

Email: yangxiaosec@gmail.com

Phone: 734-846-0743

Office: 233 James F. Hardymon Building, 301 Rose St, Lexington, KY 40508

Homepage: <https://yang-sec.github.io/>

EDUCATION	Virginia Polytechnic Institute and State University , Blacksburg, VA • Ph.D. in Computer Engineering Advisor: Prof. Wenjing Lou Dissertation: <i>Blockchain and Distributed Consensus: From Security Analysis to Novel Applications</i> University of Michigan , Ann Arbor, MI • M.S. in Electrical Engineering-Systems Shanghai Jiao Tong University (SJTU) , Shanghai, China • B.S.E. in Information Engineering • (Secondary) B.Econ. in Finance	09/2017 – 05/2022 09/2015 – 04/2017 09/2010 – 06/2014
RESEARCH INTERESTS	<input type="checkbox"/> Security and Privacy in Distributed Systems and Networking – Blockchain, Consensus Protocol, P2P Network, Fault Tolerance – Decentralized Architectures and Applications, Identity/Data Management <input type="checkbox"/> Security and Privacy in Cyber-physical Infrastructure – Dynamic Spectrum Sharing (Fault Tolerance, Privacy) – Next-Gen Mobile Networks and IoT (Identity and Data Privacy, AI Security) – Automotive Networks (Secure Communication, Intrusion Detection)	
PROFESSIONAL EXPERIENCE	Assistant Professor Department of Computer Science University of Kentucky Graduate Research Assistant Department of Electrical and Computer Engineering Virginia Tech Research Intern Mathematics and Modeling Department Schlumberger-Doll Research	08/2022 – Present 09/2017 – 05/2022 05/2016 – 08/2016
BOOK CHAPTERS	1. Distributed Consensus Protocols and Algorithms Y. Xiao , N. Zhang, J. Li, W. Lou, Y. T. Hou <i>Blockchain for Distributed Systems Security</i> , Wiley & Sons, 2019	
JOURNAL PUBLICATIONS	1. MANDA: On Adversarial Example Detection for Network Intrusion Detection System N. Wang, Y. Chen, Y. Xiao , Y. Hu, W. Lou, Y. T. Hou <i>Accepted by IEEE Transactions on Dependable and Secure Computing (TDSC)</i> . 2. Decentralized Spectrum Access System: Vision, Challenges, and a Blockchain Solution Y. Xiao , S. Shi, W. Lou, C. Wang, X. Li, N. Zhang, Y. T. Hou, J. H. Reed <i>In IEEE Wireless Communications</i> , 2022. 3. A Survey of Distributed Consensus Protocols for Blockchain Networks Y. Xiao , N. Zhang, W. Lou, Y. T. Hou	

In IEEE Communications Surveys & Tutorials (COMST), 2020.

4. [Challenges and New Directions in Securing Spectrum Access Systems](#)

S. Shi, **Y. Xiao**, W. Lou, C. Wang, X. Li, Y. T. Hou, J. H. Reed

In IEEE Internet of Things Journal (IOT-J), 2021.

5. [Offloading Decision in Edge Computing for Continuous Applications Under Uncertainty](#)

W. Chang, **Y. Xiao**, W. Lou, G. Shou

In IEEE Transactions on Wireless Communications (TWC), 2020.

6. [Performance Analysis of Random Access Network with Post-backoff](#)

C. Bu, **Y. Xiao**, T. Ye, P. Wu, X. Zhang, J. Wu

In Telecommunications Science, 2016.

CONFERENCE
PUBLICATIONS

1. [CANShield: Signal-based Intrusion Detection for Controller Area Networks](#)

M. H. Shahriar, **Y. Xiao**, P. Moriano, W. Lou, Y. T. Hou

Accepted by the 9th Embedded Security in Cars (escar) USA conference, 2022.

2. [FLARE: Defending Federated Learning against Model Poisoning Attacks via Latent Space Representations](#)

N. Wang, **Y. Xiao**, Y. Chen, Y. Hu, W. Lou, Y. T. Hou

*Accepted by the 17th ACM ASIA Conference on Computer and Communications Security (AsiaCCS), 2022.
(AR=18.4%)*

3. [Session Key Distribution Made Practical for CAN and CAN-FD Message Authentication](#)

Y. Xiao, S. Shi, N. Zhang, W. Lou, Y. T. Hou

In the Annual Computer Security Applications Conference (ACSAC), 2020. (AR=23.2%)

4. [PrivacyGuard: Enforcing Private Data Usage Control with Blockchain and Off-chain Contract Execution](#)

Y. Xiao, N. Zhang, J. Li, W. Lou, Y. T. Hou

In the 25th European Symposium on Research in Computer Security (ESORICS), 2020. (AR=19.7%)

5. [Modeling the Impact of Network Connectivity on Consensus Security of Proof-of-Work Blockchain](#)

Y. Xiao, N. Zhang, W. Lou, Y. T. Hou

In the 2020 IEEE International Conference on Computer Communications (INFOCOM), 2020. (AR=19.8%)

SUBMITTED
PAPERS

1. [DecenTruth: A Decentralized and Truth Discovering Data Feed for Blockchain DApps](#)

Y. Xiao, N. Zhang, W. Lou, Y. T. Hou

2. [BD-SAS: Enabling Dynamic Spectrum Sharing in Low-trust Environment](#)

Y. Xiao, S. Shi, W. Lou, C. Wang, X. Li, Y. T. Hou, J. H. Reed

3. [Differentially Private Federated Meta-Learning](#)

N. Wang, **Y. Xiao**, Y. Chen, N. Zhang, W. Lou, Y. T. Hou

4. [BRENTS: Byzantine Resilient Network Time Synchronization](#)

S. Shi, **Y. Xiao**, C. Du, W. Lou, Y. T. Hou

TEACHING
EXPERIENCE

Guest Lectures on Cryptocurrency & Blockchain, Virginia Tech

– CS 5560: Fundamentals of Information Security

03/2019

Graduate Teaching Assistant, Virginia Tech

– ECE 2534: Microcontroller Programming and Interfacing

Fall 2017

Undergraduate Tutor, SJTU

– CS 358: Data Structure

Fall 2014

ACADEMIC

Journal and Conference Reviewer

SERVICES	– IEEE International Conference on Computer Communications (INFOCOM)	2021
	– IEEE/ACM Transactions on Networking (TON)	2020, 2021
	– IEEE Internet of Things Journal (IOT-J)	2020, 2021
	– International Journal of Intelligent Systems (INT2)	2021
	– IEEE Transactions on Dependable and Secure Computing (TDSC)	2019, 2020
	– Digital Communications and Networks (DCAN)	2019, 2020
	– EAI International Conference on Security and Privacy in Comm. Netw. (SecureComm)	2019
	– Future Generation Computer Systems (FGCS)	2018, 2019
Panelist		
	2019 Secure and Trustworthy CyberSpace (SaTC) PI Meeting Undergraduate Track, NSF	10/2019
	– Panel: What to Expect from Grad School	
Conference Organization		
	IEEE Conference on Communications and Network Security (CNS)	
	– Web Chair, CNS 2020, virtual	09/2019 – 07/2020
	– Student Volunteer, CNS 2019, Washington DC	06/2019
TALKS, POSTERS	Session Key Distribution Made Practical for CAN and CAN-FD Message Authentication	
	– Invited talk, <i>Learning from Authoritative Security Experiment Results (LASER) Workshop</i>	12/2020
	A Layered View towards Blockchain: From Consensus Security to Smart Contract Application	
	– Invited talk, <i>CS Graduate Seminars</i> , Virginia Tech	11/2020
	Enforcing Private Data Usage Control with Blockchain and Attested Off-chain Contract Execution	
	– Poster, 2019 SaTC PI Meeting, NSF, Alexandria, VA	04/2019
AWARDS	A Graph Random-Walk Based Sampling Algorithm for Load Balancing in Cloud Systems	
	– Poster, <i>6th Midwest Workshop on Control and Game Theory</i> , Ann Arbor, MI	04/2017
	INFOCOM 2020 Student Travel Grant	2020
	– Awarded by the INFOCOM 2020 organizing committee	
	BitShares Graduate Fellowship	2019
	– Awarded by Virginia Tech CS Department, funded by BitShares Inc.	
	Completion of the Elite Engineer Cultivation Program in Information Engineering	2014
	– Certified by Shanghai Jiao Tong University	
	First Prize in the 28th National Physics Contest of College Students (Shanghai Division)	2011
	– Awarded by Shanghai Physics Society	
PROFESSIONAL MEMBERSHIPS	– IEEE Graduate Student Member, Communications Society, Computer Society	11/2017 – Present
	– ACM Professional Member	10/2020 – Present
CODING SKILLS	C/C++, Python, MATLAB, HTML, C#	