BIOGRAPHICAL SKETCH

Mahmoud Nabil Mahmoud was born in Al Bahah, KSA, on December 9, 1989. He attended elementary schools in Cairo and graduated from high school with honors in June 2007. In the fall of 2007, he entered Cairo University and received his B.S. degree and M.S. degree with honors in Computer Engineering in 2012 and 2016 respectively. In January of 2017, he began his PhD studies at Tennessee Tech University. Currently, Mahmoud Nabil Mahmoud works as a Graduate Research Assistant in the Department of Electrical & Computer Engineering at Tennessee Tech University, a position he has held since he began the program in January of 2017. While pursuing his PhD studies, Mahmoud has published many journal and conference papers in various prestigious venues such as the IEEE Internet of Things journal, IEEE Transaction of Dependable and Secure Computing, IEEE Access, the International Conference of Communication (ICC), the International Conference on Pattern Recognition (ICPR), the International Conference on Wireless Communication (WCNC), and the International Conference on the Internet of Things (iThings). Mahmoud's research interests include security and privacy in smart grid, machine learning applications, vehicular Ad Hoc networks, and blockchain applications.

EDUCATION

Cairo University
Cairo, Egypt
BS, Computer Engineering, 2012

Cairo University
Cairo, Egypt
MS, Electrical Engineering, 2016

Tennessee Technological University
Cookeville, Tennessee, USA
PhD, Engineering, August 2019 *(expected)*

College of Engineering

TENNESSEE TECH

The Department of

Electrical & Computer Engineering

Announces the Dissertation Defense

of

Mahmoud Nabil Mahmoud

In Partial Fulfillment of the Requirements

For the degree of

Doctorate of Philosophy

July 19, 2019

Held in

208 Brown Hall at 2:00 p.m.
115 West 10th Street
Tennessee Tech University

FIELD OF STUDY

Privacy-Preserving Electricity Theft Detection for Smart Grid AMI Networks.

DISSERTATION TOPIC

"Electricity Theft Detection With Privacy Preservation For Smart Grid AMI Networks Using Machine Learning"

EXAMINING COMMITTEE

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

Dr. Ghadir Radman
Professor, Electrical & Computer Engineering

Dr. Douglas Talbert
Professor, Computer Science

Dr. J. W. Bruce,
Associate Professor, Electrical & Computer Engineering

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

Abstract

Smart grid (SG) is a revolutionized upgrade to the traditional power grid. SG provides two-way communications of power and data between the grid's major components including grid operators, electricity suppliers, and consumers to ensure the efficient and reliable operation of the grid. Advanced metering infrastructure (AMI) is one of the main components of the SG. In AMI, smart meters are installed at consumer premises and they should send fine-grained power consumption readings, e.g., every few minutes, to the utility company for load monitoring, energy management, and billing. However, AMI suffers from the deceptive behavior of malicious users who report false electricity usage in order to reduce their bills, which is known as electricity theft cyber-attacks.

Although electricity theft detection for AMI has been addressed in the literature, existing schemes have several limitations as they mostly rely on shallow and static machine learning techniques and do not exploit the time-series nature of the energy consumption readings. In this work, we aim to address these limitations by presenting deep-learning detectors that can efficiently thwart electricity theft cyber-attacks in smart grid AMI networks. Firstly, we present a consumer-specific detector based on deep feed-forward and recurrent neural networks (RNN). Then, we develop generalized electricity theft detectors that are more robust against contamination attacks compared with consumer-specific detectors. In both detectors, optimization of hyper-parameters is investigated to improve the performance of the developed detectors. In particular, the hyper-parameters of the detectors are optimized via sequential, random, and genetic optimization-based grid search approaches. Extensive experiments are carried out using real energy consumption data to evaluate all detectors performance. The results of the experiments indicate that superior performance is observed for the deep-learning detectors when compared with a shallow machine learning approach. This gain in the performance is due to the exploit of the time series nature in the input data by the deep-learning detectors. Secondly, we investigate the use of vectors embeddings in building electricity theft detectors. In specific, we generate vectors embeddings offline honest and malicious electricity consumers. Then, we use these embeddings to train a classifier that fuses both types of embeddings while making its electricity theft decision. In addition, we compare this model to RNN and the feedforward model and we show the performance gain observed. Finally, existing electricity theft detection schemes do not consider the privacy of the consumers. These schemes use the consumers' fine-grained data which can reveal sensitive information about the consumers' activities. These activities include the times' consumers leave/return homes, as well as, the appliances they use since each appliance has a unique power consumption signature. On the other hand, the utility company needs this fine-grained data for grid monitoring, billing, and more importantly cyber-attacks detection. The research question we will investigate is "Can the utility achieve these goals while keeping the consumers' fine-grained data private?" Thus, we propose an efficient and privacy-preserving electricity theft detection scheme for the AMI network and refer to it as PPETD. Our scheme allows system operators to identify electricity thefts, monitor the loads for energy management, and compute electricity bills efficiently using masked fine-grained meter readings without violating the consumers' privacy. PPETD uses secret sharing to allow consumers to mask their readings and send masked readings to the system operator. The masked readings are computed in such a way that allows the system operator to compute the aggregated readings for the purpose of monitoring and billing without being able to access the individual readings of the consumers to preserve privacy. In addition, secure two-party protocols using arithmetic and binary circuits are executed by the system operator and each consumer to evaluate a generalized convolutional-neural network model on the reported masked fine-grained power consumption readings for the purpose of electricity theft detection. Experiments and analysis done on real datasets are carried out to evaluate the security and the performance of PPETD. Our results confirm that our scheme is accurate in detecting fraudulent consumers without leaking private information on consumers' activities. In addition, the communication and computation overheads are acceptable.