BIOGRAPHICAL SKETCH

Ahmed Adel Awad Shafee was born in Cairo, Egypt. Currently he is an Assistant Professor in the Department of Computer Science, Adams State University, USA, since August 2021 and pursuing his Ph.D. degree in the Department of Electrical & Computer Engineering, Tennessee Tech. University, USA since January 2019. His research interests include machine/deep learning, artificial intelligence, intrusion detection, cryptography and network security, smart-grid and AMI networks, and electric vehicles.

EDUCATION

Ph.D. Electrical and Computer Engineering
Tennessee Tech University, August 2022*(expected)*
Cookeville, Tennessee

M.Sc. Computer Engineering
Faculty of Engineering, Helwan University, 2018
Cairo, Egypt

B.Eng. Computer Engineering
Faculty of Engineering, Helwan University, 2011
Cairo, Egypt

FUNDING

Funding for the graduate studies provided by Tennessee Tech University through the Department of Electrical and Computer Engineering.

College of Engineering

TENNESSEE TECH

The Department of

Electrical and Computer Engineering

Announces the Dissertation Defense of

Ahmed Adel Awad Shafee

In Partial

Fulfillment of the Requirements

For the degree of

Doctor of Philosophy in Engineering

May 5, 2022

9:00 a.m.

Tennessee Tech University

Zoom Link – https://tntech.zoom.us/j/8978016564

FIELD OF STUDY

Cyber Security

DISSERTATION TOPIC

Towards Secure Charging Infrastructure for Electrical Vehicles Using Robust Deep Learning Models

EXAMINING COMMITTEE

Dr. Mohamed Mahmoud, Committee Chair
Associate Professor, Electrical and Computer Engineering

Dr. Ghadir Radman
Professor, Electrical and Computer Engineering

Dr. Syed Rafay Hasan
Associate Professor, Electrical and Computer Engineering

Dr. Doug Talbert
Associate Chair, Professor, Computer Science

Dr. JW Bruce
Associate Professor, Electrical and Computer Engineering

AN ABSTRACT OF A DISSERTATION

As the number of electric vehicles on the roads significantly increases, charging coordination mechanisms have been introduced for balancing the charging demand and energy supply. However, electric vehicles could send false data, such as stateof-charge (SoC), to the charging coordination mechanism for gaining high charging priority illegally. Moreover, adversaries could target these mechanisms by launching distributed denial of charge (DDoC) attacks against charging stations by submitting fake charging requests to reserve charging time slots. Accordingly, we first study the impact of such reporting false data on both the lying and honest electric vehicles. Our evaluations indicate that lying electric vehicles have higher chance of charging, whereas honest electric vehicles may not be able to charge or may charge late. Then, an anomaly-based detector based on a deep neural network is devised to identify lying electric vehicles. To train the detector, we first create an honest dataset for the charging coordination application using real driving traces and information provided by an electric vehicle manufacturer, and we then introduce a number of attacks and use them for creating malicious data. We train and evaluate a gated recurrent unit model using this dataset. Our evaluations demonstrate that our detector can identify false data accurately. For the DDoC, we first evaluate the ability of the attack to disrupt the charging process, and then propose detection techniques to identify the attack using deep neural networks with vector embedding. For training and evaluating our detectors, we build a benign charging demand dataset using real vehicles' routes and EVs' technical parameters. After that, we introduce several attacks and use them to generate the malicious dataset. To accurately detect the attacks, a vector embedding layer is combined with a deep neural network to capture/learn the spatial-temporal correlations within the charging requests. Our evaluations demonstrate that our detector can identify DDoC attacks accurately. Moreover, attackers could launch privacy attacks against the detector, such as membership inference and model inversion, for revealing sensitive information on the drivers whose data are used to train the detector. Furthermore, the attackers could launch evasion attacks against the detector by computing false SoC values that are classified benign by the detector. Accordingly, we develop an approach for training a detector that can identify false data accurately while it does not leak sensitive information about the training data and it is robust against evasion attacks. To validate our proposal, we have conducted a set of experiments and the given results confirm the security and efficiency of our approach.