MAHER AL ISLAM

Graduate Research Assistant, West Virginia University, USA
maherislam071@gmail.com mahermayer.github.io maher-al-islam

RESEARCH INTEREST

- Autonomous Vehicles
- Cybersecurity
- AI Safety & Ethics
- Adversarial AI
- Cyber-Physical System

TECHNICAL SKILLS

- **Artificial Intelligence:** Adversarial AI (FGSM, PGD, UAP, DeepFool); Vision AI (YOLO, UNet, ViT); Context-Aware AI; Reinforcement Learning (Q-Learning, DQN, MDP); Multimodal Sensor Fusion (Camera, LiDAR)
- **Autonomous Systems:** ROS, CARLA, Duckietown; Perception–Control Integration; Control Methods (PID, RL, MPC); CPS Modeling (Smart Homes, Smart Water Distribution)
- **Cybersecurity:** CPS/IoT Security; Game-Theory; Intrusion Detection & Response; Adversarial BSM Detection in CAVs; CTF (Crypto, Cracking, Network, Scanning, Forensics)

SOFTWARE & TOOLS

Programming: Python, C, MATLAB/Simulink, ROS, Bash/Linux

Frameworks: PyTorch, TensorFlow, OpenCV, Scikit-learn, Docker, Git

IoT & Robotics: NVIDIA Jetson (AGX), Raspberry Pi, ZED Stereo Camera; MQTT, TCP/UDP

Verification: Uppaal, PRISM, SPIN (model checking, temporal logic, CPS verification)

Security/CTF: Scapy, Wireshark, Aircrack-ng, John/Hashcat, Metasploit, BurpSuite, Netcat, Volatility

EDUCATION

West Virginia University (Advisor: Dr. Amr El-Wakeel) — **August, 2024 – Ongoing**
Ph.D. in Computer Engineering — *WV, USA*

Virginia Commonwealth University (Advisor: Dr. Sherif Abdelwahed) — **January, 2021 – May, 2024**
M.S. in Electrical & Computer Engineering ***GPA: 4.0/4.0*** — *VA, USA*

University of Dhaka — **Jan, 2012 – October, 2016**
B.Sc. in Electrical & Electronic Engineering ***GPA: 3.41/4.0*** — *Dhaka, Bangladesh*

EXPERIENCE

West Virginia University — iCPS Lab — **Aug 2024 – Present**
Graduate Research Assistant — *WV, USA*

- Adversarial AI, trustworthy autonomy, CPS security for AVs and robotics.
- Resilient perception–control pipelines: context-aware detection, semantic segmentation, adversarial AI, multimodal sensor fusion (ROS/Duckietown testbeds).
- DARPA **AI CRAFT (2024–26)**: Cybersecurity for AI.

Virginia Commonwealth University - OCC Testbed — **Jan 2021 – Jul 2024**
Graduate Research Assistant & Teaching Assistant — *VA, USA*

- **Graduate Research Assistant (CPS, Smart-City, Cybersecurity):**
  - OpenCyberCity (OCC) Testbed — CPS platform for smart-city, adaptive control, cybersecurity.
  - Smart Home Temperature-Control — **RF**, **LSTM**, **PID** for resilient control under **FDI** attack in HVAC.

  - Smart-Home Intrusion Response — autonomous **IRS** agents for IoT-based attacks.
  - Game-theoretic DDoS Defense — **attacker–defender strategies**, local vs. cloud mitigation (AWS).
  - Uncertainty-Aware Water Distribution — **Bayesian LSTM** with epistemic uncertainty for forecasting.
  - Adaptive CPS Control — IoT-driven **adaptive control** for smart water systems.
  - CAV BSM Anomaly Detection — **anomaly** detection of **Basic Safety Messages** in CAVs.
- **Teaching Assistant (ECE/CS Courses):**
  - *EGRE 364 Microcomputer Systems* — microcontrollers, USART, motors, line-following robot (Keil).
  - *EGRE 337 Statistical Information Processing* — statistical modeling assignments.
  - *EGRE 245 Advanced C Programming* — pointers, structures, linked lists, stacks, binary search.
  - *EGRE 354 Digital Logic Design* — FPGA/discrete-logic design (Vivado).
  - *EGRE 454 Automatic Controls* — system stability, pole-zero analysis.

Peer-Reviewed Publications [Google Scholar Link]

[J1] **M. Al Islam**, A. Srivastava, A. El-Wakeel, **"AI in Autonomous Vehicles Under Siege: Vulnerabilities, Challenges, and Path Forward."**, IEEE Transactions on Intelligent Vehicles. (In Review)

[C1] **M. Al Islam**, A. El-Wakeel, **"Towards Context-Aware Autonomous Driving in Degraded Urban Environments using LaneNet."** IEEE International Conference on Robotics and Automation 2026. (Submitted)

[C2] **M. Al Islam**, A. El-Wakeel, **"Integrating Perception and Control for Resilient Autonomous Driving under Vision Adversarial Attacks."**, IEEE Intelligent Vehicles Symposium (IV 2026). (In Progress)

[C3] M. Zaman, **M. Al Islam**, N. Zohrabi and S. Abdelwahed, **"A Machine Learning-Based Temperature Control and Security Protection for Smart Buildings"**, 2024 IEEE International Conference on Smart Computing (SMARTCOMP), Osaka, Japan, 2024

[C4] M. Zaman, **M. A. Islam**, A. Tantawy and S. Abdelwahed, **"An Uncertainty Based Predictive Analysis of Smart Water Distribution System Using Bayesian LSTM Approach"**, 2022 6th International Conference on Universal Village (UV), Boston, MA, USA, 2022

[C5] **M. Al Islam**, C. J. Fung, A. Tantawy and S. Abdelwahed, **"A Game-Theoretic Model for DDoS Mitigation Strategies with Cloud Services"**, NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, 2022

[C6] Zohrabi, N., Martin, P.J., **Al Islam, M.**, et al., 2021, September. **Opencity: An open architecture testbed for smart cities**. 2021 IEEE International Smart Cities Conference (ISC2)

[C7] M. Zaman, **M. Al Islam**, A. Tantawy, C. J. Fung and S. Abdelwahed, **"Adaptive Control for Smart Water Distribution Systems"**, 2021 IEEE International Smart Cities Conference (ISC2), Manchester, UK, 2021

Awards & Certifications

- **Diamond Badge** (97th Percentile) – NCL CTF 2025
- **3rd Place** – WVU AI Symposium 2025
- **Best Poster Award** – IEEE SmartComp (2024)

Professional Leadership

- **President**, WVU Bengali Students' Association (BSA), Aug 2024 – Present
- **Founding President**, Bengali Cultural Association of Graduate Students (BCAGS), VCU, Spring 2023 – Fall 2023
- **Event Coordinator**, Engineering Graduate Student Association (EGSA), VCU, Fall 2021 – Spring 2022