. Real data in Programmable is used for label recommendation. Experiments show that the proposed method is superior to the comparison methods in terms of precision and recall rate. Thus, the proposed method effectively improves the accuracy and rationality of Web service category recommendation. © 2023 IEEE.
**Number of references:** 19
**Main heading:** Vectors
**Controlled terms:** Classification (of information) - Quality of service - Semantic Web - Semantics - Web services - Websites
**Uncontrolled terms:** Co-occurrence - Feature words - Function vector - Recommendation methods - Semantic enhancements - Service category - Service description - Service functions - Service tag - Webs services
**Classification code:** 716.1 Information Theory and Signal Processing - 723 Computer Software, Data Handling and Applications - 903 Information Science - 903.1 Information Sources and Analysis - 921.1 Algebra
**DOI:** 10.1109/NaNA60121.2023.00118
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 2. A Novel Detector Based on Adaptive Bistable Stochastic Resonance for Spectrum Sensing at Low Signal-to-Noise Ratio

**Accession number:** 20234715078065
**Authors:** Liu, Jin (1); Li, Zan (2); Miao, Qiguang (1); Yang, Li (1)
**Author affiliation:** (1) School of Computer Science and Technology, Xidian University, Xi'an, China; (2) School of Telecommunications Engineering, Xidian University, Xi'an, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 64-71

**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** The spurring demand of wireless communication services leads to a more crowded and overlapped spectrum, and the consequent increasing of the background noise and interference make the spectrum sensing in low signal-to-noise ratio (SNR) conditions a practical and challenging issue. To improve the performance of traditional energy detector at low SNR, a new energy detector using adaptive bistable stochastic resonance (ABSR) technique is investigated. By studying the response mechanism of nonlinear bistable system, the ABSR system is realized by bistable system parameters self-adaptive adjustment, and it assures the SNR improvement of received signals by the cooperative resonance effect of ABSR system. Encouraged by the excellent SNR gain characteristics of the ABSR technique, the ABSR-based energy detector is constructed by introducing the ABSR system as the preprocessing unit of traditional energy detector. Both the theoretical analyses and experiment results validate that approximately 7dB detection performance improvement of the ABSR-based detector when compared with the traditional energy detector at low SNR. © 2023 IEEE.
**Number of references:** 22
**Main heading:** Signal to noise ratio
**Controlled terms:** Circuit resonance - Magnetic resonance - Signal detection - Stochastic systems
**Uncontrolled terms:** Adaptive bistable stochastic resonance - Bistable stochastic resonance - Energy detectors - Low signal-to-noise ratio - Overlapped spectra - Resonance technique - Signal to noise ratio gains - Spectrum sensing - Wireless communication services
**Classification code:** 701.2 Magnetism: Basic Concepts and Phenomena - 703.1 Electric Networks - 716.1 Information Theory and Signal Processing - 731.1 Control Systems - 961 Systems Science
**DOI:** 10.1109/NaNA60121.2023.00019
**Funding Details:** Number: 62001356, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: 2022YFC3301300,62121001, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China; Number: 61825104, Acronym: -, Sponsor: National Science Fund for Distinguished Young Scholars;
**Funding text:** This work was supported in part by the National Natural Science Foundation of China under Grant 62001356, in part by the National Natural Science Foundation for Distinguished Young Scholar under Grant 61825104, in part by the National Key Research and Development Program of China under Grant 2022YFC3301300 and in part by the Innovative Research Groups of the National Natural Science Foundation of China under Grant 62121001.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 3. Performance Evaluation for Grant-Free NOMA System Using Hybrid SCMA-OFDM

**Accession number:** 20234715078086
**Authors:** Chen, ZiJian (1); Peng, Limei (1)
**Author affiliation:** (1) School of Computer Science and Engineering, Kyungpook National University, Daegu, Korea, Republic of
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 711-715
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.

**Abstract:** Grant-free non-orthogonal multiple access (GF-NOMA) technology shows promise in serving massive machine-type communication (mMTC) Internet-of-Thing (IoT) users, thanks to its low signaling and transmission overhead. Nonetheless, GF-NOMA technology suffers from severe collisions due to the absence of grants, leading to incorrect decoding and transmission inefficiency. To reduce collisions in the GF-NOMA system, we propose a hybrid framework that incorporates Sparse Code Multiple Access (SCMA) in the power domain non-orthogonal multiple access (PD-NOMA) system. This framework classifies users into two different groups based on their power levels. One group of users employs SCMA, distinguishing themselves from each other using their respective codebooks. The other group consists of traditional users utilizing orthogonal frequency-division multiplexing (OFDM). By adopting this approach, we can utilize the same amount of spectrum resources as in traditional PD-NOMA while increasing the number of contention transmission units (CTUs) to reduce the probability of collisions. Simulation results indicate that our proposed framework achieves a higher decoding success rate compared to traditional PD-NOMA. © 2023 IEEE.
**Number of references:** 7
**Main heading:** Orthogonal frequency division multiplexing
**Controlled terms:** Decoding - Internet of things - Multiple access interference - Transmissions
**Uncontrolled terms:** Grant-free non-orthogonal multiple access. - Hybrid framework - Interference - Multiple access - Non-orthogonal - Power domain non-orthogonal multiple access - Powerdomains - Simulation - Sparse code multiple access - Sparse codes
**Classification code:** 602.2 Mechanical Transmissions - 722.3 Data Communication, Equipment and Techniques - 723 Computer Software, Data Handling and Applications - 723.2 Data Processing and Image Processing
**DOI:** 10.1109/NaNA60121.2023.00122
**Funding Details:** Number: -, Acronym: MSIP, Sponsor: Ministry of Science, ICT and Future Planning; Number: NRF-2022H1D3A2A01063679, Acronym: NRF, Sponsor: National Research Foundation of Korea;
**Funding text:** ACKNOWLEDGMENT This work was supported by the Brain Pool program funded by the Ministry of Science and ICT through the National Research Foundation of Korea (Grant number: NRF-2022H1D3A2A01063679).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 4. Cost-Sensitive Cold Start Latency Optimization Mechanism in Function-as-a-Service

**Accession number:** 20234715078031
**Authors:** Liu, Ruiyan (1); Ma, Tengchao (1); Huang, Yiting (1); An, Qingzhao (1); Yan, Lin (1); Li, Jiangyuan (2)
**Author affiliation:** (1) Beijing University of Posts and Telecommunications, State Key Laboratory of Networking and Switching Technology, Beijing, China; (2) The Second High School Attached, Beijing Normal University, Beijing, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 453-458
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Function-as-a-Service (FaaS), as a cloud computing service, builds, runs, and manages application packages directly in a functional way, greatly improving development and delivery efficiency, and is a major trend in the future development of cloud services. However, FaaS is executed via event-driven execution and has a cold-start problem at runtime. Most of the existing research focuses on function runtime optimization and ignores cold start time. For business scenarios with high real-time requirements, prolonged cold starts can affect business results. Therefore, cold-start optimization is particularly important for the application of function computing in latency-sensitive scenarios. To reduce the impact of cold start latency on services, this paper proposes a memory configuration to reduce cold start. Firstly, a memory-cost model is constructed based on memory resource rules and service computation time rules, and the model is optimized using a gradient descent algorithm. The results of large-scale simulations show that the memory selection scheme proposed in this paper can reduce the cold start latency by about 25% compared to the memory selection of conventional function services in existing cases. © 2023 IEEE.

**Number of references:** 20
**Main heading:** Cloud computing
**Controlled terms:** Gradient methods - Optimization - Web services
**Uncontrolled terms:** Cloud computing services - Cloud services - Cloud-computing - Cold start problems - Cold-start - Cost-sensitive - Event-driven - Function-as-a-service - Latency optimizations - Serverless computing
**Classification code:** 722.4 Digital Computers and Systems - 921.5 Optimization Techniques - 921.6 Numerical Methods
**DOI:** 10.1109/NaNA60121.2023.00081
**Funding Details:** Number: JZX6Y202211010822, Acronym: -, Sponsor: -;
**Funding text:** VI. ACKNOWLEDGEMENT This work is supported by Beijing University of Posts and Telecommunicationsadvanced research program in the 14th five-year plan (JZX6Y202211010822).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 5. Resisting Membership Inference Attacks by Dynamically Adjusting Loss Targets

**Accession number:** 20234715078036
**Authors:** Ma, Xihua (1, 2); Tian, Youliang (1, 2, 3); Ding, Zehua (1, 2)
**Author affiliation:** (1) Guizhou University, State Key Laboratory of Public Big Data, Guiyang; 550025, China; (2) College of Computer Science and Technology, Guizhou University, Guiyang; 550025, China; (3) Institute of Cryptography and Data Security, Guizhou University, Guiyang; 550025, China
**Corresponding author:** Tian, Youliang(youliangtian@163.com)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 574-579
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Machine learning (ML) models are susceptible to membership inference attacks (MIAs), which aim to infer whether a particular sample was involved in model training. Previous research suggests that the difference in loss distribution between member and non-member sample is an essential factor of MIAs. In the latest mitigation strategies to reduce the loss distribution discrepancy, the model owner must manually set a loss target for the training task. However, this can be challenging due to differences in datasets and model structures. We propose a new mitigation strategy based on existing studies, which can dynamically adjust the loss target during the training process according to the model structure and dataset characteristics, to achieve a reduced loss gap. We extensively evaluated our strategy in white-box and black-box environments, respectively. Our experimental results show that our approach avoids the problem of setting loss targets and even improves the model's resistance to attacks in most cases. Specifically, the accuracy of the attacks is reduced by an average of 4.92% and 11.3% in the black-box and white-box environments, respectively. © 2023 IEEE.
**Number of references:** 22
**Main heading:** Machine learning
**Controlled terms:** Model structures
**Uncontrolled terms:** Black boxes - Inference attacks - Loss distribution - Machine learning models - Machine-learning - Membership inference attack - Mitigation strategy - Model training - Privacy protection - White box
**Classification code:** 723.4 Artificial Intelligence
**DOI:** 10.1109/NaNA60121.2023.00100
**Funding Details:** Number: [2015]-53, Acronym: -, Sponsor: -; Number: [2020]6008, Acronym: -, Sponsor: -; Number: [2021]1-5,[2022]2-4, Acronym: -, Sponsor: -; Number: [2022]065, Acronym: -, Sponsor: -; Number: 62272123,No.U1836205, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: 2021YFB3101100, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China;

**Funding text:** VII. ACKNOWLEDGE This work was supported by the National Key Research and Development Program of China under Grant No.2021YFB3101100; Key Program of the National Natural Science Union Foundation of China under Grant No.U1836205; Project of High-level Innovative Talents of Guizhou Province under Grant No. [2020]6008; Science and Technology Program of Guiyang under Grant No.[2021]1-5; Science and Technology Program of Guiyang under Grant No.[2022]2-4; Science and TechnologyProgram of Guizhou Province under Grant No. [2020]5017, No. [2022]065; National Natural Science Foundation of China under Grant 62272123; Guizhou University Talent Introduction Research Fund under Grant No.GDRJHZ[2015]-53.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 6. The Design Method of Micro-Unit Cryptographic Service Framework

**Accession number:** 20234715078054
**Authors:** Zhao, Qi (1); Tian, Bo (1); Liu, Yiming (1)
**Author affiliation:** (1) Science and Technology on Communication Security Laboratory, Chengdu, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 698-704
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** In order to adapt to the rapid development of information technology in the digital age, it is necessary to build a general cryptographic service delivery capability to provide security protection for data exchange in various scenarios.Cryptographic services need to be combined with a variety of complex cryptographic technologies to establish a secure foundation. At the same time, the efficiency of implementation must be guaranteed. In order to meet this demand, a micro-unit cryptographic service framework is proposed. Based on microservices, plug-in, service engine and other technologies, a micro-unit crypto service platform supporting functional reconfiguration is designed. The programmable micro-unit crypto component can generate service links according to the quality of service, and provide flexible access methods for crypto service. The crypto function of the client and the server can be divided into fine-granularity units, which can be combined into a more flexible crypto system which can adapt to the rapid change of security requirements and deal with new security threats. Based on this framework, crypto service providers can quickly establish a scalable crypto service system that can adapt to various scenarios, meet different security levels and be easily expanded. © 2023 IEEE.
**Number of references:** 18
**Main heading:** Electronic data interchange
**Controlled terms:** Cryptography - Engines - Quality of service
**Uncontrolled terms:** Business engine - Cryptographic service - CryptoGraphics - Design method - Digital age - Micro unit - Microservice - Plug-ins - Service delivery - Service framework
**Classification code:** 723.2 Data Processing and Image Processing
**DOI:** 10.1109/NaNA60121.2023.00120
**Funding Details:** Number: 2022YFG0172, Acronym: -, Sponsor: Shanxi Provincial Key Research and Development Project;
**Funding text:** ACKNOWLEDGMENT This work is supported by the key research and development plan project of Sichuan Province "Research on Internet-based High Security Information Transmission and Storage Technology" (2022YFG0172).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village

## 7. A Trusted Privacy-Preserving Model for Cross-Chain Transactions Based on zk_SNARKs

**Accession number:** 20234715078073
**Authors:** Wang, Yichuan (1, 2); Tie, Jianhuan (1); Hei, Xinhong (1, 2); Zhao, Li (1); Zhang, Xiaohui (1)
**Author affiliation:** (1) School of Computer Science and Engineering, Xi'an University of Technology, Xi'an, China; (2) Shaanxi Key Laboratory for Network Computing and Security Technolog, Xi'an, China
**Corresponding author:** Hei, Xinhong(heixinhong@xaut.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 187-192
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Currently, the privacy protection technology of blockchain is not mature enough, such as user data leakage and lack of anonymity exist, and these problems are especially serious when conducting cross-chain transactions. In this paper, we propose a method of cross-chain transactions based on zk_SNARKs in a trusted environment for cross-chain transactions for privacy protection. Cross-chain transactions are performed through the features of zk_SNARKs such as efficiency, privacy, and verifiability. zk_SNARKs needs to generate trusted settings with the help of a third party during the transaction, and the process has serious privacy issues, and the private parameters generated during the transaction may be maliciously attacked and thus obtained by attackers. To address this problem, we use a hardware technology SGX for trusted computing to encrypt and store some private parameters generated by zk_SNARKs, thus ensuring the security of cross-chain transactions. The experimental results show that the privacy protection scheme using SGX for cross-chain transactions takes less time than the traditional transaction privacy protection, with a verification time of 1.2s for a number of 10 sidechains, and is more efficient than the traditional cross-chain transaction privacy protection. © 2023 IEEE.
**Number of references:** 21
**Main heading:** Blockchain
**Controlled terms:** Privacy-preserving techniques - Trusted computing
**Uncontrolled terms:** Block-chain - Component - Cross-chain transaction - Data leakage - Privacy preserving - Privacy protection - Protection technologies - User data - Verifiability - Zk_SNARK
**Classification code:** 716 Telecommunication; Radar, Radio and Television - 718 Telephone Systems and Related Technologies; Line Communications - 723.2 Data Processing and Image Processing - 723.3 Database Systems
**DOI:** 10.1109/NaNA60121.2023.00039
**Funding Details:** Number: 2021JLM-58, Acronym: -, Sponsor: -; Number: 62072368,U20B2050, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: 2022GY-040, Acronym: -, Sponsor: Shanxi Provincial Key Research and Development Project;
**Funding text:** ACKNOWLEDGMENT This research work is supported by the National Natural Science Founds of China (62072368, U20B2050), Key Research and Development Program of Shaanxi Province (2022GY-040), Basic Research in Natural Science and Enterprise Joint Fund of Shaanxi (2021JLM-58).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 8. Trajectory and Offloading Policy Optimization in Age-of-Information-Aware UAV-Assisted MEC Systems

**Accession number:** 20234715078094
**Authors:** Yang, Yulu (1); Yang, Jingce (1); Xu, Han (1); Hu, Jing (1); Song, Tiecheng (1)
**Author affiliation:** (1) Southeast University, National Mobile Communications, Research Laboratory, Nanjing, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA

**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 175-180
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Unmanned Aerial Vehicles (UAVs) have been studied in Mobile Edge Computing (MEC) networks in many researches due to their distinctive advantages, especially in emergency and dynamic scenarios. In this paper, we propose a UAV-assisted MEC system in the disaster scenario, where the UAVs are deployed to undertake the computing and relaying tasks. To ensure the freshness of data as well as the energy efficiency of the system, we jointly minimize the Age of Information (AoI) of the User Equipment (UE) and the energy consumption of the UAVs by optimizing the UAVs' trajectories and the offloading strategies. The non-convex optimization problem is solved in two steps: firstly we propose a Multi-Agent Deep Reinforcement Learning (MADRL) based algorithm to find the optimal trajectory, and then we use a traversal-based algorithm to optimize the offloading policy greedily. Numerical simulations are carried out to verify the validity of the proposed algorithm. It is shown that it has better performance than the baseline algorithms, and is highly reliable in random environments. © 2023 IEEE.
**Number of references:** 13
**Main heading:** Reinforcement learning
**Controlled terms:** Antennas - Convex optimization - Deep learning - Energy efficiency - Energy utilization - Mobile edge computing - Multi agent systems - Trajectories - Unmanned aerial vehicles (UAV)
**Uncontrolled terms:** Aerial vehicle - Age of information - Computing system - Information-aware - Mobile edge computing - Multi agent - Multi-agent deep reinforcement learning - Policy optimization - Reinforcement learnings - Unmanned aerial vehicle
**Classification code:** 461.4 Ergonomics and Human Factors Engineering - 525.2 Energy Conservation - 525.3 Energy Utilization - 652.1 Aircraft, General - 722.4 Digital Computers and Systems - 723.4 Artificial Intelligence
**DOI:** 10.1109/NaNA60121.2023.00037
**Funding Details:** Number: 2020YFB1600104, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China; Number: BE2020084-2, Acronym: -, Sponsor: Key Research and Development Program of Jiangxi Province;
**Funding text:** ACKNOWLEDGMENT This work was supported in part by the Key Research and Development Plan of Jiangsu Province under Grant BE2020084-2, in part by the National Key Research and Development Program of China under Grant 2020YFB1600104.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 9. B-Pet: The PET Model with Parameter-Efficient Learning

**Accession number:** 20234715078076
**Authors:** Zheng, Qi (1); Yu, Haizheng (1)
**Author affiliation:** (1) College of Mathematics and System Sciences, Xinjiang University, Urumqi, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 595-600
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023

**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** In recent years, under the trend of training models in big data, Few-shot learning (FSL) which aims to learn models to solve problems with a few samples has also achieved good results on many data sets. In fact, acquiring high-quality training samples is expensive in many aspects, but FSL can save the overhead costs. Among FSL models, the PET model combines semi-supervised learning, prompt learning and knowledge distillation based on the pre-training language model. However, in fine-turning the PET model has the disadvantages that consumes a lot of resources and time and requires heavy costs of storage for model preservation. Therefore, this paper proposes the B-pet model, which freezes most of the training parameters and only trains bias parameters during fine-turning process, significantly reducing the storage consumption of the model for downstream tasks. We used six data sets with tau =10 50 100 and three different data training models respectively. The results show that four data sets on the B-pet model performed better than original PET model training. It is obvious that in the memory-constrained environment deployment, multitasking fine-tunes models have practical value. It also proved that most semi-supervised models with fixed parameters are realizable. © 2023 IEEE.
**Number of references:** 23
**Main heading:** Digital storage
**Controlled terms:** Distillation - Learning systems
**Uncontrolled terms:** Data set - Efficient learning - Few-shot learning - Fine tuning - Fine turning - High quality - Learn+ - Parament efficient fine-tuning - Prompt-based learning - Training model
**Classification code:** 722.1 Data Storage, Equipment and Techniques - 802.3 Chemical Operations
**DOI:** 10.1109/NaNA60121.2023.00103
**Funding Details:** Number: 2021D01C078, Acronym: -, Sponsor: Natural Science Foundation of Xinjiang;
**Funding text:** VIII. ACKNOWLEDGE This work is supported in part by Xinjiang Natural Science Foundation of China (2021D01C078).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 10. An ASN.1 UPER Encoding Based Fuzzing Method for Radio Resource Control Protocol

**Accession number:** 20234715078080
**Authors:** Wang, Rui (1); Liu, Donglan (2); Liu, Xin (2); Ma, Lei (2); Zhang, Hao (2); Wang, Yong (3); Li, Zhenghao (3); Zhang, Fangzhe (2); Sun, Lili (2)
**Author affiliation:** (1) Shandong Smart Grid Technology Innovation Center, China; (2) State Grid Shandong Electric Power Research Institute, Jinan, China; (3) State Grid Shandong Electric Power Company, Jinan, China
**Corresponding author:** Wang, Rui(wangrui_dky@163.com)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 268-273
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Fuzz testing is one of the most direct and effective automated vulnerability mining methods. The latest approach in vulnerability mining related to protocols specified based on ASN.1 such as the Radio Resource Control (RRC) protocol is to compile a large number of manually constructed malformed ASN.1 schema and then generate messages based on these schemas thus fuzz testing the protocol. However, this approach is relatively simple and the seed construction way is not effective enough, which can affect the efficiency and effectiveness of the fuzz testing. Therefore, some works proposed to implement fuzz testing by extracting an abstract syntax tree (AST), which mutates messages on the intermediate format to trigger deeper logic. Inspired by this, this paper proposes a fuzz testing method for RRC protocols based on ASN.1 UPER encoding details, extracting the ASN.1 syntax tree at the

intermediate level and placing the mutation after compiling the ASN.1 schema. This reduces the mutation message construction time and space on the one hand, and enables the mutation to cover more fields on the other. © 2023 IEEE.
**Number of references:** 18
**Main heading:** Trees (mathematics)
**Controlled terms:** Encoding (symbols) - Signal encoding - Syntactics
**Uncontrolled terms:** 5g - ASN.1 UPER encoding - Control protocols - Encodings - Fuzz Testing - Mining methods - Radio resource control - Radio resource control protocol - Simple++ - Vulnerabilities minings
**Classification code:** 716.1 Information Theory and Signal Processing - 723.2 Data Processing and Image Processing - 921.4 Combinatorial Mathematics, Includes Graph Theory, Set Theory
**DOI:** 10.1109/NaNA60121.2023.00052
**Funding Details:** Number: 520626220016, Acronym: -, Sponsor: -;
**Funding text:** ACKNOWLEDGMENT This research is sponsored by the project of State Grid Shandong Electric Power Company Science and Technology Program, Project Name: Research on Key Technologies of Smart Grid 5G Secure Access and Trusted Data Sharing - Topic 1: Research on Key Technologies of Smart Grid 5G Terminals and Network Security Detection and Risk Assessment, ERP Number: 520626220016.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 11. Attribute-based Verifiable Outsourcing Decryption Encryption Scheme in IIoT

**Accession number:** 20234715078014
**Authors:** Li, Yang (1); Zhang, Qingyang (2); Cheng, Jun (3); Zhou, Yiyuan (2); Cui, Jie (2); Zhong, Hong (2)
**Author affiliation:** (1) Anhui Province Key Laboratory of Cyberspace Security Situation Awareness and Evaluation, Hefei, China; (2) School of Computer Science and Technology, Anhui University, Hefei, China; (3) School of Computer and Artificial Intelligence, Chaohu University, Hefei, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 332-338
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** With the continuous development of the Industrial Internet of Things (IIoT), more and more private data from IIoT devices is being outsourced to the cloud, and ensuring data privacy is becoming increasingly urgent. Attribute-based additive technology is gradually used in IIoT. However, attribute-based encryption technology will produce a lot of computing costs, which can not be satisfied by resource-constrained devices. Therefore, in the environment of edge support, some operations of encryption and decryption can be outsourced to edge nodes to reduce the computing cost of data owners. In this paper, we propose a verification-supported outsourcing attribute-based encryption scheme, which outsources part of the encryption operation and part of the decryption operation to the edge node, and adds the verifiable function to ensure that the ciphertext returned by the edge node is correct. And we analyze the security of the scheme. Experimental results show that the proposed scheme is more effective than the traditional scheme for resource-constrained IIoT devices. © 2023 IEEE.
**Number of references:** 21
**Main heading:** Outsourcing
**Controlled terms:** Cryptography - Data privacy - Edge computing - Internet of things
**Uncontrolled terms:** Attribute-based - Attribute-based encryption of outsourcing - Attribute-based encryptions - Computing cost - Continuous development - Edge nodes - Encryption schemes - Industrial internet of thing - Security - Verifiability
**Classification code:** 722.3 Data Communication, Equipment and Techniques - 722.4 Digital Computers and Systems - 723 Computer Software, Data Handling and Applications - 912.2 Management

**DOI:** 10.1109/NaNA60121.2023.00062
**Funding Details:** Number: 62272002, Acronym: NSFC, Sponsor: National Natural Science Foundation of China;
**Funding text:** The work was supported in part by Open Fund of Anhui Province Key Laboratory of Cyberspace Security Situation Awareness and Evaluation, in part by the National Natural Science Foundation of China under Grant 62272002. The authors are very grateful to the anonymous referees for their detailed comments and suggestions regarding this paper.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 12. A Novel Construction Technology of Microservice Multi-Instance System Automatic Deployment and Upgrade

**Accession number:** 20234715078008
**Authors:** Zeng, Ruiqi (1); Niu, Yiru (2); Qiao, Lanfei (2)
**Author affiliation:** (1) No.30 Research Institute of China Electronics Technology Group Corporation, China Electronics Technology Cyber Security Co., Ltd, Chengdu, China; (2) No.30 Research Institute of China Electronics Technology Group Corporation, China Electronics Technology Cyber Security Co., Ltd, Science and Technology on Communication Security Laboratory, Chengdu, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 674-679
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** With continuous development of software architecture, system has changed from single architecture to microservice multi-cluster architecture, and containerization technology has also been developed to solve the increasingly complex deployment model of microservice architecture. Compilation, packaging, image production, deployment, and upgrading during the software release process are inefficient due to manual processing. Although there are many researches on software architecture, containerization technology, construction technology, but they are relatively independent, and there are few comprehensive plans that combine these technologies together to improve overall efficiency. This paper takes software deployment and management of the containerized multi-instance system as the research object, and proposes a construction plan of operation and maintenance platform. We designed a concise comprehensive experimental platform integrating software development, software construction, image production, system deployment, system operation and maintenance and upgrade. Through the construction and testing of the actual platform environment, the utility and stability of the platform are verified, improved software release efficiency. At the same time, the solution is simple and easy to manage, it can meet the general software operation and maintenance requirements in most scenarios. © 2023 IEEE.
**Number of references:** 11
**Main heading:** Efficiency
**Controlled terms:** Cluster computing - Computer software maintenance - Containers - Software architecture - Software design - Software testing
**Uncontrolled terms:** Architecture designs - CI/CD - Code management - Construction technologies - Containerized deployment - Image production - Novel construction - Operations and maintenance - Software release - Software upgrades
**Classification code:** 722.4 Digital Computers and Systems - 723 Computer Software, Data Handling and Applications - 723.1 Computer Programming - 723.5 Computer Applications - 913.1 Production Engineering
**DOI:** 10.1109/NaNA60121.2023.00116
**Compendex references:** YES
**Database:** Compendex

**Data Provider:** Engineering Village


## 13. Joint Deployment of LAU and HAU for Hierarchical Space-Air-Ground Communications

**Accession number:** 20234715078012
**Authors:** Mo, Jiang (1); Zhao, Ke (1); Peng, Limei (1)
**Author affiliation:** (1) School of Computer Science and Engineering, Kyungpook National University, Deagu, Korea, Republic of
**Corresponding author:** Peng, Limei(auroraplm@knu.ac.kr)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 133-137
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Unmanned aerial vehicles (UAVs) are becoming increasingly crucial in facilitating flexible and on-demand wireless connections in 5G and beyond (B5G) communication systems. This paper examines the joint deployment of Low Altitude UAVs (LAUs) and High Altitude UAVs (HAUs) within a four-tier Space-Air-Ground (SAG) communication system, which comprises ground IoT nodes, LAUs, HAUs, and satellites organized in a hierarchical structure, with the objective of achieving efficient and reliable transmission. The communication between an IoT node and the satellite in the SAG system occurs through a cascading wireless channel, involving sequential connections from the IoT node to the LAU, HAU, and satellite. The minimal data capacity among the links of a cascading channel becomes a bottleneck for communication. Therefore, it is essential to avoid significant rate differences among the cascading channel links and ensure a similar data rate across all links to maximize resource utilization efficiency. In this context, we propose a joint optimization of the deployment of LAUs and HAUs to maximize the minimum data capacity of links on a cascading channel. Specifically, we present a Particle Swarm Optimization (PSO) algorithm to achieve this goal. Simulation results demonstrate that the proposed PSO algorithm, which jointly optimizes the deployment of LAUs and HAUs, outperforms scenarios where LAUs and HAUs are deployed in fixed positions. © 2023 IEEE.
**Number of references:** 12
**Main heading:** Particle swarm optimization (PSO)
**Controlled terms:** 5G mobile communication systems - Antennas - Internet of things - Satellite communication systems - Satellites - Vehicle to vehicle communications
**Uncontrolled terms:** Aerial vehicle - Air/ground communication - Communications systems - Data capacity - Joint deployment of low altitude UAV and high altitude UAV - Low altitudes - On demands - Particle swarm optimization algorithm - Space-air-ground communication system - Wireless connection
**Classification code:** 655.2 Satellites - 655.2.1 Communication Satellites - 716.3 Radio Systems and Equipment - 722.3 Data Communication, Equipment and Techniques - 723 Computer Software, Data Handling and Applications - 921.5 Optimization Techniques
**DOI:** 10.1109/NaNA60121.2023.00030
**Funding Details:** Number: 4199990214394, Acronym: KNU, Sponsor: Kyungpook National University; Number: -, Acronym: MOE, Sponsor: Ministry of Education; Number: -, Acronym: MSIP, Sponsor: Ministry of Science, ICT and Future Planning; Number: NRF-2022H1D3A2A01063679, Acronym: NRF, Sponsor: National Research Foundation of Korea;
**Funding text:** VI. ACKNOWLEDGE This work was supported by the Brain Pool program funded by the Ministry of Science and ICT through the National Research Foundation of Korea (Grant number: NRF-2022H1D3A2A01063679) and by the BK21 FOUR project (AI-driven Convergence Software Education Research Program) funded by the Ministry of Education, School of Computer Science and Engineering, Kyungpook National University, Korea (4199990214394).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village

## 14. UD-YOLOv5s: Recognition of Cattle Regurgitation Behavior Based on Upper and Lower Jaw Skeleton Feature Extraction

**Accession number:** 20234715078084
**Authors:** Gao, Guohong (1); Wang, Chengchao (1); Wang, Jianping (1); Lv, Yingying (1)
**Author affiliation:** (1) School of Computer Science and Technology, Henan Institute of Science and Technology, Xinxiang, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 532-538
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Rumination is a crucial indicator for evaluating the health status of ruminants. However, Traditional contact devices, including ear tags and pressure sensors, may raise animal welfare concerns while detecting rumination behavior. Deep learning provides robust support for non-contact rumination behavior recognition through the training of datasets using neural networks. This paper presents a novel bovine rumination recognition method called UD-YOLOv5s, which combines YOLOv5s with upper and lower jaw skeleton feature extraction techniques. Firstly, a skeleton feature extraction method is proposed for the upper and lower jaws based on skeleton heatmap descriptors and the Kalman filter algorithm. Secondly, the UD-YOLOv5s method is designed for rumination recognition. Finally, a self-built bovine rumination dataset is used to compare the performance of three deep learning techniques, including MEAN-SHIFT, MASK-RCNN, and YOLOv3, with correlations. The results of the ablation experiment demonstrate that UD-YOLOv5s achieves a precision of 98.25%, recall of 97.75%, and a mean average precision of 93.43%. To ensure fairness, we conducted generalization performance-e evaluation in a controlled experimental environment, which showed that UD-YOLOv5s converge faster than other models while maintaining comparable recognition ac-curacy. Furthermore, our study demonstrates that when convergence speed is equal, UD-YOLOv5s outperforms other models in terms of recognition accuracy. Our findings provide robust support for the identification of cattle rumination behavior.

**Number of references:** 15
**Main heading:** Feature extraction
**Controlled terms:** Behavioral research - Deep learning - Extraction - Learning systems - Mammals - Musculoskeletal system
**Uncontrolled terms:** Animal welfare - Behavior-based - Behaviour recognition - Contact device - Features extraction - Health status - Non-contact - Ruminant - Skeleton extraction - Yolov5s
**Classification code:** 461.3 Biomechanics, Bionics and Biomimetics - 461.4 Ergonomics and Human Factors Engineering - 802.3 Chemical Operations - 971 Social Sciences
**DOI:** 10.1109/NaNA60121.2023.00094
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 15. A Novel Configurable RO-Obfuscated PUF Design with Machine Learning Immunity

**Accession number:** 20234715078020
**Authors:** Fan, Lu (1, 2); Huang, Zhao (2); Wang, Junjun (2); Zhou, Lirong (2); Zhu, Yi'an (1); Wang, Quan (2)
**Author affiliation:** (1) School of Software, Northwestern Polytechnical University, Xi'an, China; (2) School of Computer Science and Technology, Xidian University, Xi'an, China
**Corresponding author:** Huang, Zhao(z_hang@xidian.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA

**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 680-685
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Strong physical unclonable function (PUF) is a low-cost hardware security primitive to protect Internet-of-Things (IoT) devices. However, it may be attacked by machine learning (ML). Various PUF models designed in complex structures, such as nonlinearity or challenge-response pair (CRP) obfuscation, have been presented to combat these risks. However, these methods mainly increase area overhead, and the prediction rate is still very high. Therefore, this paper proposes a structure obfuscated PUF named SO-PUF. Our proposal derives from the configurable ring oscillator (CRO) PUF. The CRO can be transformed into two different structures depending on the challenges by randomly deleting one of the two NOT gates in each stage. Thus, half of the CRPs generated by SO-PUF are invalid, which will confuse the attackers. We have implemented and verified the performance of SO-PUF on the Xilinx-6XC6SLX25 microboard. Experimental results show that compared with the dual-mode PUF, the SO-PUF improves uniqueness by 0.71 %, temperature reliability by 38.4 %, and voltage reliability by 1.92 %. In addition, the SO-PUF also reduces the prediction rates of LR, SVM, and ANN modeling attacks by 0.26 %, 0.38 %, and 5.62 %, respectively. The results prove that SO-PUF has better resistance to ML attacks than dual-mode PUF. © 2023 IEEE.
**Number of references:** 19
**Main heading:** Internet of things
**Controlled terms:** Cryptography - Hardware security - Machine learning
**Uncontrolled terms:** Challenge-response pair - Challenge-response pair hidden - Dual modes - Function designs - Low cost hardware - Machine-learning - Modeling attack - Prediction-rates - Ring oscillator - Structure obfuscation
**Classification code:** 722.3 Data Communication, Equipment and Techniques - 723 Computer Software, Data Handling and Applications - 723.4 Artificial Intelligence
**DOI:** 10.1109/NaNA60121.2023.00117
**Funding Details:** Number: 61972302, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: XJS220306, Acronym: -, Sponsor: Fundamental Research Funds for the Central Universities; Number: 2022JQ-680, Acronym: -, Sponsor: Natural Science Basic Research Program of Shaanxi Province;
**Funding text:** ACKNOWLEDGMENT This work was supported in part by the National Natural Science Foundation of China under Grant 61972302, in part by the Fundamental Research Funds for the Central Universities under Grant XJS220306, in part by the Natural Science Basic Research Program of Shaanxi under Grant 2022JQ-680 and part by the Key Laboratory of Smart Human-Computer Interaction and Wearable Technologyof Shaanxi Province.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 16. PPKD: Privacy-preserving Knowledge Distillation for Large Model

**Accession number:** 20234715078046
**Authors:** Xu, Mengfan (1); Li, Jin (1); Liu, Yingying (2)
**Author affiliation:** (1) School of Computer Science, Shaanxi Normal University, Xi'an, China; (2) School of Business, Xi'an University of Finance and Economics, Xi'an, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 490-496
**Language:** English
**ISBN-13:** 9798350327380

**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** With the development of deep learning technology and the application of large-scale models, high training costs and a large number of model parameters have become bottlenecks that limit technological development. To address these issues, existing model distillation techniques can transfer knowledge from large models to small models, reducing the model size and computational resource consumption while maintaining high performance. However, existing research has overlooked the privacy protection of input data and large models during the distillation process. In practical scenarios, the entities who train student models and own teacher models may be different institutions or countries, and how to protect the privacy of training data and teacher models is a challenge facing cross-institutional distillation learning. To solve this problem, this paper proposes a privacy-preserving model distillation method combining random masking and threshold encryption systems. We introduce noise based on random masking into training data and encrypt the output of the teacher model, ensuring the privacy of the input data and teacher model while ensuring the performance of the distilled student model. We rigorously prove the security and correctness of the scheme in theory and validate its effectiveness through experiments. The experimental results show that the student model trained after data protection has a similar classification performance to the student model in the original distillation learning. © 2023 IEEE.
**Number of references:** 22
**Main heading:** Distillation
**Controlled terms:** Computation theory - Deep learning - Engineering education - Learning systems - Personnel training - Privacy-preserving techniques - Students
**Uncontrolled terms:** Distillation learning - Input datas - Large models - Performance - Privacy preserving - Random mask - Student Modeling - Teacher models - Threshold decryption - Threshold decryption cryptosystem
**Classification code:** 461.4 Ergonomics and Human Factors Engineering - 716 Telecommunication; Radar, Radio and Television - 718 Telephone Systems and Related Technologies; Line Communications - 721.1 Computer Theory, Includes Formal Logic, Automata Theory, Switching Theory, Programming Theory - 723.2 Data Processing and Image Processing - 802.3 Chemical Operations - 901.2 Education - 912.4 Personnel
**DOI:** 10.1109/NaNA60121.2023.00087
**Funding Details:** Number: 62206162,RAGR20220127, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: 2022JQ-594, Acronym: -, Sponsor: Natural Science Basic Research Program of Shaanxi Province;
**Funding text:** This work was supported by the Natural Science Basic Research Plan in Shaanxi Province (2022JQ-594), the National Natural Science Foundation of China under Grant No.62206162, and CCF-Tencent Open Fund (RAGR20220127).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 17. Data Security Storage Scheme For UAV Cluster Based On Distributed Storage

**Accession number:** 20234715078021
**Authors:** Wu, Kaijun (1, 2, 3); Tian, Bo (1, 2, 3); Wang, Xue (1, 2, 3)
**Author affiliation:** (1) Science and Technology on Communication Security Laboratory, Chengdu; 610041, China; (2) No.30 Research Institute of China Electronics Technology Group Corporation, Chengdu; 610041, China; (3) China Electronics Technology Cyber Security Co., Ltd, Chengdu; 610041, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 13-17
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023

**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** UAVs have been widely used in various fields such as emergency rescue and disaster relief, weather detection, scientific research measurement, aerial surveying and mapping, and military reconnaissance. The concept of unmanned aerial vehicle (UAV) swarm is proposed and used, which solves the disadvantages of a single unmanned aerial vehicle with small load and weak information processing and storage capabilities. UAV swarms integrate computing resources and storage resources through the interconnection of individual UAVs, effectively improving the load capacity and information storage capabilities of unmanned swarms. However, there are many uncertain privacy issues in the use of UAV clusters. UAVs are at risk of being damaged, lost and captured, and the data stored on UAVs will be leaked. Therefore, it is necessary to build a safe storage scheme for unmanned swarm data to ensure that the data of unmanned swarms can be stored and used safely. This paper proposes a UAV cluster data security storage scheme based on distributed storage. Each UAV acts as a storage node to build an interstellar file system for distributed storage and shared files. UAV clusters use this system to encrypt and protect data, redundant fragmentation and distributed storage to realize the concealment and confidentiality of distributed storage and sharing of UAV cluster data. Ensure the integrity of data and enhance the invulnerability of safe storage of UAV cluster data. © 2023 IEEE.
**Number of references:** 7
**Main heading:** Unmanned aerial vehicles (UAV)
**Controlled terms:** Antennas - Digital storage - Disaster prevention - File organization
**Uncontrolled terms:** Aerial vehicle - Distributed storage - Filesystem - Interstellar file system - Redundant sharding - Safe storage - Security storages - Storage capability - Storage schemes - Unmanned aerial vehicle;
**Classification code:** 652.1 Aircraft, General - 722.1 Data Storage, Equipment and Techniques - 903.3 Information Retrieval and Use - 914.1 Accidents and Accident Prevention
**DOI:** 10.1109/NaNA60121.2023.00010
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 18. Privacy-Preserving Multi-User Joint Data Logistic Regression Inference Scheme

**Accession number:** 20234715078038
**Authors:** Zhang, Yubao (1); Tang, Lin (1); Che, Lixuan (2); Liu, Chaozhang (1); Li, Entang (3); Xing, Hongwei (3); Zhang, Jianhui (3); Di, GuanDong (3)
**Author affiliation:** (1) State Grid Dezhou Electric Power Supply Company, Dezhou, China; (2) Weifang Vocational College, Shandong Province, Weifang City, China; (3) Shandong Luruan Digital Technology Co., Shandong Province, Jinan, China
**Corresponding author:** Li, Entang
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 193-201
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Nowadays, in the era of big data with rich sources of information, machine learning technologies are developing rapidly, and they are widely used in areas such as medical treatment, genomic prediction, spam detection, face recognition, and financial prediction. As a classification model in machine learning, the logistic regression model has become an industrial focus due to the simplicity and efficiency of algorithms. In this context, the 'model as a service' business model has emerged. Specifically, companies with expertise and large-scale training data provide high-quality models to provide reasoning services for users. However, in machine learning classification models, it is important that feature data and inference models remain private. In view of this problem, the existing privacy inference technology considers that the single user has all the feature data, while the feature data of some scenarios exist

between multiple users in the form of segmentation. In this paper, based on the fully homomorphic encryption CKKS scheme and the secure computing technology, this paper designs a privacy logic regression inference scheme suitable for multi-party data combination, which can simultaneously protect the model privacy of the server side, the data feature privacy of each user and the access rights of the inference results. Finally, experimental tests of the designed scheme are performed to verify its high performance. © 2023 IEEE.
**Number of references:** 20
**Main heading:** Computation theory
**Controlled terms:** Face recognition - Logistic regression - Machine learning - Privacy-preserving techniques
**Uncontrolled terms:** Classification models - Data Sharing - Feature data - Ho-momorphic encryptions - Homomorphic-encryptions - Joint computing - Multiusers - Privacy preserving - Privacy protection - Secure computing
**Classification code:** 716 Telecommunication; Radar, Radio and Television - 718 Telephone Systems and Related Technologies; Line Communications - 721.1 Computer Theory, Includes Formal Logic, Automata Theory, Switching Theory, Programming Theory - 723.2 Data Processing and Image Processing - 723.4 Artificial Intelligence - 922.2 Mathematical Statistics
**DOI:** 10.1109/NaNA60121.2023.00040
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 19. Efficient Fine-Grained Forward Secure Encryption Scheme Based on Attributes in Mobile Healthcare

**Accession number:** 20234715078017
**Authors:** Guo, Lifeng (1); Jia, Mengfei (1); Xu, Zhuoheng (1); Zhang, Xialei (1)
**Author affiliation:** (1) School of Computer and Information Technology, Shanxi University, Taiyuan, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 344-349
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** In mobile health (mHealth), people's personal health records (PHRs) will be captured in real time. It will be managed by the cloud server and shared to authorized users. This will enable people to enjoy more timely medical services. The confidentiality and unauthorized access of PHRs is guaranteed by the attribute set encryption (CP-ABE) with ciphertext policy. However, existing CP-ABE schemes not only face heavy computation cost and storage overhead, but also once the data user's key is leaked, all the data that can be decrypted by that user will also be leaked. It is a huge challenge to ensure the forward security of data. Most of the existing solutions only support coarse-grained data protection and cannot solve the problem of excessive computation cost and storage overhead. In this paper, based on the enhanced Policy-based Puncturable Encryption (P- PUN-ENC) primitive and and-gate access structure,we propose an efficient fine-grained forward secure encryption scheme based on attributes, named EFFS-CP-ABE. In EFFS-CP-ABE, data users are able to protect the corresponding data on the cloud in a policy-based manner accurately and permanently. In addition, to solve the problem of decryption cost in our solution, we combine the decryption outsourcing technique with our scheme. This allows the decryption process of our solution to be performed only 7 times with bilinear mapping. Also the length of the ciphertext of our scheme is constant. Extensive simulation results and performance evaluations demonstrate the safety, effectiveness and practicality of the EFFS-CP-ABE scheme. © 2023 IEEE.
**Number of references:** 21
**Main heading:** Cryptography
**Controlled terms:** Digital storage - mHealth - Mobile security - Outsourcing - Security of data

**Uncontrolled terms:** AND-gate - Computation costs - CP-ABE - Decryption outsourcing - Encryption schemes - Fine grained - Forward security - Forward-secure - Personal health record - Puncture encryption
**Classification code:** 461.7 Health Care - 722.1 Data Storage, Equipment and Techniques - 723.2 Data Processing and Image Processing - 912.2 Management
**DOI:** 10.1109/NaNA60121.2023.00064
**Funding Details:** Number: 62002210, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: 202203021221012, Acronym: -, Sponsor: Natural Science Foundation of Shanxi Province;
**Funding text:** Lifeng Guo was supported by the National Science Foundation of Shanxi Province (202203021221012). The work is supported in part by the National Science Foundation of China (NSFC) under grants: 62002210.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 20. Locally Differential Private Federated Learning with Controllable Perturbation Domains

**Accession number:** 20234715078063
**Authors:** Wang, Yuhua (1); Zhu, Jianming (1)
**Author affiliation:** (1) School of Information, Central University of Finance and Economics, Beijing, China
**Corresponding author:** Zhu, Jianming(zjm@cufe.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 637-644
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** As a kind of distributed machine learning, federated learning allows each party to upload local model parameters instead of sensitive data to train a more accurate global model collaboratively. However, since it turns out that the original training data can be inferred by intercepting and analyzing the passed model parameters, local differential privacy is introduced into the federated learning to provide robust privacy guarantees and high efficiency. At present, most existing approaches prefer to adjust the perturbation domain range of the model parameters only according to the privacy budget, which is difficult to ensure the accuracy of the model under the condition of limited privacy budget or fewer participating clients, resulting in low usability and practicability of the global model. To tackle this, we propose a locally differential private federated learning with controllable perturbation domains. First, we design a local differential privacy mechanism, which generates three perturbation domains centered on the true value. The range and perturbation probability of each perturbation domain are adjusted by controlling two factors, the privacy budget and the unit size of the perturbation domain. Specially, the true value is mapped to the center perturbation domain with a large probability and to the two-side perturbation domains with a small probability. Second, to ensure the training process of federated learning is protected from inference attacks, we apply the designed mechanism to the transmission of parameters in federated learning. Finally, we analyze and prove the privacy and utility of the mechanism in detail, and conduct comparative experiments in terms of accuracy on three standard datasets. Theoretical and experimental results show that the proposed approach outperforms other state-of-the-art approaches. © 2023 IEEE.
**Number of references:** 13
**Main heading:** Sensitive data
**Controlled terms:** Budget control - Economic and social effects - Learning systems - Privacy-preserving techniques
**Uncontrolled terms:** Differential privacies - Distributed machine learning - Federated learning - Global models - Local differential privacy - Local model - Modeling parameters - Privacy and utility trade-off - Privacy preserving - Trade off
**Classification code:** 716 Telecommunication; Radar, Radio and Television - 718 Telephone Systems and Related Technologies; Line Communications - 723.2 Data Processing and Image Processing - 971 Social Sciences

**DOI:** 10.1109/NaNA60121.2023.00110
**Funding Details:** Number: 62072487,LD22F020002, Acronym: NSFC, Sponsor: National Natural Science Foundation of China;
**Funding text:** This work was supported by National Natural Science Foundation of China (62072487), and the Research on Blockchain Security Cross-Chain and Supervision Prototype System Oriented to Fusion Application (LD22F020002).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 21. Deep Reinforcement Learning-Based Task Offloading Over In-Network Computing and Multi-Access Edge Computing

**Accession number:** 20234715078029
**Authors:** Ming, Zhao (1); Guo, Qize (1); Yu, Hao (1); Taleb, Tarik (1)
**Author affiliation:** (1) Oulu University, Oulu, Finland
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 281-286
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** With the blooming of information technology and network applications/services, emerging multi-access edge computing (MEC) and in-network computing (INC) are regarded as key computing paradigms to support time-sensitive tasks and requests by task offloading. Existing studies concerning task offloading seldom considered the combinations of MEC, INC, and cloud computing. In this paper, we explore INC-enhanced task offloading in MEC networks and design a three-layer task offloading network architecture, which consists of not only user equipment, edge servers, and cloud, but also network elements like routers/switches. We focus on reducing the system latency and energy consumption (EC) and formulate the optimization problem as minimizing the weighted sum of these two indicators. To solve this problem, we propose a deep reinforcement learning-based framework and creatively map the actions of the agent to the offloading policies and resource allocation strategies for determining these two indicators simultaneously. Simulation results show that the proposed INC-enhanced task offloading framework achieves fast convergence speed with double deep Q-network and outperforms other baselines in reducing the system latency and EC. © 2023 IEEE.
**Number of references:** 19
**Main heading:** Reinforcement learning
**Controlled terms:** Deep learning - Edge computing - Energy utilization - Network architecture - Network layers
**Uncontrolled terms:** Deep reinforcement learning - Edge computing - In networks - In-networking computing - Multiaccess - Network computing - Reinforcement learnings - System energy - System latency - Task offloading
**Classification code:** 461.4 Ergonomics and Human Factors Engineering - 525.3 Energy Utilization - 722.4 Digital Computers and Systems - 723 Computer Software, Data Handling and Applications - 723.4 Artificial Intelligence
**DOI:** 10.1109/NaNA60121.2023.00054
**Funding Details:** Number: 346208,352428, Acronym: AKA, Sponsor: Academy of Finland;
**Funding text:** ACKNOWLEDGMENTS This research work is partially supported by the Business Finland 6Bridge 6Core project under Grant No. 8410/31/2022, the Academy of Finland 6G Flagship program under Grant No. 346208, and the Academy of Finland IDEA-MILL project under Grant No. 352428.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village

## 22. Requirements and Potential Key Technologies of Security for 6G Mobile Network

**Accession number:** 20234715078116
**Authors:** Du, Haitao (1); He, Shen (1); Su, Li (1); Bai, Jie (1); Yan, Ru (1)
**Author affiliation:** (1) China Mobile Research Institute, Beijing, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 1-6
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** It is anticipated that the 6th Generation (6G) mobile network security does not only solve the security problems posed by new technologies, services, and applications, but also presents endogenous feature which is different from the patching or plug-in feature appearing in the traditional networks. Based on the features of 6G network, this paper analyzes 6G network security scenarios and security challenges, and then puts forward 6G security requirements including enhanced trust, resilient autonomy, digital twin security, ubiquitous security. Finally the key network security technologies and their applications are studied to provide reference for the development of 6G network security. © 2023 IEEE.
**Number of references:** 12
**Main heading:** Network security
**Controlled terms:** 3G mobile communication systems - Cryptography - Mobile security - Queueing networks - Wireless networks
**Uncontrolled terms:** 6th generation - Digital twin security - Key technologies - Networks security - New applications - New services - Security problems - Security requirements - Technology application - Technology service
**Classification code:** 716 Telecommunication; Radar, Radio and Television - 716.3 Radio Systems and Equipment - 722.3 Data Communication, Equipment and Techniques - 723 Computer Software, Data Handling and Applications - 723.2 Data Processing and Image Processing
**DOI:** 10.1109/NaNA60121.2023.00008
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 23. An Efficient and Scalable Consensus for Main Blockchain in the Multi-Chain Network

**Accession number:** 20234715078088
**Authors:** Zhuang, Xinlu (1); Xiao, Zeyu (1); Qin, Haoping (1); Ge, Yunjie (1)
**Author affiliation:** (1) Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Key Laboratory of Aerospace Information Security and Trusted Computing, Wuhan, China
**Corresponding author:** Zhuang, Xinlu(xinluzhuang@whu.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 365-371
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023

**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** While blockchain technology has gained significant popularity and adoption, auditing the legitimacy of on-chain transactions continues to present complex technical challenges. To address the challenge of auditing the legitimacy of on-chain transactions in multi-chain systems, this paper proposes an Auditing-Service Multi-Chain architecture that utilizes a new Auditing Chain to facilitate cross-chain auditing of transactions across multiple Service Chains. However, the performance of the consensus mechanism of the Auditing Chain is limited under the increasing number of Service Chains and transaction volumes. To overcome the shortcomings of the Auditing Chain's consensus mechanism, this paper introduces a new consensus that employs a sliding window approach to determine the consensus nodes' membership and automatically selects the leader node. Moreover, the communication tree structure is utilized in the broadcast phase to optimize the network overhead in the consensus stage. Additionally, this paper applies the CoSi collective signature protocol to streamline the consensus process and enhance the throughput and scalability of the Auditing Chain. The experimental results demonstrate that the proposed consensus mechanism satisfies the performance requirements of the Auditing-Service Multi-Chain architecture in a local test network environment. © 2023 IEEE.
**Number of references:** 16
**Main heading:** Blockchain
**Controlled terms:** Network architecture - Trees (mathematics)
**Uncontrolled terms:** Block-chain - Chain architecture - Chain networks - Consensus - Cross-chain technology - Multi-chain systems - Multiple services - Performance - Service chain - Technical challenges
**Classification code:** 723.3 Database Systems - 921.4 Combinatorial Mathematics, Includes Graph Theory, Set Theory
**DOI:** 10.1109/NaNA60121.2023.00067
**Funding Details:** Number: 2020YFB1005500, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China;
**Funding text:** This work was supported by the National Key R&D Program of China under Grant 2020YFB1005500.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 24. Research on Activation Functions in Machine Learning Based Network Coding

**Accession number:** 20234715078019
**Authors:** Zhang, Xin (1); Yang, Yanbo (1); Li, Baoshan (1); Li, Minchao (1); Li, Teng (2); Zhang, Jiawei (2)
**Author affiliation:** (1) School of Information Engineering, Inner Mongolia University of Science & Technology, Baotou, China; (2) School of Cyber Engineering, Xidian University, Xi'an, China
**Corresponding author:** Zhang, Xin(zxin367520@163.com)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 307-312
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Network coding allows network Intermediate nodes to encode on top of data forwarding, which can improve network transmission efficiency, robustness and security. However, traditional nonlinear network coding suffers from the problems of coding and decoding complexity and implementation difficulties, while the real network environment is often nonlinear. Machine learning-based network coding utilizes neural networks and activation functions for coding and decoding, which solves the complexity and implementation difficulties of traditional nonlinear network coding, where activation functions, as the main factor for introducing nonlinearity, are crucial for machine learning-based

network coding. In this paper, the basic ReLU and Sigmoid-type activation functions are chosen to investigate their role by transmitting information over a butterfly network. Firstly, it is pointed out that the presence of activation functions in the absence of noise interference at intermediate nodes can cause compression or loss of coded information, Secondly, the theorem of the role of noise on the activation function is derived in the case of noisy interference at intermediate nodes. Based on this theorem, it is concluded that the ReLU activation function has a better transmission effect when the interference is small, and the Sigmoid activation function has a better transmission effect when the interference is large; meanwhile, it is pointed out that the anti-noise performance of the Sigmoid activation function is better than that of the ReLU activation function. © 2023 IEEE.
**Number of references:** 14
**Main heading:** Machine learning
**Controlled terms:** Chemical activation - Complex networks - Decoding - Network coding
**Uncontrolled terms:** Activation functions - Coding and decoding - Component - Data-forwarding - Implementation difficulties - Intermediate node - Machine-learning - Network transmission - Noise immunity - Sigmoid activation function
**Classification code:** 716.1 Information Theory and Signal Processing - 722 Computer Systems and Equipment - 723.2 Data Processing and Image Processing - 723.4 Artificial Intelligence - 802.2 Chemical Reactions - 804 Chemical Products Generally
**DOI:** 10.1109/NaNA60121.2023.00058
**Funding Details:** Number: 0406082219, Acronym: -, Sponsor: -; Number: 2020LH06006, Acronym: -, Sponsor: -; Number: XM2021BT12, Acronym: -, Sponsor: -; Number: YF2021011, Acronym: -, Sponsor: -; Number: NK20221201, Acronym: -, Sponsor: -; Number: 2019ZD025, Acronym: -, Sponsor: Science and Technology Major Project of Inner Mongolia;
**Funding text:** Foundation items#Natural Science Foundation of Inner Mongolia (2020LH06006); Inner Mongolia Major Science and Technology Project(2019ZD025); Kundulun District Science and Technology Project (YF2021011); Basic Scientific Research Project of Education Department of Inner Mongolia Autonomous Region (0406082219); Key Special Project of Science and Technology Xing Meng Action (XM2021BT12); National Agriculture Key Science & Technology Project(NK20221201);.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 25. A Robust and Scalable One-PUF-to-Many Authentication and Key Agreement Scheme for Mobile Communication Network

**Accession number:** 20234715078047
**Authors:** Wang, Yiteng (2); Ren, Zhe (1, 2); Wang, Wei (2)
**Author affiliation:** (1) School of Cyber Engineering, Xidian University, Xi'an, China; (2) The 36th Research Institute of China Electronics Technology Group Corporation, Science and Technology on Communication Information Security Control Laboratory, Jiaxing, China
**Corresponding author:** Wang, Yiteng(yitengwang@bjtu.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 84-91
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Under the multi-cloud environment of mobile communication networks, unattended terminals would possibly be involved in different tasks. For the network security, terminals should be authenticated by cloud service providers (CSPs) before being involved in various tasks. As a new cryptology primitive, Physical Unclonable Function (PUF) can be served as a trusted root for unattended terminals and provide security property against physical attacks, based

on which physical secure authentication can be executed. However, applying the PUF directly to the multi-cloud environment caused the authentication scheme to rely on the storage of the primitive challenge-response pairs, and there was a single point of failure problem. To solve these issues, we propose an authentication and key agreement scheme named RSOPM for secure authentication between terminals and CSPs. Specifically, mutual authentication without the storage of the primitive challenge-response pairs on the cloud is enabled by exploiting the trapdoor collision property of the chameleon hash function. Moreover, the redactable blockchain containing distributed registration information makes a terminal register only once, and then the terminal gains access to the various CSPs. The security properties are discussed to show our scheme resists various attacks. The results of experiments show that the overall delay is reduced by 33 % compared to other multi-cloud authentication schemes. © 2023 IEEE.
**Number of references:** 18
**Main heading:** Authentication
**Controlled terms:** Blockchain - Hardware security - Hash functions - Mobile telecommunication systems - Network security
**Uncontrolled terms:** Authentication and key agreements - Block-chain - Cloud environments - Cloud service providers - Key agreement scheme - Mobile communication networks - Multi-cloud environment - Multi-clouds - Privacy protection - Security properties
**Classification code:** 723 Computer Software, Data Handling and Applications - 723.3 Database Systems
**DOI:** 10.1109/NaNA60121.2023.00022
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 26. Formal Modeling and Defense Methods for 5G Network Endpoint Access Denial of Service Attacks

**Accession number:** 20234715078039
**Authors:** Zhang, Tong (1); Wei, Wei (1); Wang, Yichuan (1, 2); Deng, Xi (3); Zhu, Lei (1); Ji, Wenjiang (1)
**Author affiliation:** (1) School of Computer Science and Engineering, Xi'an University of Technology, Xi'an, China; (2) Shaanxi Key Laboratory for Network Computing and Security Technolog, Xi'an, China; (3) School of Computer Science, Xi'an Shiyou University, Xi'an, China
**Corresponding author:** Wang, Yichuan(chuan@xaut.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 72-77
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** 5G terminal access denial-of-service attack is one of the more common types of 5G signaling network attacks. It manifests itself as a large number of abnormal access requests occupying core network resources. Normal requests cannot obtain resources, resulting in unstable network services, and users will be unable to connect or drop connections, eventually leading to frequent terminal takeoffs and landings. This paper proposes a formal modeling scheme for a 5G terminal access denial-of-service attack. The attack principle is analyzed, a defense scheme is designed and modeled, and analyzed, and then quantitative experiments are conducted, and the experimental results show the effectiveness of the defense scheme. © 2023 IEEE.
**Number of references:** 20
**Main heading:** Network security
**Controlled terms:** 5G mobile communication systems - Denial-of-service attack - Queueing networks - Signaling
**Uncontrolled terms:** 5g signaling network - Core networks - Denialof- service attacks - Formal modeling - Network attack - Network resource - Networks security - Networks services - Petri network - Signaling networks

**Classification code:** 716.3 Radio Systems and Equipment - 723 Computer Software, Data Handling and Applications - 902.3 Legal Aspects
**DOI:** 10.1109/NaNA60121.2023.00020
**Funding Details:** Number: 62072368,U20B2050, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: 2021ZDLGY05-09,2022CGKC-09, Acronym: -, Sponsor: Shanxi Provincial Key Research and Development Project; Number: 2023-JC-QN-0742, Acronym: -, Sponsor: Natural Science Basic Research Program of Shaanxi Province;
**Funding text:** ACKNOWLEDGMENT This research work is supported by the National Natural Science Founds of China (62072368, U20B2050), Key Research and Development Program of Shaanxi Province (2021ZDLGY05-09, 2022CGKC-09), and Natural Science Basic Research Program of Shaanxi Province (2023-JC-QN-0742).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 27. GraphMal: A Network Malicious Traffic Identification Method Based on Graph Neural Network

**Accession number:** 20234715078009
**Authors:** Zhang, Lei (1); Shi, Huiling (1); Zhang, Kuichao (1); Sun, Hongyang (1); Zhang, Wei (1)
**Author affiliation:** (1) Qilu University of Technology, Shandong Academy of Sciences, Shandong Provincial Key Laboratory of Computer Networks Shandong Computer Science Center, National Supercomputer Center in Ji'nan, Shandong, Ji'nan, China
**Corresponding authors:** Shi, Huiling(kch_zhang@163.com); Zhang, Wei(wzhang@sdas.org)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 262-267
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Detecting malicious attacks in normal network traffic is critical to network security. Traditional traffic identification methods often struggle to capture the complex communication patterns in network traffic, hindering their effectiveness. We introduce GraphMal, a framework utilizing Graph Neural Networks (GNNs) for the identification of malicious traffic. This approach effectively exploits network topology and traffic characteristics to improve performance. We first apply Pearson's correlation coefficient and random forest approaches to effectively reduce the dimensionality of the dataset. Then, the E-GraphSAGE algorithm is used to extract salient features from the traffic topology graph and construct a robust graph classifier. Additionally, the focal loss function is used to solve the data imbalance problem. Experiments conducted on the UNSW-NB15 dataset demonstrate GraphMal's remarkable performance in both binary and multi-class classification tasks, while improving the learning efficiency of GNNs. © 2023 IEEE.
**Number of references:** 18
**Main heading:** Network security
**Controlled terms:** Classification (of information) - Correlation methods - Graph neural networks - Topology
**Uncontrolled terms:** Communication pattern - Data imbalance - Graph neural networks - Identification method - In networks - Malicious attack - Malicious traffic - Network traffic - Networks security - Traffic identification
**Classification code:** 716.1 Information Theory and Signal Processing - 723 Computer Software, Data Handling and Applications - 723.4 Artificial Intelligence - 903.1 Information Sources and Analysis - 921.4 Combinatorial Mathematics, Includes Graph Theory, Set Theory - 922.2 Mathematical Statistics
**DOI:** 10.1109/NaNA60121.2023.00051
**Funding Details:** Number: 2021GXRC091, Acronym: -, Sponsor: -; Number: 2022CXGC20106, Acronym: -, Sponsor: -; Number: ZR2022LZH015, Acronym: -, Sponsor: Natural Science Foundation of Shandong Province; Number: 2022GH007,2022JBZ0101, Acronym: SDAS, Sponsor: Shandong Academy of Sciences;

**Funding text:** VI. ACKNOWLEDGE This work was supported in part by the Shandong Provincial Natural Science Foundation under Grant No. ZR2022LZH015 and No.ZR2020LZH010, the Project of Key R&D Program of Shandong Province (2022CXGC20106), the Pilot International Cooperation Project for Integrated Innovation of Science, Education and Industry of Qilu University of Technology (Shandong Academy of Sciences) under Grant No.2022GH007 and No.2022JBZ0101, the One Belt One Road Innovative Talent Exchange with Foreign Experts under Grant No.DL2022024004L, and the Jinan Scientific Research Leader Studio Project under Grant No.2021GXRC091.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 28. Challenges of Livecast Computing Network: A Contemporary Survey

**Accession number:** 20234715078087
**Authors:** Zeng, Qimiao (1); Zhuang, Yirong (1); Hai, Jinxia (1); Pan, Qing (1); Yin, Zhifan (1); Chen, Qi (1); Liang, Jie (1)
**Author affiliation:** (1) China Telecom Research Institute, China
**Corresponding author:** Zhuang, Yirong(zhuangyir@chinatelecom.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 690-697
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** With the rise of Internet services in recent years, especially the flourishing development of new social platforms such as Taobao Live, Tiktok, Huya, YouTube, and Twitch, they have led to a significant increase in Internet video services. For example, YouTube Live stats reveal that 2020 was the biggest year ever for Gaming Live, with 100 billion watch time hours. As a result, the entire network communication model has gradually evolved into a Livecast computing network (LCN) architecture, where various network units involved in Internet live video services, with their computing, storage, distribution, and transmission capabilities, form an architecture that can meet high concurrency and low latency requirements. This article investigates, sorts, and analyzes LCN architecture related standards, protocols, and network model solutions from the perspective of Internet live video services. Firstly, it outlines the standards, system architecture, and main streaming media protocols of Internet live video. Secondly, it analyzes the video algorithm network architecture models, including cloud-based, edge-based, and cloud-network-edge collaborative models. Finally, it summarizes the main challenges and research directions faced by video algorithm networks in the future. © 2023 IEEE.
**Number of references:** 41
**Main heading:** Network architecture
**Controlled terms:** Computer architecture - Internet protocols - Media streaming - Web services
**Uncontrolled terms:** Architecture modeling - Internet video - Internet-services - Live video - Livecast computing network - Multicast - Network communications - Video algorithms - Video services - YouTube
**Classification code:** 722.3 Data Communication, Equipment and Techniques - 723 Computer Software, Data Handling and Applications - 723.5 Computer Applications
**DOI:** 10.1109/NaNA60121.2023.00119
**Funding text:** This work was supported by Research on Key Technologies of IP Service Network and Experimental Development of "Build-as-Your-Wish Private Network" Service No. T-2023-29.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village

## 29. SRv6-based In-band Network Telemetry: Architecture and Strategy

**Accession number:** 20234715078010
**Authors:** Yu, Kun (1); Li, Su-Ruo (2)
**Author affiliation:** (1) College of Computer, Jingchu University of Technology, Jingmen, China; (2) Big Data Research Institute, College of Computer, Jingchu University of Technology, Jingmen, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 226-230
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** In-band Network Telemetry (INT) enables data packets to carry network status information by embedding device-internal state information into each data packet along its forwarding path. This provides higher monitoring accuracy and finer monitoring granularity. However, embedding telemetry information causes additional bandwidth overhead in the data plane, leading to a decline in transmission quality and an increased processing burden. Additionally, the telemetry coverage is restricted to the forwarding path of data packets, making it incapable of realizing dynamic detection. We propose a proactive network telemetry architecture based on SRv6, which can flexibly schedule telemetry instructions and telemetry paths while ensuring fine-grained monitoring, enabling effective analysis of both queue and delay information. © 2023 IEEE.
**Number of references:** 21
**Main heading:** Network architecture
**Controlled terms:** Embeddings - Motion planning - Telemetering equipment
**Uncontrolled terms:** Data packet - Data planes - Data-plane - Embeddings - In-band - In-band network telemetry - Network status - Programmable data plane - Srv6 - Status informations
**Classification code:** 723.4 Artificial Intelligence
**DOI:** 10.1109/NaNA60121.2023.00045
**Funding Details:** Number: 2021FNA01006, Acronym: -, Sponsor: -; Number: 2021YFZD068, Acronym: -, Sponsor: -;
**Funding text:** This work of K. Yu and S. Li was supported in part by the China University Industry-University-Research Innovation Fund under Grant No.2021FNA01006, the Jingmen Science and Technology Research and Development Plan Project under Grant No.2021YFZD068.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 30. OP Mask R-CNN: An Advanced Mask R-CNN Network for Cattle Individual Recognition on Large Farms

**Accession number:** 20234715078024
**Authors:** Wang, Jianping (1); Zhang, Xueyan (1); Gao, Guohong (1); Lv, Yingying (1)
**Author affiliation:** (1) School of Computer Science and Technology, Henan Institute of Science and Technology, Xinxiang, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 601-606
**Language:** English
**ISBN-13:** 9798350327380

**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** The individual identification of cattle is crucial for the efficient management of large farms, and advanced identification technologies that can monitor cattle behavior in real time are essential for increasing agricultural efficiency, promoting the digital transformation of animal husbandry, and improving animal welfare. This paper introduces a novel network called OP Mask R-CNN for individual cattle identification, which combines Open Pose with the Mask R-CNN network. We present three key strategies to improve the identification of individual cattle. First, we optimize the number of convolutional layers in the Mask R-CNN backbone network, i.e., ResNet101. Second, we introduce an Open Pose-based bovine skeleton feature extraction method. Finally, we construct a fusion mechanism that combines the attention module, the convolutional block attention module (CBAM), the open pose module, and the ResNet101. This work strikes a balance between accuracy and complexity that supports the development of a lightweight bovine individual recognition technique. © 2023 IEEE.
**Number of references:** 18
**Main heading:** Mammals
**Controlled terms:** Computer vision - Convolution - Convolutional neural networks - Farms
**Uncontrolled terms:** Cattle identification - CNN network - Convolutional block attention module - Efficient managements - Identification technology - Individual identification - Individual recognition - Mask R-CNN network - OP mask R-CNN - Open pose
**Classification code:** 716.1 Information Theory and Signal Processing - 723.5 Computer Applications - 741.2 Vision - 821 Agricultural Equipment and Methods; Vegetation and Pest Control
**DOI:** 10.1109/NaNA60121.2023.00104
**Funding Details:** Number: 21ZD003, Acronym: -, Sponsor: -; Number: 21A520001,23B520003, Acronym: -, Sponsor: Key Scientific Research Project of Colleges and Universities in Henan Province; Number: 202110467001, Acronym: -, Sponsor: National College Students Innovation and Entrepreneurship Training Program; Number: 212102310087,222102320181,232102111128, Acronym: -, Sponsor: Henan Provincial Science and Technology Research Project;
**Funding text:** This work was partly supported by the Key Scientific and Technological Project of Henan Province (232102111128, 222102320181, 212102310087), in part by the Innovation and Entrepreneurship Training Program of National College Students in China (202110467001), in part by the Major Special Project of Xinxiang City(21ZD003), in part by the Key Scientific Research Projects of Colleges and Universities in Henan Province (23B520003, 21A520001). The authors approved the version of the manuscript to be published. They agreed to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 31. Covert Communication in the D2D-Enabled Cellular Network with Multiple Non-Colluding Wardens

**Accession number:** 20234715078081
**Authors:** Jiao, Jingsen (1, 2); Wu, Huihui (3); Sun, Ranran (1); Miao, Qifeng (1); Cao, Yizhi (1)
**Author affiliation:** (1) Hangzhou Institute of Technology, Xidian University, Hangzhou; 311200, China; (2) School of Computer Science and Technology, Xidian University, Xi'an; 710071, China; (3) Beijing Natl. Research Center for Information Science and Technology (BNRist), Tsinghua University, Department of Automation, Beijing; 100084, China
**Corresponding author:** Sun, Ranran(srr_2013@163.com)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 661-666
**Language:** English
**ISBN-13:** 9798350327380

**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** This work investigates the covert communication in a D2D (device-to-device)-enabled cellular network, where a cellular user CT wants to transmit a message covertly to another cellular user CR through a base station BS without being detected by multiple non-colluding wardens with the help of an underlaying D2D pair. Although D2D communication can confuse wardens, it can also interfere with the covert communication of the cellular link. To fully understand the impact of D2D communication on the covert communication of the cellular link, we first explore the average minimum detection error probability of non-colluding wardens. Then, the average covert rate of the cellular link is studied. Eventually, expansive numerical and simulation results are presented to demonstrate the correctness of our theoretical analysis and also to illustrate the impact of D2D communication on the covert communication of the cellular link. © 2023 IEEE.
**Number of references:** 19
**Main heading:** Wireless networks
**Controlled terms:** Mobile telecommunication systems
**Uncontrolled terms:** Cellular links - Cellular network - Cellulars - Covert communications - Covert performance analyse - D2D communications - Detection error probability - Multiple non-colluding warden - Performances analysis - Underlaying D2D-enabled cellular network
**Classification code:** 716.3 Radio Systems and Equipment - 722.3 Data Communication, Equipment and Techniques
**DOI:** 10.1109/NaNA60121.2023.00114
**Funding Details:** Number: 2023-CX-TD-02, Acronym: -, Sponsor: -; Number: 61972308,62220106004, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: 2021A1515111017, Acronym: -, Sponsor: Basic and Applied Basic Research Foundation of Guangdong Province;
**Funding text:** This work was supported in part by the National Natural Science Foundation of China under Grant No. 62220106004, No. 61972308, the Basic and Applied Basic Research Fund of Guangdong Province under Grant No.2021A1515111017, the Innovation Capability Support Program of Shaanxi (Program No. 2023-CX-TD-02). (Corresponding author: Ranran Sun)
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 32. A Study on a Reduced Indicator System for the Network Security Situational Assessment Model

**Accession number:** 20234715078079
**Authors:** Zhang, Hongbin (2); Bai, Yikang (2); Zhao, Dongmei (1); Liu, Bin (2, 3); Xu, Ying (2)
**Author affiliation:** (1) Hebei Normal University, Hebei Key Laboratory of Network and Information Security, Shijiazhuang, China; (2) Hebei University of Science and Technology, School of Information Science and Engineering, Shijiazhuang, China; (3) School of Economics and Management, Research Center of Big Data and Social Computing, Shijiazhuang, China
**Corresponding author:** Zhao, Dongmei(zhaodongmei666@126.com)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 181-186
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.

**Abstract:** It is a challenge to monitor the network security state in a large-scale network environment because the selection of situation assessment indicators is overrun by massive observational information. To address this issue, this paper proposes a network security situational assessment model based on a reduced indicator system. The model categorises the characteristics of network assets and threats into endogenous situational factors and exogenous situational factors. By applying the multi-label extremely random tree algorithm to select the importance of network features, a reduced indicator system with independence and strong comprehensiveness is established. Additionally, the weights of the reduced indicator system are calculated using an improved analytical hierarchy process, which yields the evaluation results for network security situations. The experimental results show that the model improves the accuracy and timeliness of the situation assessment model, and the method can reflect the network situation in real time. © 2023 IEEE.
**Number of references:** 14
**Main heading:** Network security
**Controlled terms:** Trees (mathematics)
**Uncontrolled terms:** Assessment models - Extremely random tree - Improved analytic hierarchy process - Indicators systems - Indices systems - Networks security - Random tree - Situation assessment - Situational assessment - Situational factors
**Classification code:** 723 Computer Software, Data Handling and Applications - 921.4 Combinatorial Mathematics, Includes Graph Theory, Set Theory
**DOI:** 10.1109/NaNA60121.2023.00038
**Funding Details:** Number: 216Z0701G, Acronym: -, Sponsor: -; Number: 18210109D,20310701D,20310802D,21310101D, Acronym: -, Sponsor: -; Number: 61572170,61672206, Acronym: NSFC, Sponsor: National Natural Science Foundation of China;
**Funding text:** This research was supported by the National Natural Science Foundation of China under Grant No.61672206, No.61572170, Central Guide Local Science and Technology Development Fund Project (216Z0701G), S&T Program of Hebei under Grant No.18210109D, No.20310701D, No. 20310802D, No. 21310101D, National cultural and tourism science and technology innovation project (2020).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 33. ST-MobileNetV3: A Lightweight Network Model for Strawberry Disease Identification

**Accession number:** 20234715078056
**Authors:** Wang, Jianping (1); Li, Zhiyu (1); Gao, Guohong (1); Lv, Yingying (1); Ma, Yuxin (1); Chen, Guanglan (1)
**Author affiliation:** (1) School of Computer Science and Technology, Henan Institute of Science and Technology, Xinxiang, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 209-214
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** The identification of strawberry diseases holds great significance in the cultivation process, and timely detection plays a vital role in promoting strawberry production and advancing the industry. This paper introduces a novel strawberry disease recognition network model named ST-MobileNetV3. Building upon MobileNetV3, the model incorporates a multilayer perception module and expands the convolutional processing, while replacing the original attention mechanism SE module with an ECA module. This research achieves a harmonious balance between accuracy and complexity, thereby supporting the development of lightweight strawberry disease identification techniques. The introduction of this innovative network model is expected to offer efficient and accurate disease identification tools to strawberry growers, thereby facilitating the progress of the strawberry industry. © 2023 IEEE.
**Number of references:** 18

**Main heading:** Fruits
**Uncontrolled terms:** Convolutional processing - Cultivation process - ECA - Lightweight - Mobilenetv3 - Multi-layer perception - Network models - ST-mobilenetv3 - Strawberry disease identification - Strawberry production
**Classification code:** 821.4 Agricultural Products
**DOI:** 10.1109/NaNA60121.2023.00042
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 34. STGAT: A Spatio-Temporal Graph Attention Network for Travel Demand Prediction

**Accession number:** 20234715078113
**Authors:** Zhang, Tao Yi (1, 2, 3); Wang, YuBo (1, 2, 3); Wei, ZhiCheng (1, 2, 3)
**Author affiliation:** (1) Key Lab of Network and Information Security, China; (2) College of Computer and Cyberspace Security, China; (3) Hebei Provincial Engineering Research Center for Supply Chain Big Data Analytics & Security, Hebei Normal University, Hebei Province, Shijiazhuang, China
**Corresponding author:** Wei, ZhiCheng(weizhicheng@hebtu.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 434-439
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Forecasting travel demand is a challenging task due to the complex spatial dependencies and dynamic temporal correlation of the traffic data. Furthermore, a limited representation of the given spatial graph structure may restrict the model's ability to effectively learn spatial-temporal dependencies. To extract latent semantic features from traffic data, this paper proposes a method to construct a traffic graph using the Markov cluster algorithm. The traffic semantic correlation matrix is constructed based on a traffic graph to obtain the deep semantic information. Specifically, this study proposes a Spatio-Temporal Graph Attention Network(STGAT) for travel demand prediction. STGAT uses a graph attention layer based on the Node2Vec graph embedding algorithm, two convolutional layers based on the Markov cluster algorithm, and a long short-term memory network to capture spatial-temporal dependencies. Experimental results on the NYC Taxi dataset and the Chengdu online car dataset demonstrate that STGAT achieved state-of-the-art performance compared to other baseline models. © 2023 IEEE.
**Number of references:** 21
**Main heading:** Forecasting
**Controlled terms:** Clustering algorithms - Intelligent systems - Semantics - Taxicabs
**Uncontrolled terms:** Cluster algorithms - Component - Demand prediction - Graph attention network - Markov cluster algorithm - Spatial temporals - Spatio-temporal graphs - Traffic data - Travel demand - Travel demand prediction
**Classification code:** 662.1 Automobiles - 723.4 Artificial Intelligence - 903.1 Information Sources and Analysis
**DOI:** 10.1109/NaNA60121.2023.00078
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 35. A Text Classification Method of Network Public Opinion Based on Information Fusion

**Accession number:** 20234715078070
**Authors:** Zhu, Lei (1, 2); Wen, Miaoqing (2); Zhang, Tong (2); Wang, Yichuan (2); Wang, Jing (2); Yang, Mingsong (2); Ma, Bing (2)

**Author affiliation:** (1) State Key Laboratory of Rail Transit Engineering Information, Fsdi, Xi'an, China; (2) School of Computer Science and Engineering, Xi'an University of Technology, Xi'an, China
**Corresponding author:** Zhang, Tong(zhangtong@xaut.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 484-489
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** With the widespread use of mobile networks and intelligent terminal devices, a large amount of public opinion text has been generated from Microblogs, posting bars, and other platforms, resulting in the difficulty of public opinion management. More and more researchers use text classification methods to identify law-related public opinion information. However, the existing text classification methods rely on labor-intensive feature engineering, and their performance mainly depends on information fusion and classification algorithms, which is unsuitable for rapidly developing fields. This paper extracts the user comments of a hunting forum to analyze the semantic information of argot and employs the Word2vec model to represent the argot feature. Combining the multi-layer information of the pre-trained BERT on the user comments, we propose a text classification method BERT_W2V_CRF to improve the classification efficiency of massive law-related public opinion texts. Specifically, we first build a terminology dictionary of Chinese hunting forum to identify the argot features in expert-marked data using the Word2vec model. Then the BERT model is pretrained and the representation of fused information is generated by combining the Word2vec and optimized BERT. Finally, the recognized result is obtained by using Softmax. Experiments are conducted on the user comment dataset to evaluate the proposed text classification method, and the results show that the information fusion approach can be used to improve the classification efficiency of the deep learning-based method. © 2023 IEEE.
**Number of references:** 18
**Main heading:** Semantics
**Controlled terms:** Classification (of information) - Data fusion - Deep learning - Efficiency - Information fusion - Learning systems - Social aspects - Text processing
**Uncontrolled terms:** Classification efficiency - Deep learning - Intelligent terminal - Large amounts - Network public opinions - Network terminals - Public opinions - Terminal devices - Text classification - Text classification methods
**Classification code:** 461.4 Ergonomics and Human Factors Engineering - 716.1 Information Theory and Signal Processing - 723.2 Data Processing and Image Processing - 901.4 Impact of Technology on Society - 903.1 Information Sources and Analysis - 903.3 Information Retrieval and Use - 913.1 Production Engineering
**DOI:** 10.1109/NaNA60121.2023.00086
**Funding Details:** Number: SKLKZ19-05, Acronym: -, Sponsor: -; Number: 51878556,:61602374, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: 2016JQ6041, Acronym: -, Sponsor: Natural Science Foundation of Shaanxi Province;
**Funding text:** VI. ACKNOWLEDGMENTS The research presented in this paper is supported in part by the National Natural Science Foundation of China (grant:61602374, 51878556), the Natural Science Foundation of Shaanxi Province (CN) (Nos. 2016JQ6041),State Key Laboratory of Rail Transit Engineering Informatization (FSDI) of China (grant: SKLKZ19-05).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 36. A Local Differential Privacy Based Method to Preserve Link Privacy in Mobile Social Network

**Accession number:** 20234715078002
**Authors:** Yan, Jun (1, 2); Tian, Yi (3); Wang, Wenli (4); Zhang, Yijun (4); Zhou, Yihui (1); Lu, Laifeng (4)

**Author affiliation:** (1) School of Computer Science, Shaanxi Normal University, China; (2) School of Mathematics and Computer Applications, Shangluo College, China; (3) School of Economics and Management, Shangluo College, China; (4) School of Mathematics and Statistics, Shaanxi Normal University, China
**Corresponding author:** Lu, Laifeng(lulaifeng@snnu.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 390-396
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** With MSNs(mobile social networks) playing an increasingly important role in our daily life, individual privacy issues in MSNs are becoming more and more important. To address these issues, differential privacy is widely adopted in MSNs. However, it is a great challenge how to preserve the individual link privacy while ensuring data sharing in a distributed environment. Therefore, a LDP based method is proposed, which is composed of three steps. Firstly, the 2-hop subgraphs of nodes are used to achieve node encoding. Then, the random response completes the edge modification of each node. Finally, after the approximate value of each node edges is obtained, the edge modification technology is employed to generate a synthetic graph that achieves privacy preserving for link privacy of each node. Specially, the properties of random response and the similarity of nodes are utilized to improve data utility. Theoretical analysis proves that the proposed method satisfies differential privacy. The experimental results demonstrate the effectiveness of this method. © 2023 IEEE.
**Number of references:** 22
**Main heading:** Social networking (online)
**Controlled terms:** Privacy-preserving techniques
**Uncontrolled terms:** Daily lives - Differential privacies - Edge modification - Individual privacy - Link privacies - Local differential privacy - Mobile social networks - Node coding - Random response - Randomiezd response
**Classification code:** 716 Telecommunication; Radar, Radio and Television - 718 Telephone Systems and Related Technologies; Line Communications - 723 Computer Software, Data Handling and Applications - 723.2 Data Processing and Image Processing
**DOI:** 10.1109/NaNA60121.2023.00071
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 37. The Differential Privacy Framework for Convolutional Neural Network using PATE, ADLM and SGD models

**Accession number:** 20234715078103
**Authors:** Tang, Suwan (1); Wang, Wu (1)
**Author affiliation:** (1) School of Mathematics and Computer Science, Yunnan Minzu University, Kunming, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 479-483
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023

**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** The use of CNNs raises concerns over privacy, especially when dealing with sensitive data, therefore, differential privacy has emerged to protect the privacy of data providers while allowing data analysis and model training. Differential privacy is a mathematical framework that protects sensitive data by adding random noise to the training data. In this study, we propose a differential privacy framework for CNNs using the PATE(Private Aggregation of Teacher Ensembles), ADLM(Adaptive Laplace Mechanism), and SGD(Stochastic Gradient Descent) models. We experimentally demonstrate that the proposed framework achieves better accuracy while providing strong privacy guarantees in image recognition tasks. © 2023 IEEE.
**Number of references:** 23
**Main heading:** Sensitive data
**Controlled terms:** Convolution - Convolutional neural networks - Gradient methods - Image recognition - Laplace transforms - Privacy-preserving techniques - Stochastic models - Stochastic systems
**Uncontrolled terms:** Adaptive laplace mechanism - Analysis and models - Convolutional neural network - Differential privacies - Privacy frameworks - Private aggregation of teacher ensemble - Private aggregations - Sensitive datas - Stochastic gradient descent - Teachers'
**Classification code:** 716 Telecommunication; Radar, Radio and Television - 716.1 Information Theory and Signal Processing - 718 Telephone Systems and Related Technologies; Line Communications - 723.2 Data Processing and Image Processing - 731.1 Control Systems - 921.3 Mathematical Transformations - 921.6 Numerical Methods - 922.1 Probability Theory - 961 Systems Science
**DOI:** 10.1109/NaNA60121.2023.00085
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 38. Leverage Generative Adversarial Network for Enhancing Fairness and Utility

**Accession number:** 20234715078028
**Authors:** Chen, Qiuling (1); Ye, Ayong (1); Wu, Fengyu (1); Zhang, Huang (1)
**Author affiliation:** (1) Fujian Normal University, College of Computer and Cyber Security, Fuzhou, China
**Corresponding author:** Ye, Ayong(yay@fjnu.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 508-513
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Datasets are crucial for training machine learning models. When datasets exist biases, trained models are prone to discriminate against groups with some sensitive attributes. To address the problem, constructing fair datasets is the straightforward method to prevent discrimination. However, fair datdasets can only meet group fairness for prediction results independent of sensitive attributes. Since some classification-based fairness such as individual fairness involves specific class labels, additional constraints need to be introduced during the training of the prediction model. Inspired by this, we propose a fairness-aware generative adversarial network. The model training combines the generative model and predictive model to generate the new adversarial coding representation and achieve classification fairness. In addition, in order to reduce the accuracy loss for the introduction of fairness constraints and eliminate potential discrimination caused by attribute correlation, the non-sensitive attributes (that are helpful for class label prediction and little correlation with sensitive information) are retained for replacing part of the random noise as the model input. Experimental evaluations are obtained using real-world census data. The results indicate that our

method can generate fair representations as well as make fairer classifications while ensuring good utility. © 2023 IEEE.
**Number of references:** 20
**Main heading:** Generative adversarial networks
**Controlled terms:** Classification (of information) - Forecasting - Population statistics
**Uncontrolled terms:** Class labels - Data bias - Fair classification - Fair representation - Machine learning models - Prediction modelling - Sensitive attribute - Specific class - Straight-forward method - Training machines
**Classification code:** 716.1 Information Theory and Signal Processing - 723.4 Artificial Intelligence - 903.1 Information Sources and Analysis
**DOI:** 10.1109/NaNA60121.2023.00090
**Funding Details:** Number: 2022H6025,U1905211, Acronym: -, Sponsor: -; Number: 61771140,61872088,61872090,61902289,61972096, Acronym: NSFC, Sponsor: National Natural Science Foundation of China;
**Funding text:** This work is supported partially by the National Natural Science Foundation of China [61972096, 61771140, 61872088, 61872090, 61902289], the University-Industry Cooperation of Fujian Province [2022H6025], and the Joint Funds of the National Natural Science Foundation of China [U1905211].
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 39. Radiofrequency Fingerprint Feature Extraction and Recognition Using a Coordinate Attention-Guided Deep Residual Shrinkage Network

**Accession number:** 20234715078034
**Authors:** Wang, Yinglin (1); Cao, Chunjie (1); Li, Yifan (1); Dong, Qianlin (1); Li, Haoran (1); Sun, Jingzhang (1)
**Author affiliation:** (1) School of Cyberspace Security, Hainan University, Haikou, China
**Corresponding authors:** Cao, Chunjie(chunjie_cao@126.com); Sun, Jingzhang(jingzhangsun@hainanu.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 551-557
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** The current radiofrequency fingerprint (RFF) feature extraction and recognition methods using deep learning (DL) lack multiple dimensions for the extracted feature vectors. At the same time, due to the black box property of deep learning, problems such as overfitting often occur in experiments, leading to a decrease in classification effect. In this paper, we proposed a DL method for RFF feature extraction and identification using the coordinate attention-guided (CA) deep residual shrinkage network (DRSN-CA). DRSN-CA integrates the advantages of CA mechanism and DRSN, optimizes the internal attention mechanism for residual shrinkage building unit (RSBU) into a better CA mechanism, and generates a new RSBU-CA module. The module combines the two dimensions of space and channel, which not only reduces the loss of information because of dimensionality reduction, but also enhances the impact of feature extraction for the model under low signal-to-noise ratio. The quantitative results indicated that the effect of DRSN-CA is promising. Compared with the traditional RFF feature extraction and recognition methods, the classification recognition accuracy of 92.5% can be achieved at the maximum distance of 62ft at the lower signal-to-noise ratio of 0dB. © 2023 IEEE.
**Number of references:** 33
**Main heading:** Shrinkage
**Controlled terms:** Classification (of information) - Deep learning - Extraction - Feature extraction - Learning systems - Palmprint recognition - Signal to noise ratio

**Uncontrolled terms:** Attention mechanisms - Coordinate attention mechanism - Feature extraction and recognition - Feature extraction methods - Features extraction - Fingerprint features - Radiofrequencies - Radiofrequency fingerprint - Recognition methods - Specific emitter identification
**Classification code:** 461.4 Ergonomics and Human Factors Engineering - 716.1 Information Theory and Signal Processing - 723.5 Computer Applications - 802.3 Chemical Operations - 903.1 Information Sources and Analysis - 951 Materials Science
**DOI:** 10.1109/NaNA60121.2023.00097
**Funding Details:** Number: 2021YFB2700600, Acronym: -, Sponsor: -; Number: U19B2044, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: 621MS017, Acronym: -, Sponsor: Natural Science Foundation of Hainan Province;
**Funding text:** ACKNOWLEDGMENT This work was supported in part by the Joint Funds of the National Natural Science Foundation of China (No. U19B2044), in part by the Key Research and Development Program of National Natural Science Foundation of China (No. 2021YFB2700600), and in part by the Natural Science Foundation of Hainan Province (No.621MS017).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 40. A Rapid Configuration Mechanism Based on Load Measurement for NETCONF in SDN Networks

**Accession number:** 20234715078051
**Authors:** Ma, Lingui (1); Yang, Fan (1); Chen, Tingting (1)
**Author affiliation:** (1) School of Telecomm. Eng, Xidian University, Xi'an, China
**Corresponding author:** Ma, Lingui(1119519415@qq.com)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 245-250
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** With the development of communication technology, there is an increasing demand for rapid deployment of services. As a widely used southbound interface in Software-Defined Networking (SDN), the NETCONF uses the TCP to transmit configuration information for network service deployment. The traditional TCP mechanism cannot set the transmission rate based on the actual network load status, thus its poor configuration efficiency for small-scale configuration services. As a novel network architecture, SDN can provide a global network view. In this paper, we propose a rapid configuration mechanism based on load measurement for NETCONF to improve the configuration efficiency of network devices. This mechanism dynamically measures the network load to select the optimal transmission path for configuration services and sets the initial transmission rate for services based on the load status of the selected path, thus achieving quick configuration of the devices. Simulation using OPNET shows that the proposed mechanism can effectively reduce the configuration service delay and improve the configuration efficiency compared with the traditional TCP mechanism. © 2023 IEEE.
**Number of references:** 10
**Main heading:** Software defined networking
**Controlled terms:** Efficiency - Network architecture - Transmission control protocol
**Uncontrolled terms:** Communicationtechnology - Configuration mechanisms - Loads measurements - Mechanism-based - NETCONF - Network configuration - Network load - Rapid deployments - Software-defined networkings - Transmission rates
**Classification code:** 722.3 Data Communication, Equipment and Techniques - 723 Computer Software, Data Handling and Applications - 913.1 Production Engineering

**DOI:** 10.1109/NaNA60121.2023.00048
**Funding Details:** Number: 2020YFB1805601, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China;
**Funding text:** ACKNOWLEDGEMENT This work is supported by the National Key Research and Development Program of China (2020YFB1805601).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 41. A Delay Guarantee Mechanism Based on Active and Passive Measurement in SDN Networks

**Accession number:** 20234715078045
**Authors:** Di, Qiong (1); Ying, Chaoran (1); Yang, Fan (1); Yu, Qing (1); Ren, Yaxin (1)
**Author affiliation:** (1) School of Telecomm. Eng, Xidian University, Xi'an, China
**Corresponding author:** Di, Qiong(21011210137@stu.xidian.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 384-389
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Delay guarantees are critical for the fast-growing network services that require low delay. Selecting the appropriate routing path for services with delay requirements is an important aspect of ensuring low delay. However, traditional routing mechanisms may have a negative impact on the delay of existing network services, as they primarily focus on satisfying the delay requirements of new services. In this paper, we present a delay guaranteed routing mechanism for software-defined network (SDN). Our mechanism employs a combination of active and passive delay measurements to determine the delays of multiple paths between the source and destination switches, and then chooses paths for services based on the load of the links on these paths and the delay requirements of the services. We also propose a rerouting mechanism in case the service delay cannot be fulfilled. The simulation results show that our proposed method provides better delay guarantees for network services. © 2023 IEEE.
**Number of references:** 13
**Main heading:** Electric loads
**Controlled terms:** Network routing - Software defined networking
**Uncontrolled terms:** Active measurement - Delay guarantee - Delay measurements - Link Loads - Low delay - Mechanism-based - Networks services - Passive measurements - Routing mechanism - Software-defined networkings
**Classification code:** 706.1 Electric Power Systems
**DOI:** 10.1109/NaNA60121.2023.00070
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 42. Joint Location and Power Optimization for Secure Communications in Multi-UAVs Enabled Cellular Networks

**Accession number:** 20234715078053
**Authors:** Deng, Fei (1, 2); Qian, Kaiguo (1, 2); Shen, Shikai (1, 2); Hong, Sunyan (1, 2); Yang, Bin (3); Li, Xuanxuan (1, 2); He, Jun (2, 4)

**Author affiliation:** (1) College of Information Engineering, Kunming University, Kunming; 650214, China; (2) Key Laboratory of Data Governance and Intelligent Decision, Universities of Yunnan, Kunming; 650214, China; (3) School of Computer and Information Engineering, Chuzhou University, Chuzhou; 239000, China; (4) Kunming University, Office of Science and Technology, Kunming; 650214, China
**Corresponding authors:** Shen, Shikai(kmssk2000@sina.com); Yang, Bin(yangbinchi@gmail.com)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 645-648
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** This paper investigates joint location and power optimization for secure communication in a multi-unmanned acrial vehicles (U A V s) enabled cellular network consisting of interference link, eavesdropping link, cellular link and D2D link. To this end, we first derive the expression of secure rate. Then, we formulate the maximization of secure rate as a constrained optimization problem. Finally, we solve it using the method of exhaustion. © 2023 IEEE.
**Number of references:** 10
**Main heading:** Wireless networks
**Controlled terms:** Constrained optimization - Mobile security - Mobile telecommunication systems - Network layers - Network security
**Uncontrolled terms:** Cellular network - Joi - Joint locations - Joint power - Location optimization - Multi-UA vs - Ocation - Physical layer security - Power Optimization - Secrecy rate
**Classification code:** 716.3 Radio Systems and Equipment - 722.3 Data Communication, Equipment and Techniques - 723 Computer Software, Data Handling and Applications - 723.2 Data Processing and Image Processing - 961 Systems Science
**DOI:** 10.1109/NaNA60121.2023.00111
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 43. GAN-Based Covert Communications Against an Adversary with Uncertain Detection Threshold in Federated Learning Networks

**Accession number:** 20234715078083
**Authors:** Feng, Yu (1); Jiang, Yu'e (1); Wang, Yutong (1)
**Author affiliation:** (1) Anhui Province School of Computer and Information, Anqing Normal University, University Key Laboratory of Intelligent Perception and Computing, Anqing, China
**Corresponding author:** Jiang, Yu'e(jiang2012118@163.com)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 613-618
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China

**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Federated learning (FL) is a promising distributed machine learning paradigm that can address privacy and security issues in the Internet of Things, Beyond 5G and 6G, and so on. Typically, numerous mobile devices in the FL network enable the server to complete model aggregation by uploading trained models obtained from local data. However, due to the broadcast nature of wireless channels, this upload process is vulnerable to adversary's monitoring or potential attacks, and it becomes one of the important risks of model leakage. Physical layer covert communications can protect the existence of covert signals or links, which is one of the effective methods to protect this model uplink. Furthermore, when there is an adversary with an uncertain detection threshold in the network, there is a competitive game between the adversary and mobile devices, which poses a challenge to the transmit power design of covert schemes. Considering the dynamic competition process in covert communications is similar to the zero-sum game process between discriminators and generators in Generative Adversarial Networks (GANs). Therefore, we propose a GAN-based physical layer covert communications against the adversary and protect the uplink in the FL networks. Moreover, the generator imitates the mobile device and the discriminator imitates the adversary. Both are constructed using neural networks, and the learning optimization process is achieved through a zero-sum game between them. Experiment results show that the designed algorithm is convergent and can obtain the optimal covert transmit power and the maximum average communication rate. © 2023 IEEE.
**Number of references:** 15
**Main heading:** Generative adversarial networks
**Controlled terms:** 5G mobile communication systems - Game theory - Learning systems - Network layers
**Uncontrolled terms:** Covert communications - Detection threshold - Federated learning network - Learning network - Network-based - Physical layer covert communication - Physical layers - Transmit power - Uncertain detection threshold - Zero-sum game
**Classification code:** 716.3 Radio Systems and Equipment - 723 Computer Software, Data Handling and Applications - 723.4 Artificial Intelligence - 922.1 Probability Theory
**DOI:** 10.1109/NaNA60121.2023.00106
**Funding Details:** Number: 2022AH051054,KJ2020A0497, Acronym: -, Sponsor: -;
**Funding text:** This work was supported in part by the Key Project on Anhui Provincial Natural Science Study by Colleges and Universities (No. KJ2020A0497, No. 2022AH051054).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 44. Classification of Hash Functions Based on Anti-Attack Ability

**Accession number:** 20234715078089
**Authors:** Wang, Yu (1); Gu, Naijie (1)
**Author affiliation:** (1) School of Computer Science and Technology, University of Science and Technology of China, Hefei, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 440-446
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Hash functions are widely used in the network field to provide support for load balancing, identity authentication, etc. Since the security problems of traditional hash functions continue to be exposed, researchers have proposed many new hash functions, such as keyed hash functions and provably secure hash functions. However, due to the existing classification methods can't fit the real-life security requirements well, it is still difficult for designers to choose appropriate hash functions in practice. This paper proposes a new classification method of hash functions based on their anti-attack ability, and classifies 301 common hash functions. The method, which considers the

performance of hash functions under different attack strategies and the characteristics of new hash functions, can provide a better classification for practical application scenarios. In addition, this paper uses classic supervised learning algorithms to study the classification results based on the performance testing indicators of hash functions. The experimental prediction accuracy of the unknown hash function can reach 88.52%, which verifies that the new classification method has good applicability. © 2023 IEEE.
**Number of references:** 45
**Main heading:** Hash functions
**Controlled terms:** Learning algorithms - Machine learning - Network security
**Uncontrolled terms:** Classification methods - Hash collisions - Identity authentication - Keyed hash functions - Load-Balancing - Networks security - Provably secure - Secure hash function - Security problems - Security requirements
**Classification code:** 723 Computer Software, Data Handling and Applications - 723.4 Artificial Intelligence - 723.4.2 Machine Learning
**DOI:** 10.1109/NaNA60121.2023.00079
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 45. Man-machine Cooperative Monitoring System to Support Detection of DoS/DDoS Attacks Through Continuous SOM Diagram Generation

**Accession number:** 20234715078005
**Authors:** Suzuki, Hikofumi (1); Iwasa, Akiyoshi (2); Uchiyama, Takumi (1); Wasaki, Katsumi (3)
**Author affiliation:** (1) Shinshu University, Center for Information Infrastructure, Nagano, Japan; (2) Hitachi Industry & Control Solutions, Ltd., Tokyo, Japan; (3) Engineering Shinshu University, Faculty of Engineering Electrical and Computer, Nagano, Japan
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 558-567
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** DoS/DDoS attacks on the Internet target various organizations and government agencies. Because DoS/DDoS attacks disguise themselves as legitimate communication, they are difficult to detect with high precision. In actual networks, network administrator detection DoS/DDoS attacks are based on thresh-olds for the number of DoS events, blacklists of DoS sources, and server conditions. However, automation and mechanization are difficult, and manual detection by administrators is inadequate. In this study, we developed a system to assist administrators in detecting DoS/DDoS attacks using a self-organizing map (SOM) neural network. The system continuously acquires traffic data from security devices and automatically generates SOM diagrams. In addition, the system generates traffic data known as an attack in advance and inserts them into the legitimate traffic data, thereby facilitating the judgment of attacks by administrators. Administrators analyzed DoS/DDoS attacks using this system over two months. As a result of analyzing 202 SOM diagrams generated periodically, the administrator was able to classify 65 abnormal SOMs diagrams into three types of abnormal states. Moreover, for 10 of the 65 SOMs, we could assist in identifying DoS/DDoS attacks. This paper describes the continuous acquisition of traffic data, insertion of pseudo-attacks, automatic generation of SOM diagrams, and administrator decision support and judgment, © 2023 IEEE.
**Number of references:** 25
**Main heading:** Self organizing maps
**Controlled terms:** Conformal mapping - Decision support systems - Network security

**Uncontrolled terms:** Attack detection - Attack detection support - Clustering techniques - DoS/DDoS - DoS/DDoS at-tack - DoS/DDoS attacks - Networks security - Self-organizing map - Self-organizing-maps - Traffic data
**Classification code:** 723 Computer Software, Data Handling and Applications - 912.2 Management
**DOI:** 10.1109/NaNA60121.2023.00098
**Funding Details:** Number: JP22K11982, Acronym: KAKEN, Sponsor: Japan Society for the Promotion of Science;
**Funding text:** This research was supported by JSPS KAKENHI Grant Number JP22K11982. We also received support from the Center for Information Infrastructure Shinshu University, which operates the UTM equipment used in this research, and Nippon Telegraph and Telephone East Corporation, which manages and operates the Shinshu University network. We want to express our gratitude to them.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 46. Security Risk Assessment of Image Classification Model Based on ANP-TOPSIS

**Accession number:** 20234715078110
**Authors:** Zhang, Zhiheng (1); Liu, Zeyu (1); Yang, Li (1); Zhe, Tingbo (2); Wu, Jian (2)
**Author affiliation:** (1) School of Computer Science and Technology, Xidian University, Xi'an, China; (2) Guiyang Aviation Motor Co., Ltd, Guizhou, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 300-306
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Recently, machine learning algorithms have been widely used in the fields of image processing, network security and natural language processing, etc., profoundly affecting human life. However, machine learning algorithms have the characteristics of uncertain output, vulnerability to adversarial attacks, and unexplained decision-making processes, which seriously threaten the security of machine learning-based face recognition, Malware detection, and autonomous driving. Hence, it is imperative for the security practitioners to evaluate algorithm security to ensure that security needs are met. In this article, the authors propose a set of security assessment index systems and methods for machine learning algorithms for image classification scenarios: Refer to the security specification of machine learning algorithms and requirements to construct the security index system of image classification model. Furthermore, The Analytic Network Process(ANP) is applied to quantify the index weights and the Technique for Order Preference by Similarity to an Ideal Solution(TOPSIS) is applied to screen the optimal model, and finally the sensitivity analysis is applied to prove the stability of the proposed method. Experimental results show that this method has certain value and effect in assessing the security and model screening of image classification models. © 2023 IEEE.
**Number of references:** 21
**Main heading:** Image classification
**Controlled terms:** Decision making - Face recognition - Learning algorithms - Machine learning - Malware - Natural language processing systems - Network security - Risk assessment - Sensitivity analysis
**Uncontrolled terms:** Algorithm security - Analytic network - Analytic network process - Classification models - Ideal solutions - Images classification - Machine learning algorithms - Network process - Security assessment - Technique for order preference by similarity to an ideal solution
**Classification code:** 723 Computer Software, Data Handling and Applications - 723.2 Data Processing and Image Processing - 723.4 Artificial Intelligence - 723.4.2 Machine Learning - 912.2 Management - 914.1 Accidents and Accident Prevention - 921 Mathematics
**DOI:** 10.1109/NaNA60121.2023.00057
**Compendex references:** YES
**Database:** Compendex

**Data Provider:** Engineering Village


## 47. A Novel On-Demand Service Architecture for Efficient Cloud-Edge Collaboration

**Accession number:** 20234715078049
**Authors:** Zhang, Yaling (1, 2); Chen, Jingjing (1); Wang, Yichuan (1, 2); Xiao, Yeqiu (1); Liu, Xiaoxue (1)
**Author affiliation:** (1) School of Computer Science and Engineering, Xi'an University of Technology, Xi'an, China; (2) Shaanxi Key Laboratory for Network Computing and Security Technology, China
**Corresponding author:** Liu, Xiaoxue(liuxiaoxue@xaut.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 169-174
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** With the advent of 5G era, the model of cloud-edge collaboration is used to handle massive data computing tasks with significant superiority. However, this architecture still uses the traditional web service model, which has problems such as single service and low resource utilization during the interaction between users and remote web servers. In this paper, we propose a novel on-demand service architecture that changes the traditional inefficient network service approach and skews the entire network service to the user. By fine- grained division of users' demands and hosting them in the corresponding functional servers for processing, the resolution of users' demands is no longer restricted by the services provided by the server, thus realizing 'information to people and services on demand'. Experiments show that the new on- demand service architecture reduces the latency by 33.3%, improves the quality and efficiency of information services, and realizes a more proactive and flexible information service model, which is more suitable for users' needs. © 2023 IEEE.
**Number of references:** 16
**Main heading:** Information services
**Controlled terms:** 5G mobile communication systems - Computer architecture - Network architecture - Web services
**Uncontrolled terms:** Cloud-edge collaboration - Computing architecture - Computing-task - Massive data - Networks services - On-demand services - Service mode - Services Architectures - User demands - Web Service modeling
**Classification code:** 716.3 Radio Systems and Equipment - 903.4 Information Services
**DOI:** 10.1109/NaNA60121.2023.00036
**Funding Details:** Number: 62072368,U20B2050, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: 2021ZDLGY05-09,2022CGKC-09, Acronym: -, Sponsor: Shanxi Provincial Key Research and Development Project; Number: 2023-JC-QN-0742, Acronym: -, Sponsor: Natural Science Basic Research Program of Shaanxi Province;
**Funding text:** ACKNOWLEDGMENT This research work is supported by the National Natural Science Founds of China (62072368, U20B2050), Key Research and Development Program of Shaanxi Province (2021ZDLGY05-09, 2022CGKC-09), and Natural Science Basic Research Program of Shaanxi Province (2023-JC-QN-0742).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 48. DDoS Attack Detection Based on Information Entropy Feature Extraction in Software Defined Networks

**Accession number:** 20234715078030
**Authors:** Ji, Wenjiang (1, 2); Yang, Yixin (1); Zhang, Yaling (1); Wang, Yichuan (1, 2); Tian, Mengjie (1); Qiu, Yuan (1)

**Author affiliation:** (1) Xi'an University of Technology, School of Computer Science and Engineering, Xi'an, China; (2) Shaanxi Key Laboratory for Network Computing and Security Technology, China
**Corresponding author:** Zhang, Yaling(ylzhang@xaut.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 459-464
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Distributed Denial of Service(DDoS) attacks target the forwarding-control separation feature of Software-Defined Networking(SDN) to launch attacks, causing network disruptions. Therefore security against DDoS attack detection for SDN controllers is the focus of current research. This paper proposes an Extreme Gradient Boosting (XGBoost) DDoS attack detection algorithm based on a combination of information gain and recursive feature elimination algorithms. We evaluated the performance of the method using the CICDDoS2019 dataset. This method works well in multi-classification model for attack detection with an accuracy of 93.41%. © 2023 IEEE.
**Number of references:** 16
**Main heading:** Software defined networking
**Controlled terms:** Denial-of-service attack - Feature extraction - Network security
**Uncontrolled terms:** Attack detection - Boosting algorithm - Denialof- service attacks - Distributed denial of service - Distributed denial of service attack detection - Extreme gradient boosting algorithm - Gradient boosting - Information gain - Recursive feature elimination - Software-defined networkings
**Classification code:** 723 Computer Software, Data Handling and Applications - 902.3 Legal Aspects
**DOI:** 10.1109/NaNA60121.2023.00082
**Funding Details:** Number: 62120106011,U20B2050, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: 2022YFB2602203, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China; Number: 2019GY-032,2020GY-039, Acronym: -, Sponsor: Shanxi Provincial Key Research and Development Project;
**Funding text:** ACKNOWLEDGMENTS This work was supported by National Key R&D Program of China (No. 2022YFB2602203), Natural Science Foundation of China under Grant U20B2050, 62120106011, and Key Research and Development Program of Shaanxi Province under Grant 2020GY-039, 2019GY-032.(Corresponding author: Yalin Zhang.)
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 49. Block Transmission Scheduling Strategy Based on Deadline Priority

**Accession number:** 20234715078104
**Authors:** Huang, Lei (1); Shi, Huiling (1); Zhang, Wei (1); Yu, Kun (2)
**Author affiliation:** (1) Qilu University of Technology, Shandong Academy of Sciences, Shandong Provincial Key Laboratory of Computer Networks, Shandong Computer Science Center, National Supercomputer Center in Jinan, Jinan, China; (2) College of Computer, Jingchu University of Technology, Jingmen, China
**Corresponding authors:** Shi, Huiling(shihl@sdas.org); Yu, Kun(17732385@qq.com)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 104-109
**Language:** English

**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Emerging network applications, such as virtual reality technology, autonomous driving, and large-scale Internet of Things, usually require a significant amount of bandwidth and have high requirements for data delivery time. However, the existing Quick UDP Internet Connection (QUIC), TCP, and other protocols cannot fully meet these needs. A scheduling algorithm based on a time-sensitive protocol can meet the above requirements at the transport layer and reduce the development difficulty of the application layer. Therefore, this paper is based on Deadline-aware Transport Protocol (DTP) and implemented in a Python 3.0 environment. It focuses on the scenario where video data blocks are sent to the transport layer. In this paper, we study the decision-making method and congestion control method for data block priority and deadline, and optimize the delay-sensitive transmission protocol. We propose a scheduling algorithm to meet the service's delay demands and enhance the overall service quality. Additionally, we introduce an improved scheduling scheme for network scenarios involving multiple senders or receivers. Our research aims to effectively address the service delay requirements under different network conditions. © 2023 IEEE.
**Number of references:** 15
**Main heading:** Scheduling algorithms
**Controlled terms:** Decision making - Delay-sensitive applications
**Uncontrolled terms:** Block-transmission - Congestion control - Data blocks - Deadline-aware - Deadline-aware transport protocol - Protocol cans - Service delays - Transmission scheduling - Transport layers - Transport protocols
**Classification code:** 731.2 Control System Applications - 912.2 Management
**DOI:** 10.1109/NaNA60121.2023.00025
**Funding Details:** Number: 2021FNA01006, Acronym: -, Sponsor: -; Number: 2021GXRC091, Acronym: -, Sponsor: -; Number: 2021YFZD068, Acronym: -, Sponsor: -; Number: 2022CXGC20106, Acronym: -, Sponsor: -; Number: ZR2020LZH010,ZR2022LZH015, Acronym: -, Sponsor: Natural Science Foundation of Shanxi Province; Number: 2022GH007, Acronym: SDAS, Sponsor: Shandong Academy of Sciences; Number: 2022JBGP005, Acronym: -, Sponsor: Fundamental Research Funds for the Central Universities;
**Funding text:** VI. ACKNOWLEDGE This work was supported in part by the China University Industry-University-Research Innovation Fund under Grant No.2021FNA01006, the Jingmen Science and Technology Research and Development Plan Project under Grant No.2021YFZD068, the Fundamental Research Funds for the Central Universities under Grant No.2022JBGP005, the Shan-dong Provincial Natural Science Foundation under Grant No. ZR2022LZH015 and No. ZR2020LZH010, the Pilot International Cooperation Project for Integrated Innovation of Science, Education and Industry of Qilu University of Technology (Shandong Academy of Sciences) under Grant No.2022GH007 and No.2022JBZ01-01, the One Belt One Road Innovative Talent Exchange with Foreign Experts under Grant No.DL2022024004L, the Jinan Scientific Research Leader Studio Project under Grant No.2021GXRC091, and the Project of Key R&D Program of Shandong Province under Grant No.2022CXGC20106.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 50. A Time Slot Averaging Algorithm for Delay Sensitive Service of Small Particle Time in Slicing Packet Networks

**Accession number:** 20234715078035
**Authors:** Wu, Changduo (1); Yang, Fan (1); Zheng, Ting (1)
**Author affiliation:** (1) School of Telecomm. Eng, Xidian University, Xi'an, China
**Corresponding author:** Wu, Changduo(493735759@qq.com)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 251-255
**Language:** English

**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** With the development of 5G+, more and more usage scenarios for small particle services have been discovered. This article focuses on the time slot equalization problem of time delay sensitive services in small particle services carried by Slicing Packet Networks (SPN). We proposes a lossless adjustment mechanism for time slot bandwidth, and based on this, proposes a priority-based time slot averaging algorithm. Simulation of time delay shows that the proposed algorithm achieves better performance than the Simple Time Slot Averaging algorithm. © 2023 IEEE.
**Number of references:** 10
**Main heading:** Packet networks
**Controlled terms:** 5G mobile communication systems - Delay-sensitive applications - Time delay
**Uncontrolled terms:** Delay-sensitive services - Equalization problem - Lossless - Sensitive service - Slicing packet network small particle - Small particles - Time slot averaging - Time-delays - Timeslots - Usage scenarios
**Classification code:** 713 Electronic Circuits - 716.3 Radio Systems and Equipment - 731.2 Control System Applications
**DOI:** 10.1109/NaNA60121.2023.00049
**Funding Details:** Number: 2020YFB1805601, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China;
**Funding text:** ACKNOWLEDGMENT This work is supported by the National Key Research and Development Program of China (2020YFB1805601).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 51. Research on Safe-Content Distribution Technology in VANETs

**Accession number:** 20234715078107
**Authors:** Fan, Jinyu (1, 2); Li, Jiayi (1, 2); Li, Chunjiao (1, 2); Du, Yuheng (1, 2); Lyu, Yahan (1, 2)
**Author affiliation:** (1) School of Cyber Science and Engineering, Southeast University, Nanjing, China; (2) Engineering Research Center of Blockchain Application, Supervision, and Management, Ministry of Education, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 110-115
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Vehicular Ad-hoc networks (VANETs), composed of vehicles and roadside infrastructure, are designed to improve transportation efficiency, passenger safety, and comfort through Vehicle-to-Vehicle (V2V) and Vehicle-to-Roadside (V2R) communication. In content distribution, vehicles receive content broadcast by the Roadside Units (RSUs). Currently, there are many literatures on content distribution technology in VANETs, such as service-oriented vehicle communication, but they do not consider the data security. Due to the openness and vulnerability of the wireless communication network and the dynamic characteristics of VANETs, malicious nodes may tamper, forge, and replay messages, seriously hindering the application of VANETs. This article proposes a mechanism for content distribution based on the collaboration of V2R and V2V. On this basis, we also propose a new anonymous authentication scheme leveraging the general theory of linear equation group solving, which can realize identity authentication between nodes while protecting the real identity of users and achieving secure content distribution. © 2023 IEEE.

**Number of references:** 10
**Main heading:** Vehicular ad hoc networks
**Controlled terms:** Authentication - Network security - Roadsides - Vehicle to roadside communications - Vehicle to vehicle communications - Vehicles
**Uncontrolled terms:** Anonymous authentication - Content distribution - Distribution vehicles - Passenger safety - Passengers comfort - Roadside units - Service Oriented - Transportation efficiency - Vehicle to vehicles - Vehicular Adhoc Networks (VANETs)
**Classification code:** 406 Highway Engineering - 716 Telecommunication; Radar, Radio and Television - 716.3 Radio Systems and Equipment - 722.3 Data Communication, Equipment and Techniques - 723 Computer Software, Data Handling and Applications
**DOI:** 10.1109/NaNA60121.2023.00026
**Funding Details:** Number: 2242023K30034,BK20202001, Acronym: -, Sponsor: -; Number: 2020YFB1005500, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China; Number: 2242022R10107, Acronym: -, Sponsor: Fundamental Research Funds for the Central Universities;
**Funding text:** This research work was supported by the National Key Research and Development Project of China (Grant No. 2020YFB1005500), the Major Research Project of Jiangsu Province:'Leading the Charge with Open Competition'(Grant No.SBA2022050016), the Fundamental Research Funds for the Central Universities (No.2242022R10107), the Leading-edge Technology Program of Jiangsu Natural Science Foundation (Grant No. BK20202001), and the Fundamental Research Funds for the Central Universities (Grant No.2242023K30034).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 52. An Efficient Blockchain-Based Certificateless Anonymous Authentication Scheme for VANETs

**Accession number:** 20234715078111
**Authors:** Bi, Changbing (1, 2, 3); Tian, Youliang (1, 2, 3, 4); Li, Ta (1, 2, 3, 4); Wu, Shihong (1, 2, 3); Zhou, Hua (5)
**Author affiliation:** (1) Guizhou University, State Key Laboratory of Public Big Data, Guiyang; 550025, China; (2) College of Computer Science and Technology, Guizhou University, Guiyang; 550025, China; (3) Guizhou University, Guizhou Province Key Laboratory of Cryptography and Block Chain Technology, Guiyang; 550025, China; (4) Institute of Cryptography & Data Security, Guizhou University, Guiyang; 550025, China; (5) College of Big Data and Information Engineering, Guizhou University, Guiyang; 550025, China
**Corresponding author:** Tian, Youliang(youliangtian@163.com)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 649-654
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Vehicle ad-hoc networks (VANETs) play a critical role in providing security and privacy protection for intelligent transportation systems. However, the limited network bandwidth and computing capacity within VANETs have resulted in existing authentication schemes having excessive computational overhead, which cannot meet the low-latency communication requirements of VANETs. To tackle these problems, we propose an efficient blockchain-based certificateless anonymous authentication scheme for VANETs. Firstly, we propose a novel signature scheme without bilinear pairing to reduce the computational overhead in VANETs. Secondly, we utilize blockchain to facilitate trusted information sharing. Thirdly, we provide privacy-preserving through the use of anonymous keys, and enable tracing of vehicle identities in the event of malicious behavior. Finally, security analysis and simulation experiments demonstrate that our proposed scheme has lower communication and computational overhead, while satisfying various security requirements for VANETs, such as anonymity, unlinkability, and traceability. © 2023 IEEE.

**Number of references:** 15
**Main heading:** Authentication
**Controlled terms:** Blockchain - Intelligent systems - Network security - Privacy-preserving techniques - Public key cryptography - Vehicular ad hoc networks
**Uncontrolled terms:** Anonymous authentication - Authentication scheme - Block-chain - Certificateless - Certificateless signature - Computational overheads - Intelligent transportation systems - Privacy preserving - Security and privacy protection - Vehicle ad-hoc networks
**Classification code:** 716 Telecommunication; Radar, Radio and Television - 718 Telephone Systems and Related Technologies; Line Communications - 722.3 Data Communication, Equipment and Techniques - 723 Computer Software, Data Handling and Applications - 723.2 Data Processing and Image Processing - 723.3 Database Systems - 723.4 Artificial Intelligence
**DOI:** 10.1109/NaNA60121.2023.00112
**Funding Details:** Number: [2020]6008, Acronym: -, Sponsor: -; Number: [2021]1-5,[2022]2-4, Acronym: -, Sponsor: -; Number: 62272123,No.U1836205, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: 2021YFB3101100, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China; Number: [2022]065, Acronym: -, Sponsor: Science and Technology Program of Guizhou Province;
**Funding text:** This work was supported by the National Key Research and Development Program of China under Grant No.2021YFB3101100, the Key Program of the National Natural Science Union Foundation of China under Grant No.U1836205, Project of High-level Innovative Talents of Guizhou Province under Grant No. [2020]6008, Science and Technology Program of Guiyang under Grant No.[2021]1-5, Science and Technology Program of Guiyang under Grant No.[2022]2-4, Science and Technology Program of Guizhou Province under Grant No. [2020]5017, No. [2022]065, National Natural Science Foundation of China under Grant 62272123, Guizhou University Talent Introduction Research Fund under Grant No. GDRJHZ [2015]-53.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 53. Learning Based Preamble Collision Detection of Cellular Random Access by Physical Layer Features

**Accession number:** 20234715078069
**Authors:** Yin, Yi (1); Zhao, Dongmei (2); Li, Xufei (3); Zeng, Shuiguang (2)
**Author affiliation:** (1) College of Software, Hebei Polytechnic Institute, Shijiazhuang, China; (2) College of Computer and Cyber Security, Hebei Normal University, Shijiazhuang, China; (3) School of Computer Science, Xidian University, Xi'an, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 28-33
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** This paper proposes an early collision detection scheme based on the physical layer features of user equipment (UE) and convolutional neural networks (CNN). Our scheme can detect preamble collisions at the first stage of the random access procedure of 4G/5G, thus reducing the average RA delay without requiring protocol modification of the UE. We only considered passive detection using the raw signal of the preamble created according to the existing protocol. The simulation results indicate that our proposed scheme can achieve high detection performance under different channels and parameter settings. © 2023 IEEE.
**Number of references:** 22
**Main heading:** Convolutional neural networks

**Controlled terms:** 5G mobile communication systems - Convolution - Feature extraction - Multilayer neural networks - Network layers
**Uncontrolled terms:** 5g - Cellulars - Collision detection - Convolutional neural network - Detection scheme - Physical layer feature - Physical layers - Ran-dom access - Random access - User equipments
**Classification code:** 716.1 Information Theory and Signal Processing - 716.3 Radio Systems and Equipment - 723 Computer Software, Data Handling and Applications
**DOI:** 10.1109/NaNA60121.2023.00013
**Funding Details:** Number: 216Z0701G, Acronym: -, Sponsor: -; Number: QN2020251, Acronym: -, Sponsor: -; Number: 61672206, Acronym: NSFC, Sponsor: National Natural Science Foundation of China;
**Funding text:** This work was supported in part by the Natural Science Foundation of China (NSFC) under Grant 61672206, the Central Government Guides Local Science and Technology Development Fund Projects under Grant 216Z0701G, the Science and Technology Project of Hebei Education Department China under Grant QN2020251.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 54. Joint Covert and Secure Communications for Intelligent Reflecting Surface (IRS)-Aided Wireless Networks

**Accession number:** 20234715078006
**Authors:** Yang, Yihuai (1, 2); Shen, Shikai (1, 2); She, Yumei (3); Wang, Wu (3); Yang, Bin (4); Gao, Yangshui (1, 2)
**Author affiliation:** (1) School of Information and Technology, Kunming University, Kunming; 650214, China; (2) Yunnan Collegiate Key Laboratory for Data Governance and Intelligent Decision, Kunming; 650214, China; (3) School of Mathmatics and Computer Science, Yunnan Minzu University, Kunming; 650500, China; (4) School of Computer and Information Engineering, Chuzhou University, Chuzhou; 239000, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 138-142
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** This work investigates joint covert and secure communications via intelligent reflecting surface (IRS) in a non-line-of-sight (NLOS) wireless network in the presence of an eavesdropper and a warden. We consider a coordinator of Ben communicates with two users, where one user requires secure communication and the other seeks covert communication. An optimization problem is proposed to maximize the covert rate subject to the constraints of covert requirement, secure communication rate, amplitudes and phase shifts of reflecting elements, and transmit powers of secure and covert communications. We use the successive convex approximation(SCA) method to solve this problem. The numerical results illustrate the effectiveness of utilizing an IRS and highlight the impact of the number of reflecting elements on enhancing communication quality. © 2023 IEEE.
**Number of references:** 13
**Main heading:** Secure communication
**Controlled terms:** Network security - Wireless networks
**Uncontrolled terms:** Covert communications - Covert rate - Eavesdroppe - Intelligent reflecting surface - Nonline of sight - Optimization problems - Reflecting elements - Reflecting surface - Secrecy rate - Successive convex approximations
**Classification code:** 716.3 Radio Systems and Equipment - 722.3 Data Communication, Equipment and Techniques - 723 Computer Software, Data Handling and Applications
**DOI:** 10.1109/NaNA60121.2023.00031
**Funding Details:** Number: 2022XJZD12,KJ2021ZD0128, Acronym: -, Sponsor: -; Number: 20200228100, Acronym: -, Sponsor: -; Number: 202001BA070001-209,202101BA070001-088, Acronym: -, Sponsor: -; Number:

61962033,62066023, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: -, Acronym: YNU, Sponsor: Yunnan University;
**Funding text:** This work is supported in part by the National Natural Science Foundation of China under Grant No. 61962033 and No. 62066023; in part by the Anhui Research Project under Grant No. KJ2021ZD0128 and No. 2022XJZD12; in part by the Yunnan Local University Joint Special Funds for Basic Research under Grant No. 202001BA070001-209 and No. 202101BA070001-088; in part by the Ministry of Education industry-University Cooperative Education Program No. 20200228100; and in part by the Key Laboratory of Data Governance and Intelligent Decision at the University of Yunnan.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 55. Improving Bipartite Networks Embedding with Partially Available Vertex Content

**Accession number:** 20234715078041
**Authors:** Yang, Shuang (1); Li, Li (1)
**Author affiliation:** (1) School of Computer Science, Shaanxi Normal University, Xi'an; 710119, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 527-531
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Most interactive networks in the real world are bipartite networks, the research and analysis of bipartite networks has very high application value. Network embedding aims to represent nodes in a network as low-dimensional dense vectors, while retaining structural information and characteristics in the original network to the greatest extent. Most of the existing bipartite network only focus on structural characteristics, ignoring the effective content information on the vertex in the network. Different from the existing work, the problem studied in this paper has the following two characteristics: (1) There exists content information on vertices in bipartite networks; (2) One type of vertices has partially content information in bipartite networks. To solve this problem, this paper proposes a novel bipartite network embedding with partially available vertex content boosted, namely BEAVC, which can effectively use the limited content information of vertices to enhance the structure-only representation. The experimental results show that the embedding algorithm compensated by vertex information can better characterize nodes. © 2023 IEEE.
**Number of references:** 17
**Main heading:** Network embeddings
**Uncontrolled terms:** Bipartite network - Content information - Embeddings - Network embedding - Network representation - Network representation learning - Real-world - Research and analysis - Structural characteristics - Vertex embedding
**Classification code:** 723.4 Artificial Intelligence
**DOI:** 10.1109/NaNA60121.2023.00093
**Funding Details:** Number: 2020JM-290,2022JM-371, Acronym: -, Sponsor: -; Number: 61303092, Acronym: NSFC, Sponsor: National Natural Science Foundation of China;
**Funding text:** VI. ACKNOWLEDGMENT This work was supported by the National Natural Science Foundation of China (61303092), and the Shaanxi Province Natural Science Basic Research Foundation (2020JM-290, 2022JM-371).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village

## 56. Research on Cross-Chain Consensus Models in Complex Trust Environments

**Accession number:** 20234715078061
**Authors:** Liu, Chaozhang (1); Tang, Lin (1); Che, Lixuan (2); Zhang, Yubao (1); Xing, Hongwei (3); Zhang, Jianhui (3); Li, Entang (3); Li, Xiangyang (3)
**Author affiliation:** (1) State Grid Dezhou Power Supply Company, Shandong, Dezhou, China; (2) Weifang Vocational College, Shandong, Weifang, China; (3) Shandong Luruan Digital Technology Company, Shandon, Ji'nan, China
**Corresponding author:** Liu, Chaozhang(13969210909@163.com)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 350-358
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** With the application of blockchain technology in the fields of energy big data, government affairs and data sharing, the types of blockchain adapted to various scenarios have gradually flourished, and the ledgers operate in isolation from each other, forming data silos and causing challenges for interchain data access and consistent collaboration. Most of the current cross-chain mechanisms based on blockchain are notary mode and relay mode, which cannot be dynamically switched according to their respective organizations' trust degree, making it difficult to meet the requirements of cross-chain data access between blockchain systems in complex trust environments. Based on this issue, a cross-chain consensus model based on trust establishment is proposed. The scheme constructs a blockchain security trust model based on the network state, blockchain system security, node data consistency and malicious node rate during blockchain operations, combines fuzzy theory and probability distributions to determine the trust components of each system, and uses those trust components and their weights to determine the system's trust value. The cross-chain consensus scheme is designed based on this model, which can be flexibly switched between the notary model and the committee relay model to satisfy cross-chain interconnection and mutual access between systems with different trust relationships. The simulation results show that the proposed model and scheme have good performance in terms of stability and performance. © 2023 IEEE.
**Number of references:** 22
**Main heading:** Blockchain
**Controlled terms:** Complex networks - Network security - Probability distributions
**Uncontrolled terms:** Block-chain - Consensus models - Cross-chain consensus - Data access - Data Sharing - Dynamic switching - Energy - Model-based OPC - Performance - Trust models
**Classification code:** 722 Computer Systems and Equipment - 723 Computer Software, Data Handling and Applications - 723.3 Database Systems - 922.1 Probability Theory
**DOI:** 10.1109/NaNA60121.2023.00065
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 57. Hybrid Resource Sharing Solution in Virtual Wireless Networks

**Accession number:** 20234715078001
**Authors:** Yi, Boyou (1); Ren, Baoquan (2); Zhan, Jie (1)
**Author affiliation:** (1) School of Physics and Electronic Sciance, Hunan University of Science and Technology, Hnust, Xiangtan, China; (2) China Electronic System Engineering Company, Cesec, Beijing, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023

**Publication year:** 2023
**Pages:** 40-45
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** To tackle the challenge of low resource utilization in wireless network virtualization, a network planning and optimization framework is proposed in this paper. The framework leverages monitoring of the occupancy and status of multiple frequency bands and enhances coordination between physical network providers and virtual service provider collections to achieve optimal wireless coverage and improve the efficiency of virtual wireless networks. Building upon this framework, a hybrid controlled resource sharing scheme is suggested, which allows for flexible switching between fixed sharing and fully shared schemes. This approach enhances resource utilization, mitigates blocking, and improves the quality of service. © 2023 IEEE.
**Number of references:** 21
**Main heading:** Quality of service
**Controlled terms:** Virtual reality - Wireless networks
**Uncontrolled terms:** Multiple frequency - Network planning and optimization - Network virtualization - Optimization framework - Physical network - Planning framework - Quality-of-service - Resources sharing - Resources utilizations - Shared solution
**Classification code:** 716.3 Radio Systems and Equipment - 722.3 Data Communication, Equipment and Techniques - 723 Computer Software, Data Handling and Applications
**DOI:** 10.1109/NaNA60121.2023.00015
**Funding Details:** Number: BJTU20221102, Acronym: -, Sponsor: -; Number: GX-ZD202210012, Acronym: -, Sponsor: -;
**Funding text:** ACKNOWLEDGMENT This work has been supported by the National Engineering Research Center of Advanced Network Technologiesat Beijing Jiaotong University (Project No. BJTU20221102) and the Xiangtan Municipal Government project with approval number GX-ZD202210012. The author would like to thank them for their valuable contributions.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 58. A Risk Path Detection Based Trusted Delivery Mechanism in Integrated Satellite and Terrestrial Internet

**Accession number:** 20234715078092
**Authors:** Liu, Jun (1); Zhang, Tianyu (1); Li, Hewu (1); Wu, Qian (1); Zheng, Shaowen (2); Lu, Lu (2)
**Author affiliation:** (1) Institude for Network Sciences, Tsinghua University, Beijing, China; (2) Mobile Research Institute, Department of Network and It Technology, Beijing, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 23-27
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.

**Abstract:** The broad coverage, high bandwidth, and low latency characteristics of low-orbit mega-constellations have inspired extensive research on content delivery in conjunction with low-orbit satellite constellations and the collaboration between cloud service providers. This environment presents a potential opportunity for attackers who may attempt to launch various attacks, such as route hijacking, on satellites along the content delivery path. This paper explores the Risk Path Detection based Trusted Delivery Mechanism(RPD-TDM) to the scenario of content delivery in Integrated Satellite-Terrestrial Internet (ISTI), which enhances the security of delivery scheduling in the content delivery network architecture. It uses risk path detection to drive secure scheduling of edge servers, avoiding risk areas and ensuring the trustworthiness of delivery paths for high-value data. The experimental results demonstrate the effectiveness of the mechanism. © 2023 IEEE.
**Number of references:** 16
**Main heading:** Network architecture
**Controlled terms:** Digital storage - Network security - Orbits - Risk perception - Satellites - Trusted computing
**Uncontrolled terms:** Contents deliveries - Delivery mechanism - Delivery path - High bandwidth - High-low - Integrated satellite and terrestrial internet - Path detections - Risk path detection - Risk paths - Trusted path
**Classification code:** 655.2 Satellites - 722.1 Data Storage, Equipment and Techniques - 723 Computer Software, Data Handling and Applications - 723.2 Data Processing and Image Processing - 914.1 Accidents and Accident Prevention
**DOI:** 10.1109/NaNA60121.2023.00012
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 59. EDF: Enhanced Deep Fingerprinting attacks on Websites

**Accession number:** 20234715078011
**Authors:** Cui, Jipeng (1); Jiang, Zhongyuan (1)
**Author affiliation:** (1) School of Cyber Engineering, Xidian University, Xi'an, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 293-299
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Website Fingerprinting (WF) attacks enable network surveillants to monitor traffic data and learn features from encrypted packet sequences, thus identifying which website user is visiting, which seriously threatens user privacy on Tor. Recently, zero-delay lightweight defense methods (i.e., FRONT and GLUE) were designed for Tor to efficiently defend many known WF attacks. But, can they defend more unknown intelligent WF attacks? Due to the efficiency of deep learning model, we explore whether there is a more intelligent deep learning model that could defeat FRONT and GLUE. In this work, we propose two deep learning based WF attacks, EDF-S and EDF-P. EDP-S incorporates a global average pooling layer and series model into Deep Fingerprinting (DF), while EDF-P introduces a global average pooling layer and parallel model into DF. We conduct extensive WF attack experiments on several datasets to prove our improvement on effectiveness. EDF-P can achieve over 97% TPR and 96% F1 score on a non-defended dataset. We also find that EDF-S and EDF-P perform better than previous attacks against GLUE. Compared with DF, EDF-S can achieve almost 10% enhancement for the attack precision and F1 score while EDF-P can achieve more than 10% enhancement for the attack precision and F1 score. Our enhanced WF attacks bring new challenges to the above mentioned WF defenses. © 2023 IEEE.
**Number of references:** 25
**Main heading:** Websites
**Controlled terms:** Deep neural networks - Glues - Gluing - Learning systems - Network security
**Uncontrolled terms:** Deep learning - F1 scores - Layer model - Learn+ - Learning models - Packet sequence - Traffic analysis - Traffic data - User privacy - Zero delay

**Classification code:** 461.4 Ergonomics and Human Factors Engineering - 723 Computer Software, Data Handling and Applications
**DOI:** 10.1109/NaNA60121.2023.00056
**Funding Details:** Number: 61502375,62076191, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: 2022YFB2701800, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China;
**Funding text:** This work was sponsored by the National Key Research & Development Program of China under Grant No. 2022YFB2701800 and the National Natural Science Foundation of China under Grant No. 62076191 and 61502375.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 60. Evolutionary Equilibrium of Mining Pools Under DDoS Attack in Blockchain System

**Accession number:** 20234715078060
**Authors:** Liu, Xiao (1); Huang, Zhao (1); Wang, Quan (1)
**Author affiliation:** (1) School of Computer Science and Technology, Xidian University, Xi'an, China
**Corresponding author:** Huang, Zhao(z_huang@xidian.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 78-83
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Consensus algorithm is widely used in blockchain system, which can solve the problems of fault tolerance, consensus and security. Proof-of-work (PoW) algorithm is one of the most widely used consensus algorithms to ensure the security and consensus on transaction data of the Bitcoin system. However, as an important part of the Bitcoin system, mining pool is often subjected to distributed denial of service (DDoS) attack by malicious nodes at the network layer, which makes it suffer significant economic losses. In order to reduce the loss of mining pools caused by DDoS attack when the Bitcoin system carries out data consensus of PoW, this paper proposes an evolutionary game model based on mining pools. This model studies how to choose effective mining strategy to get the best profit in the face of DDoS attack. At the same time, we also set up the replication dynamic equation to analyze and solve the game model. The experimental results show that honest mining has the best profit under the condition of poor network for the mining pools. In the case of better network condition, the mining pools can get the best reward by attacking each other. At the same time, the experimental results are consistent with the theoretical conclusions, which proves that our model is effective. © 2023 IEEE.
**Number of references:** 14
**Main heading:** Blockchain
**Controlled terms:** Denial-of-service attack - Evolutionary algorithms - Fault tolerance - Game theory - Lakes - Network layers - Profitability
**Uncontrolled terms:** Block-chain - Consensus algorithms - Denialof- service attacks - Distributed denial of service - Distributed denial of service attack - Evolutionary equilibriums - Evolutionary game theory - Malicious nodes - Proof of work - Transaction data
**Classification code:** 723 Computer Software, Data Handling and Applications - 723.3 Database Systems - 902.3 Legal Aspects - 911.2 Industrial Economics - 922.1 Probability Theory
**DOI:** 10.1109/NaNA60121.2023.00021
**Funding Details:** Number: 61972302, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: XJS220306, Acronym: -, Sponsor: Fundamental Research Funds for the Central Universities; Number: 2022JQ-680, Acronym: -, Sponsor: Natural Science Basic Research Program of Shaanxi Province;

**Funding text:** This work was supported in part by the National Natural Science Foundation of China under Grant 61972302, in part by the Fundamental Research Funds for the Central Universities under Grant XJS220306, in part by the Natural Science Basic Research Program of Shaanxi under Grant 2022JQ-680, and in part by the Key Laboratory of Smart Human Computer Interaction and Wearable Technologyof Shaanxi Province.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 61. A Deep Model Intellectual Property Protection Method Supporting Public Verification

**Accession number:** 20234715078109
**Authors:** Shen, Yumeng (1); Tian, Feng (1); Lu, Qiaoling (1); Cui, Kemeng (1)
**Author affiliation:** (1) School of Computer Science, Shaanxi Normal University, Xi'an, China
**Corresponding author:** Tian, Feng(tianfeng@snnu.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 568-573
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Recently, the intellectual property protection methods based on deep learning have achieved great success, but there are still serious infringement issues that the network topology or hyper parameters of the trained model are stolen by third parties. In this paper, we construct a deep learning model based on the autoencoder to remove the bone from the medical images containing chest x-ray, and the specific trigger set is trained and predicted to get the effect of the backdoor watermark. The scheme of zero-knowledge proof is applied to transform the backdoor watermark of the model into the fixed-length string, which is published in the block chain to verify the ownership of the model. Through the non-interactive verification between the model owner and the third party, the ownership of the model can be confirmed by the third party and the verification process will not disclose any information of the model itself. The method proposed in this paper can support infinite times of verification and does not reveal any information about the model, so as to achieve the protection of intellectual property rights of the model. © 2023 IEEE.
**Number of references:** 15
**Main heading:** Deep learning
**Controlled terms:** Intellectual property - Laws and legislation - Learning systems - Medical imaging - Network topology
**Uncontrolled terms:** Backdoors - Bone suppression - Chest X-ray - Deep learning - Infinite verification - Intellectual property protection - Non-interactive zero-knowledge proofs - Protection methods - Public verifications - Third parties
**Classification code:** 461.1 Biomedical Engineering - 461.4 Ergonomics and Human Factors Engineering - 703.1 Electric Networks - 746 Imaging Techniques - 902.3 Legal Aspects - 971 Social Sciences
**DOI:** 10.1109/NaNA60121.2023.00099
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 62. Cloud Data Deduplication Scheme Based on Blockchain

**Accession number:** 20234715078000
**Authors:** Shi, Pengliang (1); Hao, Dongning (2)
**Author affiliation:** (1) Cyber Security and Computer Science Hebei University, Key Laboratory on High Trusted Information System, Baoding, China; (2) International College of Hebei University, Baoding, China

**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 410-415
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** To address the problem of untrustworthiness among entities faced in the process of data deduplication in cloud storage environment, this paper proposes a cloud data deduplication scheme based on blockchain. Firstly, to ensure the trustworthiness of data ownership proof in the data deduplication process, a data ownership verification algorithm based on random location sampling is designed with the help of blockchain technology and Merkle hash tree; Secondly, an oblivious pseudo-random protocol is used to obtain convergent encryption key to facilitate deduplication by cloud servers provides. Finally, the scheme security is proved by conducting security analysis, while simulation experiments are conducted to verify the effectiveness of the scheme. © 2023 IEEE.
**Number of references:** 18
**Main heading:** Cryptography
**Controlled terms:** Blockchain - Cloud storage - Network security - Trees (mathematics)
**Uncontrolled terms:** Block-chain - Cloud data - Cloud storages - Convergent encryption - Data de duplications - Data ownership - Merkle hash tree - Ownership verification - Random location - Verification algorithms
**Classification code:** 722.1 Data Storage, Equipment and Techniques - 723 Computer Software, Data Handling and Applications - 723.3 Database Systems - 921.4 Combinatorial Mathematics, Includes Graph Theory, Set Theory
**DOI:** 10.1109/NaNA60121.2023.00074
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 63. Spatial-Temporal Correlation-Based Prediction Model for Node and Link Residual Resources in NFV Networks

**Accession number:** 20234715078007
**Authors:** Lai, Jiahong (1); Yang, Fan (1); Ying, Chaoran (1); Song, Wenchao (1)
**Author affiliation:** (1) School of Telecomm. Eng, Xidian University, Xi'an, China
**Corresponding author:** Lai, Jiahong(20011210219@stu.xidian.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 256-261
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Network functions virtualization (NFV) mainly meets the various performance requirements of network services and improves the performance/cost ratio through the decoupling of software and hardware. However, the limited resources and the dynamic nature of requests in NFV scenarios pose challenges to network operators in

allocating resources and reducing operating expenses, thus the need for surplus resource prediction. Existing models only consider either spatial or temporal correlation of the residual resource data. Moreover, existing work often considers the change of the remaining resources of the node or link separately, ignoring the potential relationship between the two resources. This paper proposes a prediction model based on spatial-temporal correlation for predicting the remaining resources of each node and link in the network. By capturing the spatial and temporal correlation of the residual resource data at the same time, the model comprehensively considers the correlation between the remaining node and link resources and constructs an improved sequence-to-sequence model. Experiments show that the proposed model can significantly improve the prediction accuracy compared with the conventional models. © 2023 IEEE.
**Number of references:** 12
**Main heading:** Network function virtualization
**Controlled terms:** Forecasting - Spatial variables measurement - Transfer functions
**Uncontrolled terms:** In networks - Neural-networks - Nodes and links - Performance requirements - Prediction modelling - Residual resource - Residual resource prediction - Resource prediction - Spatial temporal analysis - Spatial-temporal correlation
**Classification code:** 722.3 Data Communication, Equipment and Techniques - 921 Mathematics - 943.2 Mechanical Variables Measurements
**DOI:** 10.1109/NaNA60121.2023.00050
**Funding Details:** Number: 2020YFB1805601, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China;
**Funding text:** ACKNOWLEDGMENT This work is supported by the National Key Research and Development Program of China (2020YFB1805601).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 64. A Survey of Trust Assessment Technology Research for Edge Computing

**Accession number:** 20234715078044
**Authors:** Chen, Lei (1, 2); Yu, Fei (1, 2); Ni, Siyuan (1, 2); Wang, Yuyao (1, 2); He, Yuanhang (1, 2)
**Author affiliation:** (1) Science and Technology on Communication Security Laboratory, Chengdu; 610041, China; (2) No.30 Research Institute of China Electronics Technology Group Corporation, Chengdu, China
**Corresponding author:** Yu, Fei(feiyu80@foxmail.com)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 34-39
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** With the rapid development of edge computing, security has become the key to the large-scale implementation of edge computing applications. In edge computing security, trust assessment is an important means to ensure safe access of terminals and safe operation of nodes. It is the basis for reliable data fusion and efficient computing at the edge of the network. More and more researchers have realized that it is very important and urgent to strengthen the research and application of trust assessmnt technology in the edge computing environment. This paper first introduces the definition of trust assessment and explains the challenges faced in the research of trust assessment technology under the edge computing environment; then, we summarize the current research status of trust assessment technology in the edge computing environment; secondly, we sort out the research status of trust assessment technology in the edge computing environment. In the end, we summarize the whole works and analyze the development trend of trust assessment technology. Our goal is to provide support for the research and application of future trust assessment technology under edge computing. © 2023 IEEE.
**Number of references:** 17

**Main heading:** Edge computing
**Controlled terms:** Data fusion - Trusted computing
**Uncontrolled terms:** Cloud-edge collaboration - Computing environments - Computing security - Edge computing - Large-scales - Research and application - Resource-scheduling - Secure access - Technology research - Trust assessments
**Classification code:** 722.4 Digital Computers and Systems - 723.2 Data Processing and Image Processing
**DOI:** 10.1109/NaNA60121.2023.00014
**Funding Details:** Number: 2023YFQ0028, Acronym: -, Sponsor: -; Number: 6142103022205, Acronym: -, Sponsor: -; Number: -, Acronym: NSFC, Sponsor: National Natural Science Foundation of China;
**Funding text:** VI. ACKNOWLEDGEMENT This work was supported by National Natural Science Foundation of China (No.U21B2019), Regional Innovation Cooperation Project of Sichuan Province (No. 2023YFQ0028) and Science and Technology on Communication Security Laboratory Foundation (No. 6142103022205).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 65. enDRTS: Deep Reinforcement Learning Based Deterministic Scheduling for Chain Flows in TSN

**Accession number:** 20234715078003
**Authors:** Yang, Dong (1); Gong, Kai (1); Zhang, Weiting (1); Guo, Kuo (1); Chen, Jia (1)
**Author affiliation:** (1) School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing, China
**Corresponding author:** Zhang, Weiting(wtzhang@bjtu.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 239-244
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** With the rapid development of artificial intelligence (AI) technology, learning-based time-sensitive networking (TSN) technology can be used as a promising network technology to facilitate automated network configuration in the industrial Internet of Things (IIoT). However, the stricter multiple requirements of the IIoT have posed significant challenges, that is, deterministic and bounded latency for jointly chain transmission of multiple service flows. In this paper, we propose an enhanced scheduling algorithm, namely enDRTS, based on deep reinforcement learning (DRL) for chain transmission of chained service flows to jointly solve the time slot scheduling problem in TSN. By analyzing the feature of flows and scheduling constraints, the DRL algorithm model can adjust the queue bandwidth allocation and transmission slot strategy of switch ports in time to make enDRTS more salable and efficient. Simulation experiments are conducted to evaluate the performances of enDRTS, and the results show that enDRTS can schedule more flows and improve time slot utilization compared with benchmark methods. © 2023 IEEE.
**Number of references:** 12
**Main heading:** Reinforcement learning
**Controlled terms:** Deep learning - Engineering education - Scheduling algorithms
**Uncontrolled terms:** Artificial intelligence technologies - Chain flow - Deep reinforcement learning - Deterministic scheduling - Flow scheduling - Networking technology - Reinforcement learnings - Service flows - Technology learning - Time-sensitive networking
**Classification code:** 461.4 Ergonomics and Human Factors Engineering - 723.4 Artificial Intelligence - 901.2 Education
**DOI:** 10.1109/NaNA60121.2023.00047

**Funding Details:** Number: 62201029, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: 2022M710007,BX20220029, Acronym: -, Sponsor: China Postdoctoral Science Foundation; Number: 2022YFB2901302, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China;
**Funding text:** ACKNOWLEDGMENT The work is supported in part by the National Key Research and Development Program of China under Grants (2022YFB2901302), in part by the National Natural Science Foundation of China under Grant 62201029, and in part by the China Postdoctoral Science Foundation under Grant BX20220029 and 2022M710007.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 66. A Digital Twin Framework for Logical Range

**Accession number:** 20234715078043
**Authors:** Dang, Zheng (1); Chen, Hao (1); Hei, Xinhong (1); Liu, Yilong (1)
**Author affiliation:** (1) School of Computer Science and Engineering, Xi'an University of Technology, Xi'an; 710048, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 313-317
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** The Logical Range is introduced into the joint flight test because it can call cross-area test resources and improve the utilization rate of test resources. However, the Logical Range also has the problems of low reusability of test resources and low efficiency in cross regional range data acquisition and communication. For this problem, a digital twin framework for logical range is proposed. In the framework, a Logical Range system based on digital twin is built, and the data network communication methods and virtual-real mapping method are designed in detail. The feasibility of this framework has been effectively verified through flight test examples. This study lays a solid foundation for the combination of flight test and digital twin technology. © 2023 IEEE.
**Number of references:** 18
**Main heading:** Reusability
**Controlled terms:** Data acquisition
**Uncontrolled terms:** Communication method - Data network - Flight test - Joint test - Logical range - Mapping method - Network communications - Range data - Test examples - Utilization rates
**Classification code:** 723.2 Data Processing and Image Processing
**DOI:** 10.1109/NaNA60121.2023.00059
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 67. Real-Time Semantic Segmentation Algorithm Based on Tversky Loss Function and Mixed Pooling

**Accession number:** 20234715078023
**Authors:** Xu, Peng (1); Zhao, Ziyi (2); Ma, Sugang (3)
**Author affiliation:** (1) Xi'an Science and Technology Museum, Shaanxi, Xi'an; 710002, China; (2) School of Computer Science and Technology, Xi'an University of Posts and Telecommunications, Shaanxi, Xi'an; 710121, China; (3) School of Computer Science and Technology, Xi'an University of Posts and Telecommunications, Shaanxi Key Laboratory of Network Data Analysis and Intelligent Processing, Shaanxi, Xi'an; 710121, China

**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 619-624
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** In recent years, semantic segmentation methods based on deep learning have made remarkable developments. Despite achieving high segmentation accuracy, the performance of real-time segmentation methods cannot satisfy real-world applications. In order to achieve a balance between segmentation accuracy and speed, a real-time semantic segmentation algorithm based on Tversky loss function and mixed pooling is proposed in this paper. A Short-Term Dense Concatenate network (STDC network) is used to construct the encoder, and a mixed pooling module is used for the final part of the encoder, which uses strip pooling and average pooling to enhance the feature representation while expanding the receptive field. Additionally, a Tversky-based loss function is used for the detail guidance module of the backbone network in the encoder, and a joint loss function is used to supervise the whole network's training. We achieved 76.9% mIoU at 110.7 FPS on the Cityscapes dataset, a 2.4% improvement in accuracy over the benchmark algorithm STDCSeg, and 72.2% mIoU at 177.6 FPS on the Camvid dataset, satisfied the requirements of the real-time segmentation task. © 2023 IEEE.
**Number of references:** 19
**Main heading:** Semantic Segmentation
**Controlled terms:** Computer vision - Deep learning - Semantic Web - Semantics - Signal encoding
**Uncontrolled terms:** Loss functions - Mixed pooling - Real-time semantic segmentation - Real-time semantics - Segmentation accuracy - Segmentation algorithms - Segmentation methods - Semantic segmentation - Short-term dense concatenate network - Tversky loss function
**Classification code:** 461.4 Ergonomics and Human Factors Engineering - 716.1 Information Theory and Signal Processing - 723 Computer Software, Data Handling and Applications - 723.4 Artificial Intelligence - 723.5 Computer Applications - 741.2 Vision - 903 Information Science
**DOI:** 10.1109/NaNA60121.2023.00107
**Funding Details:** Number: 22GXFW0125, Acronym: -, Sponsor: -; Number: 62072370, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: 2023-JC-YB-598, Acronym: -, Sponsor: Natural Science Foundation of Shaanxi Province;
**Funding text:** ACKNOWLEDGMENT This work was supported by the National Natural Science Foundation of China (Grant No. 62072370), the Natural Science Foundation of Shaanxi Province (Grant No. 2023-JC-YB-598) and the Science and Technology Project of Xi'an City (Grant No. 22GXFW0125).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 68. LMIPv6ATK:A Labeled Dataset Containing Multiple ICMPV6-DDOS Attacks

**Accession number:** 20234715078048
**Authors:** Li, Siyuan (1); Zhang, Liumei (1); Han, Yu (1)
**Author affiliation:** (1) School of Computer Science, Xi'an Shiyou University, Xi'an, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 52-57
**Language:** English
**ISBN-13:** 9798350327380

**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Distributed denial-of-service attacks using Internet Control Message Protocol version 6 messages can cause serious damage to IPV6 networks, resulting in huge economic losses. In this paper, we propose a packet feature-based dataset that can be used as a standard dataset for IPV6 attack detection systems and we named as LMIPv6ATK. The dataset is generated from a virtual network and contains both normal and multiple ICMPV6 DDOS attack traffic. Three classifiers: Naive Bayesian, decision tree, and random forest are used to test the dataset for the sake of tesifing the accuracy of our dataset. The accuracy of all three classifiers with multiple training is greater than 95%. The average accuracy was 96.73%. Among the results,Random forest takes the longest time, with an average accuracy of 98.77%. Thus,we can draw an conclusion that LMIPv6ATK dataset can be proved to be accurately applied to the attack detection system with high detection accuracy and low false alarm rate. © 2023 IEEE.
**Number of references:** 20
**Main heading:** Decision trees
**Controlled terms:** Classification (of information) - Denial-of-service attack - Feature extraction - Internet protocols - Losses - Network security - Statistical tests
**Uncontrolled terms:** Accuracy - Attack detection - Denialof- service attacks - Detection system - Distributed denial of service - Feature - Internet control message protocols - Labeled dataset - LMIPv6ATK dataset - Random forests
**Classification code:** 716.1 Information Theory and Signal Processing - 722.3 Data Communication, Equipment and Techniques - 723 Computer Software, Data Handling and Applications - 902.3 Legal Aspects - 903.1 Information Sources and Analysis - 911.2 Industrial Economics - 921.4 Combinatorial Mathematics, Includes Graph Theory, Set Theory - 922.2 Mathematical Statistics - 961 Systems Science
**DOI:** 10.1109/NaNA60121.2023.00017
**Funding Details:** Number: -, Acronym: XSYU, Sponsor: Xi'an Shiyou University; Number: 2023-JC-QN-0742, Acronym: -, Sponsor: Natural Science Basic Research Program of Shaanxi Province;
**Funding text:** Natural Science Basic Research Program of Shaanxi Province (2023-JC-QN-0742),postgraduate innovation and practical ability training program of Xi'an Shiyou University
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 69. On UAV-IRS-Aided Covert Communication of D2D-Enabled Cellular Networks

**Accession number:** 20234715078067
**Authors:** Wang, Sibo (1); Yang, Bin (2); Wang, Wu (3); Shen, Shikai (4); Jiang, Xiaohong (5)
**Author affiliation:** (1) School of Mechanical Engineering, Jiangsu University, Zhenjiang, China; (2) School of Computer and Information Engineering, Chuzhou University, Chuzhou, China; (3) School of Mathematics and Computer Science, Yunnan Minzu University, Kunming, China; (4) School of Information Engineering, Kunming University, Kunming, China; (5) School of Systems Information Science, Future University, Hakodate, Japan
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 58-63
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** In this paper, we investigated covert communication in D2D-Enabled cellular network scenario and proposed to improve the covert transmission rate with the assistance of a UAV-IRS (Unmanned Aerial Vehicle with Intelligent

Reflecting Surface) mobile relay. The use of UAV-IRS enables D2D transmitters on the ground to transmit sensitive information covertly to D2D receivers without detection by warden Willie. We first determine an optimal detection threshold and derive the detection error probability at Willie, this probability represents the worst-case legitimate transmission. Then, we maximize the covert transmission rate through the maximum transmission power of D2D transmitters, optimal phase shift and optimal horizontal position of UAV-IRS. Simulation results are presented the effectiveness of UAV-IRS-aided covert communication of D2D-enabled cellular networks. © 2023 IEEE.
**Number of references:** 12
**Main heading:** Transmitters
**Controlled terms:** Aircraft detection - Antennas - Optimal detection - Unmanned aerial vehicles (UAV) - Vehicle to vehicle communications - Vehicle transmissions - Wireless networks
**Uncontrolled terms:** Aerial vehicle - Cellular network - Covert communications - D2D communications - Intelligent reflecting surface - Mobile relays - Network scenario - Reflecting surface - Sensitive informations - Transmission rates
**Classification code:** 602.2 Mechanical Transmissions - 652.1 Aircraft, General - 716.2 Radar Systems and Equipment - 716.3 Radio Systems and Equipment - 722.3 Data Communication, Equipment and Techniques - 921.5 Optimization Techniques
**DOI:** 10.1109/NaNA60121.2023.00018
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 70. Correction Algorithm of Multi-Person Pose Estimation Based on Improved YOLOv5

**Accession number:** 20234715078114
**Authors:** Zhao, Jinyuan (1); Jia, Di (1, 2); Wang, Qian (1)
**Author affiliation:** (1) School of Electronic and Information Engineering, Liaoning Technical University, Liaoning, China; (2) School of Electrical and Control Engineering, Liaoning Technical University, Liaoning, China
**Corresponding author:** Jia, Di(lntu_jiadi@163.com)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 631-636
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Since multi-person pose estimation in crowded scenes still suffers from problems such as small detection targets, resulting in low pose estimation accuracy, we propose a correction algorithm for multi-person pose estimation based on the improved YOLOv5. Firstly, in the backbone network of YOLOv5, the Jumping Attention Mechanism module is incorporated to help the networks find the region of interest in the images; Secondly, in the neck network, the joint use of the Jump Attention Mechanism module and the Transformer encoder allows the network to acquire global information and contextual information. Finally, the key point object information obtained from the network prediction is used to correct the pose object information to get the final multi-person pose estimation results. The experimental results show that the method in this paper improves AP50 by 2.2% and AP75 by 3.3% over YOLOv5 on the COCO dataset, which verifies the accuracy and robustness of the approach in this paper. © 2023 IEEE.
**Number of references:** 16
**Main heading:** Image segmentation
**Controlled terms:** Signal encoding
**Uncontrolled terms:** Attention mechanisms - Back-bone network - Correction algorithms - Detection targets - Human pose estimations - Jump attention mechanism - Object information - Pose-estimation - Targets detection - Transformer encoder
**Classification code:** 716.1 Information Theory and Signal Processing
**DOI:** 10.1109/NaNA60121.2023.00109

**Funding Details:** Number: 61601213, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: LJ2020FWL004,2019-ZD-0038, Acronym: -, Sponsor: Department of Education of Liaoning Province;
**Funding text:** ACKNOWLEDGMENT This work was funded by the Central Universities Basic Research Project. Supported by the National Natural Science Foundation of China (61601213); Liaoning Provincial Education Department Project (LJ2020FWL004,2019-ZD-0038)
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 71. GNN-Based Data Rate Maximization in Double Intelligent Reflecting Surface (IRS)-Aided Communication System

**Accession number:** 20234715078040
**Authors:** Li, Kaixin (1); Peng, Limei (1); Ho, Pin-Han (2)
**Author affiliation:** (1) School of Computer Science and Engineering, Kyungpook National University, Deagu, Korea, Republic of; (2) University of Waterloo, Department of Electrical and Computer Engineering, Waterloo; ON, Canada
**Corresponding author:** Peng, Limei(auroraplm@knu.ac.kr)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 447-452
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** This paper explores the utilization of double intelligent reflecting surfaces (IRSs) in wireless communication systems to enhance signal propagation. By dynamically adjusting the reflecting elements of the IRSs, we can efficiently manipulate the signal direction to improve the communication performance such as data rate. Nonetheless, due to the passive nature of the reflecting elements, it is quite challenging to accurately measure the channels directly between the base station (BS), the IRS, and the users based on the conventional channel estimation methods. To address this, we propose to apply a machine learning algorithm that bypasses the traditional channel estimation process and optimizes system parameters by directly extracting information from the received pilot signal. Through extensive simulations, we demonstrate the effectiveness of our proposed method in enhancing the performance of wireless systems incorporating double IRSs. © 2023 IEEE.
**Number of references:** 13
**Main heading:** Graph neural networks
**Controlled terms:** Backpropagation - Channel estimation
**Uncontrolled terms:** Aided communication - Communications systems - Data-rate - Graph neural network - Graph neural networks - Intelligent reflecting surface - Network-based - Reconfig-urable intelligent surface - Reflecting elements - Reflecting surface
**Classification code:** 723.4 Artificial Intelligence
**DOI:** 10.1109/NaNA60121.2023.00080
**Funding Details:** Number: NRF-2022H1D3A2A01063679, Acronym: MSIP, Sponsor: Ministry of Science, ICT and Future Planning; Number: NRF-2020R1I1A3072688, Acronym: NRF, Sponsor: National Research Foundation of Korea;
**Funding text:** This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean Government (Grant No.:NRF-2020R1I1A3072688) and the Brain Pool program funded by the Ministry of Science and ICT through the National Research Foundation of Korea (Grant number: NRF-2022H1D3A2A01063679).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village

## 72. A Detection Method for Alzheimer's Disease Based on Long-Term Visual Features

**Accession number:** 20234715078032
**Authors:** Meng, Huang (1); Shenghui, Zhao (2); Kaichuan, Sun (2); Yuyan, Zhao (2)
**Author affiliation:** (1) School of Computer Science and Engineering, Anhui University of Science and Technology, Huainan, China; (2) School of Computer and Information Engineering, Chuzhou University, Chuzhou, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 580-587
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Alzheimer's disease (AD) is a neurodegenerative disease characterized by cognitive impairment. At present, there is no effective treatment for the disease, which has brought great harm to patients and society. Therefore, it is of great significance to explore the early detection method of Alzheimer's disease. In recent years, with the development of computer vision and deep neural networks, using deep neural networks to detect early Alzheimer's disease has attracted more and more researchers' attention. And gait abnormalities caused by Alzheimer's disease are gradually known. Based on this, this paper proposes a method to detect Alzheimer's disease using long-term visual features, and proves the effectiveness of the method through experiments. And discuss the characteristics of such tasks. It provides a basis for the development of deep neural network detection methods for cognitive disorders such as Alzheimer's disease in the future. © 2023 IEEE.
**Number of references:** 25
**Main heading:** Deep neural networks
**Controlled terms:** Feature extraction - Neurodegenerative diseases - Patient treatment
**Uncontrolled terms:** Alzheimers disease - Cognitive impairment - Detection methods - Gait abnormalities - Long-term visual feature - Network detections - Visual feature
**Classification code:** 461.4 Ergonomics and Human Factors Engineering - 461.6 Medicine and Pharmacology
**DOI:** 10.1109/NaNA60121.2023.00101
**Funding text:** V. Conclusion In this paper, we aim to use long-term visual features f7Qor` 2ea r`lHyv /d2etie2c +tiiBoQnM Qof7 AHlzxh?e2iBmKe2r`'s#b /diBsbe2a sbe2 asb anM aiBd/ itoQ Kme2d/iBc+a lH /diBa g;nMoQsbiBsb. XqW2e musbe2 ith?e2 vpiBd/e2oQ Qof7 ith?e2 sbumb#Dj2ec+ti rw aHlkFiBnMg; in the daily environment, and extract 17 key points of the subject's palm, arm, shoulder, ankle, knee, crotch, torso, head and other human body key points through HRnet. hTh?e2nM,- ith?e2 ?hmumKa nM Fk2eyv TpoQiBnMit /da tia Qof7 /diBfzfe2rè2nMit itiBmKe2 Tp2er`iBoQd/sb ar`e2 +coQmK#biBnMe2d/ asb ith?e2 itr`a iBnMiBnMg; /da tia Qof7 ith?e2 Mne2umrà lH Mne2tirwQo`rFk.X 1ExtpT2er`iBmKe2nMitsb bsh?oQrw ith?a ti HlQonMg;-@tie2r`mK pviBsbuma lH 7f2ea tiumrè2sb +ca nM enhance the detection effect of neural network. According to the experimental results, it is inferred that the temporal processing network plays a more important role in this ita sbkF.X VI. Acknowledge This work was supported by Research on the de-ite2c+tiiBoQnM Qof7 AlHzxh?e2iBmKe2r`'s#b /diBsbe2a sbe2 #ba sbe2d/ QonM pviBsbuma lH 7f2ea tiumrè2sb k2y02k2kXsJCZwD.1R0y-K@Ee2yv SPr`oQg;rà mK Qof7 *Ch?muzxh?oQum UlnMiBvp2er`sbiBtivy-, AInM@ ite2lHlHiBg;e2nMti Tp2enMsbiBoQnM anMd/ ?h2ea lHtih? SPr`oQjDe2c+ti 1Extc+e2lHlHe2nMti bsc +iBe2nMitiBf}ic+ research and innovation team of universities in Anhui Province.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 73. ML-Based Detection Approaches for Covert Communication with Multi-D Signal Features

**Accession number:** 20234715078077
**Authors:** He, Ji (1, 2); Zhang, Xiaodan (3); Ren, Baoquan (2); Li, Hongjun (2); Hu, Tianzhu (2, 4); Gong, Xiangwu (2); Zhong, Xudong (2)

**Author affiliation:** (1) School of Computer Science and Technology, Xidian University, Xi'an; 710071, China; (2) Institute of Systems General, Academy of Systems Engineering, Academy of Military Sciences, Beijing; 100101, China; (3) Guangzhou Institute of Technology, Xidian University, Guangzhou; 510555, China; (4) School of Cyber Engineering, Xidian University, Xi'an; 710071, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 465-470
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** This work explores the efficacy of multidimensional (Multi-D) signal features in detecting covert communication, specifically considering time-domain features, frequency-time features, frequency offset, and SNR. To this end, we propose two novel machine learning (ML)-based detection schemes utilizing these signal features: a supervised learning approach employing k-nearest neighbors (KNN) and an unsupervised learning approach leveraging density-based spatial clustering of applications with noise (DBSCAN). To assess the performance of these schemes, we construct a covert communication testbed that enables the extraction of signal features in diverse electro-magnetic environments. Our experimental results show that both the KNN-based and DBSCAN-based schemes outperform traditional energy-based detection methods, and that our proposed schemes are more effective in identifying covert communication in complex electromagnetic environments. © 2023 IEEE.
**Number of references:** 7
**Main heading:** Signal to noise ratio
**Controlled terms:** Feature extraction - Frequency allocation - Nearest neighbor search - Signal detection
**Uncontrolled terms:** Covert communication detection - Covert communications - DBSAN - Density-based spatial clustering of applications with noise - Detection scheme - Feature frequencies - Machine-learning - Multidimensional signal feature - Multidimensional signals - Signal features
**Classification code:** 716.1 Information Theory and Signal Processing - 716.3 Radio Systems and Equipment - 716.4 Television Systems and Equipment - 921.5 Optimization Techniques
**DOI:** 10.1109/NaNA60121.2023.00083
**Funding Details:** Number: 92267204, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: 2022YFB2902202, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China; Number: 2021A1515111017,62202355, Acronym: -, Sponsor: Basic and Applied Basic Research Foundation of Guangdong Province;
**Funding text:** This work is partially supported by the in part by the National Key Research and Development Program of China under Grant 2022YFB2902202, the Major Research plan of the National Natural Science Foundation of China (Grant No. 92267204), the Basic and Applied Basic Research Fund of Guangdong Province (Grant No.2021A1515111017), the National Natural Science Foundation of China under Grant 62202355.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 74. PHY-Layer Authentication with Hardware Impairments in UAV-Aided Communication Systems

**Accession number:** 20234715078112
**Authors:** Teng, Yulin (1); Zhang, Pinchang (1); Liu, Yangyang (2); Liu, Xin (3)
**Author affiliation:** (1) School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, China; (2) School of Computer Science and Technology, Xidian University, Xi'an, China; (3) School of Electrical Engineering, Dalian Maritime University, Dalian, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA

**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 18-22
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** This paper studies a two-dimensional physical layer (PHY-layer) authentication scheme based on carrier frequency offset (CFO) and phase noise (PHN) to counteract the identity spoofing attack launched by illegitimate unmanned aerial vehicles (UAVs) in UAV-aided communication systems. Particularly, we first adopt the expectation conditional maximization (ECM) and extended Kalman filtering (EKF) methods to extract fingerprints from the received signals. Then, we formulate the problem of PHY-layer authentication as a binary hypothesis testing. Moreover, we theoretically derive the analytical expressions for the false alarm and detection probabilities based on the statistical analysis. Finally, extensive numerical simulations demonstrate the effectiveness of the proposed scheme and validate the correctness of the developed theoretical models. © 2023 IEEE.
**Number of references:** 16
**Main heading:** Authentication
**Controlled terms:** Antennas - Extended Kalman filters - Frequency allocation - Network layers - Unmanned aerial vehicles (UAV) - Vehicle to vehicle communications
**Uncontrolled terms:** Aerial vehicle - Aerial vehicle communication systems - Aided communication - Authentication scheme - Communications systems - Hardware fingerprint - Physical layer authentication - Physical layers - Two-dimensional - Unmanned aerial vehicle communication system
**Classification code:** 652.1 Aircraft, General - 716.3 Radio Systems and Equipment - 716.4 Television Systems and Equipment - 723 Computer Software, Data Handling and Applications
**DOI:** 10.1109/NaNA60121.2023.00011
**Funding Details:** Number: NY221122, Acronym: -, Sponsor: -; Number: 62272241, Acronym: NSFC, Sponsor: National Natural Science Foundation of China;
**Funding text:** This work was supported by the National Natural Science Foundation of China (62272241) and the Nanjing University of Posts and TelecommunicationsScientific Research Foundation Grant (NY221122).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 75. A Light-Weighted Machine Learning Based ECU Identification for Automotive CAN Security

**Accession number:** 20234715078026
**Authors:** Li, Jini (1); Zhang, Man (1); Lai, Yu (1)
**Author affiliation:** (1) School of Electronics and Communication Engineering, Guangzhou University, Guangzhou, China
**Corresponding author:** Zhang, Man(manzhang401@gzhu.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 545-550
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023

**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** The rise of artificial intelligence brings information security challenges for intelligent connected vehicles. Securing the CAN is crucial to ensuring the overall security of the in-vehicle network. Traditional cryptography technology faces challenges of low computational efficiency and excessive data load when identifying ECU. This paper proposes a light-weighted machine learning based identification algorithm that leverages the physical characteristics of ECU. By analyzing the CAN voltage signals in the time and frequency domains, reducing the data load and choosing a suitable classification model, this method achieves high accuracy, high efficiency and low load for safety identification in-vehicle networks. The experimental results on the data sets of both actual vehicles and CAN bus prototypes have verified the rationality and feasibility of the method. © 2023 IEEE.
**Number of references:** 25
**Main heading:** Machine learning
**Controlled terms:** Classification (of information) - Computational efficiency - Security of data - Vehicles
**Uncontrolled terms:** Automotives - CAN - Data load - ECU identification - In-vehicle networks - Learning based identification - Light-weighted - Machine-learning - Physical characteristics - Security challenges
**Classification code:** 716.1 Information Theory and Signal Processing - 723.2 Data Processing and Image Processing - 723.4 Artificial Intelligence - 903.1 Information Sources and Analysis
**DOI:** 10.1109/NaNA60121.2023.00096
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 76. Research on NAS-Oriented Blockchain Aggregation Consensus Algorithm

**Accession number:** 20234715078074
**Authors:** Tang, Lin (1); Zhang, Yubao (1); Che, Lixuan (2); Liu, Chaozhang (1); Xing, Hongwei (3); Zhang, Jianhui (3); Li, Entang (3); Xu, ChongHao (3)
**Author affiliation:** (1) State Grid Dezhou Power Supply Company, Shandong, Dezhou, China; (2) Weifang Vocational College, Shandong, Weifang, China; (3) Shandong Luruan Digital Technology Company, Shandon, Ji'nan, China
**Corresponding author:** Tang, Lin(1070572915@qq.com)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 667-673
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Blockchain technology can be used to solve the problems of single point of failure and lack of trust in network-affiliated storage systems due to the centralized characteristics, but the existing schemes suffer from poor consensus performance and low storage efficiency, etc. To this end, a blockchain aggregation consensus algorithm for NAS is designed. The algorithm ensures fairness by introducing a storage volume probability mechanism, so that the probability of a node obtaining the bookkeeping right is proportional to the size of the storage volume it has, and guarantees uniqueness by designing a position mapping mechanism to ensure that one and only one node obtains the bookkeeping right at each block out round. The bookkeeping node combines the responsibilities of a management node, while using the storage proof mechanism to ensure data security. The experiments show that the system has significantly improved in scalability, openness and security compared with the scheme using traditional consensus algorithm. © 2023 IEEE.
**Number of references:** 30
**Main heading:** Blockchain
**Controlled terms:** Digital storage - Information management - Mapping - Storage efficiency - Storage management

**Uncontrolled terms:** Block-chain - Component - Consensual algorithm - Consensus algorithms - Distributed storage - In networks - Location mapping - NAS - Single point - Storage volumes
**Classification code:** 405.3 Surveying - 525.7 Energy Storage - 722.1 Data Storage, Equipment and Techniques - 723.3 Database Systems
**DOI:** 10.1109/NaNA60121.2023.00115
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 77. A Game Theory-Based Strategy for Allocating and Offloading Computing Resources in 5G Networks

**Accession number:** 20234715078095
**Authors:** Yuan, Yuan (1); Su, Wei (1)
**Author affiliation:** (1) School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 92-97
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** With the emergence of new services in fifth generation (5G) networks, computation offloading based on mobile edge computing (MEC) has emerged as a promising research paradigm in resource-constrained networks. An unreasonable offload strategy can result in high energy consumption and uncertain latency during the offload of such latency-sensitive, computationally intensive computing tasks. In this paper, we decouple the original computational offloading problem into a resource planning problem and an offloading strategy problem. Considering the edge server load state change and user mobility, we design the computational offloading scheme using a game theory approach based on the task offloading ratio and resource allocation ratio. The simulation results show that the proposed scheme has higher system utility compared with the traditional scheme. © 2023 IEEE.
**Number of references:** 5
**Main heading:** 5G mobile communication systems
**Controlled terms:** Computation offloading - Computation theory - Computer games - Energy utilization - Game theory - Mobile edge computing - Queueing networks - Resource allocation
**Uncontrolled terms:** Computation offloading - Computing offloading - Computing resource - Edge server - Game - High energy consumption - Network computations - New services - Resource-constrained network - Resources allocation
**Classification code:** 525.3 Energy Utilization - 716.3 Radio Systems and Equipment - 721.1 Computer Theory, Includes Formal Logic, Automata Theory, Switching Theory, Programming Theory - 722.4 Digital Computers and Systems - 723 Computer Software, Data Handling and Applications - 723.5 Computer Applications - 912.2 Management - 922.1 Probability Theory
**DOI:** 10.1109/NaNA60121.2023.00023
**Funding Details:** Number: 2022YFB2901603, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China;
**Funding text:** ACKNOWLEDGMENT This paper is supported by the National Key Research and Development Project of China (No.2022YFB2901603).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village

## 78. Failure-Aware Service Request Protection in LEO Satellite Constellation Networks

**Accession number:** 20234715078052
**Authors:** Guo, Xin (1); Wang, Jiandong (1); Zhang, Zhiwei (1); Ma, Lisheng (2)
**Author affiliation:** (1) Xidian University, Xi'an; 710071, China; (2) Chuzhou University, Chuzhou; 239000, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 221-225
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** As an important infrastructure for future commu-nication networks, low earth orbit (LEO) satellite constellation networks are facing the risk of satellite failure due to equipment faults. How to protect the service requests affected by failed satellite becomes a critical issue. This paper investigates service request protection in LEO satellite constellation networks under the scenario of satellite node failure. A service request protection scheme against satellite node failure is proposed based on integer linear programming (ILP) by fully using the available resources in the LEO satellite constellation networks. We also provide numerical results to illustrate the proposed scheme. © 2023 IEEE.
**Number of references:** 14
**Main heading:** Satellites
**Controlled terms:** Integer programming - Orbits - Quality of service - Satellite communication systems
**Uncontrolled terms:** Constellation networks - Critical issues - Low earth orbit satellites - Node failure - Satellite constellation network - Satellite constellations - Satellite failures - Satellite node failure - Service request protection - Service requests
**Classification code:** 655.2 Satellites - 655.2.1 Communication Satellites - 921.5 Optimization Techniques
**DOI:** 10.1109/NaNA60121.2023.00044
**Funding Details:** Number: gxbjZD2021080, Acronym: -, Sponsor: -; Number: 2022XJZD11, Acronym: -, Sponsor: -;
**Funding text:** This work was supported by the Academic Funding Project for Top Talents of Disciplines (Majors) in Universities of Anhui Province of China (No. gxbjZD2021080) and the Key Scientific Research Project of Chuzhou University of China (No.2022XJZD11).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 79. Research on Secure Data Circulation and Sharing Protection Technology Framework for Power Monitoring System

**Accession number:** 20234715078091
**Authors:** Huang, Weicong (1); Zhou, Jieying (2); Jin, Minghui (3); Han, Zheng (3); Wei, Sijia (1)
**Author affiliation:** (1) State Grid Smart Grid Research Institute Co., LTD., State Grid Laboratory of Power Cyber-Security Protection and Monitoring Technology, Nanjing, China; (2) National Power Dispatching and Control Center, State Grid Corporation of China, Beijing, China; (3) State Grid Shanghai Municipal Electric Power Company, Shanghai, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 231-238
**Language:** English
**ISBN-13:** 9798350327380

**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** With the increasing frequency of data circulation and sharing in power monitoring systems, traditional network-centric protection strategies are insufficient to resist the growing risk of data leakage. This article analyzes the security risks in existing typical data circulation and sharing scenarios based on the demand for data security sharing in power monitoring systems. A data security protection technology framework covering the source layer, interaction layer, and terminal layer has been proposed from the perspectives of basic protection capabilities and key protection technologies, as well as an evaluation method for the protection technology capabilities of data circulation and sharing. This provides a reference idea for effectively enhancing the data circulation and sharing protection capabilities of power monitoring systems. © 2023 IEEE.
**Number of references:** 27
**Main heading:** Risk perception
**Controlled terms:** Electric power system protection - Petroleum reservoir evaluation
**Uncontrolled terms:** Capability assessment - Data circulation and sharing - Data leakage - Network-centric - Protection capabilities - Protection capability assessment - Protection strategy - Protection technologies - Protection technology framework - Secure data
**Classification code:** 512.1.2 Petroleum Deposits : Development Operations - 706.1 Electric Power Systems - 914.1 Accidents and Accident Prevention
**DOI:** 10.1109/NaNA60121.2023.00046
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 80. A Review of Authentication Methods in Internet of Drones

**Accession number:** 20234715078085
**Authors:** Huang, Yuyang (1, 2); Mu, Jian (1, 2); Wang, Yuzhen (1, 2); Zhao, Renmin (1, 2)
**Author affiliation:** (1) School of Cyber Science and Engineering, Southeast University, Nanjing, China; (2) Engineering Research Center of Blockchain Application, Supervision, and Management, Ministry of Education, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 7-12
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Unmanned aerial vehicles (UAV), also known as drones, are wireless communication devices that have flexibility, mobility, and efficiency as their core attributes. These features enable UAV to play vital roles in various application scenarios, such as traffic prediction, emergency rescue, military reconnaissance, etc. Therefore, UAV have attracted considerable attention in the rapidly developing wireless communication technology. Internet of Drones(IoD) is an internet formed by a large number of UAV. To ensure the security and legitimacy of IoD, authentication of UAV nodes is required. However, the dynamic change of IoD topology and the frequent authentication may cause instability of inter-node communication. Therefore, designing efficient and lightweight authentication solutions has significant meaning. In this paper, we review the latest research on UAV authentication mechanisms. We also discuss the application of traditional techniques and the development of emerging technologies. Finally, we provide a further outlook on the development direction of the authentication research in IoD. © 2023 IEEE.
**Number of references:** 33
**Main heading:** Drones

**Controlled terms:** Antennas - Authentication - Traffic control
**Uncontrolled terms:** Aerial vehicle - Application scenario - Authentication methods - Emergency rescue - Identity authentication - Security - Traffic prediction - Trust strategy - Unmanned aerial vehicle - Wireless communication devices
**Classification code:** 652.1 Aircraft, General - 723 Computer Software, Data Handling and Applications
**DOI:** 10.1109/NaNA60121.2023.00009
**Funding Details:** Number: 2242023K30034,BK20202001, Acronym: -, Sponsor: -; Number: 2020YFB1005500, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China; Number: 2242022R10107, Acronym: -, Sponsor: Fundamental Research Funds for the Central Universities;
**Funding text:** ACKNOWLEDGMENT This research work was supported by the National Key Research and Development Project of China (Grant No. 2020YFB1005500), the Major Research Project of Jiangsu Province:'Leading the Charge with Open Competition'(Grant No.SBA2022050016), the Fundamental Research Funds for the Central Universities (No.2242022R10107), the Leading-edge Technology Program of Jiangsu Natural Science Foundation (Grant No. BK20202001), and the Fundamental Research Funds for the Central Universities (Grant No.2242023K30034).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 81. Covert Communication-Assisted Computation Offloading Schemes in Blockchain-Enabled IoT*

**Accession number:** 20234715078102
**Authors:** Wang, Yutong (1); Jiang, Yu'e (1); Feng, Yu (1)
**Author affiliation:** (1) University Key Laboratory of Intelligent Perception and Computing of Anhui Province, School of Computer and Information, Anqing Normal University, Anqing, China
**Corresponding author:** Jiang, Yu'e(jiang2012118@163.com)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 318-323
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Blockchain-enabled Internet of Things (IoT) can ensure security and trust in distributed environments through consensus mechanisms, becoming important application scenarios for secure computation offloading of smart devices. In the IoT, smart devices usually upload complex computing tasks to the base station (BS), and then obtain corresponding mobile edge computing (MEC) servers to perform computing tasks. However, considering the broadcast characteristics of wireless links and the limited resources of smart devices, task upload links with weak security protection are easy to be monitored by adversaries. Since traditional information encryption technology and physical layer security (PLS) technology focus on protecting information content, the existence of upload links is difficult to be protected, which may attract potential adversaries to launch serious attacks after discovering links. Due to the fact that physical layer covert communications aim to complete information transmission without being discovered by adversaries, we propose covert communication-assisted computation offloading schemes in blockchain-enabled IoT for smart devices. The energy consumption of the computation offload schemes is optimized while ensuring the covertness of the task upload link, the matching satisfaction of sensors and MEC servers. Numerical results show that the proposed schemes can obtain the maximum effective covert rate while reducing the energy consumption of computation offloading. © 2023 IEEE.
**Number of references:** 15
**Main heading:** Internet of things

**Controlled terms:** Blockchain - Computation offloading - Cryptography - Energy utilization - Mobile edge computing
**Uncontrolled terms:** Application scenario - Block-chain - Computation offloading - Computing-task - Covert communications - Distributed environments - Energy-consumption - Secure computation - Security and trusts - Smart devices
**Classification code:** 525.3 Energy Utilization - 722.3 Data Communication, Equipment and Techniques - 722.4 Digital Computers and Systems - 723 Computer Software, Data Handling and Applications - 723.3 Database Systems
**DOI:** 10.1109/NaNA60121.2023.00060
**Funding Details:** Number: 2022AH051054,KJ2020A0497, Acronym: -, Sponsor: -;
**Funding text:** This work was supported in part by the Key Project on Anhui Provincial Natural Science Study by Colleges and Universities (No. KJ2020A0497, No. 2022AH051054).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 82. On the Topology Scaling of Interplanetary Networks

**Accession number:** 20234715078022
**Authors:** Tian, Xiaojian (1); Zhu, Zuqing (1)
**Author affiliation:** (1) School of Information Science and Technology, University of Science and Technology of China, Hefei, China
**Corresponding author:** Zhu, Zuqing(zqzhu@ieee.org)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 274-280
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** The increase of deep space (DS) exploration missions suggests that it would be difficult for the existing interplanetary networks (IPNs) to cope with the growing interplanetary data transfer (IP-DT) demands without topology scaling. Therefore, this paper studies how to expand an IPN by deploying new relay satellites and optimizing their orbit parameters in account of the routing and scheduling of IP-DTs, such that the improvement on the IPN's overall performance can be maximized. We formulate an optimization model to tackle the IPN topology scaling problem and propose an effective heuristic for time-efficient problem-solving. Simulations verify the performance of our proposal. © 2023 IEEE.
**Number of references:** 24
**Main heading:** Topology
**Controlled terms:** Data transfer - Internet protocols - Interplanetary flight - Optimization
**Uncontrolled terms:** Deep-space exploration - Interplanetary networks - Optimization models - Orbit parameters - Performance - Relay satellites - Routing and scheduling - Scalings - Space exploration mission - Transfer demands
**Classification code:** 656.1 Space Flight - 722.3 Data Communication, Equipment and Techniques - 723 Computer Software, Data Handling and Applications - 921.4 Combinatorial Mathematics, Includes Graph Theory, Set Theory - 921.5 Optimization Techniques
**DOI:** 10.1109/NaNA60121.2023.00053
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village

## 83. New Traceable and Revocable Attribute Based Encryption on Lattices

**Accession number:** 20234715078058
**Authors:** Guo, Lifeng (1); Wang, Lingxia (1); Ma, Xueke (1); Zhang, Xialei (1)
**Author affiliation:** (1) School of Computer and Information Technology, Shanxi University, Taiyuan, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 359-364
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** This scheme proposes a new traceable and revocable attribute-based encryption scheme on the lattice (LTR-ABE). First, the attribute-based encryption scheme is more suitable for today's distributed networks and can provide flexible access control. The access control policy used in this paper is the access tree structure, which is applied to the ciphertext policy attribute-based encryption. Second, when a user leaves the system or the key is compromised, the user needs to be revoked from the system. Therefore, the user is tracked to determine whether it is a malicious user and then revoked. More importantly, our proposed revocation mechanism does not need to update the key to achieve revocation. The algorithm is run by an honest and trusted data service manager (DSM) in a cloud server. With the development of quantum computers, the traditional cryptographic mechanism based on bilinear pairs cannot resist quantum attacks. Therefore, our cryptographic scheme is proposed based on lattice theory, specifically the Learning with Error (LWE) problem in lattice, which is resistant to quantum computer attacks. Thus, a new revocation mechanism is implemented in the study of postquantum cryptography. © 2023 IEEE.
**Number of references:** 20
**Main heading:** Lattice theory
**Controlled terms:** Access control - Cryptography - Quantum computers - Trees (mathematics)
**Uncontrolled terms:** Access tree - Attribute-based encryption schemes - Attribute-based encryptions - Distributed networks - Lattice - Learning with Errors - Quanta computers - Revocation mechanism - Traceable - User revocation
**Classification code:** 722 Computer Systems and Equipment - 723 Computer Software, Data Handling and Applications - 921.4 Combinatorial Mathematics, Includes Graph Theory, Set Theory - 922.2 Mathematical Statistics
**DOI:** 10.1109/NaNA60121.2023.00066
**Funding Details:** Number: 62002210, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: 202203021221012, Acronym: -, Sponsor: Natural Science Foundation of Shanxi Province;
**Funding text:** Lifeng Guo was supported by the National Science Foundation of Shanxi Province (202203021221012). The work is supported in part by the National Science Foundation of China (NSFC) under grants: 62002210.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 84. A Multivariate Time Series Anomaly Detection Model Based on Spatio-Temporal Dual Features

**Accession number:** 20234715078090
**Authors:** Wang, Fangwei (1); Yan, Man (1); Li, Qingru (1); Wang, Changguang (1)
**Author affiliation:** (1) College of Computers, Hebei Normal University, Shijiazhuang, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023

**Pages:** 416-421
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** This paper proposes a novel unsupervised model for multivariate time series anomaly detection (TSAD), targeting the challenges of sparse and unlabeled abnormal data, as well as high dimensionality in IoT applications. The core of our model is to extract spatiotemporal dual features through a coherent architecture that captures both temporal dependencies and spatial correlations among multiple variables. Specifically, a deep autoencoder is employed to capture the spatial features of multivariate time series data, while a multi-scale sparse Transformer network is used to extract the temporal features. An anomaly detection module based on the dynamic threshold POT method is used for detect anomalies, and extensive experiments are conducted on publicly available datasets. The result on the SMAP dataset show that our proposed model improves the precision and F1 score by 11.3% and 5.48% respectively compared with the latest baseline method. On the NAB dataset, the F1 score is increased by 0.47%. On the SWaT dataset, the precision is improved by 0.62%. © 2023 IEEE.
**Number of references:** 31
**Main heading:** Anomaly detection
**Controlled terms:** Learning systems - Time series
**Uncontrolled terms:** Anomaly detection - Anomaly detection models - Auto encoders - Deep convolutional autoencoder - F1 scores - Model-based OPC - Multivariate time series - Spatio-temporal - Times series - Transformer
**Classification code:** 922.2 Mathematical Statistics
**DOI:** 10.1109/NaNA60121.2023.00075
**Funding Details:** Number: F2021205004,ZD2021062, Acronym: NSFC, Sponsor: National Natural Science Foundation of China;
**Funding text:** T2his rsa rc$h was fu n d#d #by NSFC u n d#r GDrant 6>1'5,7*2;1'7*0), Natural Sci?nc? Foundation of H?b?i Provinc? und?r Grant F2021205004, Sci?nc? and T?chnology Foundation Proj?ct of H?b?i Normal Univ?rsity und?r Grant L2021K06, Sci?nc? Foundation of R?turn?d Ov?rs?as of H?b?i Provinc? Und?r Grant C2020342, and K?y Sci?nc? Foundation of H?b?i Education Dpa rtmnt und?r Grant ZD2021062.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 85. Scaling Blockchain via a Lightweight Tree-based Sharding System

**Accession number:** 20234715078055
**Authors:** Guan, Zhenyu (1); Zhang, Yang (1); Li, Shizhong (1); Chen, Ruonan (1); Li, Dawei (1)
**Author affiliation:** (1) School of Cyber Science and Technology, Beihang University, Beijing, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 397-403
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** The scalability issue in blockchain seriously restricts the performance of blockchain and limits the practical development of blockchain applications. Existing schemes are mainly divided into blockchain sharding and off-chain payment channels. Blockchain sharding technology splits the blockchain network into multiple sub-networks, each of

which is called a shard. Each shard contains only some nodes, which can independently verify, store, and process transactions in parallel, thus improving the performance and handling capacity of the system. Most of the existing shard technologies start from the complete shard type, dividing each shard in terms of storage and communication, in order to maximize the system handling capacity. However, these approaches also bring with them the processing burden of cross-shard transactions. This paper proposes a sharding system with a tree-based structure, dividing the shard system into i-shards and b-shards according to their respective functions. Combining these two features with the consensus approach in design, we reduce the communication and consensus complexity of cross- shard transaction processing. In addition, we use a lightweight storage design, which reduces the storage pressure on the system. Finally, we analyze the safety of the system during operation and investigate the pressure advantage of utilizing this particular structure. With 6,400 nodes and 32 shards in the system, we come up with a pretty good security guarantee. 
**Number of references:** 25
**Main heading:** Scalability
**Controlled terms:** Binary trees - Blockchain
**Uncontrolled terms:** Block-chain - Handling capacity - Lightweight - Performance - Scalability issue - Scalings - Sharding - Subnetworks - Tree-based - Tree-based structures
**Classification code:** 723.3 Database Systems - 961 Systems Science
**DOI:** 10.1109/NaNA60121.2023.00072
**Funding Details:** Number: JCKY2021211B017, Acronym: -, Sponsor: -; Number: 61932011,61932014,61972018,61972019,62002006,62172025,U21B2021,U2241213, Acronym: NSFC, Sponsor: National Natural Science Foundation of China;
**Funding text:** This work was supported by the Natural Science Foundation of China through projects 62002006, 62172025, U21B2021, 61932011, 61932014, 61972018, 61972019, U2241213, and the Defense Industrial Technology Development Program (JCKY2021211B017).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 86. Defense Against Adversarial Attacks via Adversarial Noise Denoising Networks in Image Recognition

**Accession number:** 20234715078018
**Authors:** Li, Chengxuan (1, 2); Yang, Zhou (1, 2); Xiao, Yang (1, 3); Liu, Haozhao (1, 3); Zhang, Yuning (1, 2); Pei, Qingqi (1, 4)
**Author affiliation:** (1) Xidian University, State Key Laboratory of Integrated Services Networks, Xi'an, China; (2) School of Telecommunications Engineering, Xidian University, Xi'an, China; (3) School of Cyber Engineering, Xidian University, Xi'an, China; (4) Xidian University, Shaanxi Key Laboratory of Blockchain and Secure Computing, Xi'an, China
**Corresponding authors:** Xiao, Yang; Pei, Qingqi
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 520-526
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Deep learning-based image recognition technology has significantly advanced the development of modern industrial intelligence. However, the issue of image adversarial examples that follows has gradually garnered the attention of researchers. By injecting adversarial disturbances that are difficult for humans to detect into the image, the deep learning model generates incorrect results, severely impacting the security of deep learning applications. To address this problem and improve the accuracy and robustness of deep learning image recognition models,

a combined adversarial examples detection method based on residual learning and difference assessment has been proposed. To start, an image denoising module, based on residual learning and named ANDNet, is designed. This method incorporates a depth separable convolution structure and conducts step processing on the channel number of the hidden layer in ANDNet, which significantly reduces the model's memory consumption and improves its computational efficiency. In addition, the difference assessment involves computing the l1 norm distance between the original image and the denoised image softmax output of the classification model, to measure the disparity between the input image before and after denoising. The obtained detection threshold from the training dataset is integrated with this difference evaluation to accomplish the task of testing the input image for adversarial detection. Both theoretical analysis and experimental results confirm the effectiveness of the ANDNet noise reduction network, as well as the efficacy of the adversarial examples detection scheme in identifying adversarial examples. The model exhibits exceptional performance in terms of detection accuracy and F1 value. © 2023 IEEE.
**Number of references:** 33
**Main heading:** Image recognition
**Controlled terms:** Computational efficiency - Deep learning - Image denoising - Image enhancement - Learning systems - Noise abatement - Statistical tests
**Uncontrolled terms:** Adversarial example - Convolution structure - Deep learning - Detection methods - Image recognition technology - Image-recognition model - Input image - Learning models - Module-based - Noise denoising
**Classification code:** 461.4 Ergonomics and Human Factors Engineering - 716.1 Information Theory and Signal Processing - 723.2 Data Processing and Image Processing - 751.4 Acoustic Noise - 922.2 Mathematical Statistics
**DOI:** 10.1109/NaNA60121.2023.00092
**Funding Details:** Number: 2018KCXTD030, Acronym: -, Sponsor: -; Number: 2016LJ06D658, Acronym: -, Sponsor: -; Number: 62102295,62132013,62202358, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: 2022YFB3102700, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China; Number: 2021ZDLGY06-03, Acronym: -, Sponsor: Key Research and Development Projects of Shaanxi Province;
**Funding text:** This work is supported by the National Key Research and Development Program of China under Grant 2022YFB3102700, the National Natural Science Foundation of China under Grant 62132013, 62102295, 62202358, the Key Research and Development Programs of Shaanxi under Grants 2021ZDLGY06-03, the Guangdong Leading Talent Program No. 2016LJ06D658 and the Guangdong Innovation Team Program No. 2018KCXTD030. We also appreciate Al-ibaba Cloud Intelligent Computing LINGJUN to provide the powerful computation ability in the experiments.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 87. A Survey on Cross-Chain Asset Transfer Schemes: Classification, Challenges, and Prospects

**Accession number:** 20234715078106
**Authors:** Lin, Lu (1, 2); Li, Jiayi (1, 2); Wang, Yuzhen (1, 2); Wang, Qiong (1, 2)
**Author affiliation:** (1) School of Cyber Science and Engineering, Southeast University, Nanjing, China; (2) Engineering Research Center of Blockchain Application, Supervision, and Management, Ministry of Education, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 202-208
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.

**Abstract:** Blockchain technology has experienced a rapid growth in recent years, leading to the emergence of various blockchain-based applications. One of the most prominent examples of such applications is the creation of asset in the form of token. However, asset on a chain are difficult to transfer to another chain due to the heterogeneity of different types of blockchains. Cross-chain asset transfer technology enables the transfer of value between blockchains and can improve the scalability of blockchains. This paper provides a systematic overview of cross-chain asset transfer schemes, introducing their classification, main challenges, and representative implementations. Furthermore, this paper summarizes and proposes the future research directions of cross-chain asset transfer schemes. © 2023 IEEE.
**Number of references:** 40
**Main heading:** Blockchain
**Uncontrolled terms:** Asset transfer - Block-chain - Cross-chain transaction - Future research directions - Rapid growth - Transfer scheme - Transfer technologies
**Classification code:** 723.3 Database Systems
**DOI:** 10.1109/NaNA60121.2023.00041
**Funding Details:** Number: 2242023K30034,BK20202001, Acronym: -, Sponsor: -; Number: 2020YFB1005500, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China; Number: 2242022R10107, Acronym: -, Sponsor: Fundamental Research Funds for the Central Universities;
**Funding text:** VI. ACKNOWLEDGE This research work was supported by the National Key Research and Development Project of China (Grant No. 2020YFB1005500), the Major Research Project of Jiangsu Province:'Leading the Charge with Open Competition'(Grant No.SBA2022050016),the Fundamental Research Funds for the Central Universities (No.2242022R10107), the Leading-edge Technology Program of Jiangsu Natural Science Foundation (Grant No. BK20202001), and the Fundamental Research Funds for the Central Universities (Grant No.2242023K30034).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 88. A Real-Time Attack Detection Scheme Based on Multi-Source Information with False Flag Data

**Accession number:** 20234715078068
**Authors:** Li, Han (1); Zhang, Zhiwei (1, 2); Duan, Hao (1); He, Yi (3); Xi, Ning (4)
**Author affiliation:** (1) School of Computer Science and Technology, Xidian University, Shaanxi, Xian; 710071, China; (2) Institute of Network Information, Academy of Systems Engineering, Academy of Military Sciences, Beijing; 100141, China; (3) Tencent Technology Co., Ltd., Chengdu; 610095, China; (4) School of Cyber Engineering, Xidian University, Shaanxi, Xi'an; 710071, China
**Corresponding author:** Zhang, Zhiwei(zwzhang@xidian.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 46-51
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** In recent years, the issue of cyber security has received unprecedented widespread attention and in-depth research. Network false flag attacks have characteristics of stealthiness and persistence, which leads to the static feature matching-based methods misjudging the attack category. At present, the dynamic behavior detection methods based on audit logs have the disadvantages of low reliability, poor real-time performance and low efficiency. Therefore, in this paper, we propose a multidimensional information-based network false flag attacks detection method, which generates state subgraphs by extracting and processing real-time operation information and audit logs of the system. Then, by comparing the clustering results of the current system operation with the historical state, we determine whether the behavior is malicious or not. For malicious behaviors, we cluster the behaviors with the same purpose into

groups, and the security analysts label the attack type of each group. The subsequent behaviors can be automatically labeled with attack type according to their clustering results and therefore realize semi-supervised classification. We demonstrate the effectiveness of our method in an attack scenario, our approach achieves an accuracy of 94.55% for false flag attacks detection and an accuracy of 89.62% for semi-supervised classification. © 2023 IEEE.
**Number of references:** 17
**Main heading:** Clustering algorithms
**Controlled terms:** Classification (of information) - Cybersecurity - Supervised learning
**Uncontrolled terms:** Attack detection - Audit logs - Clustering results - Data provenance graphs - Detection methods - Detection scheme - False flag attack - Multi-source informations - Real- time - Semisupervised classification (SSC)
**Classification code:** 716.1 Information Theory and Signal Processing - 723.2 Data Processing and Image Processing - 903.1 Information Sources and Analysis
**DOI:** 10.1109/NaNA60121.2023.00016
**Funding Details:** Number: 92267204, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: 2021MD703967, Acronym: -, Sponsor: China Postdoctoral Science Foundation; Number: ZR2021LZH006, Acronym: -, Sponsor: Natural Science Foundation of Shandong Province; Number: 2021ZDLGY03-10, Acronym: -, Sponsor: Key Research and Development Projects of Shaanxi Province;
**Funding text:** VI. ACKNOWLEDGE This work was supported by the Major Research plan of the National Natural Science Foundation of China (Grant No. 92267204), the Chinese Postdoctoral Science Foundation (2021MD703967), the Key R&D Program of Shaanxi Province (2021ZDLGY03-10), Shandong Provincial Natural Science Foundation (ZR2021LZH006).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 89. Research on Lightweight Human Pose Estimation Model Based on Knowledge Distillation

**Accession number:** 20234715078078
**Authors:** Cao, Guoyi ; Mo, Wanghao ; Wu, Zhaozhen
**Corresponding author:** Cao, Guoyi(cgy1599@163.com)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 156-162
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Most of the existing state-of-the-art human pose estimation methods mainly pursue improving the precision of human pose estimation, ignoring the model's complexity and making it impossible to deploy it on resource-constrained devices. In addition, some other methods overly pursue the model's lightweight, which significantly decreases the model's precision and affects the experience of practical applications. However, in reality, fast and accurate applications are often more popular, so this area of research is of some practical significance. To achieve lightweight deployment and better practical application, A lightweight human pose estimation model based on knowledge distillation is proposed, which firstly uses group convolution and channel shuffle operation to lighten the HRNet model to obtain the S-HRNet model. Secondly, a response-based knowledge distillation algorithm is proposed to use the pre-trained HRNet as the teacher model and S-HRNet as the student model with the help of an offline knowledge distillation strategy, and the prediction results of the teacher model are used to supervise the learning of the student model together with the real labels. Finally, this paper conducts a large number of experiments on the MS COCO dataset proposed by Microsoft, and the experimental results show that the model in this paper has a higher

average precision and lower number of parameters and computations compared to the other models mentioned. © 2023 IEEE.
**Number of references:** 24
**Main heading:** Distillation
**Controlled terms:** Large dataset
**Uncontrolled terms:** Estimation methods - Estimation models - Human pose estimations - Knowledge distillation - Lightweight model - Model-based OPC - Model-making - State of the art - Student Modeling - Teacher models
**Classification code:** 723.2 Data Processing and Image Processing - 802.3 Chemical Operations
**DOI:** 10.1109/NaNA60121.2023.00034
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 90. A Survey on Automatic Discover Approach by Using Static Analysis for Smart Contract Vulnerability

**Accession number:** 20234715078015
**Authors:** Deng, Yifan (1, 2); Wang, Liangmin (1, 2); Wang, Liang (1, 2); Li, Jiayi (1, 2); Yong, Quan (1, 2)
**Author affiliation:** (1) School of Cyber Science and Engineering, Southeast University, Nanjing, China; (2) Engineering Research Center of Blockchain Application, Supervision, and Management, Ministry of Education, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 163-168
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Smart contract runs on blockchain platforms and plays a critical role in decentralized applications. Unfortunately, since smart contracts manage valuable digital assets, attacks against them can result in substantial economic losses. Especially, most of the attack are carried out by exploiting the vulnerabilities in smart contracts. Aiming to perform efficient and comprehensive identification for contract vulnerabilities, there emerges a number of research on smart contract security and vulnerability detection. This paper provides a comprehensive surveys on various smart contract vulnerabilities and corresponding detection methods proposed in recent years. Meanwhile, this paper implements an automatic discover approach by using static analysis for smart contract vulnerability, which can effectively identify and localize vulnerabilities within contracts. Experimental results show this method can precisely locate and classify contract vulnerabilities. © 2023 IEEE.
**Number of references:** 20
**Main heading:** Smart contract
**Controlled terms:** Losses - Static analysis
**Uncontrolled terms:** Block-chain - Decentralised - Detection methods - Digital assets - Economic loss - Security detection - Vulnerability detection
**Classification code:** 723.5 Computer Applications - 902.3 Legal Aspects - 911.2 Industrial Economics
**DOI:** 10.1109/NaNA60121.2023.00035
**Funding Details:** Number: 2242023K30034,BK20202001, Acronym: -, Sponsor: -; Number: 2020YFB1005500, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China; Number: 2242022R10107, Acronym: -, Sponsor: Fundamental Research Funds for the Central Universities;
**Funding text:** This research work was supported by the National Key Research and Development Project of China (Grant No. 2020YFB1005500), the Major Research Project of Jiangsu Province:'Leading the Charge with Open Competition'(Grant No.SBA2022050016), the Fundamental Research Funds for the Central Universities (No.2242022R10107), the Leading-edge Technology Program of Jiangsu Natural Science Foundation (Grant No. BK20202001), and the Fundamental Research Funds for the Central Universities (Grant No.2242023K30034).

**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 91. Product Retrieval Based on Subtractive Angular Margin Loss

**Accession number:** 20234715078066
**Authors:** Wei, Wei (1); Zang, Feng (2); Huang, Liben (3); Bai, Mingxiao (1)
**Author affiliation:** (1) Zztf Nanjing Aviation Research Institute, Jiangsu, China; (2) Nanjing Urban Lighting Construction and Operation Group Co., Ltd., Jiangsu, China; (3) Jiangsu Future Urban Public Space Development and Operation Co., Ltd., Jiangsu, China
**Corresponding author:** Wei, Wei(109799514@qq.com)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 339-343
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** This paper proposes a new loss function called Subtractive Angular Margin Loss (SAML) for product retrieval in the electronic retail industry. Product retrieval aims to find specific goods from a large classification of items at the Stock-Keeping Unit (SKU) level. SAML improves upon ArcFace loss by changing the decision boundary from an additive angle to a subtractive angle, which prevents over-compressing sample features of each class in angular space and better distinguishes complex patterns of different products. The performance of SAML is compared with other conventional loss functions using ResNet as standard backbone network on the Products-10k dataset, which contains almost 10,000 SKU-level products. Experimental results show that SAML outperforms other loss functions and achieves 1.58% improvement on top-1 accuracy compared to ArcFace. © 2023 IEEE.
**Number of references:** 25
**Main heading:** Deep learning
**Controlled terms:** Computer vision
**Uncontrolled terms:** Angular margin - Arcface - Complex pattern - Decision boundary - Deep learning - Loss functions - Product retrieval - Retail industry - Sample features - Stock keeping unit
**Classification code:** 461.4 Ergonomics and Human Factors Engineering - 723.5 Computer Applications - 741.2 Vision
**DOI:** 10.1109/NaNA60121.2023.00063
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 92. A Dimensional Perspective Analysis on the Cybersecurity Risks and Opportunities of ChatGPT-Like Information Systems

**Accession number:** 20234715078105
**Authors:** Hu, Chunhui (1); Chen, Jianfeng (2)
**Author affiliation:** (1) Zhongguancun Laboratory, Rongxin Yard, Haidian District, Beijing, China; (2) No.30 Research Institute of Cetc, Sichuan Chuangye Road, Gaoxing District, Chengdu, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023

**Pages:** 324-331
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** As a recent breakthrough in generative artificial intelligence, ChatGPT is capable of creating new data, images, audio, or text content based on user context. In the field of cybersecurity, it provides generative automated AI services such as network detection, malware protection, and privacy compliance monitoring. However, it also faces significant security risks during its design, training, and operation phases, including privacy breaches, content abuse, prompt word attacks, model stealing attacks, abnormal structure attacks, data poisoning attacks, model hijacking attacks, and sponge attacks. This paper starts from the risks and events that ChatGPT has recently faced, proposes a framework for analyzing cybersecurity in cyberspace, and envisions adversarial models and systems. It puts forward a new evolutionary relationship between attackers and defenders using ChatGPT to enhance their own capabilities in a changing environment and predicts the future development of ChatGPT from a security perspective. © 2023 IEEE.
**Number of references:** 8
**Main heading:** Cybersecurity
**Controlled terms:** Malware - Risk analysis - Risk assessment
**Uncontrolled terms:** Attack modeling - Audio content - ChatGPT - Cyber security - Cyberspace security - Cyberspaces - Data images - Dimensional analysis - Risk and opportunity - Text content
**Classification code:** 723 Computer Software, Data Handling and Applications - 723.2 Data Processing and Image Processing - 914.1 Accidents and Accident Prevention - 922 Statistical Methods
**DOI:** 10.1109/NaNA60121.2023.00061
**Funding Details:** Number: 2020JDTD0034, Acronym: -, Sponsor: Sichuan Province Science and Technology Support Program; Number: 2019YFB2101701, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China;
**Funding text:** ACKNOWLEDGMENT This work is supported by National Key R&D Program of China with project No. 2019YFB2101701 and is supported by Sichuan Science and Technology Program under project No. 2020JDTD0034.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 93. Research on Privacy Preserving Computing Technology in Edge Computing

**Accession number:** 20234715078075
**Authors:** Wang, Yuyao (1, 2); Chen, Lei (1, 2); Ni, Siyuan (1, 2); Yu, Fei (1, 2); He, Yuanhang (1, 2); Fang, Qiang (3); Zhou, Yuzheng (3)
**Author affiliation:** (1) Science and Technology on Communication Security Laboratory, Chengdu; 610041, China; (2) No.30 Research Institute of China Electronics Technology Group Corporation, Chengdu, China; (3) School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu; 611731, China
**Corresponding author:** Yu, Fei(feiyu80@foxmail.com)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 98-103
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.

**Abstract:** With the rapid development of mobile Internet and Internet of Things applications, the traditional cloud computing model can provide centralized remote services, but when the amount of data increases sharply, it has been unable to effectively process the data generated by edge devices. To address these challenges and efficiently utilize distributed computing resources, edge computing emerges. With the rise of edge computing, more and more attention has been paid to its security threats and countermeasures. This paper first introduces the basic definition, architectural features, and current security threats of edge computing, then discusses the privacy protection issues in edge computing, and systematically expounds the latest research results at home and abroad. The application of privacy-preserving computing technology in computing, discusses the development trend of edge computing, and proposes further research directions. © 2023 IEEE.
**Number of references:** 16
**Main heading:** Edge computing
**Controlled terms:** Privacy-preserving techniques - Security systems
**Uncontrolled terms:** Computing technology - Differential privacies - Edge computing - Federated learning - Homomorphic encryptions - Homomorphic-encryptions - Privacy preserving - Privacy protection - Secure multi-party computing - Security threats
**Classification code:** 716 Telecommunication; Radar, Radio and Television - 718 Telephone Systems and Related Technologies; Line Communications - 722.4 Digital Computers and Systems - 723.2 Data Processing and Image Processing - 914.1 Accidents and Accident Prevention
**DOI:** 10.1109/NaNA60121.2023.00024
**Funding Details:** Number: 2023YFQ0028, Acronym: -, Sponsor: -; Number: 6142103022205, Acronym: -, Sponsor: -; Number: -, Acronym: NSFC, Sponsor: National Natural Science Foundation of China;
**Funding text:** This paper was supported by Science and Technology on Communication Security Laboratory Foundation (No. 6142103022205), National Natural Science Foundation of China (No.U21B2019) and Regional Innovation Cooperation Project of Sichuan Province (No. 2023YFQ0028).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 94. DLPriv: Deep Learning Based Dynamic Location Privacy Mechanism for LBS in Internet-of-Vehicles

**Accession number:** 20234715078082
**Authors:** Wang, Ziwen (1); Ma, Baihe (2); Liu, Zhihong (1); Zeng, Yong (1); Wang, Zhe (1); Shi, Kaichao (1)
**Author affiliation:** (1) School of Cyber Engineering, Xidian University, Xi'an, China; (2) University of Technology Sydney, Global Big Data Technologies Centre, Sydney, Australia
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 514-519
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** In the Internet of Vehicles (IoV), location-based service providers rely on collecting and analyzing user-generated trajectory data to deliver high-quality experiences anytime and anywhere. However, the utilization of data mining technologies raises concerns regarding the potential inference of personal privacy information, posing security risks to user privacy. Existing studies typically use differential privacy to obfuscate actual trajectories, albeit at the cost of reduced data utility. To address this challenge and strike a balance between privacy and data utility, we propose DLPriv, a dynamic location privacy mechanism. DLPriv leverages a Long Short-Term Memory (LSTM) network to predict a driver's next location, which in turn determines the level of data obfuscation. This mechanism considers two optimization objectives, trajectory privacy and utility, and enables fine-grained control over privacy levels. Experimental

results demonstrate that our proposed mechanism improves data utility by 37% compared to existing work, while providing the same level of privacy. © 2023 IEEE.
**Number of references:** 18
**Main heading:** Vehicles
**Controlled terms:** Data mining - Data privacy - Dynamics - Location - Location based services - Long short-term memory - Telecommunication services - Trajectories
**Uncontrolled terms:** Data utilities - Differential privacies - Generated trajectories - Internet-of-vehicle - Location privacy - Location-based services - Privacy mechanisms - Service provider - User-generated - Vehicle location
**Classification code:** 716 Telecommunication; Radar, Radio and Television - 723.2 Data Processing and Image Processing
**DOI:** 10.1109/NaNA60121.2023.00091
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 95. UAV Camera Re-localization Based on Image Retrieval

**Accession number:** 20234715078013
**Authors:** Zang, Feng (1); Huang, Liben (2); Wei, Wei (3); Shen, Weiqi (3)
**Author affiliation:** (1) Nanjing Urban Lighting Construction and Operation Group Co., Ltd., Nanjing, China; (2) Jiangsu Future Urban Public Space, Development and Operation Co., Ltd., Nanjing, China; (3) Zztf Nanjing Aviation Research Institute Co., Ltd., Nanjing, China
**Corresponding author:** Zang, Feng(781854707@qq.com)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 372-377
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Camera relocalization is a challenging problem in computer vision, particularly for unmanned aerial vehicles (UAVs) due to their mobility, limited resources, and harsh conditions. Although several methods exist for camera relocalization, they suffer from limitations such as indoor bias, limited accuracy and range, high computational cost, and single-camera assumption. This highlights the need for more efficient and robust camera relocalization methods for UAVs. To address this challenge, We propose a realtime UAV camera relocation system that utilizes an unsupervised deep learning framework to learn image relationships. Transfer learning from large-scale classified data enables faster training and higher accuracy. The system employs image retrieval and a convolutional neural network to match features from a single RGB image with location information in a database. It achieves strong rotational invariance, enhancing its performance and versatility in various scenarios. The system has demonstrated high accuracy and robustness in large outdoor scenes, with each image taking only 0.6 seconds to compute. © 2023 IEEE.
**Number of references:** 22
**Main heading:** Cameras
**Controlled terms:** Antennas - Convolutional neural networks - Deep learning - Image retrieval - Search engines - Unmanned aerial vehicles (UAV)
**Uncontrolled terms:** Aerial vehicle - Camera relocation - Computational costs - Condition - Feature match - High-accuracy - Re-localization - Real- time - Rotational invariances - Single cameras
**Classification code:** 461.4 Ergonomics and Human Factors Engineering - 652.1 Aircraft, General - 723 Computer Software, Data Handling and Applications - 742.2 Photographic Equipment
**DOI:** 10.1109/NaNA60121.2023.00068
**Compendex references:** YES
**Database:** Compendex

**Data Provider:** Engineering Village


## 96. A Deep Reinforcement Learning Approach for Online Taxi Dispatching

**Accession number:** 20234715078101
**Authors:** Wang, YuBo (1, 2, 3); Zhang, TaoYi (1, 2, 3); Wei, ZhiCheng (1, 2, 3)
**Author affiliation:** (1) Key Lab of Network and Information Security, China; (2) College of Computer and Cyber Security, China; (3) Hebei Prov. Eng. Res. Center for Supply Chain Big Data Analytics Security, Hebei Normal University, Hebei Province, Shijiazhuang, China
**Corresponding author:** Wei, ZhiCheng(weizhicheng@hebtu.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 655-660
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** With the development of smart city transportation systems, developing reasonable dispatching strategies for idle ride-hailing vehicles has become an urgent research problem. In this paper, we address the short-sightedness issue of existing dispatching strategies and design a ride-hailing dispatching model based on deep reinforcement learning in the Markov decision process(MDP) framework to obtain long-term dispatching strategies with foresight. Firstly, we define the basic framework of agent and optimize the dispatching strategy of ride-hailing services by defining a metric that combines instant revenue with the demand situation of the next state in the action space as a reward function. Then, we construct an order-matching system simulator based on historical order data sets to facilitate interaction between the intelligent agent and the environment. Finally, based on the Bellman optimality equation, we approximate the value function using the Eval Net and Target Net, and train the model using Temporal Difference Learning. Simulation experiments demonstrate that this approach can increase driver income, provide more services to passengers, and effectively improve the operating efficiency of the transportation network. © 2023 IEEE.
**Number of references:** 23
**Main heading:** Reinforcement learning
**Controlled terms:** Computer aided instruction - Deep learning - Dynamic programming - E-learning - Learning algorithms - Learning systems - Markov processes - Taxicabs
**Uncontrolled terms:** Component - Deep reinforcement learning - Dispatching models - Model-based OPC - Order assignment - Reinforcement learning approach - Reinforcement learnings - Research problems - Transportation system - Vehicle dispatching
**Classification code:** 461.4 Ergonomics and Human Factors Engineering - 662.1 Automobiles - 723.4 Artificial Intelligence - 723.4.2 Machine Learning - 723.5 Computer Applications - 901.2 Education - 921.5 Optimization Techniques - 922.1 Probability Theory
**DOI:** 10.1109/NaNA60121.2023.00113
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 97. A Survey of Edge Computing Resource Allocation Strategies Based on Federated Learning

**Accession number:** 20234715078072
**Authors:** Ni, Siyuan (1, 2); He, Yuanhang (1, 2); Chen, Lei (1, 2); Wang, Yuyao (1, 2); Yu, Fei (1, 2)
**Author affiliation:** (1) Science and Technology on Communication Security Laboratory, Chengdu; 610041, China; (2) No.30 Research Institute of China Electronics Technology Group Corporation, Chengdu, China
**Corresponding author:** He, Yuanhang(kevin0319@163.com)

**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 116-121
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** In the edge computing environment, the data on edge computing is at risk of leakage due to the variety and wide distribution of nodes. As a new distributed machine learning framework, federated learning can effectively solve the privacy and security problems of users' information data in different fields. However, in federated learning, with the continuous landing of AI applications and the growing demand for model reasoning services, the resources consumed by federated learning will exceed the computing power of edge computing, so it is necessary to study the resource allocation strategy of edge computing for federated learning. This paper first introduces the concepts of federated learning and edge computing, and resource allocation strategies based on edge computing; Then it introduces the challenges faced by federated learning and the operating system framework of edge computing based on federated learning; Secondly, it combs the resource allocation strategy of edge computing based on federated learning; Finally, the paper summarizes the work of the full text and analyzes the future development trend of resource allocation under Federated learning. © 2023 IEEE.
**Number of references:** 28
**Main heading:** Resource allocation
**Controlled terms:** Artificial intelligence - Computing power - Edge computing - Learning systems
**Uncontrolled terms:** Computing environments - Computing resource - Distributed machine learning - Edge computing - Federal learning - Learning frameworks - Privacy and security - Privacy problems - Resource allocation strategies - Resources allocation
**Classification code:** 722.2 Computer Peripheral Equipment - 722.4 Digital Computers and Systems - 723 Computer Software, Data Handling and Applications - 723.4 Artificial Intelligence - 912.2 Management
**DOI:** 10.1109/NaNA60121.2023.00027
**Funding Details:** Number: 2023YFQ0028, Acronym: -, Sponsor: -; Number: 6142103022205, Acronym: -, Sponsor: -; Number: 2022, Acronym: -, Sponsor: -; Number: -, Acronym: NSFC, Sponsor: National Natural Science Foundation of China;
**Funding text:** This work was supported by National Natural Science Foundation of China (No.U21B2019), Regional Innovation Cooperation Project of Sichuan Province (No. 2023YFQ0028), Stability Program of Science and Technology on Communication Security Laboratory (2022) and Science and Technol- ogy on Communication Security Laboratory Foundation (No. 6142103022205).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 98. Enhancing Robustness Against Heterogeneity via Class-Difficulty Based Weights

**Accession number:** 20234715078064
**Authors:** Liu, Teng (1); Shang, Menghan (1); Li, Haoshuo (1); Zhang, Tao (1)
**Author affiliation:** (1) School of Computer Science and Technology, Xidian University, Shaanxi, Xi'an, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 150-155
**Language:** English
**ISBN-13:** 9798350327380

**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Federated learning (FL) is a collaborative learning method on distributed data, which can protect data privacy, reduce server burden, and improve model performance. However, in practical applications, the data of different clients often do not satisfy the independent and identically distributed (IID) assumption, causing the instability, and non-convergence of model training. To solve this problem, some schemes have been proposed, such as personalized federated learning, data augmentation, model update and aggregation improvement, etc. However, these schemes do not fully consider the difficulty difference between client data, which may affect the robustness and generalization ability of the model on different clients. Therefore, in this paper, we propose an effective FL optimization method (CDB-W-FL) for non-IID data via Class-Difficulty Based Weights. We utilize the class-difficulty based weights to measure the difficulty level of each class sample on each client. Then, we apply the class difficulty weight to the model update and aggregation process, so that the model can pay more attention to the more difficult samples and balance the contributions of different clients. We conduct experiments on famous public datasets and show that the proposed CDB-W-FL achieves better performance than existing schemes in terms of accuracy, convergence speed, and robustness under non-IID data. © 2023 IEEE.
**Number of references:** 23
**Main heading:** Data privacy
**Controlled terms:** Image classification - Image enhancement - Learning systems
**Uncontrolled terms:** Collaborative learning - Distributed data - Federated learning - Images classification - Learning methods - Model aggregations - Model updates - Modeling performance - Non-identically distributed - Weighted-loss
**Classification code:** 723.2 Data Processing and Image Processing
**DOI:** 10.1109/NaNA60121.2023.00033
**Funding Details:** Number: 2020YFB1005500, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China; Number: 2021ZDLGY07-05, Acronym: -, Sponsor: Key Research and Development Projects of Shaanxi Province;
**Funding text:** This work was supported in part by the National Key Research and Development Program of China (No. 2020YFB1005500) and the Key Research and Development Program of Shaanxi (No. 2021ZDLGY07-05).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 99. A Pseudonym Exchange-Based Traceable Location Privacy Protection Scheme for IoV

**Accession number:** 20234715078098
**Authors:** Ma, Weigang (1); Yu, Yaping (1); Wang, Yichuan (1, 2); Liu, Xiaoxue (1); Wang, Zhoukai (1)
**Author affiliation:** (1) School of Computer Science and Engineering, Xi'an University of Technology, Xi'an, China; (2) Shaanxi Key Laboratory for Network Computing and Security Technology, China
**Corresponding author:** Yu, Yaping(2211221076@stu.xaut.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 287-292
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Internet of Vehicles (IoV) is a network built by communicating entities such as vehicles and roadside infrastructure, etc. The entities can communicate with each other, sharing data and providing services. However, the

openness and interoperability (location services) of IoV makes the communication entity vulnerable to attacks. when the vehicle requests location services, it will expose its own location information, which will cause serious personal safety problems. To address the location privacy leakage problem in the IoV, this paper proposes a pseudonym exchange-based traceable location privacy protection scheme for IoV. Our scheme not only provides location privacy protection, but has the following properties: First, the whole pseudonym exchange process does not require trusted third-party participation; Second, each vehicle performs a series of hash operations on several dynamic anonyms and obtains a corresponding fixed-length hash value as the corresponding account in order to cut off the connection between the real identity, which is different in each run. If a vehicle is compromised and utilized to launch attack, the trusted center (CA) can also recover his/her real identity; Last, the experimental results show that the pseudonym exchange process and pseudonym update process cost less time compared to relevant literature. Hence, these features make our scheme very suitable for computation-limited mobile devices compared with other related existing schemes. © 2023 IEEE.
**Number of references:** 15
**Main heading:** Vehicles
**Controlled terms:** Interoperability - Location - Location based services
**Uncontrolled terms:** Communication entities - Exchange process - Internet of vehicle - Location privacy - Location privacy protection - Location services - Protection schemes - Pseudonym exchange - Pseudonym traceability - Pseudonym update
**Classification code:** 716 Telecommunication; Radar, Radio and Television
**DOI:** 10.1109/NaNA60121.2023.00055
**Funding Details:** Number: 2021JLM-58, Acronym: -, Sponsor: -; Number: 62072368,U20B2050, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: 2022GY-040, Acronym: -, Sponsor: Shanxi Provincial Key Research and Development Project;
**Funding text:** ACKNOWLEDGMENT This research work is supported by the National Natural Science Founds of China (62072368, U20B2050), Key Research and Development Program of Shaanxi Province (2022GY-040), Basic Research in Natural Science and Enterprise Joint Fund of Shaanxi (2021JLM-58).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 100. Privacy Enhanced Federated Learning via Privacy Masks and Additive Homomorphic Encryption

**Accession number:** 20234715078033
**Authors:** Shen, Cong (1); Zhang, Wei (1)
**Author affiliation:** (1) School of Cryptography Engineering, Engineering University of People's Armed Police, Xi'an, China
**Corresponding author:** Zhang, Wei(zhaangweei@yeah.net)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 471-478
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Federated learning has become an effective method to realize collaborative learning among multiple data centers. However, the problem of privacy leakage has not been perfectly solved. We proposed a scheme based on homomorphic encryption with random privacy masks to cope with the problem of private leakage caused by honest but curious participants. Through combining Paillier encryption scheme with privacy mask, security of the learning process is enhanced with a trivial computation and communication cost. Experimental results show that the decryption time is reduced by more than half after using CRT optimization, without degrading the training precision. © 2023 IEEE.

**Number of references:** 44
**Main heading:** Cryptography
**Controlled terms:** Gradient methods - Learning systems - Stochastic systems
**Uncontrolled terms:** Collaborative learning - Datacenter - Federated learning - Ho-momorphic encryptions - Homomorphic-encryptions - Multiple data - Privacy leakages - Privacy mask - Problem of privacy - Stochastic gradient descent
**Classification code:** 731.1 Control Systems - 921.6 Numerical Methods - 961 Systems Science
**DOI:** 10.1109/NaNA60121.2023.00084
**Funding Details:** Number: 62102452,62172436, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: 2023-JC-YB-584, Acronym: -, Sponsor: Natural Science Foundation of Shaanxi Province;
**Funding text:** ACKNOWLEDGMENT This work was supported by National Natural Science Foundation of China (62102452,62172436), Natural Science Foundation of Shaanxi Province (2023-JC-YB-584).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 101. Distributed Storage Method for Data Security Sharing and Exchange

**Accession number:** 20234715078042
**Authors:** Xiaolong, Chen (1); Yue, Zhao (1); Qi, Zhao (1)
**Author affiliation:** (1) The 30th Research Institute of China Electronics Technology Group Corporation, Key Laboratory of Secure Communication, Chengdu, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 404-409
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** the traditional distributed storage method realizes the decentralized storage of data to a certain extent, but there are still some problems, such as excessive waste of storage space, low security, low storage efficiency and so on. In order to solve these problems, this paper designs a high security storage scheme with adaptive selection of storage nodes, anti-loss and theft, and anti-repudiation, among which, on the one hand, it realizes the efficient storage of data and reduces the space occupation rate. On the other hand, it maintains the security, integrity and availability of the data throughout the life cycle of storage. © 2023 IEEE.
**Number of references:** 15
**Main heading:** Digital storage
**Controlled terms:** Life cycle - Storage efficiency
**Uncontrolled terms:** Decentralised - Distributed storage - Encrypted transmission - Erasure codes - High securities - IPFS - Low-storage - Redundant slicing - Storage efficiency - Storage spaces
**Classification code:** 525.7 Energy Storage - 722.1 Data Storage, Equipment and Techniques
**DOI:** 10.1109/NaNA60121.2023.00073
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 102. A Decentralized Quality Management Scheme for Content Moderation

**Accession number:** 20234715078071
**Authors:** Niu, Yanhua (1, 2); Gao, Shuai (1); Zhang, Hongke (1); Gong, Yuanjia (1, 2)
**Author affiliation:** (1) Beijing Jiaotong University, Beijing, China; (2) Academy of Broadcasting Science, Beijing, China

**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 215-220
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Content moderation is a critical issue for media providers to protect viewers from harmful content and also to build a good reputation with the public. Due to the lack of a trustworthy and effective quality management mechanism for content moderation, the heavy workload of content moderation remains difficult for media providers. In this paper, we propose a decentralized management mechanism for content moderation, in which the permissioned blockchain provides credible, transparent and verifiable infrastructure and the smart contracts ensure the automatic execution of pre-set management rules. The proposed mechanism combines a quality evaluation and monetary incentive method based on authenticity historical data, aiming to achieve long-term sustainable quality improvement. Experimental results show that our mechanism can successfully execute the preset management rules automatically, which can simplify the management complexity and avoid human intervention. © 2023 IEEE.
**Number of references:** 33
**Main heading:** Smart contract
**Controlled terms:** Quality management
**Uncontrolled terms:** Content moderation - Critical issues - Decentralised - Decentralized autonomous organization - Decentralized management - Decentralized quality management - Heavy workloads - Management mechanisms - Management scheme
**Classification code:** 902.3 Legal Aspects - 912.2 Management
**DOI:** 10.1109/NaNA60121.2023.00043
**Funding Details:** Number: JBKY20230230, Acronym: -, Sponsor: -;
**Funding text:** This work was supported by the Fundamental Research Fund for Academy of Broadcasting Science, China under project JBKY20230230.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 103. E-PBFT: An Improved Consensus Mechanism Based on PBFT

**Accession number:** 20234715078115
**Authors:** Ma, WeiGang (1); Wang, YiChuan (1); Hu, DengFang (1); Wang, ZhouKai (1)
**Author affiliation:** (1) School of Computer Science and Engineering, Xi'an University of Technology, Xi'an, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 143-149
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.

**Abstract:** To address the problems of high communication overhead and complexity of the practical Byzantine fault-tolerant (PBFT) consensus algorithm applied to federated chains, an efficient Byzantine fault-tolerant consensus algorithm E-PBFT is proposed based on the improved PBFT algorithm. First, the random matching rules are designed to design the all-nodes broadcast communication between nodes as a single communication of random nodes. Second, the random matching rules are embedded in the Commit phase of the PBFT algorithm. Finally, the progress of lagging nodes is synchronized using an acknowledgement mechanism. Experimental analysis shows that compared with the PBFT algorithm, the E-PBFT algorithm can significantly reduce the transaction latency and increase the throughput of the federated chain by more than 30% while having Byzantine fault tolerance. © 2023 IEEE.
**Number of references:** 16
**Main heading:** Blockchain
**Controlled terms:** Fault tolerance
**Uncontrolled terms:** Block-chain - Byzantine fault - Byzantine fault tolerance - Consensus algorithms - Fault-tolerant - Fault-tolerant algorithms - Matching rules - Mechanism-based - Practical byzantine fault tolerance - Random matching
**Classification code:** 723.3 Database Systems
**DOI:** 10.1109/NaNA60121.2023.00032
**Funding Details:** Number: 2021JLM-58, Acronym: -, Sponsor: -; Number: 62072368,U20B2050, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: 2022GY-040, Acronym: -, Sponsor: Shanxi Provincial Key Research and Development Project;
**Funding text:** VII. ACKONWLEDGMENT This research work is supported by the National Natural Science Founds of China (62072368, U20B2050), Key Research and Development Program of Shaanxi Province (2022GY-040), Basic Research in Natural Science and Enterprise Joint Fund of Shaanxi (2021JLM-58).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 104. Jamming with Zero-Forcing Beamforming for Covert Communication in MIMO Systems

**Accession number:** 20234715078108
**Authors:** Zhu, He (1); Wu, Huihui (2); Jiang, Xiaohong (1)
**Author affiliation:** (1) School of Systems Information Science, Future University Hakodate, Hokkaido, Japan; (2) Tsinghua University, Department of Automation, Beijing, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 122-126
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** This paper focuses on the covert communication in a multi-input multi-output (MIMO) system, where a multiantenna transmitter A conducts covert communication with a multi-antenna receiver B with the help of a multi-antenna jammer J, against the detection of a single-antenna warden W. We first provide theoretical modeling for the detection error probability at W and covert rate from A to B. We then explore the optimal jamming design of J based on zero-forcing (ZF) beamforming and devise an iterative algorithm to determine the related optimal precoding matrix for covert rate maximization. Finally, we provide extensive numerical results to illustrate the impact of system parameters on covert performance. © 2023 IEEE.
**Number of references:** 23
**Main heading:** MIMO systems
**Controlled terms:** Antennas - Beamforming - Iterative methods - Jamming
**Uncontrolled terms:** Covert communications - Jammers - Multi-antenna - Multi-antenna receivers - Multi-antenna transmitters - Multi-input multi-output - Multi-Input Multi-Output systems - Single antenna - Theoretical modeling - Zeroforcing beamforming (ZFBF)

**Classification code:** 711 Electromagnetic Waves - 711.2 Electromagnetic Waves in Relation to Various Structures - 921.6 Numerical Methods
**DOI:** 10.1109/NaNA60121.2023.00028
**Funding Details:** Number: 23H03386, Acronym: KAKEN, Sponsor: Japan Society for the Promotion of Science;
**Funding text:** VI. ACKNOWLEDGE This work was supported in part by the Japan Society for the Promotion of Science (JSPS) under Grant No.23H03386.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 105. Topological Loss on Graph Auto-Encoders

**Accession number:** 20234715078037
**Authors:** Gao, Jie (1); Liu, Zhihong (1); Zeng, Yong (1)
**Author affiliation:** (1) School of Cyber Engineering, Xidian University, Xi'an, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 497-501
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Low-dimensional embeddings of nodes in large graphs remain a main topic of graph representation learning and have proven useful in addressing many problems such as link prediction and node clustering. However, most transductive learning results can only address one problem at a time because when embedded vectors fit into a space that is suitable for an exact task, lots of information that is critical for other tasks is lost. We present a new model that uses topological data analysis methods to regularize graph auto-encoder so as to preserve topological structures of node feature space on latent space. Our method not only extends the representational capability of embedded vectors but also promotes accuracy of the model when applying it to some real-world datasets. © 2023 IEEE.
**Number of references:** 32
**Main heading:** Vector spaces
**Controlled terms:** Data handling - Graph theory - Information analysis - Learning systems - Signal encoding
**Uncontrolled terms:** AS-links - Auto encoders - Graph auto-encoder - Graph representation - Graph representation learning - Large graphs - Link nodes - Link prediction - Low dimensional embedding - Topological data analysis
**Classification code:** 716.1 Information Theory and Signal Processing - 723.2 Data Processing and Image Processing - 903.1 Information Sources and Analysis - 921 Mathematics - 921.4 Combinatorial Mathematics, Includes Graph Theory, Set Theory
**DOI:** 10.1109/NaNA60121.2023.00088
**Funding Details:** Number: 2022YFB2701800, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China;
**Funding text:** ACKNOWLEDGE This work was supported by the National Key Research & Development Program of China under Grant 2022YFB2701800.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 106. Online Tobacco Width Detection Based on Skeleton Detection Algorithm

**Accession number:** 20234715078062
**Authors:** Jiang, Huayuan (1); Xie, Xin (1); Fan, Jianan (1); Hou, Shicong (1); Chen, Huan (1)

**Author affiliation:** (1) China Tobacco Jiangsu Industrial Co. Ltd, Nanjing Cigarette Factory, No.31 Xinglong Street, Jianye District, Nanjing; 210019, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 428-433
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** The width of cut tobacco is a crucial factor that affects the quality and performance of cigarettes. However, conventional methods for measuring tobacco width are time-consuming, labor-intensive, and prone to errors. In this paper, we propose a novel method for online tobacco width detection based on a skeleton detection algorithm. Our method can automatically extract suitable points for width measurement from irregularly shaped and occluded tobacco images, and calculate their widths based on the skeleton slope. We evaluate our method on different tobacco samples with various widths and demonstrate that it can achieve high accuracy and efficiency, as well as real-time monitoring of tobacco width on the production line. © 2023 IEEE.
**Number of references:** 21
**Main heading:** Tobacco
**Controlled terms:** Computer vision - Musculoskeletal system - Signal detection
**Uncontrolled terms:** Conventional methods - Detection algorithm - Labour-intensive - Novel methods - Performance - Tobacco samples - Tobacco width detection - Width calculation - Width detections - Width measurements
**Classification code:** 461.3 Biomechanics, Bionics and Biomimetics - 716.1 Information Theory and Signal Processing - 723.5 Computer Applications - 741.2 Vision - 821.4 Agricultural Products
**DOI:** 10.1109/NaNA60121.2023.00077
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 107. A Comparison of Finetune and Meta Learning Methods for Few-Shot Object Detection in Sonar Images

**Accession number:** 20234715078093
**Authors:** Wei, Wei (1); Zang, Feng (2); Huang, Liben (3); Xue, Wei (1)
**Author affiliation:** (1) Zztf Nanjing Aviation Research Institute Co.,Ltd., Nanjing, China; (2) Nanjing Urban Lighting Construction and Operation Group Co., Ltd., Nanjing, China; (3) Jiangsu Future Urban Public Space Development and Operation Co., Ltd., Nanjing, China
**Corresponding author:** Wei, Wei(109799514@qq.com)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 539-544
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China

**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Object detection in sonar images is a key task for underwater exploration and surveillance. However, existing methods either rely on manual feature extraction or suffer from limited data availability. To address these challenges, we propose to apply few-shot object detection algorithms on sonar image datasets with scarce samples. Specifically, we use two state-of-the-art few-shot learning algorithms, TFA and Meta R-CNN, to detect and locate underwater object in side-scan sonar images. Our experimental results show that these algorithms can achieve high accuracy and robustness in few-shot object detection scenarios, demonstrating their potential for enhancing underwater sonar image object detection. © 2023 IEEE.
**Number of references:** 26
**Main heading:** Object detection
**Controlled terms:** Feature extraction - Image enhancement - Learning algorithms - Learning systems - Object recognition - Sonar - Underwater acoustics
**Uncontrolled terms:** Data availability - Features extraction - Few-shot learning - Learning methods - Limited data - Metalearning - Objects detection - Sonar image - Underwater exploration and surveillance - Underwater objects
**Classification code:** 723.2 Data Processing and Image Processing - 723.4.2 Machine Learning - 751.1 Acoustic Waves - 752.1 Acoustic Devices
**DOI:** 10.1109/NaNA60121.2023.00095
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 108. Privacy-preserving Federated Learning Against Byzantine Attack via Top-k Indexes

**Accession number:** 20234715078100
**Authors:** Shang, Menghan (1); Tong, Ze (1); Liu, Teng (1); Zhang, Tao (1)
**Author affiliation:** (1) School of Computer Science and Technology, Xidian University, Shaanxi, Xi'an, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 625-630
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Federated learning as an emerging machine learning paradigm has received much attention due to its security feature of only uploading trained model gradients instead of raw data. However, it has been demonstrated that shared gradients may expose sensitive client data, and malicious clients could upload poisoned model gradients, disrupting the global model's convergence. Although existing privacy protection schemes and malicious client detection schemes for federated learning have been proposed, these detection schemes under privacy protection still have high communication and computational overhead. To address the above issues, we propose TGS-SM, a privacy-preserving, byzantine-robust, and computationally-efficient federated learning framework. Specifically, we identify the malicious client based on the similarity of the index mask generated by the Top-k mechanism. Additionally, we combine the shuffle mechanism and the dual-server framework to ensure privacy protection. Extensive experiments have shown that our scheme can achieve efficient defense while ensuring the accuracy of the global model. © 2023 IEEE.
**Number of references:** 22
**Main heading:** Privacy-preserving techniques
**Controlled terms:** Sensitive data
**Uncontrolled terms:** Byzantine attacks - Detection scheme - Federated learning - Global models - Learning paradigms - Machine-learning - Malicious client detection - Poisoning attacks - Privacy preserving - Privacy protection

**Classification code:** 716 Telecommunication; Radar, Radio and Television - 718 Telephone Systems and Related Technologies; Line Communications - 723.2 Data Processing and Image Processing
**DOI:** 10.1109/NaNA60121.2023.00108
**Funding Details:** Number: 2020YFB1005500, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China; Number: 2021ZDLGY07-05, Acronym: -, Sponsor: Key Research and Development Projects of Shaanxi Province;
**Funding text:** This work was supported in part by the National Key Research and Development Program of China (No. 2020YFB1005500), the Key Research and Development Program of Shaanxi (No. 2021ZDLGY07-05).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 109. Hierarchical Clustering Combination Method Using Intuitionistic Fuzzy Similarity in Software Module Clustering

**Accession number:** 20234715078096
**Authors:** Xia, Hong (1, 2, 3); Wang, Bo (1); Zhang, Yongkang (1); Chen, Yanping (1, 2, 3)
**Author affiliation:** (1) School of Computer Science and Technology, Xi'an University of Posts and Telecommunications, China; (2) Shaanxi Key Laboratory of Network Data Analysis and Intelligent Processing, China; (3) Xi 'An Key Laboratory of Big Data and Intelligent Computing, Shaanxi, Xi'an; 710121, China
**Corresponding authors:** Xia, Hong(xiahong@xupt.edu.cn); Chen, Yanping(chenyanping@xupt.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 502-507
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** In order to solve the problem that the similarity method used in software module clustering can produce arbitrary decision, and the description matrix of dendrogram generated by base clustering in hierarchical clustering combination does not consider more characteristics of entities, a hierarchical clustering combination method based on intuitionistic fuzzy similarity (HCC-IFS) was proposed. In the process of entity similarity calculation, the intuitionistic fuzzy set theory and similarity calculation method are used to provide membership and non-membership attributes for each entity, so as to improve the merging efficiency and solve arbitrary decision problems. In the description matrix representation of base clustering, the absolute and relative features obtained from the dendrogram are used to construct the description matrix, and the generated description matrix is combined. Finally, the proposed algorithm is verified by experiments. Experimental results show that HCC-IFS can produce better clustering results and improve the recovery quality of software architecture. © 2023 IEEE.
**Number of references:** 13
**Main heading:** Fuzzy set theory
**Controlled terms:** Clustering algorithms - Decision theory - Fuzzy logic - Fuzzy sets - Software architecture
**Uncontrolled terms:** Clustering combination - Clusterings - Description matrixes - Fuzzy similarity - Hier-archical clustering - Hierarchical Clustering - Hierarchical clustering combination - Intuitionistic fuzzy - Intuitionistic fuzzy similarity - Software architecture recovery
**Classification code:** 721.1 Computer Theory, Includes Formal Logic, Automata Theory, Switching Theory, Programming Theory - 723.1 Computer Programming - 723.5 Computer Applications - 903.1 Information Sources and Analysis - 921.4 Combinatorial Mathematics, Includes Graph Theory, Set Theory - 961 Systems Science
**DOI:** 10.1109/NaNA60121.2023.00089
**Funding Details:** Number: 21JP115, Acronym: -, Sponsor: -; Number: CXY-2022-162, Acronym: -, Sponsor: -; Number: 22GXFW0129, Acronym: -, Sponsor: Ji'an Science and Technology Bureau; Number: 2023-YBGY-211, Acronym: -, Sponsor: Shaanxi Provincial Science and Technology Department; Number: 2019ZDLGY07-08, Acronym:

-, Sponsor: Key Science and Technology Program of Shaanxi Province; Number: 2021JQ-719, Acronym: -, Sponsor: Natural Science Basic Research Program of Shaanxi Province;
**Funding text:** VI. ACKNOWLEDGE This work is supported by the Science and Technology Project in Shaanxi Province of China (Program No. 2019ZDLGY07-08), Natural Science Basic Research Program of Shaanxi (Program No. 2021JQ-719), Special Funds for Construction of Key Disciplines in Universities in Shaanxi,Scientific Research Program of the Science and Technology Department of Shaanxi Province, China (2023-YBGY-211), the Scientific Research Program of Shaanxi Provincial Education Department, China (21JP115), the Scientific Research Program of the Science and Technology Bureau of Xi'an, China (22GXFW0129), the Scientific Research Program of the Science and TechnologyBureau of Yulin, China (CXY-2022-162).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 110. FLAP: Federated Learning Aggregation Scheme Based on Privileged Secret Sharing

**Accession number:** 20234715078050
**Authors:** Mu, Xianyu (1); Tian, Youliang (1); Xiong, Jinbo (2); Wang, Shuai (1); Gong, Boxiang (3)
**Author affiliation:** (1) College of Computer Science and Technology, Guizhou University, State Key Laboratory of Public Big Data, Guiyang; 550025, China; (2) College of Computer and Cyber Security, Fujian Normal University, Fujian Provincial Key Laboratory of Network Security and Cryptology, Fuzhou; 350117, China; (3) Guizhou Xishan Technology Co., Ltd, China
**Corresponding author:** Tian, Youliang(youliangtian@163.com)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 588-594
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Federated Learning (FL) is a privacy-preserving machine learning technique that trains models on client devices and only uploads new model gradients to servers for aggregation. However, transmitting the true gradients introduces the risk of reverse inference attack, which can compromise client privacy. To address this issue, we present the federated learning aggregation scheme based on privileged secret sharing (FLAP). Firstly, we present privileged secret sharing by combining the one-time pad with shamir secret sharing. Secondly, we introduce game theory to generate games between servers to resist collusion attacks. Finally, the analysis demonstrates that FLAP enables the server to successfully update the global gradient while ensuring the utmost protection of client privacy and FLAP achiev the effect of resisting collusion attack and reverse inference attack. We have proved through experiments that FLAP is 26.42% more efficient than the current scheme, and has strong robustness to drop out. © 2023 IEEE.
**Number of references:** 26
**Main heading:** Game theory
**Controlled terms:** Learning systems - Privacy-preserving techniques
**Uncontrolled terms:** Aggregation schemes - Client devices - Client privacy - Collusion attack - Federal learning - Inference attacks - Machine learning techniques - Privacy preserving - Secret-sharing - Train model
**Classification code:** 716 Telecommunication; Radar, Radio and Television - 718 Telephone Systems and Related Technologies; Line Communications - 723.2 Data Processing and Image Processing - 922.1 Probability Theory
**DOI:** 10.1109/NaNA60121.2023.00102
**Funding Details:** Number: [2015]-53, Acronym: -, Sponsor: -; Number: [2020]6008, Acronym: -, Sponsor: -; Number: [2021]1-5,[2022]2-4, Acronym: -, Sponsor: -; Number: [2022]065, Acronym: -, Sponsor: -; Number: 62272123,No.U1836205, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: 2021YFB3101100, Acronym: NKRDPC, Sponsor: National Key Research and Development Program of China;
**Funding text:** This work was supported by the National Key Research and Development Program of China under Grant No.2021YFB3101100; Key Program of the National Natural Science Union Foundation of China under Grant

No.U1836205; Project of High-level Innovative Talents of Guizhou Province under Grant No. [2020]6008; Science and Technology Program of Guiyang under Grant No.[2021]1-5; Science and Technology Program of Guiyang under Grant No.[2022]2-4; Science and TechnologyProgram of Guizhou Province under Grant No. [2020]5017, No. [2022]065; National Natural Science Foundation of China under Grant 62272123; Guizhou University Talent Introduction Research Fund under Grant No.GDRJHZ[2015]-53.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 111. Least Co-Residence: A Novel Virtual Migration Algorithm for Mitigating Side-Channel Attacks

**Accession number:** 20234715078027
**Authors:** Dong, Wei (1); Zhou, Zan (1); Yang, Shujie (1); Lian, Yibo (1); Li, Hongjing (1); Xu, Changqiao (1)
**Author affiliation:** (1) Beijing University of Posts and Telecommunications, State Key Laboratory of Networking and Switching Technology, Beijing, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 607-612
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** The advent of cloud platforms has revolutionized the landscape of modern business and user computing by providing a scalable and cost-effective alternative to the traditional model of purchasing and maintaining equipment. However, the coresidence feature, which is inherent to virtual machines (VMs) in cloud platforms, creates vulnerabilities that attackers can exploit to launch cache-based side-channel attacks, thereby compromising the security of user information. To address this problem, this paper proposes a hot migration algorithm based on a multiarmed bandit (MAB) model, which leverages physical machine (PM) migration between PMs to mitigate side-channel attacks in the cloud. Our proposed algorithm achieves the optimal timeaverage reward and ensures the security of the cloud platform, thereby outperforming other algorithms. The findings of this study have significant implications for the development of secure cloud computing systems, with the potential to enhance user privacy and safeguard against cyber threats. © 2023 IEEE.
**Number of references:** 23
**Main heading:** Cost effectiveness
**Controlled terms:** Cloud computing - Cybersecurity - Side channel attack
**Uncontrolled terms:** Cloud platforms - Cost effective - Hot migration - Migration algorithms - Multiarmed bandits (MABs) - Secure cloud computing - Side-channel attacks - Time averages - Traditional models - User information
**Classification code:** 722.4 Digital Computers and Systems - 723.2 Data Processing and Image Processing - 911.2 Industrial Economics
**DOI:** 10.1109/NaNA60121.2023.00105
**Funding Details:** Number: 62001057, Acronym: NSFC, Sponsor: National Natural Science Foundation of China;
**Funding text:** VII. ACKNOWLEDGE This work is partially supported by the National Natural Science Foundation of China under grant No. 62001057 and Advanced Research Program in the 14th Five-Year Plan (JZX6Y2022110108226).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 112. Joint Distribution Analysis of Multi-Dimensional Randomized Response

**Accession number:** 20234715078059
**Authors:** Wang, Wenli (1); Zhang, Yijun (1); Yan, Jun (2, 3); Zhou, Yihui (2); Lu, Laifeng (1)
**Author affiliation:** (1) School of Mathematics and Statistics, Shaanxi Normal University, Xi'an; 710119, China; (2) School of Computer Science, Shaanxi Normal University, Xi'an; 710119, China; (3) School of Mathematics and Computer Applications, Shangluo College, Shangluo; 726000, China
**Corresponding author:** Zhou, Yihui(zhouyihui@snnu.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 422-427
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Data collection can provide services and convenience for people, but disclosure of personal privacy during data collection can be harmful. So, it is needed to protect personal privacy while collecting data. Randomized response is a reliable privacy-preserving technique. For multi-dimensional data, the most direct mechanism is RR-Independent, which applies randomized response on each attribute independently. After applying the RR-independent mechanism, the joint distribution of perturbed data needs to be modified in order to be close to that of input data better. Two estimation methods of joint distribution, Naive estimation and Castell estimation, are studied in this paper. Then, we propose a sufficient and necessary condition for the two estimations to be equal. In addition, a mathematical study shows that Castell estimation is closer to the original distribution of data than that of Naive estimation if the condition is not satisfied. Finally, numerical experiments are carried out to show that Castell estimation is better than Naive estimation and the results obtained by the two protocols in the paper are consistent. © 2023 IEEE.
**Number of references:** 10
**Main heading:** Data acquisition
**Controlled terms:** Privacy-preserving techniques
**Uncontrolled terms:** Castell - Data collection - Direct mechanism - Distribution analysis - Joint distributions - Multi dimensional - Multidimensional data - Personal privacy - Randomized response - RR-independent
**Classification code:** 716 Telecommunication; Radar, Radio and Television - 718 Telephone Systems and Related Technologies; Line Communications - 723.2 Data Processing and Image Processing
**DOI:** 10.1109/NaNA60121.2023.00076
**Funding Details:** Number: 2021-C-0004, Acronym: -, Sponsor: -; Number: No.2020JM-288, Acronym: -, Sponsor: Natural Science Foundation of Shaanxi Province; Number: 21SKY126, Acronym: -, Sponsor: Shangluo University; Number: GK201903011,GK201903091, Acronym: -, Sponsor: Fundamental Research Funds for the Central Universities;
**Funding text:** ACKNOWLEDGMENT This work was supported by the Shaanxi Provincial Natural Science Foundation project under Grant No.2020JM-288, the Fundamental Research Funds for the Central Universities (GK201903091, GK201903011), the Scientific and Technological Project of Shangluo (No. 2021-C-0004) and the research project of Shangluo University (21SKY126).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 113. Physical-Sensing Inconsistency Vulnerability Mitigation for Multi-UAV Crowdsensing

**Accession number:** 20234715078025
**Authors:** Cao, Yujuan (1); Liu, Zhao (2); Axi, Wuhe (1); Wei, Dawei (1); Xi, Ning (1)
**Author affiliation:** (1) Xidian University, School of Cyber Engineering, Xi'an, China; (2) Weinan Meteorological Bureau, Meteorological Observatory, Weinan, China
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1

**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 705-710
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Multiagent deep reinforcement learning (MADRL)-based methods have been widely used to control the flight of multiple UAVs in high dynamic mobile crowdsensing (MCS). The existing MADRL-based methods assume that the state used for decision-making, such as GPS position, is accurate. However, the integrity of state is fragility to the GPS attacks. We formulate this vulnerability as the Physical-Sensing Inconsistency (PSI). Different from the existing methods that use additional hardware and software to judge the authenticity of GPS signals, we use the technology of robust deep reinforcement learning to overcome the impact of GPS attacks on UAV flight. Specifically, based on the existing MADRL algorithm, i.e., Multi-Agent Deep Deterministic Policy Gradient (MADDPG), we add a regularizer to its policy updating to mitigate the impact of the PSI. Finally, we use theoretical analysis and experiments to verify the security and effectiveness of the proposed method. © 2023 IEEE.
**Number of references:** 24
**Main heading:** Reinforcement learning
**Controlled terms:** Antennas - Decision making - Deep learning - Global positioning system - Learning systems - Multi agent systems - Unmanned aerial vehicles (UAV)
**Uncontrolled terms:** Aerial vehicle - Learning-based methods - Mobile crowdsensing - Multi agent - Multi UAV - Multi-agent deep reinforcement learning - Physical-sensing inconsistency - Reinforcement learnings - Unmanned aerial vehicle - Vulnerability mitigation
**Classification code:** 461.4 Ergonomics and Human Factors Engineering - 652.1 Aircraft, General - 723.4 Artificial Intelligence - 912.2 Management
**DOI:** 10.1109/NaNA60121.2023.00121
**Funding Details:** Number: 92267204, Acronym: NSFC, Sponsor: National Natural Science Foundation of China; Number: XJSJ23185, Acronym: -, Sponsor: Fundamental Research Funds for the Central Universities;
**Funding text:** This research work is supported by the Major Research Plan of the National Natural Science Foundation of China (Grant No. 92267204) and the Fundamental Research Funds for the Central Universities (XJSJ23185).
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 114. Taxi Station Location Model Based on Spatio-Temporal Demand Cube

**Accession number:** 20234715078097
**Authors:** Gao, LuLu (1, 2, 3); Li, XiaoNan (1, 2, 3); Wei, ZhiCheng (1, 2, 3)
**Author affiliation:** (1) Key Lab of Network and Information Security, Hebei Province, Shijiazhuang, China; (2) College of Computer and Cyber Security, Hebei Province, Shijiazhuang, China; (3) Hebei Normal University, Hebei Provincial Engineering Research Center for Supply Chain Big Data Analytics & Security, Hebei Province, Shijiazhuang, China
**Corresponding author:** Wei, ZhiCheng(weizhicheng@hebtu.edu.cn)
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 378-383
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023

**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** With the widespread use of mobile apps, empty taxis can easily receive new orders without having to roam around. Therefore, it is necessary to plan taxi stations where empty taxis can park. In the location selection problem, the spatial and temporal distribution of passenger demand needs to be considered to ensure that the selected location can meet the actual needs of passengers. In this paper, a Spatio-Temporal Cube Demand Coverage Model (STC-DCM) is proposed for taxi station location selection. Firstly, a spatiotemporal demand cube is constructed to obtain fine-grained user demands based on time and space, and genetic algorithm is used to maximize the demand coverage rate. Then, the final location selection results are obtained using the fusion module and adjustment optimization module, where the fusion module integrates multiple location selection solutions using ensemble learning method. Experimental results show that our proposed model can better cover dynamic passenger demand compared to traditional models. © 2023 IEEE.
**Number of references:** 20
**Main heading:** Genetic algorithms
**Controlled terms:** Geometry - Learning systems - Location - Parks - Taxicabs
**Uncontrolled terms:** Fusion modules - Location modeling - Location selection - Mobile app - Model-based OPC - Passenger demands - Spatio-temporal - Spatiotemporal demand cube - Station location - Taxi station location selection
**Classification code:** 662.1 Automobiles - 921 Mathematics
**DOI:** 10.1109/NaNA60121.2023.00069
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village


## 115. Covert Terahertz Communication for UAV-Aided Wireless Relay Systems

**Accession number:** 20234715078057
**Authors:** Pi, Xinzhe (1); Yang, Bin (2); Jiang, Xiaohong (1)
**Author affiliation:** (1) School of Systems Information Science, Future University Hakodate, Hakodate, Japan; (2) School of Computer and Information Engineering, Chuzhou University, Anhui, China
**Corresponding authors:** Pi, Xinzhe; Yang, Bin
**Source title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Abbreviated source title:** Proc. - Int. Conf. Netw. Netw. Appl., NaNA
**Part number:** 1 of 1
**Issue title:** Proceedings - 2023 International Conference on Networking and Network Applications, NaNA 2023
**Issue date:** 2023
**Publication year:** 2023
**Pages:** 127-132
**Language:** English
**ISBN-13:** 9798350327380
**Document type:** Conference article (CA)
**Conference name:** 2023 International Conference on Networking and Network Applications, NaNA 2023
**Conference date:** August 18, 2023 - August 21, 2023
**Conference location:** Qingdao, China
**Conference code:** 193846
**Publisher:** Institute of Electrical and Electronics Engineers Inc.
**Abstract:** Unmanned aerial vehicle (UAV)-aided Terahertz (THz) relay systems can provide high-speed wireless line-of-sight (LoS) communications at THz bands, which are envisioned as a key component of 6G and beyond. However, security is still a significant challenge when adversaries reside in the THz signal beam. This paper investigates the covert THz communications in a UAV-aided two-hop relay system consisting of a transmitter, a UAV relay, a receiver, and two UAV wardens detecting the existence of transmissions in both hops. To enhance security, we consider a friendly jamming scheme that the UAV relay and receiver also serve as jammers to interfere with the two UAV wardens. We then derive the closed-from expressions for the optimal thresholds of wardens and the minimum cascaded detection error probability (DEP). Additionally, we derive the cascaded outage probability and average covert capacity of the covert THz communications. Numerical results are presented to demonstrate the impact of crucial system parameters on the covert THz performances. © 2023 IEEE.
**Number of references:** 18
**Main heading:** Unmanned aerial vehicles (UAV)
**Controlled terms:** Aircraft detection - Antennas - Jamming - Vehicle to vehicle communications

**Uncontrolled terms:** Aerial vehicle - Covert communications - High speed wireless - Line of sight communications - Relay system - Tera Hertz - Terahertz band - Terahertz signals - Unmanned aerial vehicle - Wireless relay system
**Classification code:** 652.1 Aircraft, General - 711 Electromagnetic Waves - 716.2 Radar Systems and Equipment - 716.3 Radio Systems and Equipment
**DOI:** 10.1109/NaNA60121.2023.00029
**Funding Details:** Number: 2022XJZD12,KJ2021ZD0128, Acronym: -, Sponsor: -; Number: 23H03386, Acronym: KAKEN, Sponsor: Japan Society for the Promotion of Science; Number: 61962033, Acronym: NSFC, Sponsor: National Natural Science Foundation of China;
**Funding text:** ACKNOWLEDGE This work is supported in part by the National Natural Science Foundation of China under Grant No. 61962033; in part by the Anhui Research Project under Grant No. KJ2021ZD0128 and No. 2022XJZD12; in part by the Japan Society for the Promotion of Science (JSPS) under Grant No.23H03386.
**Compendex references:** YES
**Database:** Compendex
**Data Provider:** Engineering Village