Yang Xiao

Updated July 11, 2022

Email: xiaoy@vt.edu
Phone: 734-846-0743
Address: 2230 George C Marshall Dr Apt 600, Falls Church, VA 22043
Homepage: https://yang-sec.github.io/

Education

Virginia Polytechnic Institute and State University, Blacksburg, VA — 09/2017 – 05/2022

- Ph.D. in Computer Engineering @ ECE Department
  Advisor: Prof. Wenjing Lou
  Dissertation: *Blockchain and Distributed Consensus: From Security Analysis to Novel Applications*
  Committee: Professors Wenjing Lou, Thomas Hou, Luiz DaSilva, Jeffrey Reed, Ning Zhang

University of Michigan, Ann Arbor, MI — 09/2015 – 04/2017

- M.S. in Electrical Engineering-Systems @ EECS Department

Shanghai Jiao Tong University (SJTU), Shanghai, China — 09/2010 – 06/2014

- B.S.E. in Information Engineering @ School of Electronic Information and Electrical Engineering
- B.Econ. in Finance @ Antai College of Economics and Management

Research Interests

□ **Blockchain, Security and Privacy in Distributed Systems and Networking**
  - Consensus Protocol, P2P Network, Fault Tolerance
  - Decentralized Architectures and Applications, Identity/Data Management

□ **Security and Privacy in Cyber-physical Systems**
  - Automotive Networks (Secure Communication, Intrusion Detection)
  - Intelligent IoT (Distributed and Robust Machine Learning, Privacy)

Research Experience

Graduate Research Assistantship, Virginia Tech — 09/2017 – 05/2022
(Affiliated with the Complex Networks and Security Research (CNSR) Lab)

□ Blockchain, Consensus, Distributed Systems and Networking
  - Authored a book chapter and a comprehensive survey & tutorial on blockchain consensus protocols and their security properties (received 300+ citations since 2020 per Google Scholar);
  - Performed a modeling analysis on security of Nakamoto Consensus from a networking perspective;
  - Developed PrivacyGuard, a privacy-preserving data access and usage control architecture leveraging blockchain smart contract and trusted execution environment (TEE);
  - Developed BD-SAS, a blockchain-based decentralized spectrum access system, for policy-compliant dynamic spectrum sharing in low-trust 5G/nextG networks;
  - Developed DecenTruth, a decentralized data feed system harmonizing Byzantine fault-tolerant (BFT) consensus and truth discovery (TD) to bring truthful external data into decentralized applications;
  - Working on a cross-layer analysis to find security bottlenecks of blockchain networks.

□ Automotive Security
  - Developed session key establishment schemes for Controller Area Network (CAN) and CAN Flexible Data-Rate (CAN FD) buses for bootstrapping secure onboard communication efficiently;
  - Collaborating on ML-based real-time intrusion detection systems (IDS) for CAN bus.

□ Distributed Machine Learning Security and Privacy
  - Co-authored a robust aggregation scheme to protect federated learning from model poisoning attack;
  - Co-developed federated meta-learning algorithms with differential privacy for intelligent IoT;
  - Working on extending PrivacyGuard to accommodate federated/distributed learning tasks, breaking down information silos among mutually distrustful parties.

Directed Study, University of Michigan, Ann Arbor — 09/2016 – 04/2017

(Mentored by Prof. Vijay G. Subramanian)

□ Load Balancing in Cloud Systems
- Applied queuing theory and distributed sampling to load balancing algorithm design;
- Implemented a random walk-based sampling scheme of good throughput and queuing performance.

Research Internship, Schlumberger-Doll Research, Cambridge, MA 05/2016 – 08/2016
(Affiliated with the Mathematics and Modeling Department)

□ Robust Telemetry Systems
- Developed ML-based channel equalization/tracking techniques for a telemetry system;
- Investigated secure and robust clock synchronization technologies.

Bachelor Thesis, SJTU, China 01/2014 – 12/2014
(Mentored by Prof. Tong Ye and Prof. Tony T. Lee)

□ Performance Simulation of the IEEE 802.11 DCF Protocol
- Focused on queuing-theoretical analysis (throughput, delay, stability) on random access networks;
- Started from the simpler ALOHA protocol, extended to CSMA/CA with post back-off (DCF feature);
- Performed event-driven simulations to validate analytical results.

Book Chapters

1. Distributed Consensus Protocols and Algorithms
   Y. Xiao, N. Zhang, J. Li, W. Lou, Y. T. Hou
   Blockchain for Distributed Systems Security, 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
   *Accepted by IEEE Transactions on Dependable and Secure Computing (**TDSC**).*
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
   In IEEE Wireless Communications, 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 Services

Journal and Conference Reviewer
- 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, *Learning from Authoritative Security Experiment Results (LASER) Workshop* — 12/2020

A Layered View towards Blockchain: From Consensus Security to Smart Contract Application

- Invited talk, *CS Graduate Seminars*, 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

A Graph Random-Walk Based Sampling Algorithm for Load Balancing in Cloud Systems

- Poster, *6th Midwest Workshop on Control and Game Theory*, Ann Arbor, MI 04/2017

Awards

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#