

EDUCATION

M.S. in Electrical and Computer Engineering, Duke University. GPA: 3.43 09/2015 – present

M.S. in Software reliability engineering (Industrial Engineering), BeiHang University (BUAA), Beijing, China
GPA: 3.60 09/2012 – 01/2015

Bachelor in Engineer, Detection Guidance and Control Techniques (Electrical Engineering), Northwestern
Polytechnic University, China. GPA: 3.40 09/2008 – 07/2012

PROFESSIONAL EXPERIENCE AND PROJECT

Network anomaly detection by machine learning models JASK AI Lab, San Francisco, CA

Data science intern 05/2017 – present

- Responsible for designing and developing machine learning framework by **Python and Scala**, including file parsing module (Json/log files), feature engineering modules of different types of traffic data (feature hashing, feature encoding etc.), classifier module (random forest, SVM and deep neural network etc.) and data visualization module. The current project is to detect beaconing. Our model has high detection accuracy (**92.9%**) and low false positive rate (**4.3%**), which has been added to the production now.

Using deep learning model to analyze malicious intrusion Symantec, mountain view, CA

Data science intern 07/2016 – 08/2016

- Implemented the deep belief network, deep neural network algorithm by **Python and R** to detect host state (secure or not) in Symantec. The result shows that Deep Belief Network (DBN) performs much better than other algorithms and is **6 times** more effective than the current rule-based system.
- Due to its effectiveness, the DBN based compromised host detection system has been **put into practice in the company**. **The paper related to this project is accepted** to IEEE Conference on Communications and Network Security (CNS 2017)

Using GA-HMM to Evaluate Hosts Risks Symantec, mountain view, CA

Software engineer intern 05/2016 – 07/2016

- Design and implement the Genetic Algorithm Hidden Markov Model model algorithm by **Python and R** to score host by analyzing sequence of its related alerts.

Attack Countermeasure Tree Modeling Tool for SHARPE Duke University, Durham, NC

Chief software engineer and researcher, sponsored by NSF CNS 04/2016 - 01/2017

- Responsible for implementation of attack countermeasure tree (ACT) modeling package for Sharpe.
- Responsible for GUI design by **Java** and implementation of ACT tool by Java and modeling engine implementation by **C** which is related to lexical and grammar analysis (Lex, Yacc).

Implementation of enhanced algorithm to compute mean time to security failure into Symbolic Hierarchical Automated Reliability and Performance Evaluator Duke University, Durham, NC

Chief software engineer 09/2016 – 10/2016

- Implemented the topological sort based mean time to security failure computation algorithm by **C**. The new algorithm is 200 times faster than the old one.

Software Vulnerability and Moving Target Defense Duke University, Durham, NC

Chief Researcher, sponsored by NSF CNS 09/2015 – 12/2016

- Conduct the research which focuses on security failures caused by vulnerabilities at operational phase as opposed to system reliability. The research involves vulnerability classification, exploitation of security vulnerability, identification of effective environmental triggering factor, stochastic modeling of network system with MTD considering optimized security mitigation strategy.
- Responsible for fundamental theory, experiment and software implementation of vulnerability classification and attack repository module by C.

Reliability Analysis of Fault-tolerance Software Systems Considering Correlated Component Failures

Project Assistant Director and Chief Researcher

Beihang University, Beijing, China

03/2014 – 12/2014

- Led a team to design and develop the tool for assessing the architecture-based software reliability considering correlated failures by discrete time Markov model.
- Responsible for the theory on which the tool is based, the function allocation of the tool, the development of core algorithm to assess the reliability of the software by **Matlab**, and the development of part of the module of correlation extraction by C.

KEY SKILLS AND COMPETENCIES

- Good communicator and cooperator.
- Experienced in programming with Python, R, C, C++ and Java.
- Familiar with processing data using Excel, SQL and linux, Windox OS.
- Good understanding of knowledge about Mathematics Probability and Statistics.

SELECTED PAPERS

- Wangyan (Charles) Feng, Shuning Wu, **Xiaodan Li**, Kevin Kunkle, *A Deep Belief Network based Machine Learning System for Risky Host Detection*, IEEE Conference on Communications and Network Security (CNS 2017). (Accepted) (Cooperated with data science group from Symantec)
- **Xiaodan Li**, Xiaolin Chang, Jose M. Martinez, John A. Board, Kishor S. Trivedi, *A Novel Approach for Software Vulnerability Classification*, 2017 Annual Reliability and Maintainability Symposium (RAMS), January 2017, Orlando, Florida (published).
- Fangyun Qin, Zheng Zheng, **Xiaodan Li**, Yu Qiao and Kishor S. Trivedi, *An Empirical Investigation of Fault Triggers in Android Operating System*, 2017 22th Pacific Rim International Symposium on Dependable Computing (PRDC'17). IEEE, 2017. (Accepted)
- Rodriguez, R.J., Xiaolin Chang, **Xiaodan Li**, and Kishor S. Trivedi, *Survivability Analysis of a Computer System under an Advanced Persistent Threat Attack*. June 2016, In book: Graphical Models for Security, pp.134-149 (published).
- Xiaolin Chang, Zhenjiang Zhang, **Xiaodan Li**, and Kishor S. Trivedi, *Model-based Survivability Analysis of a Virtualized System. Local Computer Networks*, 2016. *Proceedings. LCN 2016. 41th Annual IEEE Conference on.* IEEE, 2016 (published).
- **Xiaodan Li**, YIN Yong-feng, *A Unified Framework for Software Coupling Measurement*, 2014 2nd International Conference on Software Engineering, Knowledge Engineering and Information Engineering (EI) (published).
- **Xiaodan Li**, YIN Yong-feng, Lance Fiondella, Yi-bin Zhou. *Software reliability analysis considering correlated component failures with coupling measurement framework*, Journal of Systems Engineering and Electronics (SCIE) (published).
- **Xiaodan Li**, YIN Yong-feng, Lance Fiondella. *Reliability and Performance Analysis of Architecture-Based Software Implementing Restarts and Retries Subject to Correlated Component Failures*, International Journal of Software Engineering and Knowledge Engineering (SCIE) (published).