AI-Assisted Cybersecurity for 5G and Beyond

Dr. Glaucio Carvalho
gdecarvalho@brocku.ca

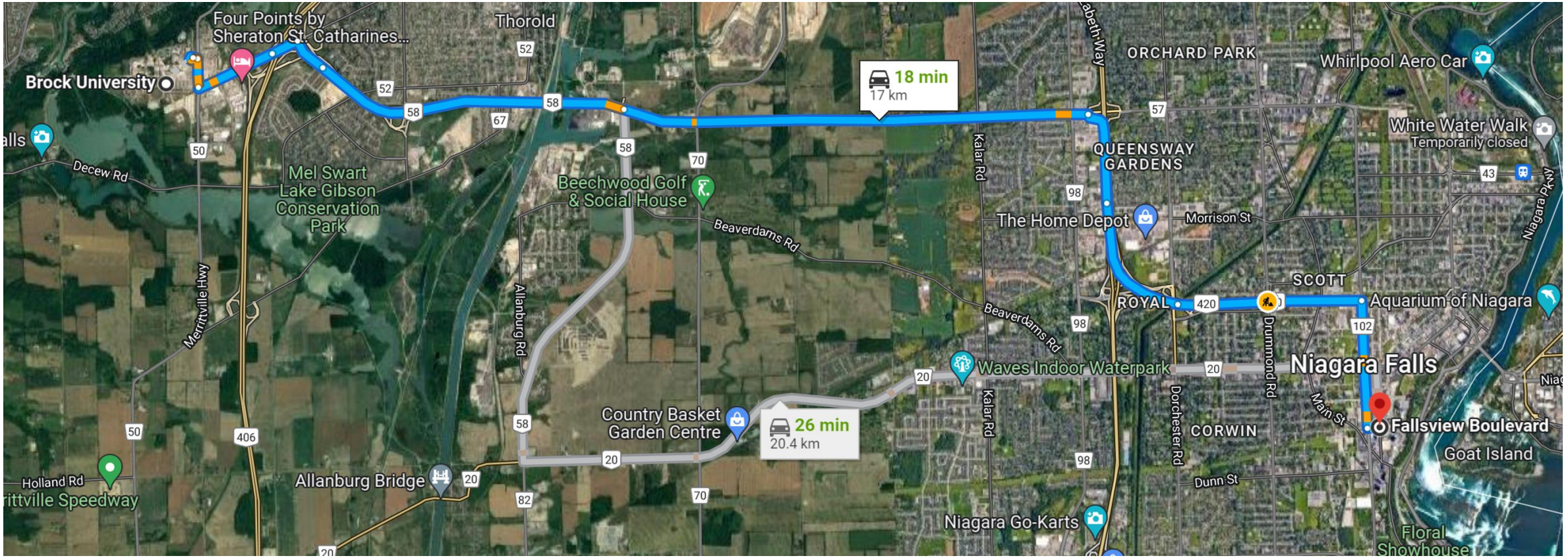
Outline

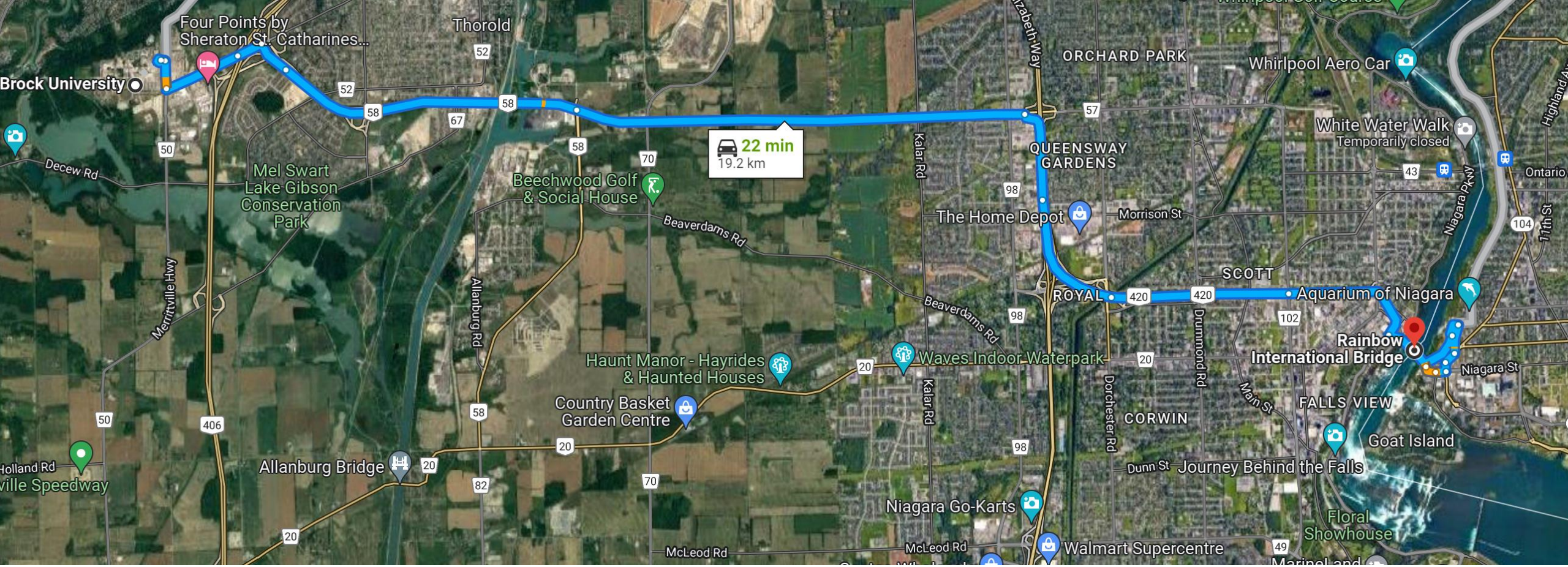
- Introduction
- AI-Empowered Cybersecurity
- Opportunities for AI-Empowered Cybersecurity
- Challenges for AI-Empowered Cybersecurity
- Some Results
- Looking ahead

Introduction

Brock University

Attractive Features: Horseshoe Falls

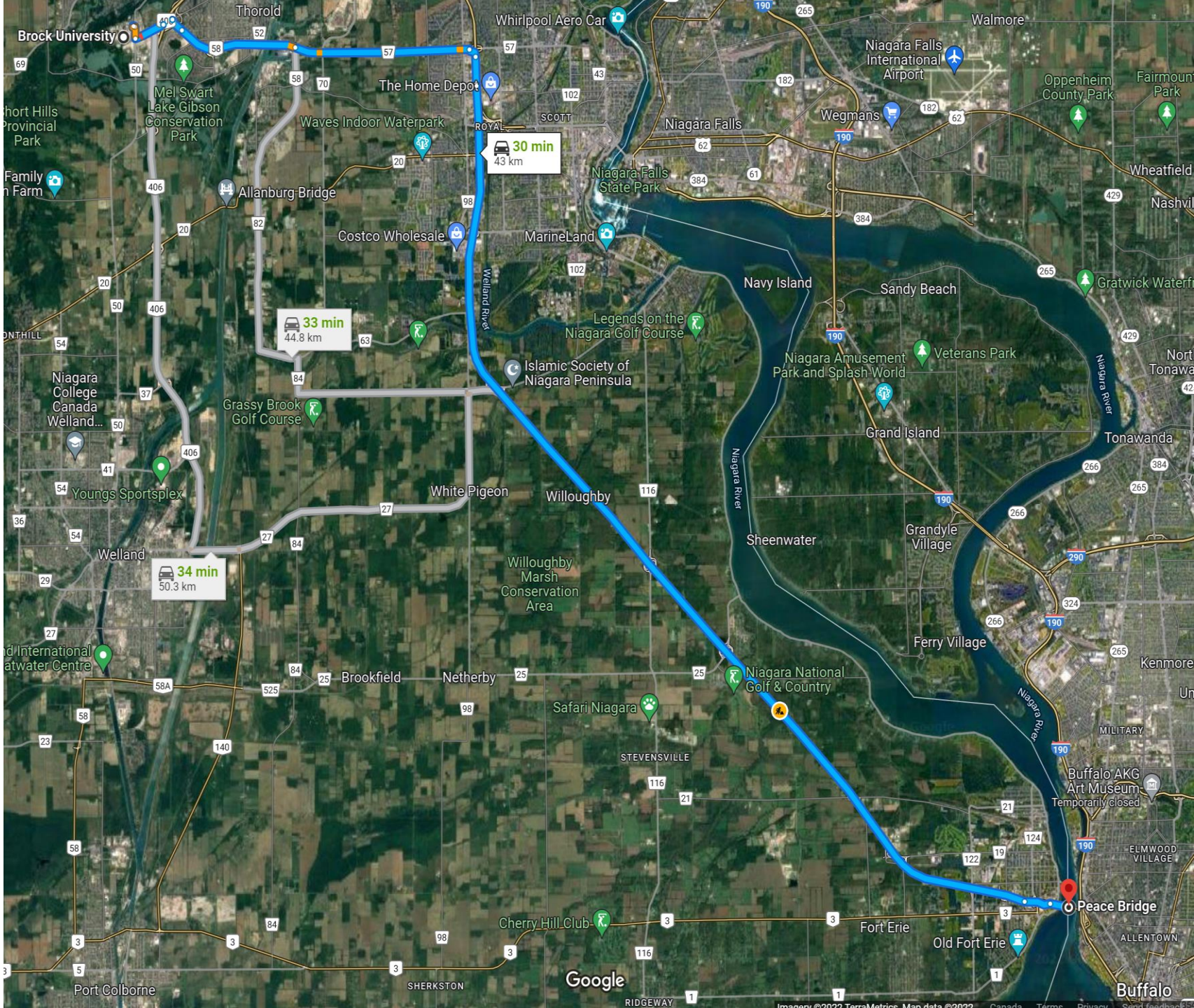




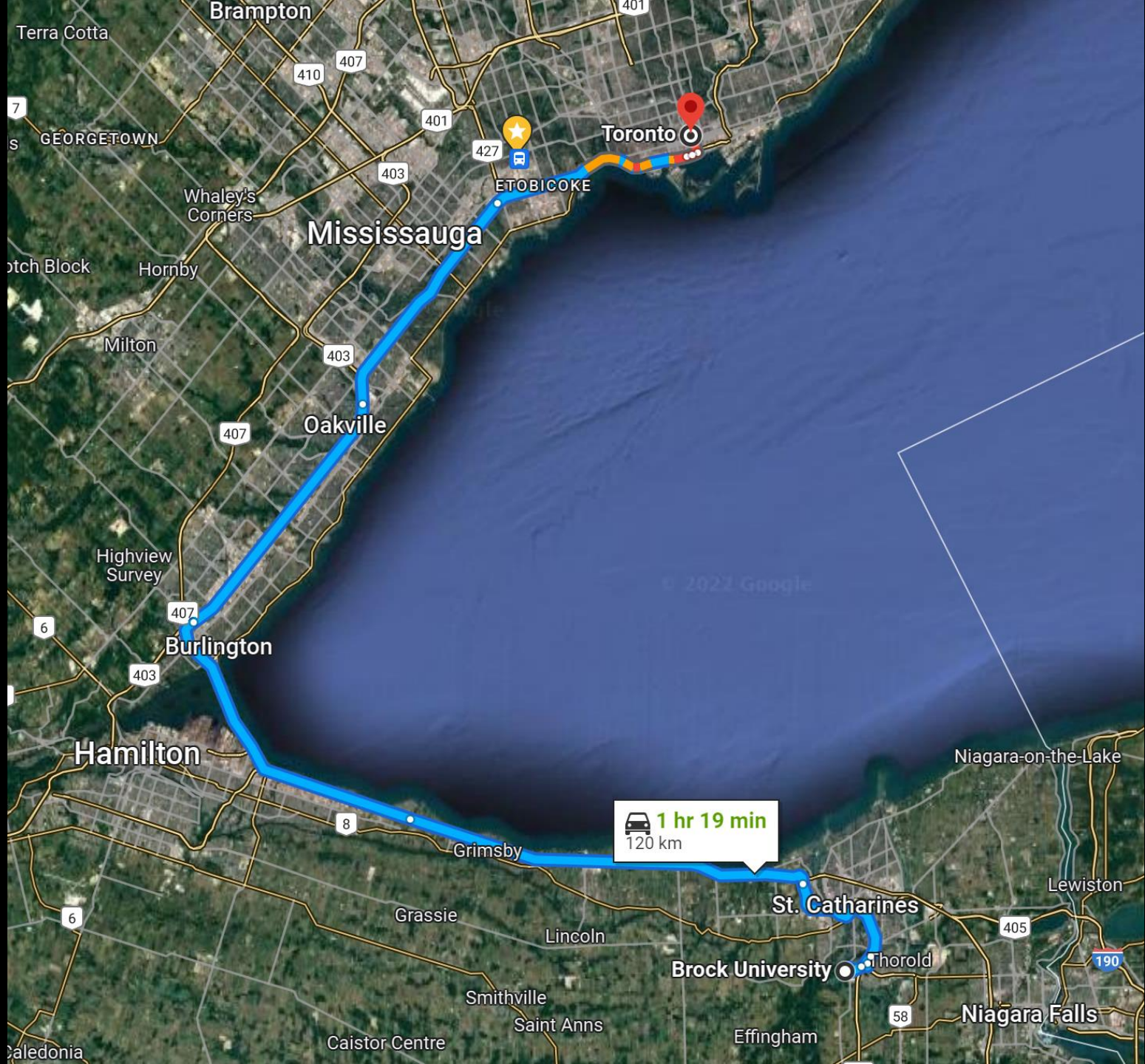
Attractive Features: Crossing to NY

Attractive Features

Crossing to NY



Attractive Features: I can see the CN Tower ☺



Who I am

Dr. Glaucio Carvalho (he/him)

Cross-Appointed Assistant Professor

- Department of Computer Science and the Department of Engineering
  - Undergraduate Program.
  - Master of Science (MSc)
  - Doctor of Philosophy (PhD)
    - Intelligent Systems and Data Science (PhD)

Research Interests

- Cybersecurity
  - Cyber Critical Infrastructure Protection
    - 5G, B5G & 6G
  - Ever Evolving Cyber Analytics
    - Control Techniques, Game theory, RL, ML, System Optimization.
    - Observability
  - Offensive Security
    - Attack & Defense approach

AI-Empowered Cybersecurity

What is it?

The use of AI to execute and enforce security, protection, and privacy mechanisms

Why

5G, B5G & 6G will be characterized by a massive number of connected devices, high traffic volume, diverse technologies, and services

Lead to a complex and dynamic cyber-threat landscape.

AI is a promising approach.

Empower intelligent, adaptive and autonomous security management.

Opportunities for AI-Empowered Cybersecurity

AI as a Shield

Traditional cybersecurity techniques might not be enough to defend against advanced cyber threats to 5G, B5G, & 6G

AI can be leveraged to add intelligence and augment the defense capabilities

AI CyberSec use cases will promote innovations.

Challenges for AI-Empowered Cybersecurity

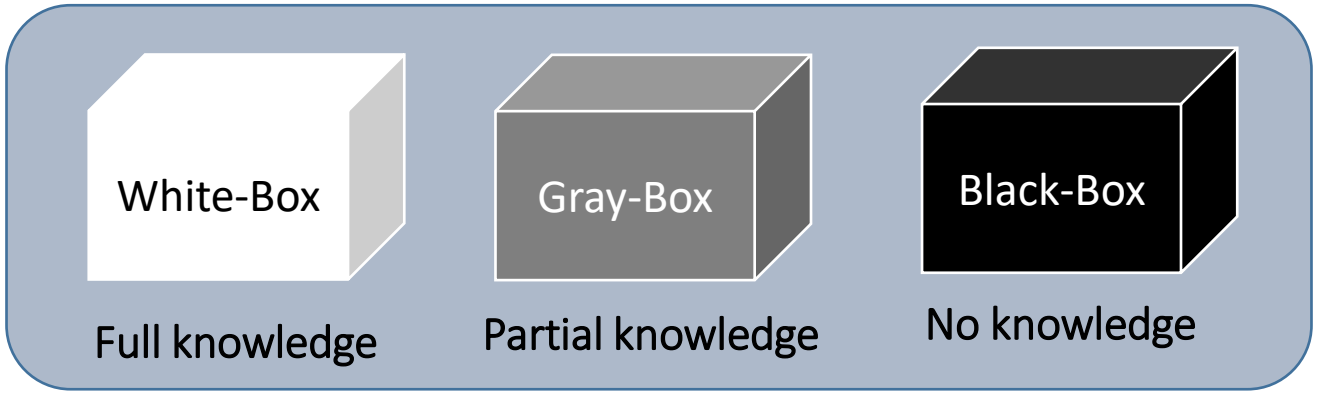
AI as a Target

- B5G & 6G networks will depend upon AI to realize the Self-X O&M
- AI an attractive target for attackers
- AI is vulnerable to **Adversarial Attacks**
  - ML systems can be deceived to make wrong decisions.

Adversarial ML Attacks

Box testing

- Specify the level of access the attacker has to the training data, the learning algorithm and its hyper-parameters.



Hacking CIA Triad

Confidentiality	• Goal: gaining knowledge of sensitive information about the training data, the ML system, or its users
Integrity	• Goal: evading detection without affecting normal behavior of the system
Availability	• Goal: deteriorating the system usability

Brock University

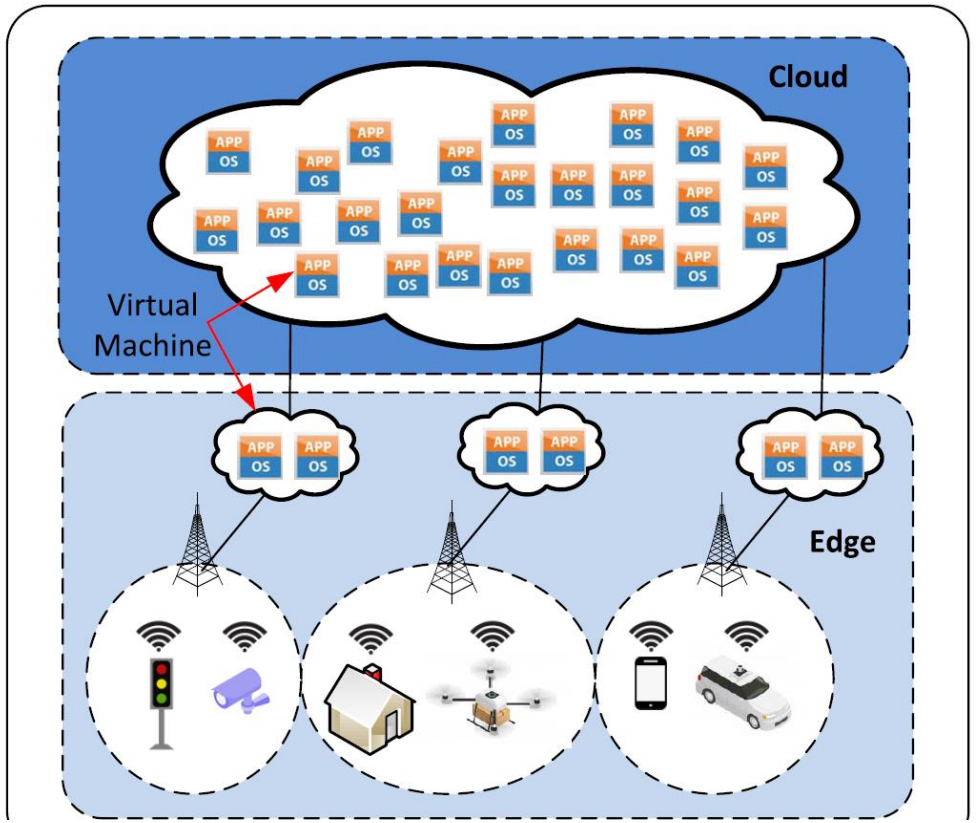
AI as a Hacker

AI can be weaponized to

- Perform massive online surveillance
- Attack systems – *DeepLocker (IBM)*

Some Results

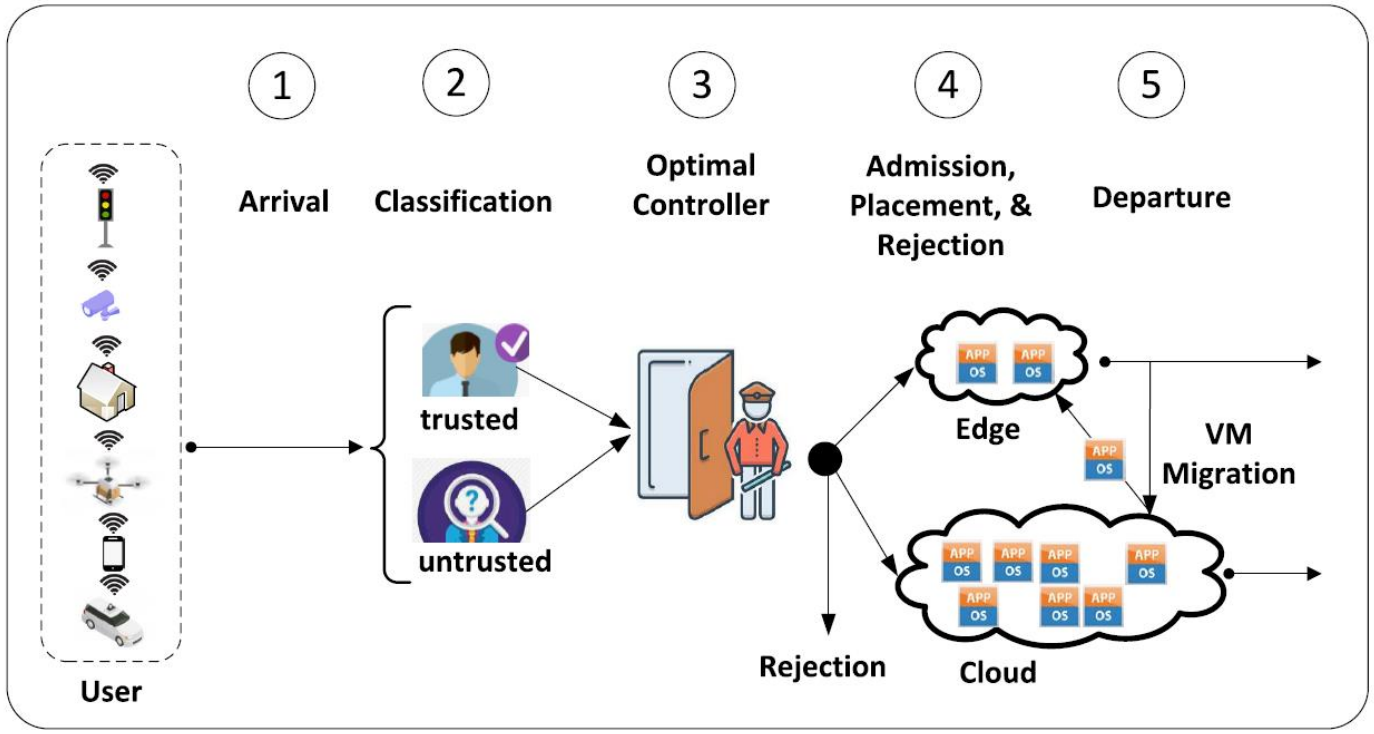
AI as a Shield



Optimal Security Risk Management for 5G Cloudified Infrastructure

- Manage the cyber risk dynamically across the edge-cloud systems
- Specify the system as a sequential decision-making process
- Use Markov Decision Process framework to model the system

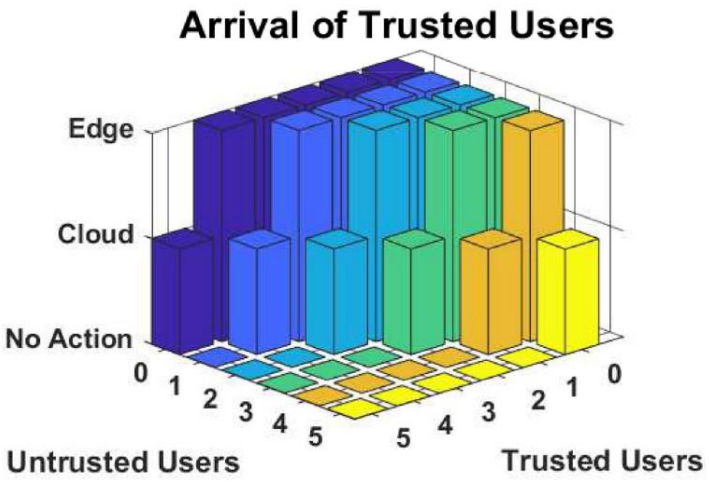
Brock University

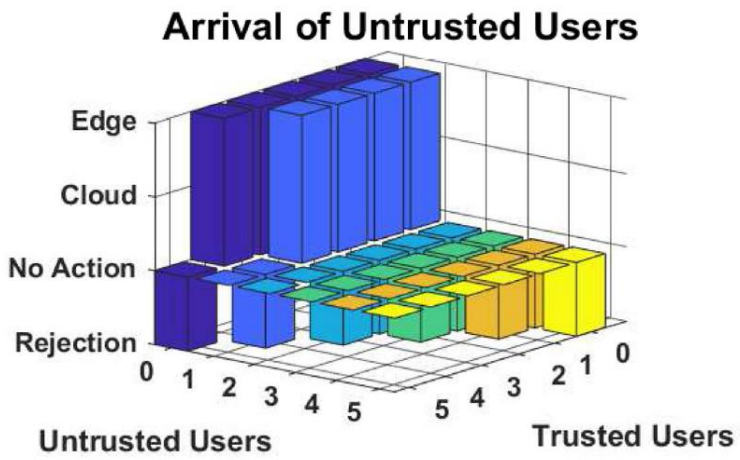


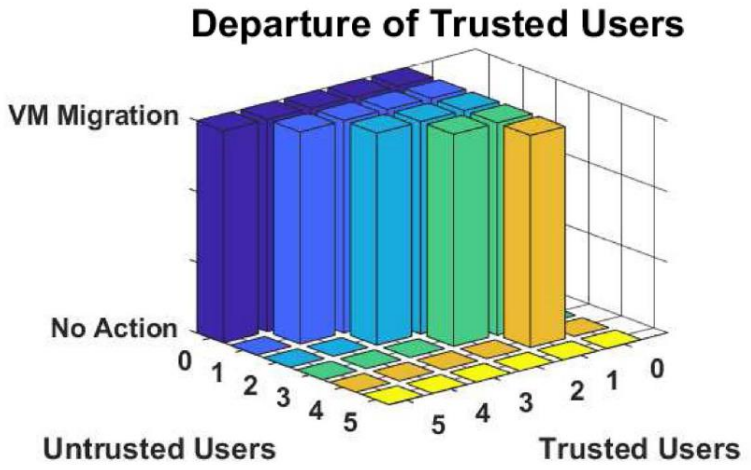
Objective

- Deflate the risk of DoS
- Maximize latency compliance

Structural Analysis of the Optimal Policy

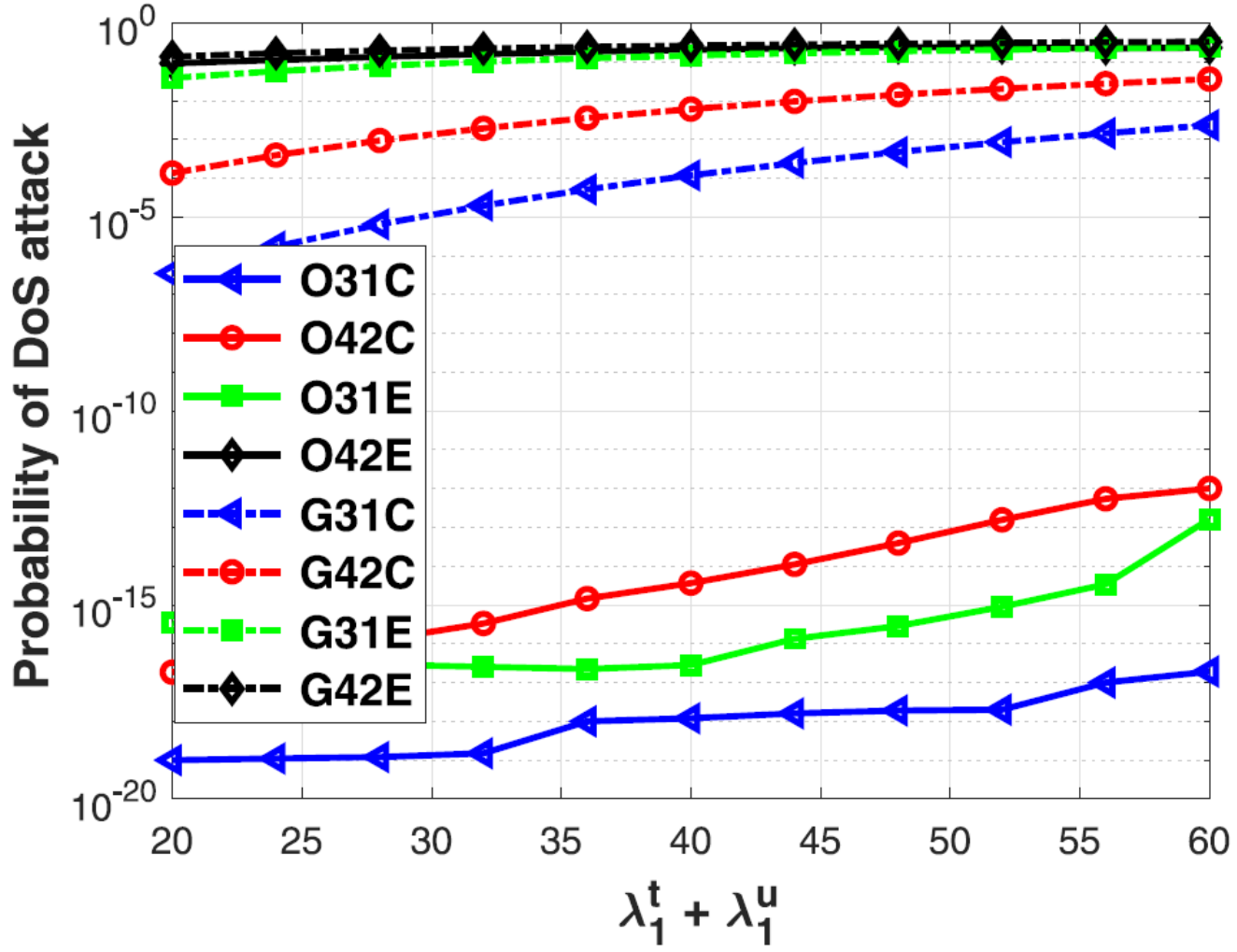






Brock University

Performance Comparison



Full Reference

Optimal Security Risk Management Mechanism for the 5G Cloudified Infrastructure

Glaucio H. S. Carvalho, Isaac Woungang, *Senior Member, IEEE*, Alagan Anpalagan, *Senior Member, IEEE*, and Issa Traore, *Member, IEEE*

***Abstract*—This work proposes an optimal security risk management mechanism to holistically minimize the risks of a Denial of Service (DoS) attack and Service Level Agreement (SLA) violations that might unfold at the 5G edge-cloud ecosystem. Using the Semi-Markov Decision Process framework, a cyber risk-aware controller is designed to optimally decide on the admission, placement, and migration of a service taking into consideration a user taxonomy and the service requirements. A new cost structure that balances the targeted security risks as well as the cost and the reward of a secure service provisioning is introduced to pave the way for a safe edge-cloud operation. To proactively restrict the population of untrusted users, we consider security controls in the form of a linear and an exponential cost functions and show that the former represents a more flexible and profitable pathway for a Mobile Network Operator to operate at the expense of an inflated security risk while the latter leads to the opposite outcome. Results show that the baseline mechanism might violate the SLA and expose the edge and the cloud to a DoS attack in levels that are 10^2, 10^{12}, and 10^{14} times higher than those of the proposed controller.**

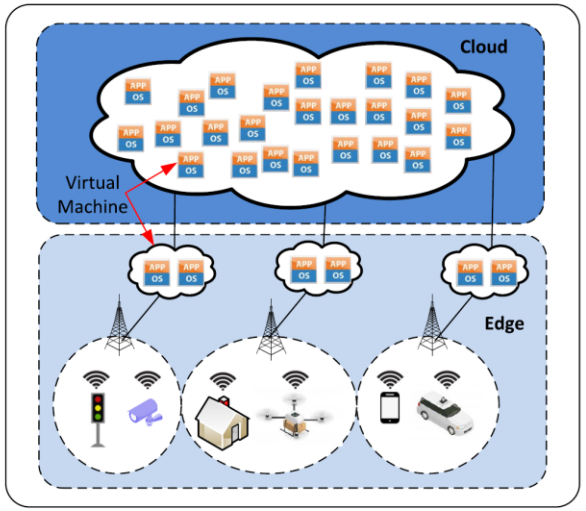
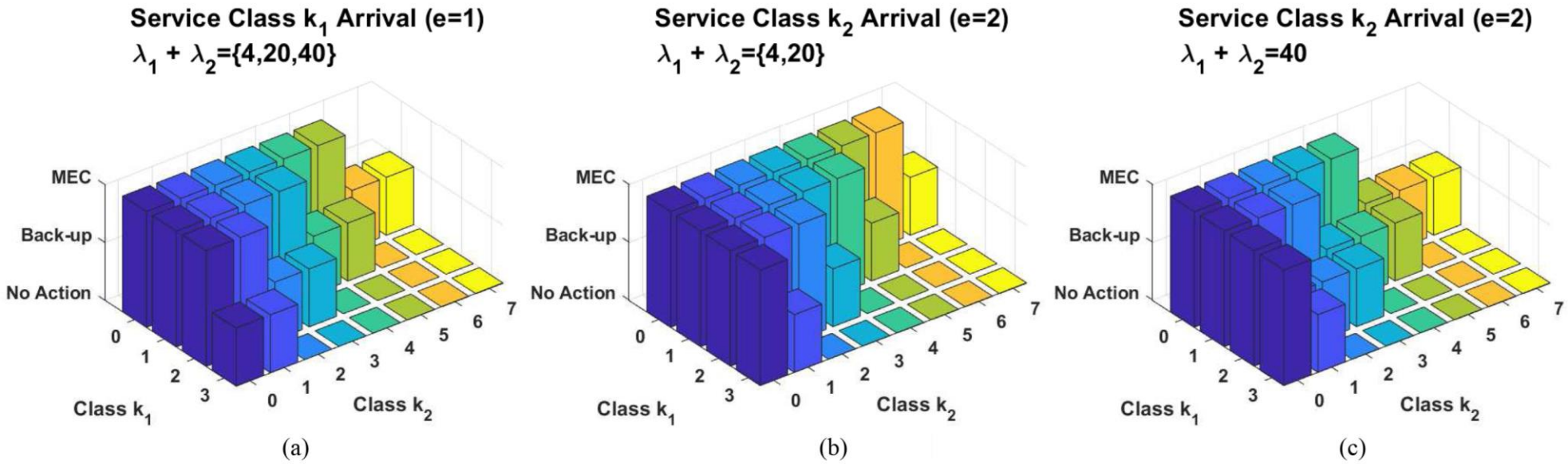


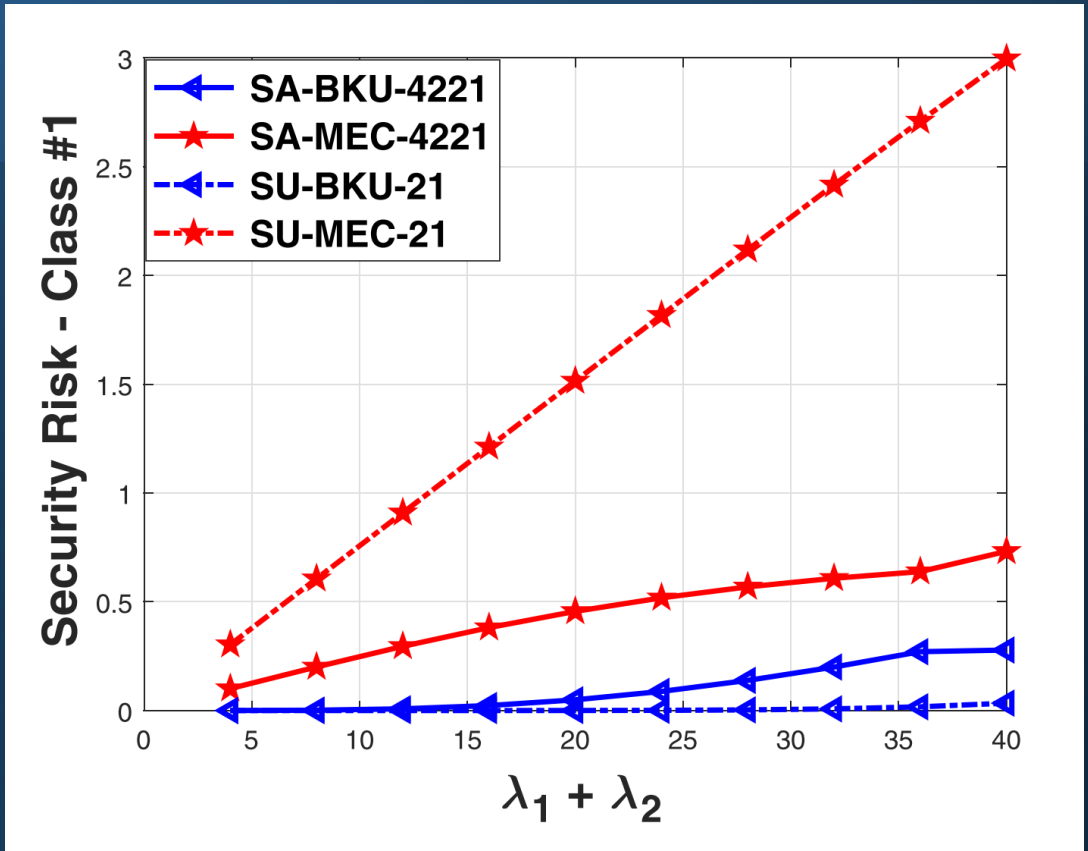
Fig. 1. Edge-cloud 5G architecture.

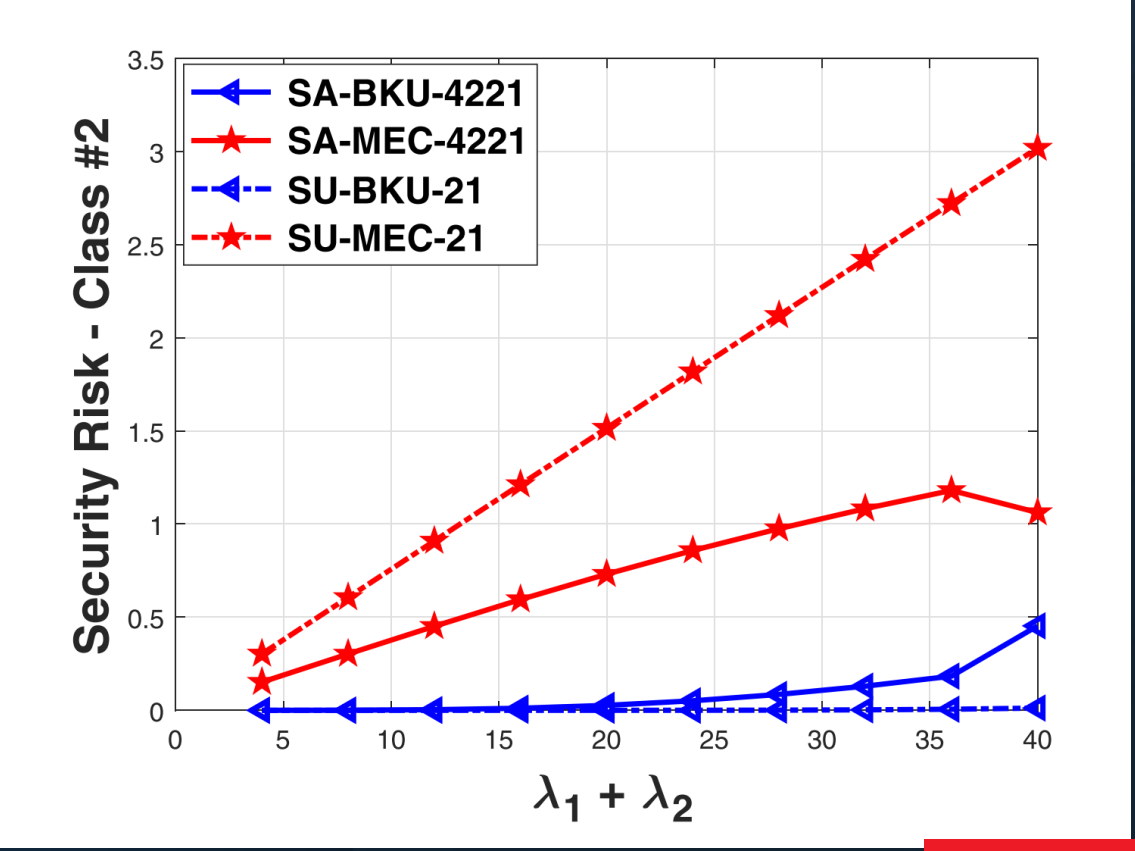
Optimal Security-Aware Virtual Machine Management for Mobile Edge Computing over 5G Networks

- Assess the cyber risk based on the attack surface area and defense capabilities
- Maximize latency compliance for service classes



Performance Comparison





Brock University

Full Reference

IEEE SYSTEMS JOURNAL, VOL. 15, NO. 3, SEPTEMBER 2021

Optimal Security-Aware Virtual Machine Management for Mobile Edge Computing Over 5G Networks

Glaucio H. S. Carvalho, Isaac Woungang, Alagan Anpalagan, *Senior Member, IEEE*, and Issa Traore

***Abstract*—A secure execution of offloaded tasks in the 5G-driven mobile edge computing (MEC) deployment is critical for all societal sectors. To realize it, mobile network operators have to intelligently orchestrate virtual resources in multiple cloud layers to satisfy 5G security requirements. In this article, we formulate a secure virtual machine management (VMM) mechanism using the semi-Markov decision process framework that seeks to jointly minimize the service rejection and the security risk, while meeting the location awareness requirements of latency-sensitive applications in a decentralized fashion. A new metric called mean security risk is proposed to quantify the perceived risk of an offloaded application considering the number of virtual machines (VMs) that is used to execute and to protect it. We also propose a new cost structure that allows for an efficient assessment of the long-term impact of providing additional VMs to foster security services. A comparison with an optimal security-unaware VMM mechanism shows that our model provides a less risky operation at the cost of an increase in service rejection, which is caused by the use of additional VMs to shield the computation task. Finally, we show that the cost of providing security services can be significantly reduced by fine-tuning the economic gains of it.**

***Index Terms*—Cloud security, mobile edge computing (MEC) security, stochastic optimal control, 5G security.**

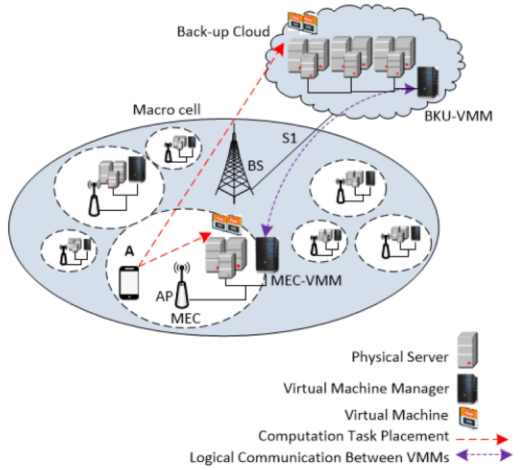


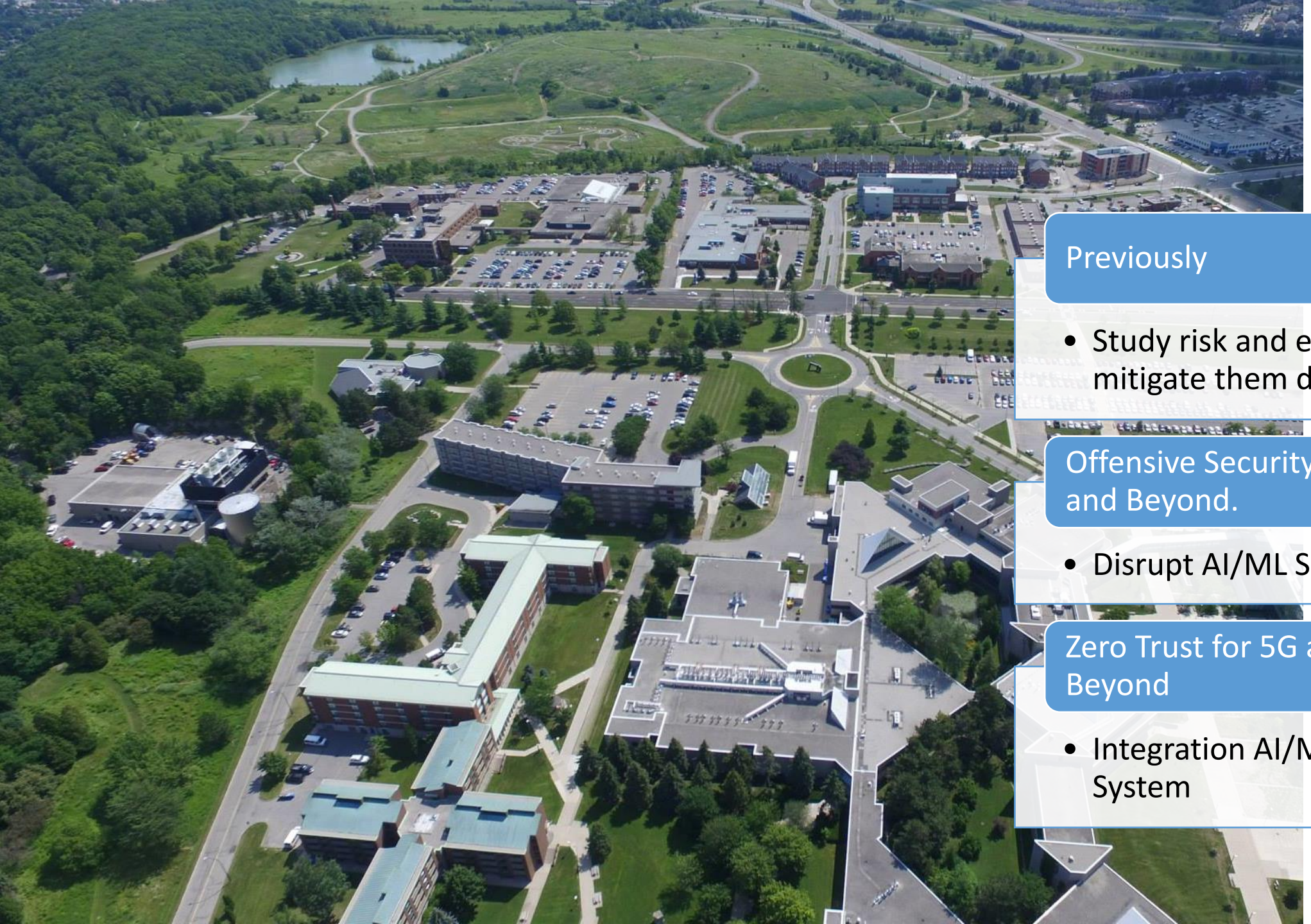
Fig. 1. 5G-driven MEC deployment with backup cloud.

I. Introduction

mobile network operators (MNO) may also leverage multiple cooperative cloud layers [1]–[3]. An instance of this practice is the use of a robust and resource-rich backup cloud to augment

Brock University

Looking Ahead



Previously

- Study risk and embed controls to mitigate them dynamically.

Offensive Security for 5G and Beyond.

- Disrupt AI/ML Self X O&M

Zero Trust for 5G and Beyond

- Integration AI/ML and Zero Trust System

Thank you and how can I help IEEE INGR Security WG?