Jingkang Wang

https://wangjksjtu.github.io

Email : wangjksjtu@gmail.com
Mobile : +86-158-2117-0337

Education

- **Shanghai Jiao Tong University (SJTU)** Shanghai, China
  B.Eng. in Information Security, School of Cyber Security *Sept. 2015 – June. 2019 (Expected)*
  - **GPA**: 3.96/4.3 (91.6/100) **Rank**: 2/97

Research Interests

- **Machine Learning, Security (Cryptography), Computer Vision**

Publications

- **LiDAR-Video Driving Dataset: Learning Driving Policies Effectively** **[pdf]**
  Jingkang Wang*, Chenyi Ping*, Jonathan Li, Cewu Lu, Zhipeng Luo, Han Xue and Cheng Wang.
  In Proceedings of IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018

Submissions & Pre-prints

- **Reinforcement Learning with Perturbed Rewards** **[pdf]**
  Jingkang Wang, Yang Liu and Bo Li.
  In Submission to 7th International Conference on Learning Representations (ICLR), 2019 (*arXiv:1810.01032*)
- **One Bit Matters: Understanding Adversarial Examples as the Abuse of Redundancy** **[pdf]**
  Jingkang Wang, Ruoxi Jia, Gerald Friedland, Bo Li and Costas Spanos.
  In Submission to 7th International Conference on Learning Representations (ICLR), 2019 (*arXiv:1810.09650*)
- **The Helmholtz Method: Using Perceptual Compression to Reduce Machine Learning Complexity** **[pdf]**
  Gerald Friedland, **Jingkang Wang**, Ruoxi Jia, Bo Li and Nathan Mundhenk.
  In Submission (*arXiv:1807.10569*)
- **Multiple Character Embeddings for Chinese Word Segmentation** **[pdf]**
  Jingkang Wang, Jianing Zhou and Gongshen Liu.
  In Submission (*arXiv:1808.04963*)

Research Experience

- **Reinforcement Learning with Perturbed Rewards** *July 2018 - Sept. 2018*
  - ***Advisor:*** *Profs. Yang Liu and Bo Li* *UIUC, USA*
  - Introduce an unbiased estimator of reward in reinforcement learning which guarantees risk minimization without any assumptions on the true distribution.
  - Propose an efficient iterative algorithm for estimating the confusion matrices of corrupted rewards in the training.
  - Study the convergence and finite sample complexity theoretically under the proposed reward proxy.
- **Understanding Adversarial Examples as the Abuse of Redundancy** *March 2018 - June. 2018*
  - ***Advisor:*** *Profs. Bo Li and Dawn Song* *UC Berkeley, USA*
  - Propose a model for adversarial examples consistent with related work, physics and information theory.
  - Reinterpret the Helmholtz free energy formula to explain the relationship between content and noise for sensor-based data.
  - Prove that input redundancy is indeed a necessary condition for being able to generate adversarial examples.
  - Validate that adversarial examples are indeed overflowing perceptrons trained on a certain level of redundancy.
- **Multiple Embeddings for Chinese Word Segmentation** *Feb. 2018 - May. 2018*
  - ***Advisor:*** *Prof. Gongshen Liu* *SJTU, China*
  - Leverage both semantic and phonetic meanings of Chinese characters in NLP tasks by introducing *Pinyin Romanization* and *Wubi Input* Embeddings.
  - Achieve the state-of-the-art performance in AS and CityU corpora with F1 scores 96.9 and 97.3.
- **Benchmark for Driving Policy Learning** *Apr. 2017 - Feb. 2018*
  - ***Advisor:*** *Prof. Cewu Lu* *SJTU, China*
  - Propose a dataset which is the first policy learning benchmark composed of driving videos, LiDAR data, and corresponding driving behaviors.
  - Conduct the complete analysis on how important depth information is, how to leverage depth information and what we can achieve by utilizing current techniques.

Selected Projects

- **Blockchain-Based Genetic Privacy-Preserving System** *May 2018 - July. 2018*
  - ***Advisor:*** *Prof. Lei Fan* ***Award:*** *National First Price in CISCN 2018*
  - Design a protocol of private set intersection (PSI) on the blockchain, namely BPSI, which establishes a crowdsourcing ecology and calculates PSI against collusion.
  - Propose security, effectiveness and arbitration mechanism in BPSI, which guarantee the efficiency of the proposed protocol theoretically.
- **Dynamic Searchable Encryption System Based on Graph Database** *May 2017 - July. 2017*
  - ***Advisor:*** *Prof. Lei Fan* ***Award:*** *National Second Price in CISCN 2017*
  - Adopt the parallel-DSSE algorithm in graph database and propose several policies to enhance the robustness.
  - Implement the improved algorithm utilizing Neo4j Graph Database and validate its effectiveness, efficiency and scalability based on large-scale ciphers.

Honors & Awards

- **National Scholarships (*Top 0.2% Nationwide*)** *2016, 2017, 2018*
- **Level-A SJTU Outstanding Scholarships (*Top 1%*)** *2016, 2017, 2018*
- **Yitu Technology Scholarship (*Top 1%*)** *2017*
- **First Prize in National College Student Information Security Contest** *2018*
- **Meritorious Winner Prize of Mathematical Contest in Modeling** *2018*
- **Second Prize in National College Student Information Security Contest** *2017*
- **Second Prize in The Chinese Mathematics Competitions (Shanghai)** *2017*
- **SJTU Merit Students** *2016, 2017, 2018*
- **SJTU Excellent League Cadres** *2016, 2017*
- **First Prize in Chinese Mathematical Olympiad (*10th in Shanxi Province*)** *2014*