Shengping Bi

+1 (336) 709 8327 | sbi082796@gmail.com | https://linkedin.com/in/shengping-bi-792476192

Education

4.00/4.0 **PhD in Computer Science**, *University of North Texas* | Texas, USA *2024-26*
3.50/4.0 **PhD in Software and Information System**, *UNC at Charlotte* | North Carolina, USA *2023-23*
3.76/4.0 **PhD in Computer Science**, *New Mexico State University* | New Mexico, USA *2021-23*
3.55/4.0 **MS in Computer Engineering**, *North Carolina State University* | North Carolina, USA *2019-20*
3.86/4.0 **BS in Electrical Engineering**, *North Carolina A&T State University* | North Carolina, USA *2017-19*
3.05/4.0 **BS in Electrical Engineering**, *Henan Polytechnic University* | Henan, China *2015-17*

Research Interests

Network Security, Web Security, Wireless Networking and Communication, Machine Learning for Cybersecurity, Adversarial Machine Learning, and IoT Security

Publications

- Tao Hou*, Shengping Bi*, Tao Wang, Zhuo Lu, Yao Liu, Satyajayant Misra, and Yalin Sagduyu (The first two authors are co-first authors). "MUSTER: Subverting User Selection in MU-MIMO Networks." (IEEE INFOCOM'22), Virtual Conference, 2022.
- Shengping Bi, Tao Hou, Tao Wang, Yao Liu, Zhuo Lu, and Qingqi Pei. "DyWCP: Dynamic and Lightweight Data-Channel Coupling towards Confidentiality in IoT Security." (ACM WiSec'22), San Antonio, Texas, 2022.
- Tao Hou, Shengping Bi, Mingkui Wei, Tao Wang, Zhuo Lu, and Yao Liu. "When Third-Party JavaScript Meets Cache: Explosively Amplifying Security Risks on the Internet." (IEEE CNS'22), Austin, Texas, 2022.
- Hamidah Alanazi, Shengping Bi, Tao Wang, and Tao Hou. "Exquisite Feature Selection for Machine Learning Powered Probing Attack Detection." (IEEE ICC'23), Rome, Italy, 2023.
- Hamidah Alanazi, Shengping Bi, Tao Wang, and Tao Hou. "Adaptive Feature Engineering via Attention-Based LSTM Towards High Performance Reconnaissance Attack Detection." (IEEE MILCOM'23), Boston, Massachusetts, 2023.

Skills

Programming	Python, C/C++, Java, System Verilog, LaTeX, HTML, Socket Programming.
Software	GNU Radio, Matlab, Wireshark, Modelsim, Cadence (Virtuoso, Calibre, Hspice).
Python Basic Package	Scikit-learn, Numpy, Matplotlib, Pandas, Tensorflow, Keras, Pytorch, Seaborn, Scipy, Pyshark.
Machine Learning Model	Decision Tree, Random Forest, SVM, CNN, RNN, XGBoost, Logistic Regression, Naïve Bayes, LSTM, Attention, K-nearest Neighbors.
Spoken Language	Mandarin Chinese, English.

Projects

Real-time Network Feature Extraction Tool *May 2022 - Now*

Research Project

- Developed an advanced packet- and flow-based network security data extraction tool to collect high-volume network threats trends, patterns and anomalies for the enhanced intrusion detection system analysis.
- Designed a new network flow identification technique by using size the adjustable packet cache to store the Markov chain-based traffic flows, enabling the real-time flow feature extraction.
- Implemented techniques to resist Adversarial Machine Learning attacks, improving the robustness of security systems by distinguishing between reliable and susceptible features.

Securing the NextG Wireless Communication via Strategic Deception *Aug 2021 - May 2024*

Research Project

- Developed a defense system to secure NextG wireless communications from cooperative known-plaintext eavesdropping.
- Innovated Channel Masque to obscure genuine channels and deliver fabricated information to eavesdroppers.
- Implemented and evaluate Message Obfuscation, protecting genuine messages by delivering fake information.

Adaptive Feature Engineering via Attention-based LSTM towards High Performance Reconnaissance Attack Detection *Nov 2022 - June 2023*

Research Project

- Developed a self-adaptive feature selection for identifying most relevant features and removing the redundant features to reduce the computational overhead and improve the training efficiency.
- Developed a lightweight attention-based LSTM to find the temporal dependency of reconnaissance behaviors and effectively characterize the packet correlations of incoming traffics in feature learning.
- Conducted extensive validation of detection models across multiple datasets (e.g., KDDCUP99, NSL-KDD, UNSW-NB15) and customized real-world network testbeds, significantly improving the accuracy and efficiency of reconnaissance attack identification.

Exquisite Feature Selection for Machine Learning Powered Probing Attack Detection *June 2022 - Nov 2022*

Research Project

- Developed an efficient feature correlation analyzer to measure the correlation between two features and remove highly correlated features.
- Developed an optimized coarse-grain feature selection through mutual information analysis and feature importance ranking to improve model training efficiency and detection precision.
- Developed a novel fine-grain feature refinement using LSTM, enhancing the detection of network probing attacks by analyzing temporal and spatial correlations among packets.

When Third-Party JavaScript Meets Cache: Explosively Amplifying Security Risks on the Internet *Jan 2022 - June 2022*

Research Project

- Proved the ability to mitigate security risks and optimize performance through comprehensive third-party JavaScript analysis.
- Enhanced web security by identifying and rectifying vulnerabilities in third-party script inclusion and caching practices.
- Applied a groundbreaking study on third-party JavaScript, impacting the security strategies of over 824,290 websites.

Dynamic and Lightweight Data-Channel Coupling towards Confidentiality in IoT Security *Aug 2021 - Feb 2022*

Research Project

- Developed and implemented an encryption scheme enhancing IoT security by leveraging the additive features of wireless channels to achieve high secrecy with minimal computational resources.
- Applied a comprehensive study on lightweight encryption methods for IoT devices, focusing on practical applications of one-time pad encryption without key negotiation.
- Demonstrated the design and experimentation of a dynamic channel cipher and channel poisoning techniques to thwart eavesdropping in wireless communications, ensuring robust confidentiality in critical IoT applications.

Subverting User Selection in MU-MIMO Networks *Jan 2021 - Aug 2021*

Research Project

- Developed a system to analyze and exploit vulnerabilities in MU-MIMO networks, using a combination of Recurrent Neural Networks and Monte Carlo Tree Search to reverse-engineer user selection algorithms and predict potential attack vectors, enhancing proactive threat detection capabilities.
- Implemented advanced attack strategies targeting network throughput and user fairness, demonstrating the ability to subvert critical network operations through strategic manipulation of channel state information.

LSTM Cell Neural Network Gate ASIC Design *August 2020 - December 2020*

Course Project

- Designed a single Long Short Term Memory unit file interfaced with ROM, SRAM and Testbench.
- Checked the design by using Modelsim, Synopsys and completed synthesis run. And using pipeline for clock cycle optimization to shorten the clock cycle and minimize area.

Cache & Memory Hierarchy Design *August 2020 - December 2020*

Course Project

- Implemented a flexible cache and memory hierarchy simulator and use it to compare the performance, area, and energy of different memory hierarchy configurations, using a subset of the SPEC-2000 benchmark suite.
- Used C++ to design a generic cache module that can be used at any level in a memory hierarchy.

16 bit (4x4) Synchronous CAM Design *Jan 2020 - April 2020*

Course Project

- Used FreePDK15nm process design kit to design CAM bitcell, Searchline & Bitline Driver, Priority Encoderand passed DRC & LVS check.
- Measured the area of the bounding box around the entire layout and optimize the design for the minimum energy-delay-area product (EDA).

CMOS instrumentation amplifier *August 2019 - December 2019*

Course Project

- Designed the bias module, amplification module and output buffer module in a single operational transconductance amplifier with Cadence.
- Assembled individual OTA into an instrument amplifier and verify gain range, 3dB bandwidth, common mode rejection ratio based on project specification.

Experiences

Teaching & Researching Assistant (University of North Texas) *Jan 2024 - Now*

- TA for Data Structures and Algorithms.
- Worked on Machine Learning-based network intrusion detection, Adversarial machine learning, NextG networks security.

Teaching & Researching Assistant (University of North Carolina at Charlotte) *Aug 2023 - Dec 2023*

- TA for Network and Info Security.
- Worked on Network security protocols, Intrusion detection, Traffic scanning.

Teaching & Researching Assistant (New Mexico State University) *Jan 2021 - Aug 2023*

- TA for Object Oriented Programming, Introduction to Data Structures, Computer Networks
- Work on Network-attack (DDoS, Probing) Mitigation, IDS invasion & avoidance, Network (IoT, 5G) performance improvement.

Honors

2022	**Student Travel Grant of ACM WiSec 2022 ,** New Mexico State University, New Mexico	*United States*
2022	**Student Travel Grant of INFOCOM 2022 ,** New Mexico State University, New Mexico	*Virtual Conference*
2019	**Certificate of Outstanding Academic Achievement ,** North Carolina A&T State University, North Carolina	*United States*
2017	**Sun Yueqi Scholarship for Outstanding Student ,** Henan Polytechnic University, Henan	*China*