Li Lu (卢立) Ph.D.

Research Professor (特聘研究员)

State Key Laboratory of Blockchain and Data Security
School of Cyber Science and Technology
College of Computer Science and Technology
Zhejiang University

Email: li.lu@zju.edu.cn
https://lynnlilu.github.io
319 Yifu Business Management Building
38 Zheda Road
Hangzhou, Zhejiang 310027
P. R. China

RESEARCH INTERESTS

Intelligent Voice Security, Autonomous Driving Security, IoT Security, Ubiquitous Computing.

EDUCATIONAL BACKGROUND

- Ph.D. in Computer Science and Technology, Shanghai Jiao Tong University, Shanghai, China, 2020.
- B.E. in Computer Science and Technology & B.Admin in Business Administration, Xi'an Jiaotong University, Xi'an, Shaanxi, China, 2015.

RESEARCH EXPERIENCE

- Research Professor, Zhejiang University
  - Location: Hangzhou, Zhejiang, China.
  - Duration: Jul. 2020 -present.
  - Duties: I am a tenure-track research professor of School of Cyber Science and Technology, College of Computer Science and Technology and State Key Laboratory of Blockchain and Data Security at Zhejiang University, also being a doctoral and master advisor. Currently, I am working on the area of intelligent system security, IoT security, and ubiquitous computing.
- Research Assistant, Shanghai Jiao Tong University
  - Location: Shanghai, China.
  - Duration: Sep. 2015-Jun. 2020.
  - Supervisor: Prof. Jiadi Yu and Prof. Minglu Li (IEEE Fellow).
  - Duties: Mainly worked on mobile and ubiquitous computing, cyber security and privacy, human-computer interactions. The main work is to adopt signal processing and machine learning techniques in mobile network and applications. Previously also worked on cloud computing and network economic during the early stage of Ph.D. study.
- Visiting Research Student, Rutgers University
  - Location: New Brunswick, NJ, USA.
  - Duration: Oct. 2018-Sep. 2019.
  - Supervisor: Prof. Yingying Chen (ACM Fellow, IEEE Fellow, NAI Fellow, AAIA Fellow).
  - Duties: Mainly worked on acoustic-based communication system and mmWave radar-based sensing applications. The joint Ph.D. training program is supported by China Scholarship Council.
- Summer Internship, Zhejiang University
  - Location: Hangzhou, Zhejiang, China.
  - Duration: Jul. 2014-Aug. 2014.
  - Supervisor: Prof. Gang Pan (CAAI Fellow).
  - Duties: Mainly worked on Biocomputing, specifically, implementing a PCA algorithm for EEG signals.

PUBLICATIONS

Conference Papers

[C1]. Kun Wang, **Li Lu***, Meng Chen, Jingwen Feng, Qianniu Chen, Zhongjie Ba, Kui Ren, "From One Stolen Utterance: Assessing the Risks of Voice Cloning in the AIGC Era," in *Proceedings of IEEE Symposium on Security and Privacy (IEEE S&P 2025)*, San Francisco, CA, USA, May 2025, doi: 10.1109/SP61157.2025.00238. [CSRankings-Computer security]

[C2]. Meng Chen, Xiangyu Xu, **Li Lu***, Zhongjie Ba, Feng Lin, Kui Ren, "Devil in the Room: Triggering Audio Backdoors in the Physical World," in *Proceedings of USENIX Security Symposium* (*USENIX SEC 2024*), Philadelphia, PA, USA, Aug. 2024, link: url. [CSRankings-Computer security]

[C3]. Kun Wang, Xiangyu Xu, **Li Lu***, Zhongjie Ba, Feng Lin, Kui Ren, "FraudWhistler: A Resilient, Robust and Plug-and-play Adversarial Example Detection Method for Speaker Recognition," in *Proceedings of USENIX Security Symposium* (*USENIX SEC 2024*), Philadelphia, PA, USA, Aug. 2024, link: url. [CSRankings-Computer security]

[C4]. Meng Chen, **Li Lu***, Junhao Wang, Jiadi Yu, Yingying Chen, Zhibo Wang, Zhongjie Ba, Feng Lin, Kui Ren, "VoiceCloak: Adversarial Example Enabled Voice De-Identification with Balanced Privacy and Utility," in *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* (*IMWUT*)/*ACM UbiComp 2023*, vol. 7, no. 2, pp. 48:1-48:21, Cancun, Mexico, Jun. 2023, doi: 10.1145/3596266. [CSRankings-Human-computer interaction]

[C5]. Lei Wang, Meng Chen, **Li Lu***, Zhongjie Ba, Feng Lin, Kui Ren, "VoiceListener: A Training-free and Universal Eavesdropping Attack on Built-in Speakers of Mobile Devices," in *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* (*IMWUT*)/*ACM UbiComp 2023*, vol. 7, no. 1, pp. 32:1-32:22, Cancun, Mexico, Mar. 2023, doi: 10.1145/3580789. [CSRankings-Human-computer interaction]

[C6]. Qianniu Chen, Meng Chen, **Li Lu***, Jiadi Yu, Yingying Chen, Zhibo Wang, Zhongjie Ba, Feng Lin, Kui Ren, "Push the Limit of Adversarial Example Attack on Speaker Recognition in Physical Domain," in *Proceedings of ACM Conference on Embedded Networked Sensor Systems* (*ACM SenSys 2022*), pp. 710-724, Boston, MA, USA, Nov. 2022, doi: 10.1145/3560905.3568518. [CSRankings-Mobile computing]

[C7]. Meng Chen, **Li Lu***, Zhongjie Ba, Kui Ren, "PhoneyTalker: An Out-of-the-Box Toolkit for Adversarial Example Attack on Speaker Recognition," in *Proceedings of IEEE International Conference on Computer Communications* (*IEEE INFOCOM 2022*), pp. 1419-1428, London, United Kingdom, May 2022, doi: 10.1109/INFOCOM48880.2022.9796934.

[C8]. **Li Lu**, Jiadi Yu, Yingying Chen, Yan Wang, "VocalLock: Sensing Vocal Tract for Passphrase-Independent User Authentication Leveraging Acoustic Signals on Smartphones," in *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* (*IMWUT*)/*ACM UbiComp 2020*, vol. 4, no. 2, pp. 51:1-51:24, Cancun, Mexico, Jun. 2020, doi: 10.1145/3397320. [CSRankings-Human-computer interaction]

[C9]. **Li Lu**, Jiadi Yu, Yingying Chen, Yanmin Zhu, Minglu Li, Xiangyu Xu, "I^3: Sensing Scrolling Human-Computer Interactions for Intelligent Interest Inference on Smartphones, " in *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* (*IMWUT*)/*ACM Ubicomp 2019*, vol. 3, no. 3, pp. 97:1-97:22, London, England, Sep. 2019, doi: 10.1145/3351255. [CSRankings-Human-computer interaction]

[C10]. **Li Lu**, Jiadi Yu, Yingying Chen, Yanmin Zhu, Xiangyu Xu, Guangtao Xue, Minglu Li, "KeyListener: Inferring Keystrokes on QWERTY Keyboard of Touch Screen through Acoustic Signals," in *Proceedings of IEEE International Conference on Computer Communications* (*IEEE INFOCOM 2019*), pp. 775-783, Paris, France, Apr. 2019, doi: 10.1109/INFOCOM.2019.8737591.

[C11]. **Li Lu**, Jiadi Yu, Yingying Chen, Hongbo Liu, Yanmin Zhu, Yunfei Liu, Minglu Li, "LipPass: Lip Reading-based User Authentication on Smartphones Leveraging Acoustic Signals," in *Proceedings of IEEE International Conference on Computer Communications* (*IEEE INFOCOM 2018*), pp. 1466-1474, Honolulu, HI, USA, Apr. 2018, doi: 10.1109/INFOCOM.2018.8486283.

[C12]. **Li Lu**, Zhongjie Ba, Feng Lin, Jinsong Han, Kui Ren, "ActListener: Imperceptible Activity Surveillance by Pervasive Wireless Infrastructures," in *Proceedings of IEEE International Conference on Distributed Computing Systems* (*IEEE ICDCS 2022*), pp. 776-786, Bologna, Italy, Jul. 2022, doi: 10.1109/ICDCS54860.2022.00080.

[C13]. Qianniu Chen, Zhehan Gu, **Li Lu***, Xiangyu Xu, Zhongjie Ba, Feng Lin, Zhenguan Liu, Kui Ren, "Conan's Bow Tie: A Streaming Voice Conversion for Real-Time VTuber Livestreaming," in *Proceedings*

of ACM Conference on Intelligent User Interface (ACM IUI 2024), pp. 35-50, Greenville, SC, USA, Mar. 2024, doi: 10.1145/3640543.3645146.

[C14]. Junhao Wang, **Li Lu***, Zhongjie Ba, Feng Lin, Kui Ren, "Shift to Your Device: Data Augmentation for Device-Independent Speaker Verification Anti-Spoofing," in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing* (*IEEE ICASSP 2023*), Rhodes Island, Greece, Jun. 2023, doi: 10.1109/ICASSP49357.2023.10097168.

[C15]. Hao Kong and **Li Lu**[1], Jiadi Yu, Yingying Chen, Yanmin Zhu, Linghe Kong, Minglu Li, "FingerPass: Finger Gesture-based Continuous User Authentication for Smart Homes Using Commodity WiFi," in *Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing* (*ACM MobiHoc 2019*), pp. 201-210, Catania, Italy, Jul. 2019, doi: 10.1145/3323679.3326518.

[C16]. **Li Lu**, Jian Liu, Jiadi Yu, Yingying Chen, Yanmin Zhu, Xiangyu Xu, Minglu Li. "VPad: Virtual Writing Tablet for Laptops Leveraging Acoustic Signals," in *Proceedings of IEEE International Conference on Parallel and Distributed Systems* (*IEEE ICPADS 2018*), pp. 244-251, Sentosa, Singapore, Dec. 2018, doi: 10.1109/PADSW.2018.8644615.

[C17]. **Li Lu**, Jiadi Yu, Yanmin Zhu, Shiyou Qian, Guangtao Xue, Minglu Li, "Cost-Efficient VM Configuration Algorithm in the Cloud using Mix Scaling Strategy," in *Proceedings of IEEE International Conference of Communications* (*IEEE ICC 2017*), pp. 1-6, Paris, France, May 2017, doi: 10.1109/ICC.2017.7997241.

[C18]. Yuhan Wu, **Li Lu***, Yuli Wu, Shuguo Zhuo, Zhan Qin, Kui Ren, "GFuzz4CAN: A Generative Model-based Fuzzing Method for In-vehicle Controller Area Network," in *Proceedings of IEEE International Conference of Communications* (*IEEE ICC 2025*), Montreal, Canada, Jun. 2025, doi: 10.1109/ICC52391.2025.11160828.

[C19]. Qianniu Chen, Xiaodi Zhao, Zhehan Gu, Xiao Li, **Li Lu***, "Evaluating Robustness of Voice Conversion Systems under Multi-source Channel Interference," in *Proceedings of IEEE International Joint Conference on Neural Networks (IEEE IJCNN 2025)*, Rome, Italy, Jun. 2025, doi: to appear.

[C20]. Qianniu Chen, Kang Fu, **Li Lu***, Meng Chen, Zhongjie Ba, Feng Lin, Kui Ren, "BypTalker: An Adaptive Adversarial Example Attack to Bypass Prefilter-enabled Speaker Recognition," in *Proceedings of IEEE International Conference on Mobility, Sensing and Networking (IEEE MSN 2023)*, pp. 496-503, Nanjing, China, Dec. 2023, doi: 10.1109/MSN60784.2023.00077.

[C21]. Yunlang Cai, Hanxue Shi, Xiaohang Wang, Haoting Shen, **Li Lu**, Kui Ren, "On Bit-level Reverse Engineering of Vehicular CAN Bus," in *Proceedings of Design Automation Conference* (*DAC 2025*), Moscone West, San Francisco, USA, Jun. 2025, doi: to appear. [CSRankings-Design automation]

[C22]. Peng Huang, Kun Pan, Qinglong Wang, Peng Cheng, **Li Lu**, Zhongjie Ba, Kui Ren, "SecHeadset: A Practical Privacy Protection System for Real-time Voice Communication," in *Proceedings of ACM International Conference on Mobile Systems, Applications, and Services* (*MobiSys 2025*), Anaheim, CA, USA, Jun. 2025, doi: 10.1145/3711875.3729142. [CSRankings-Mobile computing]

[C23]. Tiantian Liu, Feng Lin, Zhongjie Ba, **Li Lu**, Zhan Qin, Kui Ren, "MicGuard: A Comprehensive Detection System against Out-of-band Injection Attacks for Different Level Microphone-based Devices," in *Proceedings of USENIX Security Symposium* (*USENIX SEC 2024*), Philadelphia, PA, USA, Aug. 2024, link: url. [CSRankings-Computer security]

[C24]. Zhongjie Ba, Qingyu Liu, Zhenguang Liu, Shuang Wu, Feng Lin, **Li Lu**, Kui Ren, "Exposing the Deception: Uncovering More Forgeries Clues for Deepfake Detection," in *Proceedings of AAAI Conference on Artificial Intelligence (AAAI 2024)*, Vancouver, BC, Canada, Feb. 2024, doi: 10.1609/aaai.v38i2.27829. [CSRankings-Artificial intelligence]

[C25]. Xiangyu Xu, Yu Chen, Zhen Ling, **Li Lu**, Junzhou Luo, Xinwen Fu, "mmEar: Push the Limit of COTS mmWave Eavesdropping on Headphones," in *Proceedings of IEEE International Conference on Computer Communications* (*IEEE INFOCOM 2024*), pp. 351-360, Vancouver, Canada, May 2024, doi: 10.1109/INFOCOM52122.2024.10621229.

[C26]. Peng Cheng, Yuwei Wang, Peng Huang, Zhongjie Ba, Xiaodong Lin, Feng Lin, **Li Lu**, Kui Ren, "ALIF: Low-Cost Adversarial Audio Attacks on Black-Box Speech Platforms Using Linguistic Features,"

[1] Hao Kong and **Li Lu** are the co-first authors of this paper.

in *Proceedings of IEEE Symposium on Security and Privacy (IEEE S&P 2024)*, San Francisco, CA, USA, May 2024, doi: 10.1109/SP54263.2024.00056. [CSRankings-Computer security]

[C27]. Ziwei Liu, Feng Lin, Teshi Meng, Benaouda Chouaib Baha-eddine, **Li Lu**, Qiang Xue, Kui Ren, "EMTrig: Physical Adversarial Examples Triggered by Electromagnetic Injection towards LiDAR Perception," in *Proceedings of ACM Conference on Embedded Networked Sensor Systems (ACM SenSys 2024)*, pp. 351-364, Hangzhou, China, Nov. 2024, doi: 10.1145/3666025.3699343. [CSRankings-Mobile computing]

[C28]. Liu Liu, Xinwen Fu, Xiaodong Chen, Jianpeng Wang, Zhongjie Ba, Feng Lin, **Li Lu**, Kui Ren, "FITS: Matching Camera Fingerprints Subject to Software Noise Pollution," in *Proceedings of ACM Conference on Computer and Communications Security (ACM CCS 2023)*, pp. 1660–1674, Copenhagen, Denmark, Nov. 2023, doi: 10.1145/3576915.3616600. [CSRankings-Computer security]

[C29]. Tiantian Liu, Feng Lin, Zhangsen Wang, Chao Wang, Zhongjie Ba, **Li Lu**, Wenyao Xu, Kui Ren, "MagBackdoor: Beaware of Your Loudspeaker as Backdoor of Magnetic Attack for Malicious Command Injection," in *Proceedings of IEEE Symposium on Security and Privacy (IEEE S&P 2023)*, San Francisco, CA, USA, May 2023, doi: 10.1109/SP46215.2023.00132. [CSRankings-Computer security]

[C30]. Peng Huang, Yao Wei, Peng Cheng, Zhongjie Ba, **Li Lu**, Feng Lin, Fan Zhang, Kui Ren, "InfoMasker: Preventing Eavesdropping Using Phoneme-Based Noise," in *Proceedings of Network and Distributed System Security Symposium (NDSS 2023)*, San Diego, CA, USA, Feb. 2023, doi: 10.14722/ndss.2023.24457. [CSRankings-Computer security]

[C31]. Ziwei Liu, Feng Lin, Chao Wang, Yijie Shen, Zhongjie Ba, **Li Lu**, Wenyao Xu, Kui Ren, "CamRadar: Hidden Camera Detection Leveraging Amplitude-modulated Sensor Images Embedded in Electromagnetic Emanations," in *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* (*IMWUT*)/*ACM Ubicomp 2023*, vol. 6, no. 4, pp. 173:1-173:25, Cancun, Mexico, Dec. 2022, doi: 10.1145/3569505. [CSRankings-Human-computer interaction]

[C32]. Yijie Shen, Zhe Ma, Feng Lin, Hao Yan, Zhongjie Ba, **Li Lu**, Wenyao Xu, Kui Ren, "FingerFaker: Spoofing Attack on COTS Fingerprint Recognition Without Victim's Knowledge," in *Proceedings of ACM Conference on Embedded Networked Sensor Systems (ACM SenSys 2023)*, pp. 167-180, Istanbul, Turkiye, Nov. 2023, doi: 10.1145/3625687.3625783. [CSRankings-Mobile computing]

[C33]. Zhongjie Ba, Qing Wen, Peng Cheng, Yuwei Wang, Feng Lin, **Li Lu**, Zhenguang Liu, "Transferring Audio Deepfake Detection Capability across Languages," in *Proceedings of ACM Web Conference (ACM WWW 2023)*, pp. 2033-2044, Austin, TX, USA, Apr. 2023, doi: 10.1145/3543507.3583222. [CSRankings-The Web & information retrieval]

[C34]. Hao Kong, **Li Lu**, Jiadi Yu, Yanmin Zhu, Feilong Tang, Yi-Chao Chen, Linghe Kong, Feng Lyu, "Push the Limit of WiFi-based User Authentication towards Undefined Gestures," in *Proceedings of IEEE International Conference on Computer Communications* (*IEEE INFOCOM 2022*), pp. 410-419, London, United Kingdom, May 2022, doi: 10.1109/INFOCOM48880.2022.9796740.

[C35]. Yike Chen, Ming Gao, Yimin Li, Lingfeng Zhang, **Li Lu**, Feng Lin, Jinsong Han, Kui Ren, "Big Brother is Listening: An Evaluation Framework on Ultrasonic Microphone Jammers," in *Proceedings of IEEE International Conference on Computer Communications* (*IEEE INFOCOM 2022*), pp. 1119-1128, London, United Kingdom, May 2022, doi: 10.1109/INFOCOM48880.2022.9796834.

[C36]. Chao Wang, Feng Lin, Tiantian Liu, Ziwei Liu, Yijie Shen, Zhongjie Ba, **Li Lu**, Wenyao Xu, Kui Ren, "mmPhone: Acoustic Eavesdropping on Loudspeakers via mmWave-characterized Piezoelectric Effect," in *Proceedings of IEEE International Conference on Computer Communications* (*IEEE INFOCOM 2022*), pp. 820-829, London, United Kingdom, May 2022, doi: 10.1109/INFOCOM48880.2022.9796806.

[C37]. Hao Kong, **Li Lu**, Jiadi Yu, Yingying Chen, Xiangyu Xu, Feilong Tang, Yi-chao Chen, "MultiAuth: Enable Multi-User Authentication with Single Commodity WiFi Device," in *Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing* (*ACM MobiHoc 2021*), pp.31-40, Shanghai, China, Jul. 2021, doi: 10.1145/3466772.3467032.

[C38]. Yang Bai, Jian Liu, **Li Lu**, Yilin Yang, Yingying Chen, Jiadi Yu, "BatComm: Enabling Inaudible Acoustic Communication with High-throughput for Mobile Devices," in *Proceedings of ACM Conference on Embedded Networked Sensor Systems* (*ACM SenSys 2020*), Yokohama, Japan, Nov. 2020, doi: 10.1145/3384419.3430773. [CSRankings-Mobile computing]

[C39]. Hua Xue, Jiadi Yu, Yanmin Zhu, **Li Lu**, Shiyou Qian, Minglu Li, "WiZoom: Accurate Multipath Profiling using Commodity WiFi Devices with Limited Bandwidth," in *Proceedings of Annual IEEE International Conference on Sensing, Communication, and Networking* (*IEEE SECON 2019*), pp. 1-9, Boston, MA, USA, Jun. 2019, doi: 10.1109/SAHCN.2019.8824859.

[C40]. Liu Liu, Hanlin Yu, Zhongjie Ba, **Li Lu**, Feng Lin, Kui Ren, "PassFace: Enabling Practical Anti-Spoofing Facial Recognition with Camera Fingerprinting," in *Proceedings of IEEE International Conference on Communications* (*IEEE ICC 2021*), pp. 1-6, Montreal, Canada, Jun. 2021, doi: 10.1109/ICC42927.2021.9501053.

[C41]. Yanhua Cao, **Li Lu**, Jiadi Yu, Shiyou Qian, Yanmin Zhu, Minglu Li, "Online Cost-Aware Service Requests Scheduling in Hybrid Clouds for Cloud Bursting," in *Proceedings of the 18th International Conference on Web Information Systems Engineering* (*WISE 2017*), pp. 259-274, Moscow, Russia, Oct. 2017, doi: 10.1007/978-3-319-68783-4_18.

[C42]. Qiang Wu, Jiadi Yu, **Li Lu**, Shiyou Qian, Guangtao Xue, "Dynamically Adjusting Scale of a Kubernetes Cluster Under QoS Guarantee," in *Proceedings of IEEE International Conference on Parallel and Distributed Systems* (*IEEE ICPADS 2019*), pp. 193-200, Tianjin, China, Dec. 2019, doi: 10.1109/ICPADS47876.2019.00037.

[C43]. Ahmad Ali, **Li Lu**, Yanmin Zhu, Jiadi Yu, "An Energy Efficient Algorithm for Virtual Machine Allocation in Cloud Datacenters," in *Proceedings of Conference on Advanced Computer Architecture* (*CCF ACA 2016*), pp. 61-72, Weihai, Shandong, China, Aug. 2016, doi: 10.1007/978-981-10-2209-8_6.

Journal Papers

[J1]. Junhao Wang, **Li Lu***, Hao Kong, Feng Lin, Zhongjie Ba, Kui Ren, "Liquid Crystal Mimics Your Heart: A Physical Spoofing Attack against PPG-based Systems," *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 8628-8642, Aug. 2025. doi: 10.1109/TIFS.2025.3598472. [JCR-Q1]

[J2]. Meng Zhang, **Li Lu***, Yuhan Wu, Zheng Yan, Jiaqi Sun, Feng Lin, Kui Ren, "DroneAudioID: A Lightweight Acoustic Fingerprint-Based Drone Authentication System for Secure Drone Delivery," *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 1447-1461, Jan. 2025. doi: 10.1109/TIFS.2025.3527814. [JCR-Q1]

[J3]. **Li Lu**, Meng Chen, Jiadi Yu, Zhongjie Ba, Feng Lin, Jinsong Han, Yanmin Zhu, Kui Ren, "An Imperceptible Eavesdropping Attack on WiFi Sensing Systems," *IEEE/ACM Transactions on Networking*, vol. 32, no. 5, pp. 4009-4024, Oct. 2024. doi: 10.1109/TNET.2024.3403839. [JCR-Q2]

[J4]. Meng Chen, **Li Lu***, Jiadi Yu, Zhongjie Ba, Feng Lin, Kui Ren, "AdvReverb: Rethinking the Stealthiness of Audio Adversarial Examples to Human Perception," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 1948-1962, Jan. 2024. doi: 10.1109/TIFS.2023.3345639. [JCR-Q1]

[J5]. Hao Kong, **Li Lu***, Jiadi Yu, Yingying Chen, Xiangyu Xu, Feng Lyu, "Towards Multi-User Authentication Using WiFi Signals," *IEEE/ACM Transactions on Networking*, vol. 31, no. 5, pp. 2117-2132, Oct. 2023. doi: 10.1109/TNET.2023.3237686. [JCR-Q2]

[J6]. **Li Lu**, Jiadi Yu, Yingying Chen, Hongbo Liu, Yanmin Zhu, Minglu Li, "Lip Reading-Based User Authentication Through Acoustic Sensing on Smartphones," *IEEE/ACM Transactions on Networking*, vol. 27, no. 1, pp. 447-460, Feb. 2019. doi: 10.1109/TNET.2019.2891733. (Reported by multiple media including IEEE Spectrum, Sohu Tech, etc.) [JCR-Q2]

[J7]. **Li Lu**, Jiadi Yu, Yanmin Zhu, Minglu Li, "A Double Auction Mechanism to Bridge Users' Task Requirements and Providers' Resources in Two-Sided Cloud Markets," *IEEE Transactions on Parallel and Distributed Systems*, vol. 29, no. 4, pp. 720-733, Dec. 2018. doi: 10.1109/TPDS.2017.2781236. [JCR-Q1]

[J8]. **Li Lu**, Jiadi Yu, Minglu Li, "Towards a Real-Time Anti-Theft Method for Mobile Devices Leveraging Acoustic Sensing," *Chinese Journal of Computers*, vol. 43, no. 10, pp. 2002-2018, Oct. 2020. doi: 10.11897/SP.J.1016.2020.02002.

[J9]. **Li Lu**, Jian Liu, Jiadi Yu, Yingying Chen, Yanmin Zhu, Linghe Kong, Minglu Li, "Enable Traditional Laptops with Virtual Writing Capability Leveraging Acoustic Signals," *The Computer Journal*, vol. 64, no. 12, pp. 1814-1831, Dec. 2021. doi: 10.1093/comjnl/bxz153. [JCR-Q3]

[J10]. Jiadi Yu, **Li Lu**, Yingying Chen, Yanmin Zhu, Linghe Kong, "An Indirect Eavesdropping Attack of Keystrokes on Touch Screen through Acoustic Sensing," *IEEE Transactions on Mobile Computing*, vol. 20, no. 2, pp. 337-351, Feb. 2020. doi: 10.1109/TMC.2019.2947468. [JCR-Q1]

[J11]. Hao Kong, **Li Lu**, Jiadi Yu, Yingying Chen, Feilong Tang, "Continuous Authentication through Finger Gesture Interaction for Smart Homes Using WiFi," *IEEE Transactions on Mobile Computing*, vol. 20, no. 11, pp. 3148-3162. May 2020. doi: 10.1109/TMC.2020.2994955. [JCR-Q1]

[J12]. Ziwei Liu, Feng Lin, Zhongjie Ba, **Li Lu**, Kui Ren, "MagShadow: Physical Adversarial Example Attacks via Electromagnetic Injection," *IEEE Transactions on Dependable and Secure Computing*, vol. 22, no. 4, pp. 3307-3323. Jul. 2025. doi: 10.1109/TDSC.2025.3529197. [JCR-Q1]

[J13]. Biyun Sheng, Jiabin Li, Hui Cai, Yiping Zuo, **Li Lu**, Fu Xiao, "mmZeAR: Zero-effort Cross-category ActionRecognition with MmWave Radar," *IEEE Transactions on Mobile Computing*, May 2025. doi: 10.1109/TMC.2025.3573168. [JCR-Q1]

[J14]. Yu Xin, Xiaohang Wang, **Li Lu**, Shuguo Zhuo, Yingtao Jiang, Amit Kumar Singh, Kui Ren, Mei Yang, Kaiwei Wu, "LUFT-CAN: A lightweight unsupervised learning based intrusion detection system with frequency-time analysis for vehicular CAN bus," *Journal of Systems Architecture*, vol. 168, 103567, Sep. 2025. doi: 10.1016/j.sysarc.2025.103567. [JCR-Q1]

[J15]. Liu Liu, Xinwen Fu, Xiaodong Chen, Jianpeng Wang, Zhongjie Ba, Feng Lin, **Li Lu**, Kui Ren, "ACL: Account Linking in Online Social Networks with Robust Camera Fingerprint Matching," *IEEE Transactions on Dependable and Secure Computing*, vol. 22, no. 3, pp. 2925-2942. May 2025. doi: 10.1109/TDSC.2024.3522117. [JCR-Q1]

[J16]. Peng Huang, Yao Wei, Peng Cheng, Zhongjie Ba, **Li Lu**, Feng Lin, Yang Wang, Kui Ren, "Phoneme-Based Proactive Anti-Eavesdropping with Controlled Recording Privilege," *IEEE Transactions on Dependable and Secure Computing*, vol. 22, no. 3, pp. 1924-1940. Oct. 2024. doi: 10.1109/TDSC.2024.3473695. [JCR-Q1]

[J17]. Zhongjie Ba, Bin Gong, Yuwei Wang, Yuxuan Liu, Peng Cheng, Feng Lin, **Li Lu**, Kui Ren, "Indelible “Footprints” of Inaudible Command Injection," *IEEE Transactions on Information Forensics and Security,* vol. 19, pp. 8485-8499, Sep. 2024. doi: 10.1109/TIFS.2024.3459728. [JCR-Q1]

[J18]. Xinyu Zhang, Qingyu Liu, Zhongjie Ba, Yuan Hong, Tianhang Zheng, Feng Lin, **Li Lu**, Kui Ren, "FLTracer: Accurate Poisoning Attack Provenance in Federated Learning," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 9534-9549, May 2024. doi: 10.1109/TIFS.2024.3410014. [JCR-Q1]

[J19]. Feng Lin, Hao Yan, Jin Li, Ziwei Liu, **Li Lu**, Zhongjie Ba, Kui Ren, "PhaDe: Practical Phantom Spoofing Attack Detection for Autonomous Vehicles," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 4199-4214, Mar. 2024. doi: 10.1109/TIFS.2024.3376192. [JCR-Q1]

[J20]. Feng Lin, Chao Wang, Tiantian Liu, Ziwei Liu, Yijie Shen, Zhongjie Ba, **Li Lu**, Wenyao Xu, Kui Ren, "High-quality Speech Recovery Through Soundproof Protections via mmWave Sensing," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 4, pp. 3065-3081, Jul. 2024. doi: 10.1109/TDSC.2023.3322295. [JCR-Q1]

[J21]. Yijie Shen, Feng Lin, Chao Wang, Tiantian Liu, Zhongjie Ba, **Li Lu**, Wenyao Xu, Kui Ren, "MotoPrint: Reconfigurable Vibration Motor Fingerprint via Homologous Signals Learning," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 1, pp. 372-387, Mar. 2023. doi: 10.1109/TDSC.2023.3253507. [JCR-Q1]

[J22]. Ming Gao, Yike Chen, Yimin Li, Lingfeng Zhang, Jianwei Liu, **Li Lu**, Feng Lin, Jinsong Han, Kui Ren, "A Resilience Evaluation Framework on Ultrasonic Microphone Jammers," *IEEE Transactions on Mobile Computing*, vol. 23, no. 2, pp. 1914-1929, Feb. 2023. doi: 10.1109/TMC.2023.3244581. [JCR-Q1]

[J23]. Peng Cheng, Yuexin Wu, Yuan Hong, Zhongjie Ba, Feng Lin, **Li Lu**, Kui Ren, "UniAP: Protecting Speech Privacy with Non-targeted Universal Adversarial Perturbations," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 1, pp. 31-46, Feb. 2023. doi: 10.1109/TDSC.2023.3242292. [JCR-Q1]

[J24]. Yang Bai, **Li Lu**, Jerry Cheng, Jian Liu, Yingying Chen, Jiadi Yu, "Acoustic-based Sensing and Applications: A Survey," *Computer Networks*, vol. 181, pp. 107447:1-107447:19, Nov. 2020. doi: 10.1016/j.comnet.2020. 107447. [JCR-Q1]

[J25]. Yanhua Cao, **Li Lu**, Jiadi Yu, Shiyou Qian, Yanmin Zhu, Minglu Li, "Online Cost-rejection Rate Scheduling for Resource Requests in Hybrid Clouds," *Parallel Computing*, vol. 81, pp. 85-103, Jan. 2019. doi: 10.1016/j.parco.2018.12.003. [JCR-Q3]

[J26]. Cong Shi, **Li Lu**, Jian Liu, Yan Wang, Yingying Chen, Jiadi Yu, "mPose: Environment- and Subject-Agnostic 3D Skeleton Posture Reconstruction Leveraging a Single mmWave Device", *Smart Health/IEEE/ACM CHASE*, vol. 23, pp. 100228:1-100228:14, Nov. 2021. doi: 10.1016/j.smhl.2021.100228. (Invited Paper of *IEEE/ACM CHASE 2021*)

Posters

[CP1]. Meng Chen, **Li Lu***, Jiadi Yu, Yingying Chen, Zhongjie Ba, Feng Lin, Kui Ren, "A Non-intrusive and Adaptive Speaker De-Identification Scheme Using Adversarial Examples," in *Proceedings of the 28th Annual International Conference on Mobile Computing and Networking* (*ACM MobiCom 2022*), pp. 853-855, Sydney, Australia, Oct. 2022. doi: 10.1145/3495243.3558260. [CSRankings-Mobile computing]

[CP2]. Yang Bai, Jian Liu, Yingying Chen, **Li Lu**, Jiadi Yu, "Poster: Inaudible High-throughput Communication Through Acoustic Signals," in *Proceedings of the 25th Annual International Conference on Mobile Computing and Networking* (*ACM MobiCom 2019*), pp. 79:1-79:3, Los Cabos, Mexico, Oct. 2019. doi: 10.1145/3300061.3343405. [CSRankings-Mobile computing]

FUNDING

- Software-Hardware Collaborated Unknown Cyber Attacks Autonomous Detection Techniques for Intelligent Driving Systems, National Key R&D Program of China, 2023.12-2026.11, PI.
- Research on Novel Black-box Adversarial Technique on Speech Language Model, National Natural Science Foundation of China, 2026.01-2029.12, PI.
- Research on Enhancing Voiceprint Authentication by Sensing Vocal Tract Leveraging Acoustic Signals, National Natural Science Foundation of China, 2022.01-2024.12, PI.
- Research on Real-time Voice Anonymization Techniques in Physical Domain, Natural Science Foundation of Zhejiang Province, 2024.01-2026.12, PI.
- Acoustic-based Voiceprint Anti-spoofing Techniques, ZJU-Huawei Joint Lab, 2021.09-2022.09, PI.
- Large Language Model Framework for Verticals, ZJU-Ant Joint Lab, 2025.01-2025.12, PI.
- Research on Native Multi-modality Security Framework OmniGuard, ZJU-Alibaba AI Safaty and Security Joint Lab, 2025.07-2026.06, PI.
- Research on Universal Adversarial Example Generation for Voiceprint Authentication, Fundamental Research Funds for the Central Universities, 2021.01-2023.12, PI.

TEACHING

- Computer Systems II, Undergraduate teaching reform course for information security and Turing class, CS2052M/21121840, Fall-Winter 2021-2025.
- Computer Systems I, Undergraduate teaching reform course for information security and Turing class, CS1028M/21121830, Spring-Summer 2021-2025.
- Wireless and IoT Security, Graduate, 2124096001, Fall-Winter 2020-2024.
- Frontier Techniques and Research Methodology in Cyber Science, Graduate, 2102001001, Spring-Summer 2021-2022.
- Foundations of Wireless and IoT Security, Undergraduate, CS3193M/21191930, Spring-Summer 2021-2025.

AWARDS

- Notable Reviewer, USENIX Security, 2025.
- Best Paper Award, IEEE ICC, 2025.
- Excellent Reviewer of IEEE Transactions on Network Science and Engineering at 2023, IEEE Communications Society, 2024.

- Distinguished Member of the INFOCOM 2024 Technical Program Committee, IEEE Communications Society, 2024.
- ACM China SIGAPP Chapter Rising Star Award, ACM China, 2023.
- Distinguished Service Award, IEEE GreenCom, 2023.
- Outstanding Collaboration Award, Huawei-ZJU Joint Laboratory on System and Data Security, 2023.
- 3rd Award of National College Student Information Security Contest (Advisor), Education Steering Committee of the Ministry of Education for the Major of Cyber Science, 2023.
- Best Poster Runner-up Award, ACM MobiCom, 2022.
- Shanghai Computer Society Doctoral Dissertation Award Nominations, Shanghai Computer Society, 2020.
- ACM China SIGAPP Chapter Doctoral Dissertation Award, ACM China SIGAPP, 2020.
- Outstanding Graduate of Shanghai, Shanghai Education Committee, 2020.
- First Runner-up Poster Award, ACM MobiCom, 2019.
- Travel Grant of Global Young Scientist Summit of Singapore, National Research Foundation, 2019.
- Joint Ph.D. Training Grant, China Scholarship Council, 2018.
- National Scholarship for Doctoral Students, Ministry of Education of the People's Republic of China, 2018, 2019.
- Outstanding Graduate, Xi'an Jiaotong University, 2015.
- Excellent Undergraduate Student, Xi'an Jiaotong University, 2012-2014.
- National Encouragement Scholarship, Xi'an Jiaotong University, 2012, 2014.

PROFESSIONAL SERVICES

- Academic Organization Service: Executive Committee Member in China Computer Federation Technical Committee on Pervasive Computing (CCF TCPC), Data Governance Development Committee, and Technical Committee on Internet of Things (CCF TCIoT)

  Member of IEEE Vehicular Technology Society (VTS) Technical Committee on Autonomous Vehicles

  Member of IEEE Computer Society (CS) Technical Community on Computer Communications (TCCC) and Security and Privacy (TCSP)

  Member of IEEE Communications Society (ComSoc) Technical Committees on Internet of Things, Ad Hoc & Sensor Networks (AHSN TC) and Signal Processing and Computing for Communications (SPCC TC)

  Deputy Secretary-general of Technical Committee in Zhejiang Cyber Space Security Association (2021-2024)
- Editorial Board Member: Associate Editor of IEEE Transactions on Information Forensics and Security
- Academic Events Service: Session Chair of PCC 2024 at CCF HHME 2024, Moderator of FISITA Intelligent Safety Conference 2025 Cybersecurity Track
- Technical Program Committee: USENIX Security 2025-2026, IEEE INFOCOM 2022-2026, AAAI 2026, IEEE/ACM IWQoS 2021, 2023-2025, IEEE ICDCS 2022-2023, USENIX VehicleSec 2025, IEEE AIoTSys 2025, IEEE TrustCom 2024-2025, IEEE MSN 2024, IEEE ICPADS 2019, 2022-2023, IEEE Metaverse 2023, IEEE GreenCom 2023-2024, CCF DPCS 2023
- Reviewer: IEEE Transactions on Information Forensics and Security, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Mobile Computing, IEEE/ACM Transactions on Networking, IEEE Transactions on Services Computing, IEEE Transactions on Computers, Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, ACM MM 2023-2024 [CCF-A]

  ACM Computing Surveys, Computer Science Review, IEEE Transactions on Network Science and Engineering, IEEE Transactions on Vehicular Technology, IEEE Network, IEEE Internet of Things

Journal, Expert Systems with Applications, Automotive Innovation, Computer Methods and Programs in Biomedicine, ACM Transactions on Computing for Healthcare [JCR-Q1]

ACM Transactions on Sensor Networks, ACM Transactions on Embedded Computing Systems, IEEE Transactions on Multimedia, Computer Networks, Pattern Recognition, Neural Networks, Knowledge-based Systems, IEEE ICASSP 2023-2024 [CCF-B]

IEEE Transactions on Sustainable Computing, Neurocomputing, Journal of Information Security and Applications, Pervasive and Mobile Computing, ISCA Interspeech 2025, IEEE IJCNN 2025, IEEE ICC 2017 [CCF-C]

Chinese Journal of Electronics, Chinese Journal of Computers, CCF HHME 2024-2025, CCF CWSN 2023-2025

Smart Health, Journal of Cloud Computing, IEEE Access, Sensors, Journal of Cybersecurity and Privacy

- Membership: China Computer Federation (CCF) Senior Member
  Association of Computing Machinery (ACM) Professional Member
  Institute of Electrical and Electronics Engineers (IEEE) Member
  Chinese Institute of Electronics (CIE) Member