Zuchao Ma

PERSONAL DATA

ADDRESS: 29 Jiangjun Road, Nanjing, China, 211106 **PHONE:** +86 15150667018
EMAIL: macher@nuaa.edu.cn / zuchao.macher.ma@gmail.com
RESEARCH INTERESTS: The intrusion detection system of IoT networks

EDUCATION

2018 – date **Master of Computer Science and Technology**
College of Computer Science and Technology,
Nanjing University of Aeronautics and Astronautics (NUAA), China
Supervised by Associate Professor. Liang Liu and Assistant Professor. Weizhi Meng (Technical University of Denmark)
GPA: 90.4/100.0, Ranking A

2014 – 2018 **Bachelor of Computer Science and Technology**
College of Computer Science and Technology,
Nanjing University of Aeronautics and Astronautics (NUAA), China
GPA: 4.0/5.0, Ranking 6/110

SELECTED AWARDS AND HONOURS

Oct 2019 Advanced individual in research and innovation of NUAA (2018-2019)
Oct 2019 Advanced postgraduate award of NUAA (2018-2019)
2018-2020 First Class Scholarship for Graduate Students of NUAA (CNY 10,000/year)
2016-2018 Second Class Scholarship of NUAA (CNY 2500/year)
Jul 2016 Second Prize of Training Camp of App Development of NUAA
Jan 2016 Second Prize of Honour Cup Programming Contest of NUAA
Nov.2015 Third Class Scholarship of NUAA (CNY 1500/year)

PUBLICATIONS AND PATENTS

Publications:

- **Zuchao Ma**, Liang Liu and Weizhi Meng, "ELD: Adaptive Detection of Malicious Nodes under Mix-Energy-Depleting-Attacks Using Edge Learning in IoT Networks" in **23rd Information Security Conference (ISC 2020)**. Grand Mirage Resort & Thalasso, Bali, Indonesia, 16-20 Dec 2020.
- **Zuchao Ma**, Liang Liu and Weizhi Meng, "Towards Multiple-Mix-Attack Detection via Consensus-based Trust Management in IoT Networks" in **Computer & Security (COSE)**, ELSEVIER. Volume 96, September 2020, 101898. IF 3.476
- **Zuchao Ma**, Liang Liu and Weizhi Meng, "DCONST: Detection of Multiple-Mix-Attack Malicious Nodes Using Consensus-based Trust in IoT Networks" in **25th Australasian Conference on Information Security and Privacy (ACISP 2020)**. Perth, Australia, 15-17 July 2020. **Best Student Paper Award**
- Liang Liu, **Zuchao Ma** and Weizhi Meng, "Detection of multiple-mix-attack malicious nodes using perceptron-based trust in IoT networks" in **Future Generation Computer Systems (FGCS)**, ELSEVIER. Volume 101, December 2019, Pages 865-879. IF 5.768

Patents:

- PRC Patent Application No.: 201911084500.7, A Method of Detecting Malicious Nodes Using Perceptron-based Trust in IoT Networks, Liang Liu, **Zuchao Ma** and Jie Wan.
- PRC Patent Application No.: 201911084666.9, EGAPT: A Scheduling Strategy for Planned Task in Cloud Computing Environment, Liang Liu, **Zuchao Ma** and Yiting Wang.

RESEARCH EXPERIENCE

Oct 2018 – date **Master Research**
Applied Security and Cryptography Research Laboratory (ASC)
Nanjing University of Aeronautics and Astronautics (NUAA)
Supervisor: Associate Professor. Liang Liu and Assistant Professor. Weizhi Meng

- **Topic: Malicious Nodes Detection Schemes in IoT networks**
- Proposed **perceptron-based model** to detect **multiple-mix-attack** consisting of tamper attack, drop attack and replay attack with an uncertain probability, by tracking the **routes** that packets pass and comparing received packets with sent packets to support **the regression of attack models**, finally using clustering algorithms to distinguish malicious nodes. (2018-2019)
- Conducted **consensus-based model (DCONST)** to detect **multiple-mix-attack**, which enables each IoT node to evaluate the **trustworthiness** of other nodes automatically with a low cost by sharing certain information called **cognition** in networks, designing **evidences**, **punishments** and **awards** corresponding to tamper attack, drop attack and replay attack individually to achieve **trust evaluation**, and DCONST is blessed with the ability to detect malicious nodes as well as **identify their concrete attack behaviours**. (2019-2020)
- Put forward **edge-based model (ELD)** to detect **energy-exhausting-attack** consisting of carousel attack, flooding attack and replay attack with an uncertain probability, by collecting **traffic logs** to analyse the traffic of networks and constructing **intrusion edges** based on malicious traffic to build **intrusion graphs** to locate malicious nodes, aiming at detecting malicious nodes by **labeling traffic automatically** without other labeled data for system training in advance. (2020)
- Working on proposing a kind of **adversarial traffic attack (ATA)** by capturing some normal traffic of IoT networks to build a **shadow model** to support the adversarial training, which can penetrate some existing **clustering based** and **autoencoder based** intrusion detection systems (IDS), also designing a **distributed evolving detection system (DEDS)** to confront ATA, which can be deployed in IoT networks. (date)

Jun 2018 – Sep 2018 **Master Project**
Institute of Data Management and Knowledge Engineering
Nanjing University of Aeronautics and Astronautics (NUAA)
Supervisor: Associate Professor. Liang Liu

- **Topic: The Application of Cloud Platform in Computer Teaching Experiments of College**
- Developed a private cloud (**Teaching Experiment Cloud, TEC**) based on **OpenNebula**, a famous open source cloud management platform, for providing virtual machines (VM) to students to execute their experiments and TEC allows teachers to customize their **teaching templates** (VM set) by choosing various operating system images, installing different software, combining multiple kinds of VMs and arranging the **plans** of teaching lessons. To sum up, teachers define their teaching templates and import the plans of teaching lessons then have one click to deploy all VMs.
- Proposed a scheduling scheme for planned cloud task (**EGAPT**), utilizing the information of teaching templates and teaching plans to optimize the scheduling of VMs to keep the load balance of physical machines and reduce the total energy consumption of cloud.

ADDITIONAL SKILLS

- Solid programming skills in android application development (Second Prize of Training Camp of App Development of NUAA) and J2EE development.
- Full stack development skills: Front-end[Vue.js, React.js] + Http-Interface Server[Vert.x, Java servlet] + Database[MySQL, SQL Server].