YI ZENG

(858)-952-2135 ◇ y4zeng@eng.ucsd.edu
Google Scholar ◇ Github ◇ LinkedIn
Personal Webpage

SUMMARY

Currently pursuing a master's degree in machine learning and data science under the ECE department at the University of California, San Diego. Expected graduating around January 2021. I value myself as a self-motivated and innovative young researcher with great interest and outstanding experience in **Security-concerned & Trustworthy Deep Learning** algorithms.

Beforehand, with the help of Deep Learning, scenarios including **Network Traffic Classification and Intrusion Detection**, **Mobile Ad-hoc Network Security**, were studied. I am currently researching on acquiring sound inference results for Deep Learning models against **Adversarial Learning** and **Backdoor Learning**.

EDUCATION

University of California, San Diego (#21 Best Global Univ.–U.S.News Ranking 2021) *Aug. 2019 - Present*
Master Degree on Machine Learning and Data Science GPA: **3.80/4.00**
Xidian University (#15 Best Univ. for EE–U.S.News Ranking 2021) *Sep. 2015 - Jun. 2019*
Bachelor Degree on Electrical and Information Engineering GPA: **3.71/4.00**

SELECTED COURSEWORK

Deep Learning & Applications, Optimization & Acceleration of Deep Learning on Various Hardware Platforms, Statistical Learning, Probability & Statistics for Data Science, Random Processes, Programming for Data Analysis

SELECTED PROJECTS

Project ① (2020): Mitigating White-box Adversarial Attacks toward Deep Learning Models with Preprocessing-only Techniques as the Defense. *Advisor:* ***Dr. Han Qiu & Prof. Meikang Qiu***

- Designed the first preprocessing-only adversarial defense method that demonstrates robustness against advanced interactive adversarial attacks (BPDA and EOT) on an Inception V3 model pre-trained on ImageNet.
- Developed the first preprocessing-only adversarial defense framework for DNNs includes fifteen methods.
- Lead writing three papers summarize three different contributions of this project, sent to IEEE TDSC, AAAI 2020, and ICA3PP 2020 (accepted), respectively.

Project ② (2020): Research on Developing Preprocessing-based Techniques to Mitigate Backdoor Attacks in DNNs. *Advisor:* ***Dr. Han Qiu & Prof. Tianwei Zhang***

- Surveyed and evaluated 64 existing preprocessing methods on mitigating six different advanced backdoor attacks over three different target models trained on three different datasets.
- Proposed the GYM, a comprehensive backdoor defense method, which is the first defense that considers invisible backdoor attacks and successfully mitigates different advanced attacks in attack agnostic settings.

Project ③ (2019): Designing of Light-weight Network Traffic Classification/Identification Methods only Requires Raw Packets Based on Deep Learning Techniques. *Advisor:* ***Prof. Huaxi Gu***

- Developed an Encrypted Traffic Classification (ETC) and Intrusion Detection (ID) method based on CNN, LSTM, and SAE, outperforming published methods by 13.49 % on ETC's F1 and 12.15% on ID's F1.
- Proposed a Spatio-Temporal network traffic examination method based on 1D-CNN and LSTM, which attained an averaging accuracy of 99.98% on 2 public datasets.
- Wrote 2 papers summarize project's 2 phases, published on IEEE Access, SmartCloud 2019, respectively.

Project ④ (2018): Research on Machine Learning Based Techniques Countering Security Issues in the Vehicle Ad-hoc Network (VANET). *Advisor:* ***Prof. Meikang Qiu***

- Designed a detection method for the VANET based on SVM, DNN, and Game Theory to overcome scenarios where most units are compromised, demonstrated a 7.23% higher accuracy than state-of-art methods
- Designed a detection method inputs raw traffic data to monitor and inspect malicious communications between vehicles based on Deep Learning, achieved 0.97 F1 out of 1.
- Lead writing two works summarize the details, published on SmartCom 2018, SmartCloud 2019.

EXPERIENCE OVERVIEW

Jacobs School of Engineering, UCSD, CA, USA	*Aug. 2019 - Present*
Research Assistant @ Adaptive Computing and Embedded Systems Lab	**3** Publications
School of Info. and Comm. Engineering, BUPT, Beijing, China	*Jul. 2019 - Oct. 2019*
Research Assistant @ BUPT ROHDE & SCHWARZ Joint Lab	**3** Publications
College of Electrical Engineering, Columbia University, NY, USA	*Mar. 2018 - Mar. 2019*
Research Intern @ Signal Processing & Communications Lab	**3** Publications
College of Electrical Engineering, XDU, Shaanxi, China	*Sep. 2015 - Jun. 2019*
Research Assistant @ State Key Lab of Integrated Service Networks	**4** Publications

TECHNICAL STRENGTHS

Programming: Python, Matlab, C/C++, HTML
Languages: Mandarin (Native), English (Full professional proficiency)
Frameworks: Tensorflow, Pytorch, Numpy, Cleverhans, Foolbox, SciPy, Scikit-learn

PROFESSIONAL SERVICES

Reviewer: Springer, 20th International Conference on Algorithms and Architectures for Parallel Processing
Reviewer: IEEE, 22nd International Conference on Computational Science and Engineering
Reviewer: IEEE, 18th International Conference on Optical Communications and Networks
Reviewer: IEEE, 17th International Conference on Embedded and Ubiquitous Computing

SELECTED PUBLICATIONS & MANUSCRIPTS

(i) **GYM: A Comprehensive Defense Approach against DNN Backdoor Attacks**
Yi Zeng, Han Qiu, Shangwei Guo, Tianwei Zhang, Meikang Qiu and Bhavani Thuraisingham
Under Reviewing by AAAI, 2020.

(ii) **Defending Adversarial Examples in Computer Vision based on Data Augmentation Techniques**
Yi Zeng, Han Qiu, Gerard Memmi and Meikang Qiu
Best Paper of the International Conference on Algorithms & Architectures for Parallel Processing (ICA3PP), 2020.

(iii) **An Effective and Efficient Preprocessing-based Approach to Mitigate Advanced Adversarial Attacks**
Han Qiu*, **Yi Zeng***, Qinkai Zheng, Tianwei Zhang, Meikang Qiu and Bhavani Thuraisingham
Under Reviewing by AAAI, 2020. [**Equal Contribution*].

(iv) **FenceBox: A Platform for Defeating Adversarial Examples with Data Augmentation Techniques**
Han Qiu, **Yi Zeng**, Tianwei Zhang and Meikang Qiu
Submitted to IEEE Transactions on Dependable and Secure Computing, 2020.

(v) **The Hidden Vulnerability of Watermarking for Deep Neural Networks**
Shangwei Guo, Tianwei Zhang, Han Qiu, **Yi Zeng**, Tao Xiang and Yang Liu
Under Reviewing by AAAI, 2020.

(vi) **Deep Learning Based Network Encrypted Traffic Classification and Intrusion Detection Framework**
Yi Zeng, Huaxi Gu, Wenting Wei and Yantao Guo
IEEE Access, 2019. **33 Citations**.

(vii) **End-to-End Network Traffic Classification System With Spatio-Temporal Features Extraction**
Yi Zeng, Zihao Qi, Wencheng Chen and Yanzhe Huang.
IEEE International Conference on Smart Cloud (IEEE SmartCloud), IEEE, 2019.

(viii) **DeepVCM: A Deep Learning Based Intrusion Detection Method in VANET**
Yi Zeng, Meikang Qiu, Dan Zhu, Zhihao Xue, Jian Xiong and Meiqin Liu
IEEE Intl Conference on High Performance and Smart Computing (IEEE HPSC), IEEE, 2019.

(ix) **Using Adversarial Examples to Bypass Deep Learning Based URL Detection System**
Wencheng Chen, **Yi Zeng** and Meikang Qiu
IEEE International Conference on Smart Cloud (IEEE SmartCloud), IEEE, 2019.

(x) **V-PSC: A Perturbation-Based Causative Attack Against DL Classifiers' Supply Chain in VANET**
Yi Zeng, Meikang Qiu, Jingqi Niu, Yanxin Long, Jian Xiong and Meiqin Liu
IEEE International Conference on Embedded and Ubiquitous Computing (IEEE EUC), IEEE, 2019.

(xi) **Model Uncertainty for Annotation Error Correction in DL Based Intrusion Detection System**
Wencheng Chen, Hongyu Li, **Yi Zeng**, Zichang Ren and Xingxin Zheng
IEEE International Conference on Smart Cloud (IEEE SmartCloud), IEEE, 2019.

(xii) **Senior2local: A Machine Learning Based Intrusion Detection Method for VANETs**
Yi Zeng, Meikang Qiu, Zhong Ming and Meiqin Liu
International Conference on Smart Computing and Communication (SmartCom), Springer, 2018.