Weicheng Zhang

wzhang81@jhu.edu | (+1) 443-319-3931
LinkedIn: https://www.linkedin.com/in/weicheng-zhang/ | Website: samz.co

About

Natural language processing researcher with information security background.

Education

Johns Hopkins University / MS in Information Security (GPA 4.0/4.0 for major courses)

August 2016 - May 2018, Baltimore, MD

- Coursework: Natural Language Processing, Algorithms, Cryptography and Coding, Security Analytics, Security & Privacy in Computing, Advanced Topics in Computer Security

Beijing University of Posts and Telecommunications / B.Eng. in Communication Engineering (GPA 3.4/4.0) with Scholarship

September 2012 - July 2016

- Honorable Mention, Mathematical Contest in Modeling, 2015
- Coursework: Voice Recognition, Pattern Recognition, Data Structures, Computer Networks, Linux System, Image Processing, Discrete Mathematics

Research

Johns Hopkins University - Language & Speech Processing Group

Jun 2017 - Present, Baltimore

Research Assistant in Information Retrieval (Elasticsearch)

- Built a Lucene/ ElasticSearch based system for Cross-lingual Information Retrieval and Question-Answering projects.

Tsinghua University – Natural Language Processing and Computational Social Science Lab

Apr 2015 – Jun 2016, Beijing, China

NLP Researcher (Neural Network, DeepWalk, SVM, t-SNE)

- Designed and implemented matrix factorization based highly discriminative representation learning method called Max-Margin DeepWalk. Paper accepted by IJCAI 2016 (Acceptance Rate 18.9%).
- Designed and optimized Online Neural Network based Max-Margin DeepWalk with better efficiency.

Publication

Cunchao Tu, Weicheng Zhang, Zhiyuan Liu, Maosong Sun. Max-Margin DeepWalk: Discriminative Learning of Network Representation. *International Joint Conference on Artificial Intelligence (IJCAI 2016)* (Co-first author). [pdf]

Projects

Developing De-anonymizing Attack and Defense to Social Networks

2017, Baltimore, MD

Software Developer (MLE, Jaccard)

- Implement a de-anonymizing MLE attack towards social networks to reveal personal data in real world.
- Designed and accomplished a defense by change the topologival graph of the social network.

Real-time Detection of Social Network Attacks

2016, Baltimore, MD

Software Developer (Crawler, Twitter REST/Streaming API, SVM)

- Implement a machine learning based detecting system for real-time social media attacks.
- Succeeded in detecting 95% real-time malicious posts in testing using SVM for classification.

Using Power Levels to Infer Unauthorized Use in Wireless Sensor Nodes

2016, Baltimore, MD

Software Developer (IDS, WSN) (Matlab and Java)

- Designed and accomplished a two-layer network IDS to detect WSN abnormal power levels.
- Succeeded in detecting 92% attacks.

Skills

Java (including Android developing), Python (TensorFlow), Matlab, C++, HTML+CSS, C, Javascript. Working with Unix/ Linux system. Android application development.