COLLEGE OF ENGINEERING AND COMPUTER SCIENCE
FLORIDA ATLANTIC UNIVERSITY

Announces the Ph.D. Dissertation Defense of

Easa Alalwany

for the degree of Doctor of Philosophy (Ph.D.)

"An Effective Ensemble Learning-Based Real-Time Intrusion Detection Scheme for In-Vehicle Network"

October 26, 2023, Time 3:00 PM - 4:30 PM.
Building, Room EE 405
777 Glades Road
Boca Raton, FL
Zoom Meeting
Meeting ID: 875 6339 0513
Passcode: c4LcgU

DEPARTMENT:

Department of Electrical Engineering and Computer Science

ADVISOR:
Imadeldin Mahgoub, Ph.D.

PH.D. SUPERVISORY COMMITTEE:
Imadeldin Mahgoub, Ph.D., Chair
Mohammad Ilyas, Ph.D.
Waseem Asghar, Ph.D.
Dingding Wang, Ph.D.

ABSTRACT OF DISSERTATION

An Effective Ensemble Learning-Based Real-Time Intrusion Detection Scheme for In-Vehicle Network

Connectivity and automation have expanded with the development of autonomous vehicle technology. One of several automotive serial protocols that can be used in a wide range of vehicles is the controller area network (CAN). The growing functionality and connectivity of modern vehicles make them more vulnerable to cyberattacks aimed at vehicular networks. The CAN bus protocol is vulnerable to numerous attacks as it lacks security mechanisms by design. It is crucial to design intrusion detection systems (IDS) with high accuracy to detect attacks on the CAN bus.

In this dissertation, to address all these concerns, we design an effective machine learning-based IDS scheme for binary classification that utilizes eight supervised ML algorithms, along with ensemble classifiers, to detect normal and abnormal activities in the CAN bus. Moreover, we design an effective ensemble learning-based IDS scheme for detecting and classifying DoS, fuzzing, replay, and spoofing attacks. These are common CAN bus attacks that can threaten the safety of a vehicle's driver, passengers, and pedestrians. For this purpose, we utilize supervised machine learning in combination with ensemble methods. Ensemble learning aims to achieve better classification results through the use of different classifiers that are combined into a single classifier. Furthermore, in the pursuit of real-time attack detection and classification, we propose IDS scheme that accurately detects and classifies CAN bus attacks in real-time using ensemble techniques and the Kappa architecture. The Kappa architecture enables real-time attack detection, while ensemble learning combines multiple machine learning classifiers to enhance the accuracy of attack detection. We build this system using the most recent CAN intrusion dataset provided by the IEEE DataPort. We carried out the performance evaluation of the proposed system in terms of accuracy, precision, recall, F1-score, and area under curve receiver operator characteristic (ROC-AUC). For the binary classification, the ensemble classifiers outperformed the individual supervised ML classifiers and improved the effectiveness of the classifier. For detecting and classifying CAN bus attacks, the ensemble learning methods resulted in a robust and accurate multi-classification IDS for common CAN bus attacks. The stacking ensemble method outperformed other recently proposed methods, achieving the highest performance. For the real-time attack

detection and classification, the ensemble methods significantly enhance the accuracy of real-time CAN bus attack detection and classification. By combining the strengths of multiple models, the stacking ensemble technique outperformed individual supervised models and other ensembles.

BIOGRAPHICAL SKETCH
Born in Nabt, Yanbu, Saudi Arabia
B.S., Taibah University, Yanbu, Madinah, Saudi Arabia, 2014
M.S., Nova Southeastern University, Fort Lauderdale, Florida, 2019
Ph.D., Florida Atlantic University, Boca Raton, Florida, 2023

CONCERNING PERIOD OF PREPARATION
& QUALIFYING EXAMINATION

Time in Preparation: 2020 - 2023

Qualifying Examination Passed: Semester Fall 2020

Published Papers:

Alalwany, E., & Mahgoub, I. (2022). Classification of Normal and Malicious Traffic Based on an Ensemble of Machine Learning for a Vehicle CAN-Network. Sensors, 22(23), 9195.

Alalwany, E., & Mahgoub, I. (2023). An Intelligent Ensemble-Based Detection of In-Vehicle Networks Intrusion. IEEE Transactions on Intelligent Vehicles Journal (Submitted)

Alalwany, E., & Mahgoub, I. (2023). Ensemble Learning for Real-Time Attacks Detection to Secure In-Vehicle Network. IEEE Internet of Things Journal (Submitted)

Alalwany, E., & Mahgoub, I. (2023). Security and Trust Management in the Internet of Vehicles (IoV): Challenges and Machine Learning Solutions. Sensors MDPI Journal (Submitted)