Hybrid ML-based Anomaly Detection System for Intra-Vehicular Communication Networks and Cyber Investment Optimization using Game Theory for EV Charging Infrastructure

This presentation was given at the 2023 National Cybersecurity Education Colloquium

CAE-R COP RESEARCH SYMPOSIUM 2023

Shaurya Purohit

Major Professor: ***Dr. Manimaran Govindarasu***

IOWA STATE UNIVERSITY

Contents

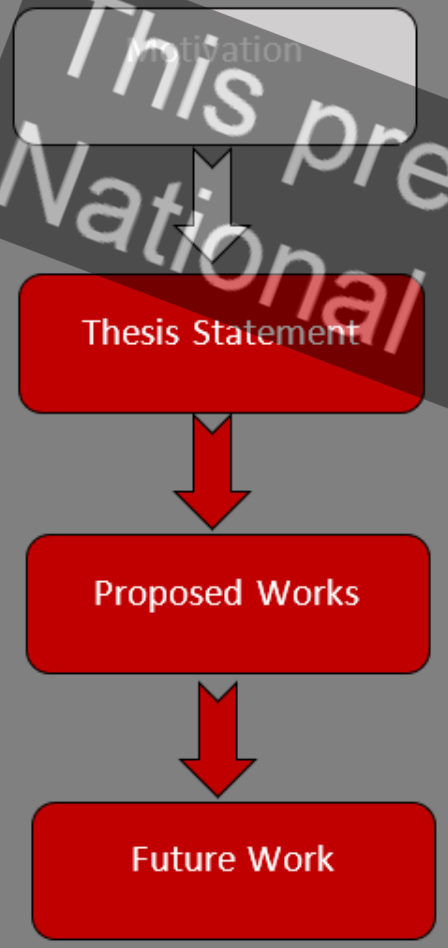
- ✓ Motivation
- ✓ Thesis Statement
- ✓ Proposed Works
- ✓ Conclusion/ Future Work

This presentation was given at the 2023 National Cybersecurity Education Colloquium

This presentation was given at the 2023 National Cybersecurity Education Colloquium

MOTIVATION

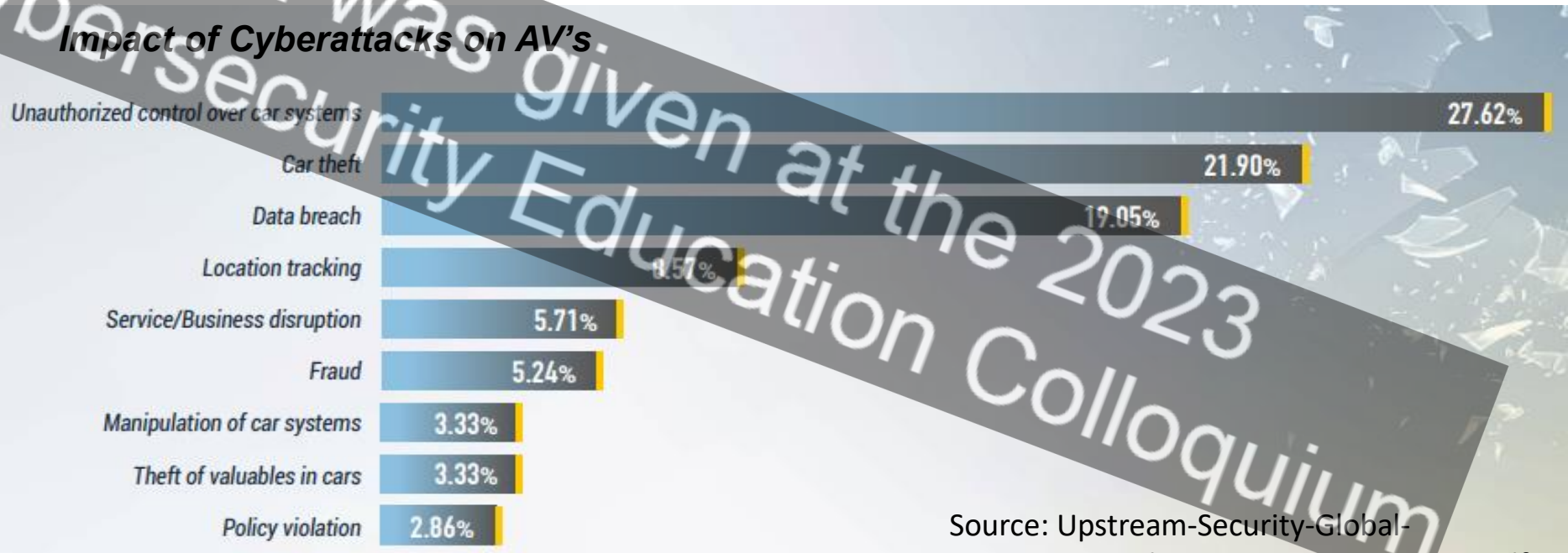
Cybersecurity of Modern Vehicles



This presentation was given at the 2023 National Cybersecurity Education Colloquium

- ✓ The use of autonomous and connected vehicles has become more and more common, a trend that will continue in the foreseeable future.
- ✓ However, with the higher level of autonomy, security problems are escalated due to the complex software and increased functionality to adversaries.

Impact of Cyberattacks on AV's



Source: Upstream-Security-Global-Automotive-Cybersecurity-Report-2019.pdf

How do attackers get in?

This presentation was given at the 2023 National Cybersecurity Education Colloquium

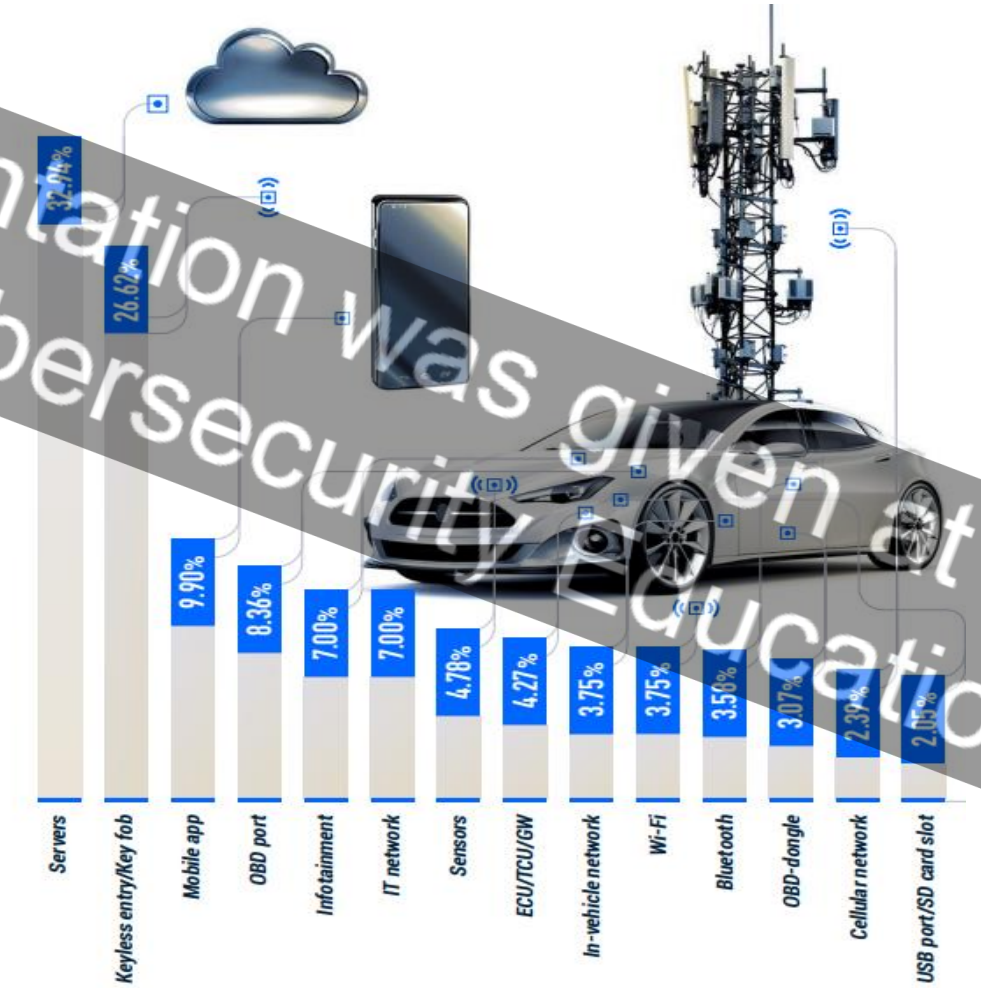
Motivation

Thesis Statement

Proposed Works

Future Work

Breakdown of Top Attack Vectors (2010-2020)



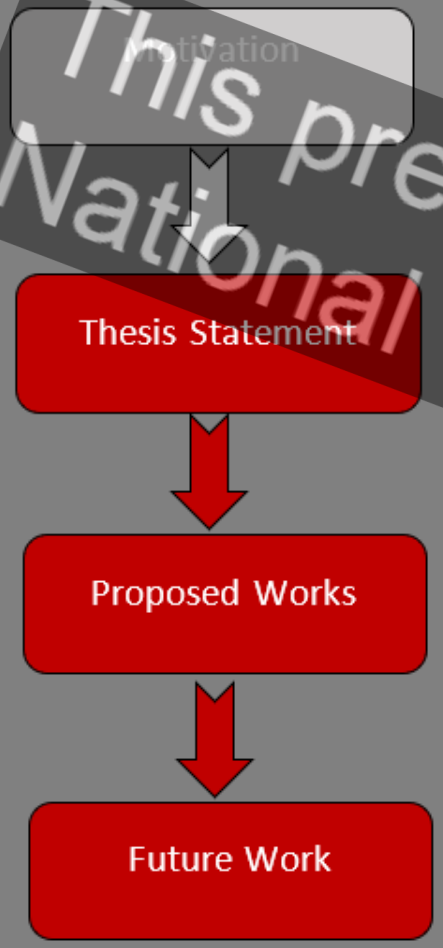
Source: Upstream-Security-Global-Automotive-Cybersecurity-Report-2021.pdf

- ✓ Remotely hijacking vehicles via compromised CAN bus.
- ✓ Exploiting vulnerabilities in software, hardware, operating systems, and protocols.

.

- ✓ Attacking via a malicious app installed on a mobile phone connected via bluetooth.
- ✓ Electronically jamming an autonomous car's safety systems, such as radar and lidar.
- ✓ Compromising a third-party software supply chain to push malicious updates.
- ✓ Injecting malicious scripts via malvertising.

Scenario: AV Attack Surface



This presentation was given at the 2023 National Cybersecurity Education Colloquium

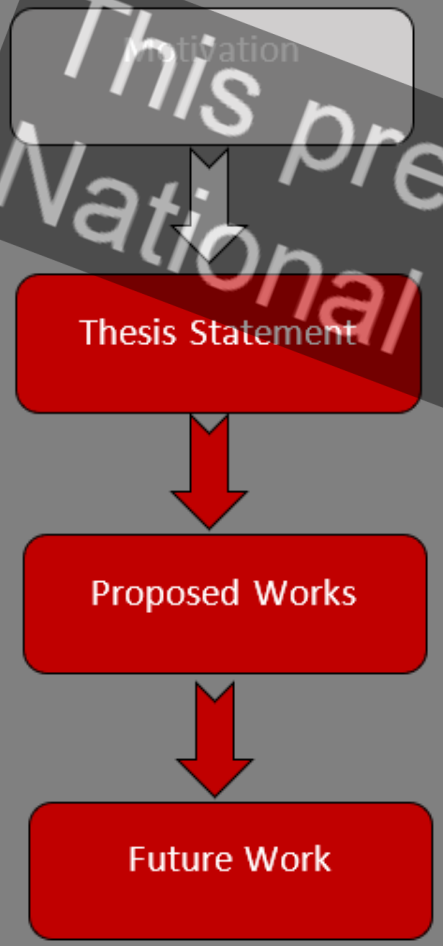
Hackers Remotely Kill a Jeep on the Highway

Tesla: A Tragic Loss

- First fatal crash while using Autopilot on May 7, 2016.
- Reliability of sensors.

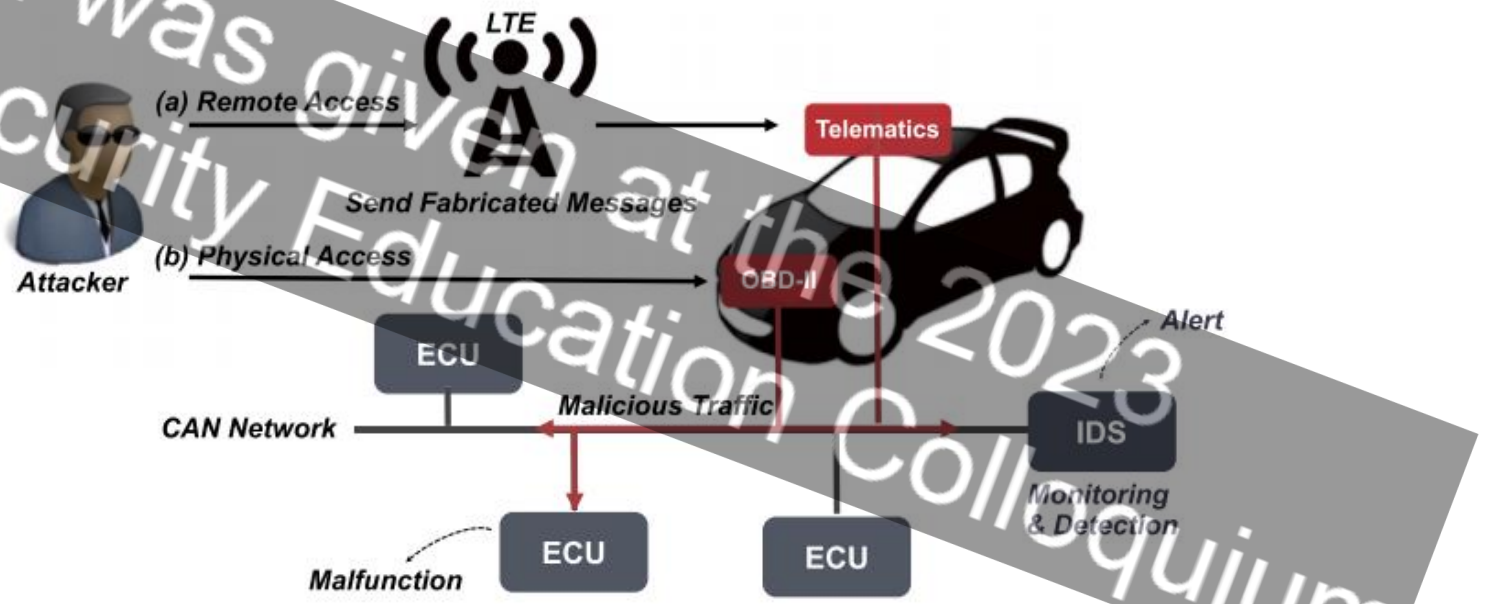
Source: https://www.theguardian.com/technology/2016/jun/30/tesla-autopilot-death-self-driving-car-elon-musk

This presentation was given at the 2023 National Cybersecurity Education Colloquium



Scenario: How CAN BUS can be attacked

- ✓ The authenticity of the received message cannot be confirmed – easily leads to forgery and tampering of the CAN bus message by injecting false information.
- ✓ An attacker can replay or flood the vehicle bus by means of sniffing or listening.
- ✓ For example, a malicious attacker will set an attack in a target frame of the CAN bus, which will cause the driver to lose control of the throttle position and thus prevent the car from moving.



Typical Fabricated Message Scenario [2]

Motivation

Thesis Statement

Proposed Works

Future Work

CPS Perspective of EV Charging Ecosystem

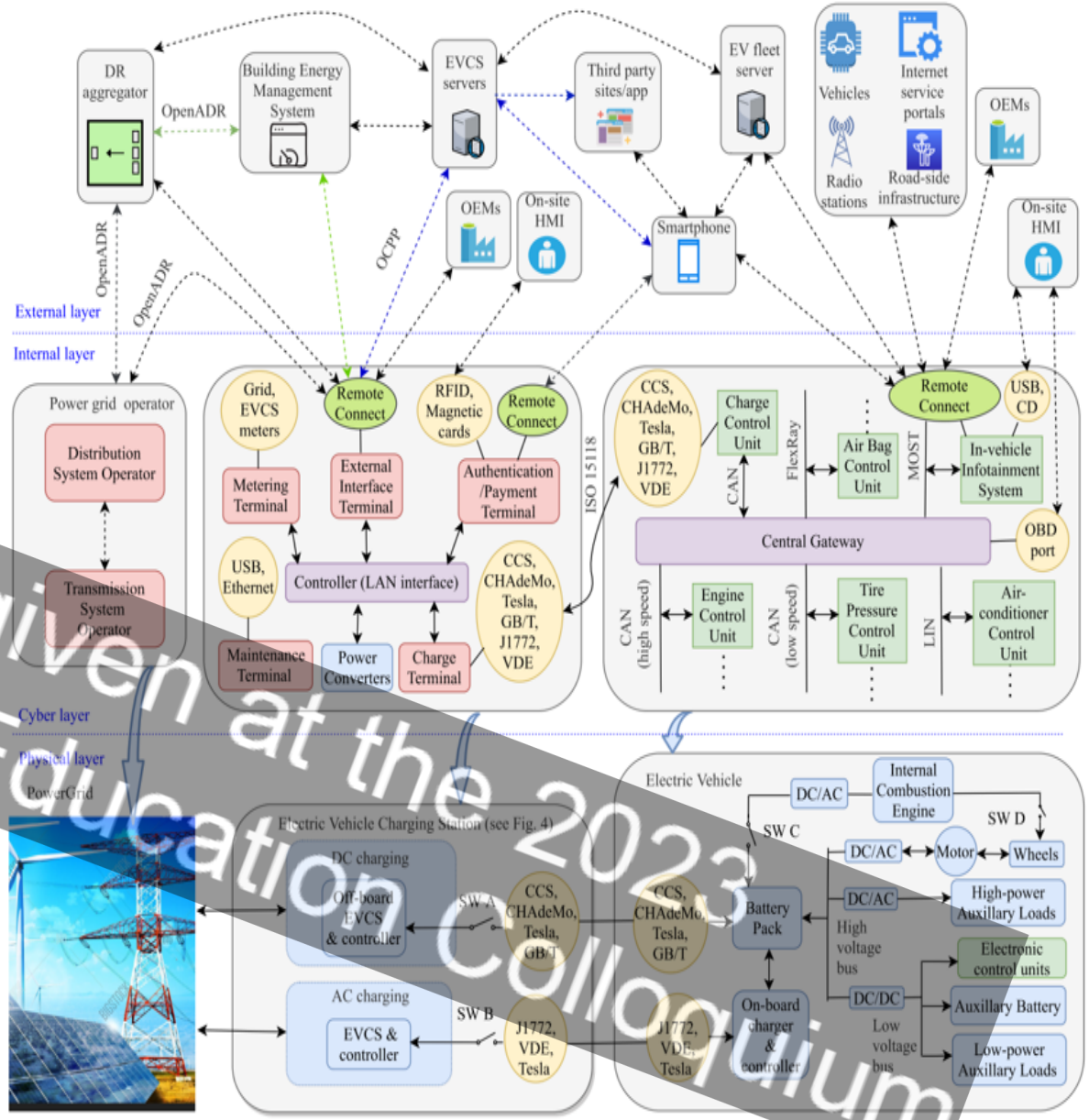
- *EVs are classified based on source of energy:*
  - *Battery Electric Vehicles (BEV)*
  - *Plug-in Hybrid Electric Vehicles (PHEV)*
  - *Hybrid Electric Vehicles (HEV)*
- ***Collectively called Plug-in Electric Vehicles (PEV)***

Cyber Layer Components:

- ECU
- Communication Protocols
- EVCS
- Physically Accessible Ports
- Internet Service Portals
- Radio Stations
- OEM/Vendors
- Roadside Infrastructure

Physical Layer Components:

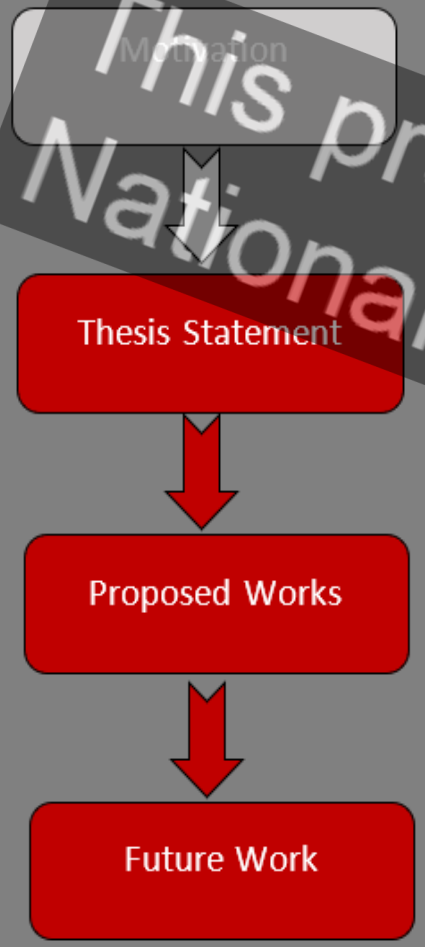
- Battery Unit
- Power Conditioning Unit (PCU)
- Motor & Loads

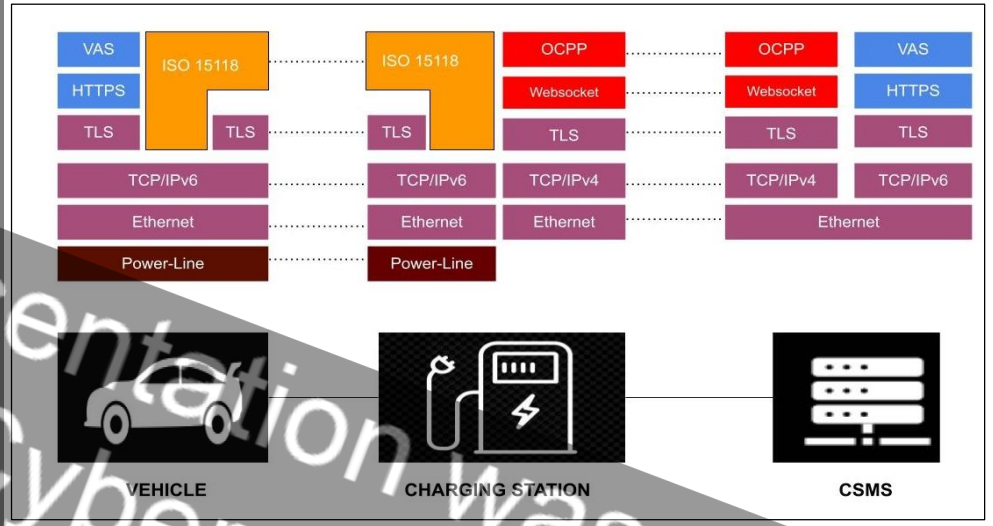


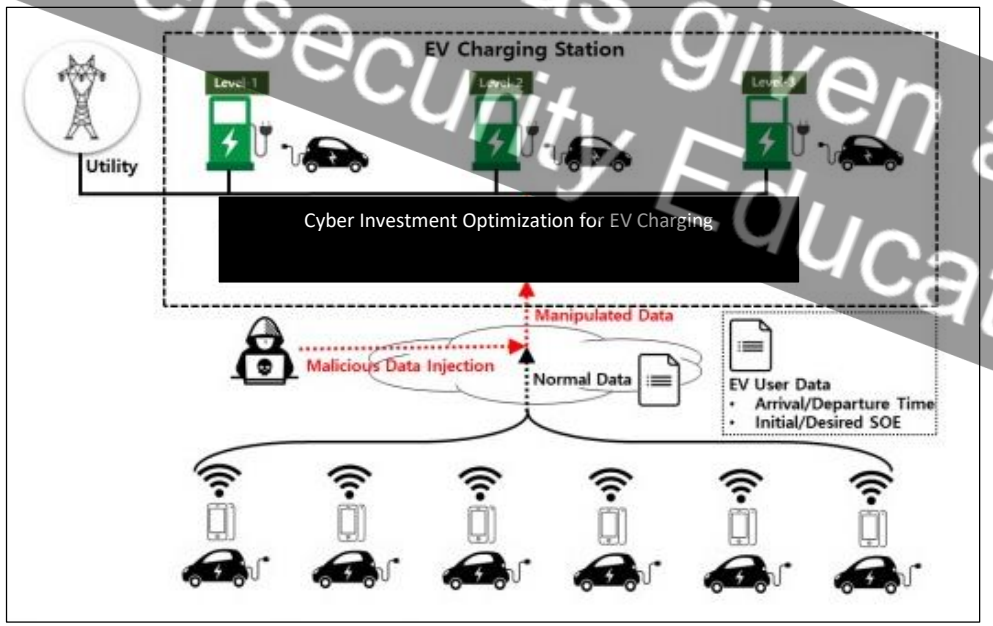
Ref: S. Acharya, Y. Dvorkin, H. Pandžić and R. Karri, "Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective," in IEEE Access, vol. 8, pp. 214434-214453, 2020, doi: 10.1109/ACCESS.2020.3041074.

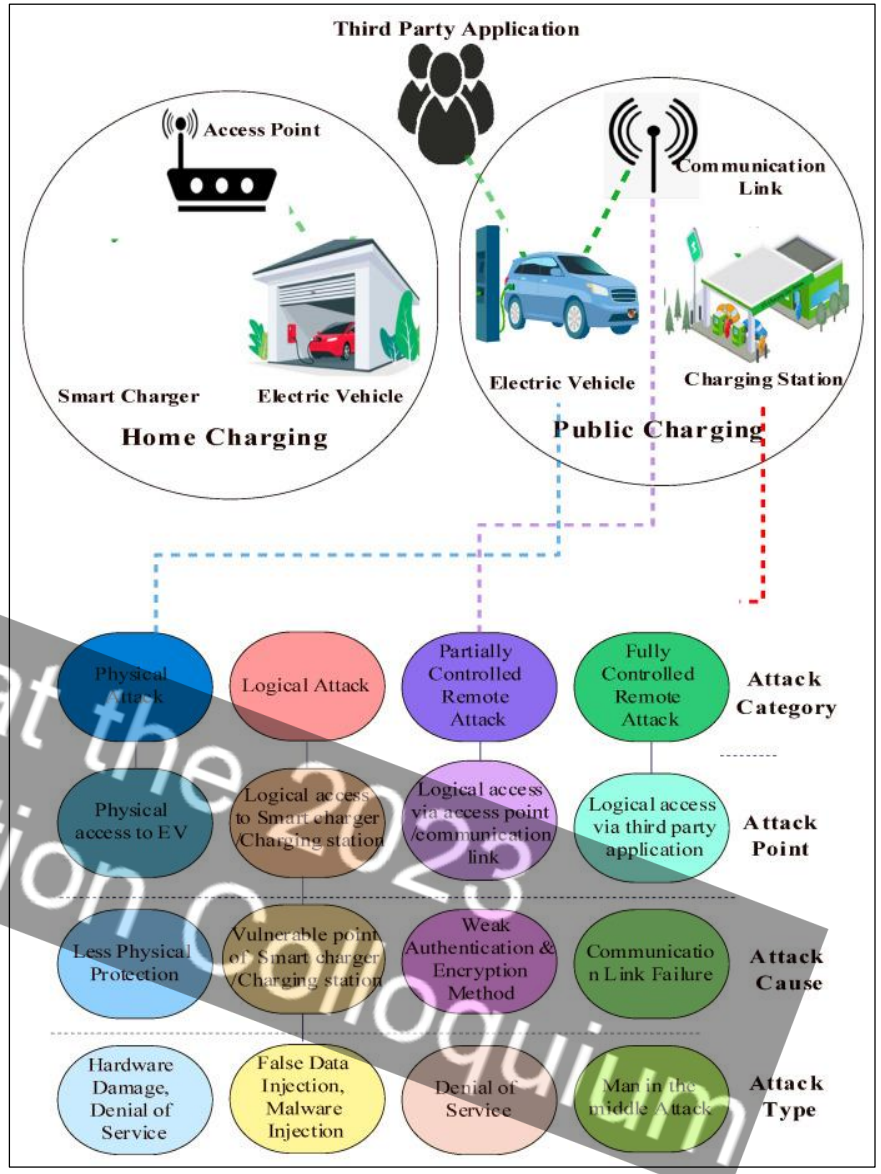
This presentation was given at the 2023 National Cybersecurity Education Colloquium

Communication in EVCS Infrastructure and Possible cyberattack on EV charging Infrastructure







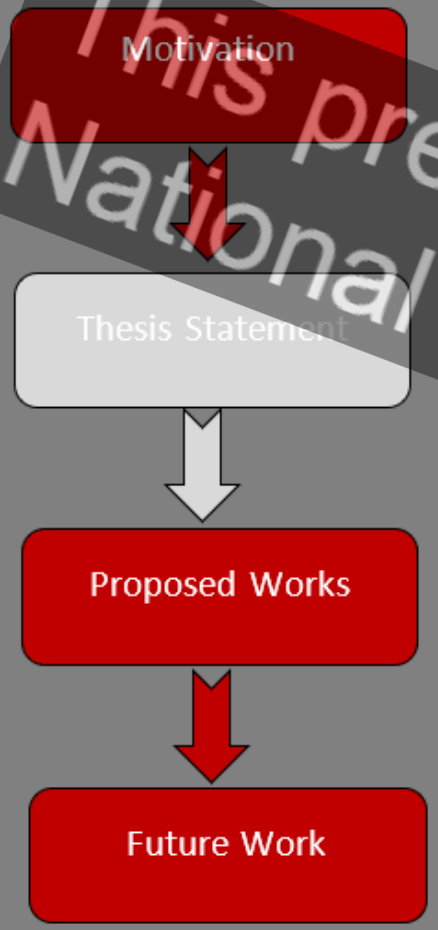


This presentation was given at the 2023 National Cybersecurity Education Colloquium

THESIS STATEMENT

This presentation was given at the 2023 National Cybersecurity Education Colloquium

Thesis Statement



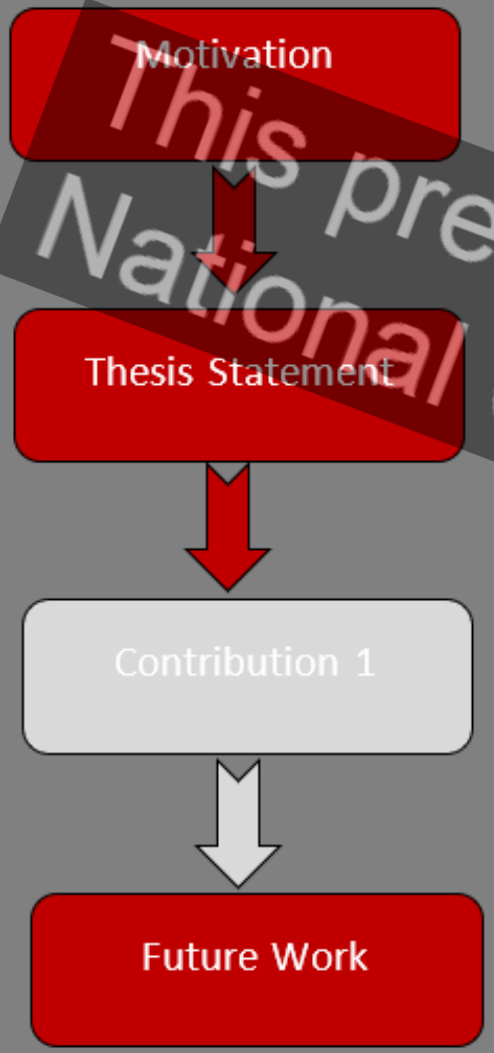
This presentation was given at the 2023 National Cybersecurity Education Colloquium

- ✓ In a world rapidly advancing towards digitization and automation, the *Autonomous vehicles and EV Charging Infrastructure* are pivotal elements in modern society, wielding the power to significantly influence the global social and economic spheres.
  - These systems, however, are increasingly becoming susceptible to *cyber-attacks* that exploit vulnerabilities in their control, information, and physical layers, posing catastrophic threats.
  - Recognizing the risk of adverse cyber-attack events, it becomes imperative to forge paths to secure the EV charging environment and autonomous vehicle networks steadfastly against adversarial actions, ensuring their stable, secure, and reliable operation.

- ✓ Our research steps in here, crafting resilient solutions through Machine Learning and Game Theory synergy.
  - ***Our work revolves around developing a hybrid anomaly detection system using ML and Neural Networks to secure CAN-bus intra-vehicular communications while strategically analyzing and optimizing investments in EV charging infrastructure using a combination of Attack defense trees and game theory, aiming for a future with advanced, secure transportation grids.***

PROPOSED WORKS

This presentation was given at the 2023 National Cybersecurity Education Colloquium



Contribution-1: Anomaly Detection System for Intra-Vehicular CAN-bus Networks

Topic-1: Hybrid Rule-ML based ADS

Research Objectives:
(1) Detection of cyber attacks in CAN-bus Networks of Autonomous Vehicles
(2) Achieving high accuracy and low false negatives with very low latency over major network attacks like DOS, Fuzzy, and Impersonation attacks.

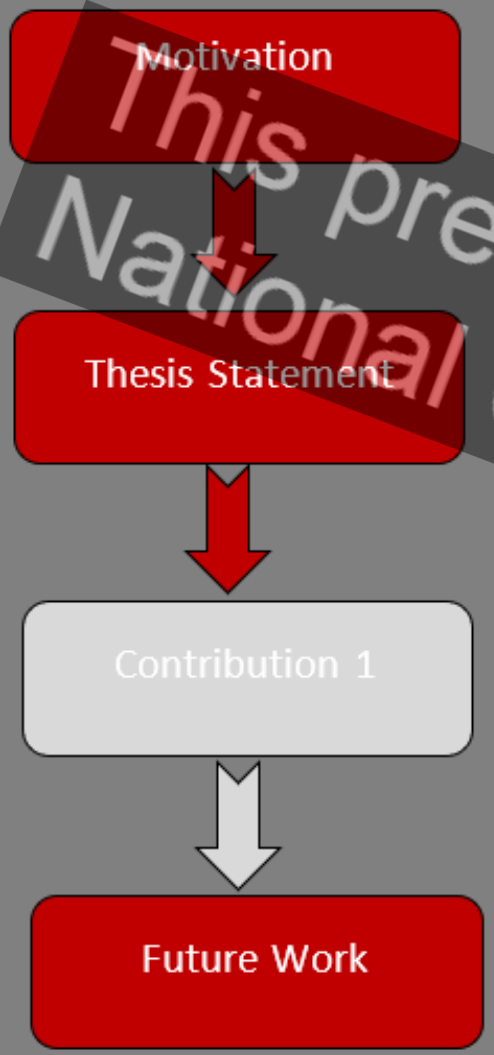
Methodology Used:
(1) Rule-based model for initial attack detection;
(2) Feature extraction
(3) Hybrid model of Rule based and ML algorithms like DT, RF and XGBoost to achieve high accuracy incurring low execution time.

Topic-2: HAVEN: Hybrid ADS for Intra-Vehicular CAN-bus Communication using Rule-based and Neural Networks

Research Objectives:
(1) Detection and mitigation of Broader network-based cyber attacks
(2) Enhancing Classification
(3) Expanded Assessment on different datasets

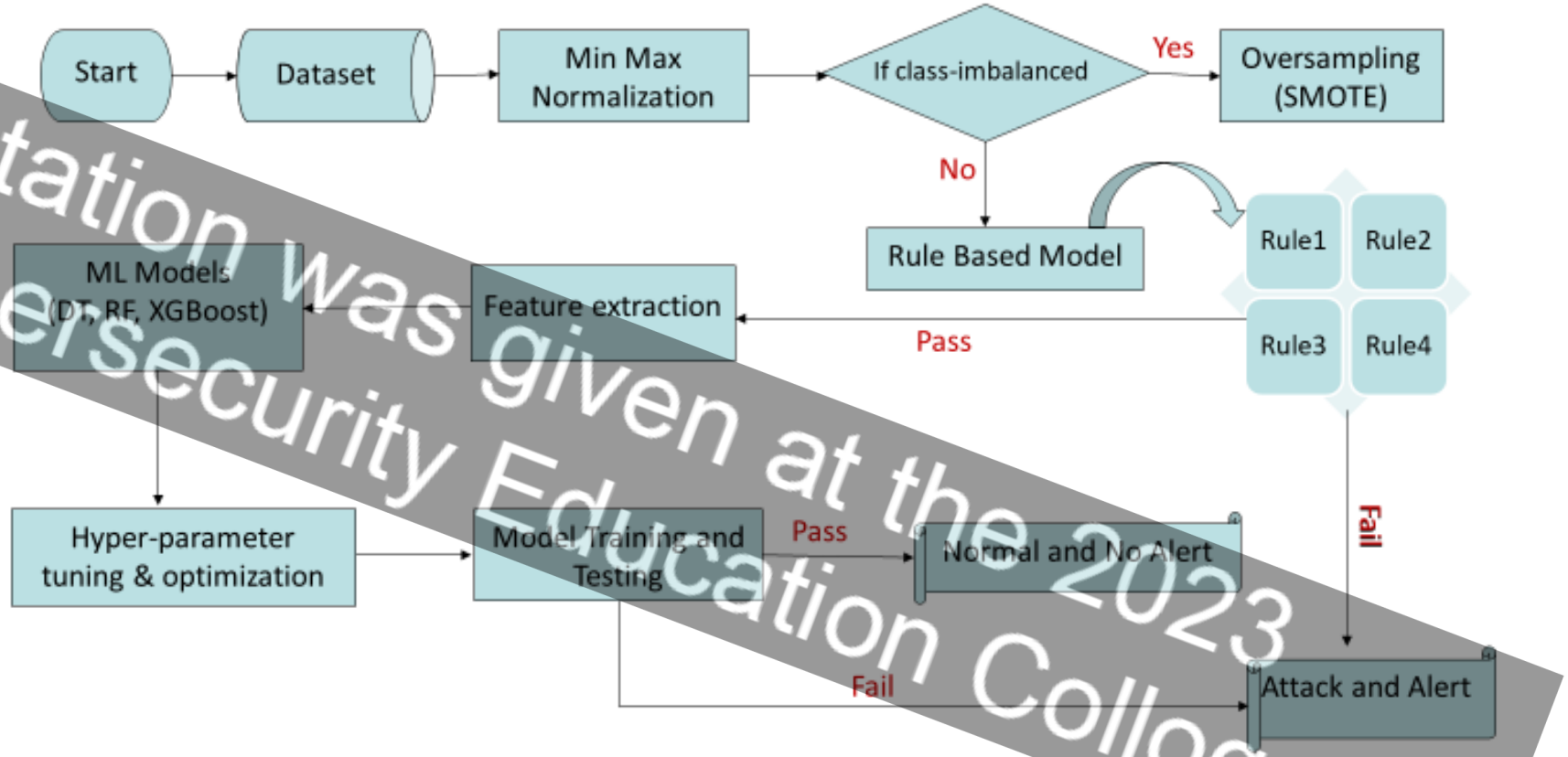
Methodology Used:
(1) Rule-based model for initial attack detection;
(2) Hybrid model of Rule based and Neural Networks to achieve even higher accuracy and much lower execution time on 3 different datasets (2 sourced from real cars and 1 simulated)

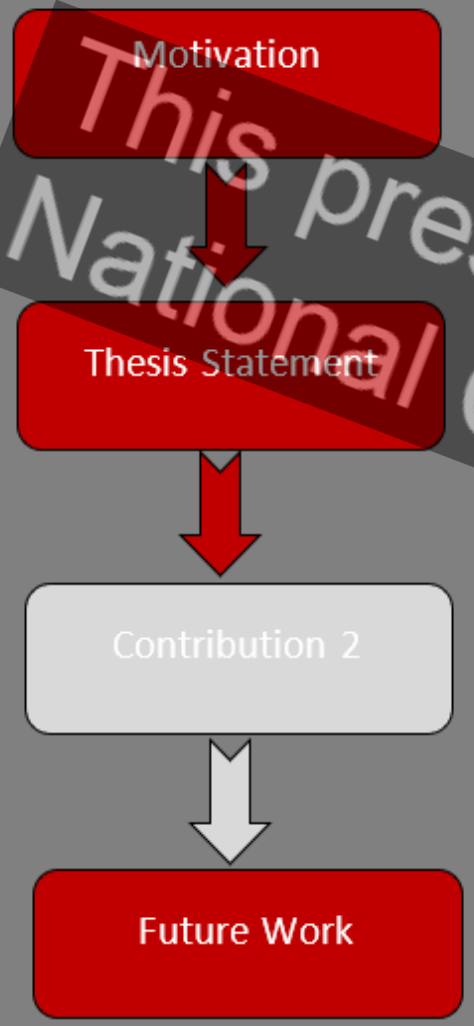
This presentation was given at the 2023 National Cybersecurity Education Colloquium



This presentation was given at the 2023 National Cybersecurity Education Colloquium

Proposed Hybrid ADS





Contribution-2: Cybersecurity Risk Investment Optimization for EV charging Infrastructure

Topic-1: Optimization of cybersecurity investments using Attack-Defense Trees and Game Theory

Research Objectives:
(1) Optimization of cybersecurity resource investments

Methodology Used:
(1) Attack defense trees for modeling attack surfaces in the EV Charging infrastructure
(2) CIA Triad Model and MITRE ATTACK Framework and defender models
(3) Game theory for optimization of cybersecurity resource investments using complete game like zero-sum game and Nash Equilibrium.

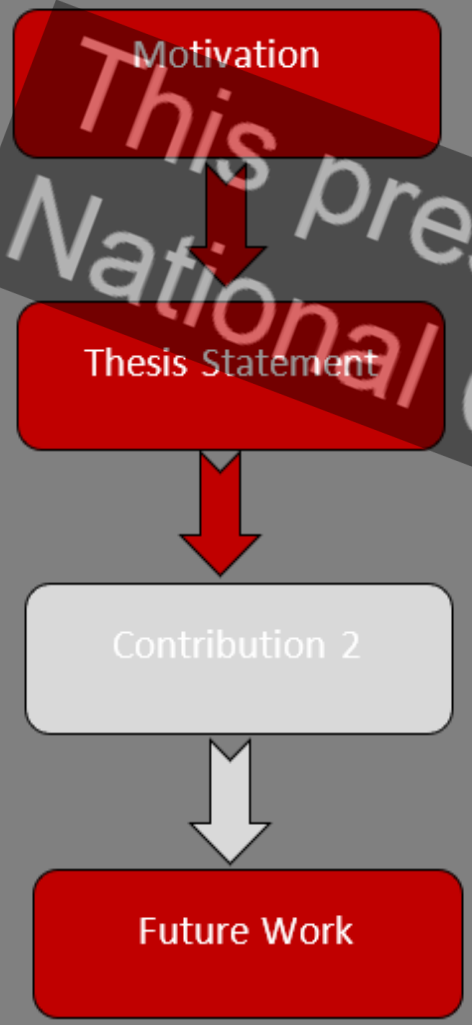
Topic-2: Risk Assessment and Optimization Enhancement of Security Investments using Game Theory (*Ongoing*)

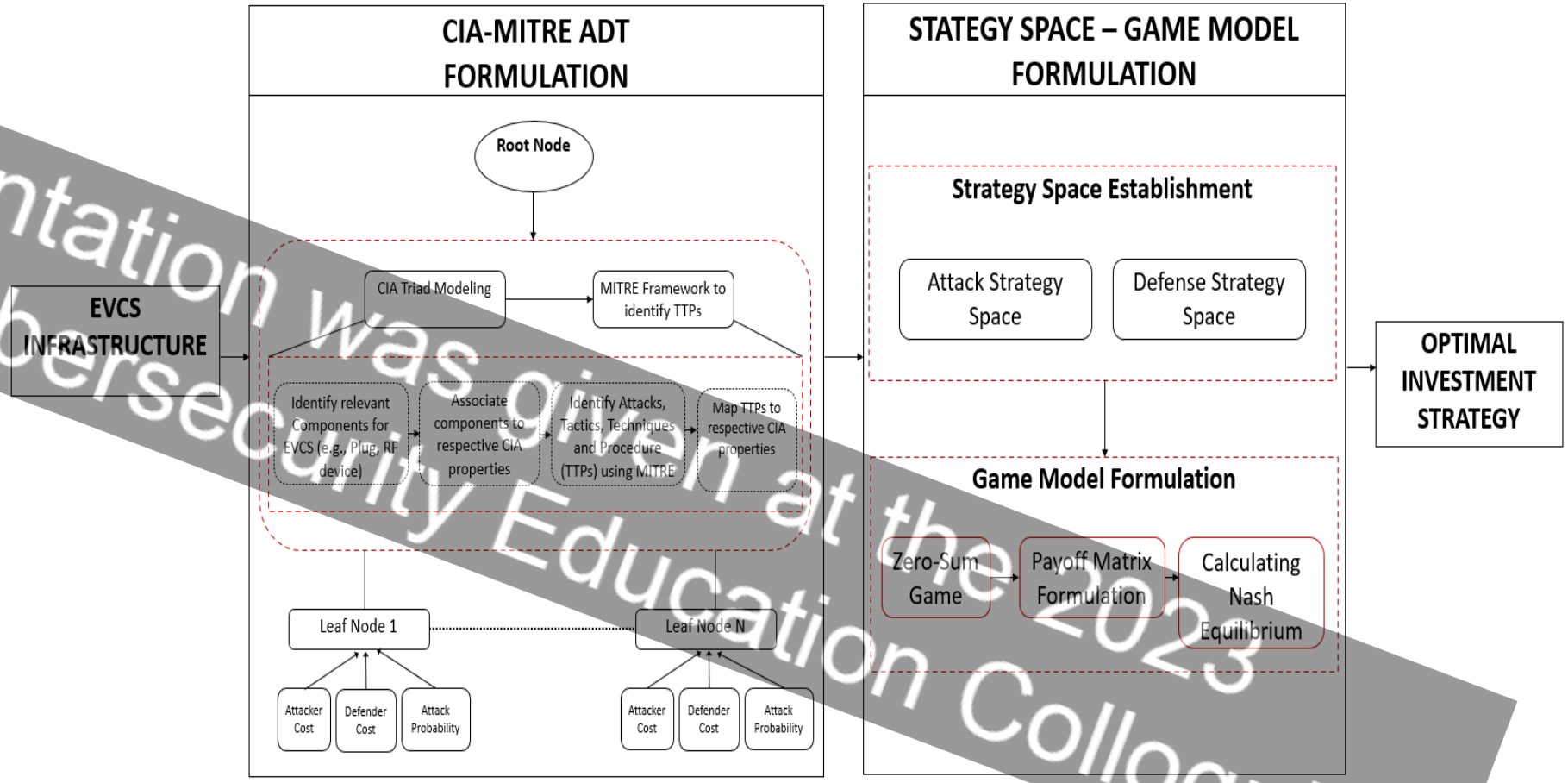
Research Objectives:
(1) Enhance the optimization of resource allocation for the cybersecurity infrastructure in EVCS.
(2) Quantitative Cyber Risk Assessment for EVCS.

Methodology Used:
(1) Game theoretic framework using different games like Stackelberg game, Bayesian game for quantitative risk assessment and cybersecurity investment optimization

This presentation was given at the 2023 National Cybersecurity Education Colloquium

Workflow of ADT-GT Methodology





This presentation was given at the National Cybersecurity Education Colloquium

This presentation was given at the 2023 National Cybersecurity Education Colloquium

CONCLUSION/FUTURE WORK

- ✓ This work proposed novel models, methodologies and algorithms for:
  (1) Anomaly Detection System for Intra-Vehicular CAN-bus Networks
  (2) Cybersecurity resource investment optimization and cybersecurity risk assessment using game theory and attack-defense trees for achieving long-term cybersecurity of the EV charging infrastructure and concurrently the grid.

- ✓ For future work:
  (1) The proposed results can be further improved by using rigorous optimization techniques such as particle swarm optimization and Bayesian optimization.
  (2) Incorporate online dynamic cyber contingency studies; Incorporate real-time risk assessment and defense measure deployment; Real-time attack injection and optimization evaluation.

This presentation was given at the 2023 National Cybersecurity Education Colloquium

This presentation was given at the 2023 National Cybersecurity Education Colloquium

THANK YOU!!