

# Yong-Hao Zou

Email: yonghaoz1994@gmail.com Mob: (86) 18521350120 Homepage: [zouyonghao.github.io](http://zouyonghao.github.io)

## RESEARCH INTEREST

---

Fuzzing, System Software Reliability, Network Protocols, Robot Operating System, Distributed Systems, Program Analysis

## EDUCATION

---

**Tsinghua University** (Advisor: Prof. Shi-Min Hu)

*Sep. 2019-Jun. 2022*

M.E. in Computer Technology

Main Courses: Computer System Performance Measurement, Advanced Operating Systems, Computer Security

Honor & Award: Outstanding Graduate, Tsinghua University

**Zhejiang University**

*Sep. 2011-Jun. 2015*

B.E. in Computer Science and Technology

## PUBLICATION

---

- [1] **Yong-Hao Zou**, Jia-Ju Bai, Jielong Zhou, Jianfeng Tan, Chenggang Qin, Shi-Min Hu. TCP-Fuzz: Detecting Memory and Semantic Bugs in TCP Stacks with Fuzzing. USENIX ATC, 2021.
- [2] **Yong-Hao Zou**, Jia-Ju Bai. Effective Crash Recovery of Robot Software Programs in ROS. ICRA, 2021.
- [3] Kai-Tao Xie, Jia-Ju Bai, **Yong-Hao Zou**, Yu-Ping Wang. ROZZ: Property-based Fuzzing for Robotic Programs in ROS. ICRA, 2022.

## EXPERIENCE & RESEARCH

---

**Work Experience: Software backend engineer**

Shanghai, China

*Software architecture group member*

*Sep. 2015-Apr. 2018*

1. Develop a microservice framework to help transform several monolithic architecture applications into microservices, including configuration management system, RPC framework, service management and service discovery, code generation tools, etc.
2. Develop a message system for scale and availability, providing critical functions including at-least-once message delivery, high availability servers, server load balance, manual message management, etc.

**Research Project I: Research on Robot Operation System (ROS) reliability and security**

Beijing, China

*Project core member*

*Sep. 2019-Mar. 2020, May. 2021-Jul. 2021*

1. Develop a new lightweight recovery tool name RORY with checkpoint and message replay to recover ROS nodes effectively. RORY can effectively recover six common ROS programs in both virtual and realistic environments. (ICRA 20)
2. Develop a ROS fuzzing tool named ROZZ with three key techniques, including a multi-dimensional generation method, a distributed branch coverage and a temporal mutation strategy, to effectively test ROS nodes. ROZZ has successfully found 43 real bugs on 10 common robotic programs in ROS 2. (ICRA 21)

**Research Project II: Research on reliability and correctness testing of TCP Stacks**

Beijing, China

*Project core member*

*Apr. 2020-Feb. 2021*

1. Develop a novel fuzzing framework name TCP-Fuzz, to effectively test TCP stacks and detect bugs with three key techniques: a dependency-based generation strategy, a transition-guided fuzzing approach, a differential checker. (ATC 21)
2. TCP-Fuzz is adapted to 5 TCP stacks and find 56 real bugs, some of these bugs are listed [here](#).

**Research Project III: Research on reliability and correctness testing of distributed systems**

Beijing, China

*Project core member*

*Mar. 2021-Now*

1. Propose a coverage guided fuzzing approach to test distributed systems.
2. Develop a novel fuzzing framework which has found dozens of real bugs in different distributed systems. The framework is further extended to distributed database systems. Bugs found for opensource projects are listed [here](#).

## SKILLS

---

- System programming including Linux driver development, scheduling, networking, distributed systems, and ROS
- Dynamic analysis based on LLVM
- Programming language: Java, C/C++, Python and Clojure