ABDULLAH AL ARAFAT

2482 Avent Ferry Rd, Apt 301, Raleigh, NC 27606
✉ aalaraf@ncsu.edu ⋄ https://abdullahaarafat.github.io/

RESEARCH INTERESTS

- Real-Time Computing and Scheduling Theory
- Robust Learning Theory
- Formal Methods and Control Theory
- Cyber-physical Systems

EDUCATION

Ph.D. in Computer Science May 2025 (Expected)
North Carolina State University, Raleigh, NC
Dissertation Title (tentative): Towards Resilient and Secure Real-Time Intelligent Systems
Advisor: Dr. Zhishan Guo

M.Sc. in Computer Engineering May 2020
University of Central Florida, Orlando, FL

B.Sc. in Electrical & Electronic Engineering March 2016
Bangladesh University of Engineering and Technology, Dhaka

RESEARCH EXPERIENCE

Graduate Research Assistant

North Carolina State University, Raleigh, NC — Fall 2022 - Present

University of Central Florida, Orlando, FL — Fall 2019 - Summer 2022

TEACHING EXPERIENCE

Instructor

North Carolina State University, Raleigh, NC

- CSC 714: Real-time Computer Systems (co-teach with Dr. Zhishan Guo) — Spring'24
  Teaching Evaluation (students' rating): 4.80 out of 5.00

Graduate Teaching Assistant

North Carolina State University, Raleigh, NC

- CSC 495: Advanced Algorithms — Spring'23, Fall'23
- CSC 520: Artificial Intelligence — Fall'23
- CSC 591/714: Real-Time Computer Systems — Spring'24
- CSC 505: Design and Analysis of Algorithms — Fall'24

University of Central Florida, Orlando, FL

- EEL 4742C: Embedded System — Spring'21, Summer'21, Spring'22, Summer'22
- EEL 3801C: Computer Organization — Summer'21
- EEL 4768: Computer Architecture — Summer'21
- EEE 4775: Real-Time Systems — Fall'21
- EEE 4346: Hardware Security and Trusted Circuit Design — Fall'21
- EGN 3211: Engineering Analysis and Design — Spring'22
- EEL 4781: Computer Communication Networks — Summer'22

PUBLICATIONS

Research Summary

I have published **12** top-tier journals and conference papers on topics related to secure and resilient real-time cyber-physical systems. I have a total of **8 papers published at the prestigious CSRankings** listed conferences. My DAC 2022 paper was recognized as a **Publicity Paper** at the conference. Following is the list of papers for each research topic:

- Real-Time Scheduling — RTAS'23, RTSS'23
- Robot Operating System (ROS 2) — DAC'22, EMSOFT'24
- Robust Learning/AI Security — VR'21, ICCV'23, ECCV'24, CCS'24
- End-to-end Verification/Formal Methods — MEMOCODE'24

Note. Authors with '*' contributed equally to the paper.

Conferences

10. [**CCS'24**] Abdullah Al Arafat*, Nazmul Karim*, Adnan Siraj Rakin, Zhishan Guo, Nazanin Rahnavard. '*Fisher Information Guided Purification against Backdoor Attacks*' in 31st ACM SIGSAC Conference on Computer and Communications Security **(CCS)**, 2024.

9. [**ECCV'24**] Abdullah Al Arafat*, Nazmul Karim*, Umar Khalid, Zhishan Guo, Nazanin Rahnavard. '*Augmented Neural Fine-Tuning for Efficient Backdoor Purification*' in The European Conference on Computer Vision **(ECCV)**, 2024.

8. [**EMSOFT'24**] Abdullah Al Arafat, Kurt Wilson, Kecheng Yang, Zhishan Guo. '*Dynamic Priority Scheduling of Multi-Threaded ROS 2 Executor with Shared Resources*' in ACM SIGBED International Conference on Embedded Software **(EMSOFT)**, 2024.

7. [**MEMOCODE'24**] Kurt Wilson, Abdullah Al Arafat, John Baugh, Ruozhou Yu, Zhishan Guo. '*Physics-Aware Mixed-Criticality Systems Design via End-to-End Verification of CPS*' in 22nd International Symposium on Formal Methods and Models for System Design **(MEMOCODE)**, 2024.

6. [**RTSS'23**] Zhishan Guo*, Sudharsan Vaidhun*, Abdullah Al Arafat*, Nan Guan, and Kecheng Yang. '*Stealing Static Slack via WCRT and Sporadic P-Servers in Deadline-Driven Scheduling*' in 44th IEEE Real-Time Systems Symposium **(RTSS)**, 2023.

5. [**ICCV'23**] Abdullah Al Arafat*, Sabbir Ahmed*, Mamshad Nayeem Rizve*, Rahim Hossain, Zhishan Guo, and Adnan Siraj Rakin. '*SSDA: Secure Source-Free Domain Adaptation*' in International Conference on Computer Vision **(ICCV)**, 2023.

4. [**RTAS'23**] Abdullah Al Arafat, Sudharsan Vaidhun, Liangkai Liu, Kechang Yang, and Zhishan Guo. '*Compositional Mixed-Criticality Systems with Multiple Executions and Resource-Budgets Model*' in 29th IEEE Real-Time and Embedded Technology and Applications Symposium **(RTAS)**, 2023.

3. [**WMC'22**] Abdullah Al Arafat, Sudharsan Vaidhun, Bryan C. Ward, and Zhishan Guo. '*A Secure Resilient Real-Time Recovery Model, Scheduler, and Analysis*' in 10th International Workshop on Mixed Criticality Systems **(WMC)**@RTSS, 2022.

2. [**DAC'22**] Abdullah Al Arafat, Sudharsan Vaidhun, Kurt M. Wilson, Jinghao Sun, and Zhishan Guo. '*Response Time Analysis for Dynamic Priority Scheduling in ROS2*' in 59th IEEE/ACM Design Automation Conference **(DAC)**, 2022. (Publicity Paper Award) [News coverage]

1. [**VR'21**] Abdullah Al Arafat, Zhishan Guo, and Amro Awad. '*VR-Spy: A Side-Channel Attack on Virtual Key-Logging in VR Headsets*' in IEEE Conference on Virtual Reality and 3D User Interfaces **(IEEE VR)**, 2021.

Journals

2. [**TCAD'24**] Abdullah Al Arafat, Kurt Wilson, Kecheng Yang, and Zhishan Guo. '*Dynamic Priority Scheduling of Multi-Threaded ROS 2 Executor with Shared Resources*' in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **(TCAD)**, 2024.

1. **[IoT-J'22]** Abdullah Al Arafat*, Jiang Bian*, Haoyi Xiong, Jing Li, Li Li, Hongyang Chen, Jun Wang, Dejing Dou, and Zhishan Guo. '*Machine Learning in Real-Time Internet of Things (IoT) Systems: A Survey*' in IEEE Internet of Things Journal **(IoT-J)**, 2022.

TALKS

T7. CCS, Fisher Information Guided Purification against Backdoor Attacks, 2024

T6. Ph.D. Forum, ESWEEK, Towards Resilient and Secure Real-Time Intelligent Systems, 2024

T5. EMSOFT, Dynamic Priority Scheduling of Multi-Threaded ROS 2 Executor with Shared Resources, 2024

T4. RTAS, Compositional MC Systems with Multiple Executions and Resource-Budgets Model, 2023

T3. WMC, A Secure Resilient Real-Time Recovery Model, Scheduler, and Analysis, 2022

T2. IEEE/ACM DAC, Response Time Analysis for Dynamic Priority Scheduling in ROS 2, 2022

T1. IEEE VR, VR-Spy: A Side-Channel Attack on Virtual Key-Logging in VR Headsets, 2021

AWARDS AND SCHOLARSHIPS

Graduate Merit Award (NCSU)	2024
Mentored Teaching Fellowship (NCSU)	Spring 2024
DAC 2022 Publicity Paper	2022
Doctoral Research Support Award (UCF)	2021
ORC Fellowship (UCF)	2018
Runner-Up (Cadence DSP Design Contest)	2016
CCS Student Travel Award	2024 (ACM)
CPS-IoT Week Student Travel Grant	2023 (SIGBED); 2024 (NSF)
COE Student Travel Grant (NCSU)	2023
RTSS Student Travel Grant	2022 (IEEE)
Presentation Fellowship (UCF)	2022

SKILLS

Programming	Python, C/C++, MATLAB
Verification Tools	UPPAAL
Real-Time OS	ROS 2, FreeRTOS, LinuxRT

MENTORING EXPERIENCE

Kurt Wilson, CS Undergraduate Student at the University of Central Florida, now Ph.D. Student at North Carolina State University
Publications: DAC'22 [**Publicity Paper Award**], EMSOFT'24

Srishti Swarnima, MS Student at North Carolina State University

Farhad Bhatti, CS Undergraduate Student at North Carolina State University

PROFESSIONAL SERVICES

Reviewer

IEEE Internet of Things Journal (IoT-J)	2023
AAAI Conference on Artificial Intelligence (AAAI)	2024
International Conference on Real-Time Networks and Systems (RTNS)	2021, 2022, 2023
Embedded and Real-Time Computing Systems and Applications (RTCSA)	2021, 2022, 2023

Secondary Reviewer 2021 – 2024

Journals

IEEE IoT-J, IEEE TNNLS, IEEE TCAD, IEEE TIME, IEEE TPDS, ACM TECS, etc.

Conferences

Real-Time Systems Symposium (**RTSS** 2021, 2022, 2023, 2024)
ACM SIGBED International Conference on Embedded Software (**EMSOFT** 2024)
Euromicro Conference on Real-Time Systems (**ECRTS** 2024)
Real-Time and Embedded Technology and Applications (**RTAS** 2022, 2024)
Design Automation Conference (**DAC** 2021, 2022)

REFERENCES

Available upon request.