JEROME DINAL HERATH

Full Name: Jerome Dinal Herath Muthukumaranage
www.dinalherath.com ◇ jherath1@binghamton.edu ◇ github.com/dherath

EDUCATION

State University of New York at Binghamton, USA *August 2018 - Present*
PhD in Computer Science GPA: 3.93/4.00

University of Colombo, Sri Lanka *January 2013 - January 2017*
Bachelor of Science, Specialization in Computational Physics GPA: 3.66/4.00
Recipient of Dr. Sarath Gunapala Gold Medal for Computational Physics (2017)

RESEARCH

Machine Learning and Deep Learning for anomaly detection, Adversarial Machine Learning, Interpretable Machine Learning

RESEARCH EXPERIENCE

State University of New York at Binghamton, USA *August 2018 - Present*
Research done in fulfillment of PhD

- Log-Anomaly-Mask: Designed a real-time adversarial evasion attack leveraging deep reinforcement learning to understand the robustness of deep learning based online anomaly detection from distributed system logs *[CODASPY'21]*
- RAMP: Built a real-time machine learning model designed for anomaly detection in a streaming multivariate time-series *[BIGDATA'19]*
- SciBlock: Investigated the potential use of Blockchain technology to improve the safety and reproducability of scientific research *[CIC'19]*

State University of New York at Binghamton, USA *August 2017 - August 2018*
Graduate Research Assistant

- Designed a Markovian model to understand the use of opportunistic routing in cached wireless networks *[ICC'18, TVT'19]*
- Designed a LSTM/GRU based sequence-to-sequence deep learning model for wireless signal strength prediction *[ICC'19, TVT'20]*

TECHNICAL STRENGTHS

Programming Languages	Python and Matlab, Java, C
Modelling Experience	Markovian modelling
Machine Learning (ML)	ML for anomaly detection, deep learning, reinforcement learning
Deep Learning Frameworks	Pytorch, Tensorflow
Experience with	Time series and graph data

SELECTED PUBLICATIONS

1. *"Real-Time Evasion Attacks against Deep Learning-Based Anomaly Detection from Distributed System Logs"*. By **J. Dinal Herath**, Ping Yang, Guanhua Yan. In: Proceedings of The 11th ACM Conference on Data and Application Security and Privacy (CODASPY-2021).

2. *"RAMP: Real-Time Anomaly Detection in Scientific Workflows"*. By **J. Dinal Herath**, Changxin Bai, Guanhua Yan, Ping Yang, Shiyong Lu. In: IEEE International Conference on Big Data (Big Data-2019).
3. *"SciBlock: A Blockchain-Based Tamper-Proof Non-Repudiable Storage for Scientific Workflow Provenance"*. By Dinuni Fernando, Siddharth Kulshrestha, **J. Dinal Herath**, Nitin Mahadik, Yanzhe Ma, Changxin Bai, Ping Yang, Guanhua Yan, Shiyong Lu. In: International Conference on Collaboration and Internet Computing (CIC-2019)
4. *"DeepChannel: Wireless Channel Quality Prediction using Deep Learning"*. By Adita Kulkarni, Anand Seetharam, Arti Ramesh, **J. Dinal Herath**. In: IEEE Transactions in Vehicular Technology (TVT-2020)
5. *"A Deep Learning Model for Wireless Channel Quality Prediction"*. By **J. Dinal Herath**, Anand Seetharam, Arti Ramesh. In: IEEE International Conference on Communications (ICC-2019).
6. *"A Markovian Model for Analyzing Opportunistic Request Routing in Wireless Cache Networks"*. By **J. Dinal Herath** and Anand Seetharam. In: IEEE Transactions in Vehicular Technology (TVT-2018).
7. *"Analyzing Opportunistic Request Routing in Wireless Cache Networks"*. By **J. Dinal Herath** and Anand Seetharam. In: IEEE International Conference on Communications (ICC-2018).

SELECTED RESEARCH PROJECTS

LAM (Log Anomaly Mask) [CODASPY'21]

- Log Anomaly Mask (LAM) is an adversarial evasion attack designed to evaluate the robustness of Deep Learning models used for anomaly detection from distributed system logs.
- Built leveraging Deep Reinforcement Learning, LAM is able to attack models in whitebox, graybox and blackbox scenarios.
- Attacks generated from LAM are imperceptible (∼9.9% difference from original sample) and LAM can attack in an online fashion with low latency (∼0.46 milliseconds).

RAMP (Real-Time Aggregated Matrix Profile) [BIGDATA'19]

- Real-Time Aggregated Matrix Profile (RAMP) is a machine learning model that is capable of identifying anomalies given a stream of multivariate time series data in real time.
- A semi-supervised model that has online training and provides insight into root causes of anomalies.
- Shows superior anomaly detection capability for both direct and adversarialy hidden attacks when experimented on scientific workflows running on Amazon EC2 Virtual Machines.

AWARDS

Academic awards and Scholarships

1. Recipient of Dr. Sarath Gunapala Gold Medal for Computational Physics, University of Colombo, Sri Lanka (2017).
2. Recipient of MIND (Munasinghe Institute for Development) Scholarship, Sri Lanka (2015-2016).

Travel Grants

1. NSF funded student travel grant to attend IEEE International Conference on Collaboration and Internet Computing (CIC-2019).
2. Student travel grant to attend ACM/IEEE Symposium on Architectures for Networking and Communications (ANCS-2018).
3. NSF funded student travel grant to attend IEEE International Conference on Communications (ICC-2018).