BIOGRAPHICAL SKETCH

Mr. Alsharif received the B.Sc. and M.Sc. degrees in electrical engineering from Benha University, Egypt, in 2009 and 2015, respectively. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, Tennessee Tech University, USA. He is also a Cybersecurity Instructor with the Computer Science Department, University of Central Arkansas, USA where he will be appointed as tenure-track assistant professor upon completion of his PhD degree requirement. His research interests include security and privacy in smart grid, cyber physical systems, vehicular ad hoc networks, and multi-hop cellular networks. In 2009, he was one of the recipients of the Young Innovator Award from the Egyptian Industrial Modernization Centre. He is a professional IEEE member since 2018. He authored/co-authored 5 IEEE journals and 7 IEEE conference papers since he joined Tennessee Tech

EDUCATION

PhD – Tennessee Tech. University
Expected graduation May 2019

M.Sc. – Benha University, Egypt
Electrical Engineering, 2015

B.Sc. – Benha University, Egypt
Electrical Engineering, 2009

College of Engineering

TENNESSEE TECH

The Department of

Electrical & Computer Engineering

Announces the Dissertation Defense

of

Ahmad Alsharif

In Partial Fulfillment of the Requirements

For the degree of

Doctorate of Philosophy

March 29th, 2019

Held in

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

FIELD OF STUDY

Security and Privacy-Preservation

DISSERTATION TOPIC

Secure and Efficient Data Collecting with Access control and Multicast Schemes for Smart Grid AMI Networks

EXAMINING COMMITTEE

Dr. Mohamed Mahmoud, Committee Chair
Electrical & Computer Engineering

Dr. Ghadir Radman
Electrical & Computer Engineering

Dr. Syed Rafay Hasan
Electrical & Computer Engineering

Dr. J. W. Bruce
Electrical & Computer Engineering

Dr. Mohamed Ashiqur Rahman
Electrical & Computer Engineering,
Florida International University

Abstract

The smart grid (SG) is identified as the next generation of the traditional power grid. It provides two-way communications between the grid's major components including grid operators, electricity suppliers, and end-users to ensure the efficient and reliable operation of the grid. One of the main components of the SG is the advanced metering infrastructure (AMI) networks that enable automated collection of metering data. Although security and privacy have been addressed for current AMI networks, the existing schemes have several limitation and thus we propose in this dissertation several data collection, access control and data multicast schemes to address these limitations. Firstly, existing data collection schemes allow users to periodically report their encrypted power consumption data and use data aggregation to preserve privacy. However, if power consumption does not change, periodic data reporting becomes inefficient and incurs large overhead. A naive solution for an efficient AMI network is that each SM should report its encrypted power consumption data only when the consumption changes. However, using traffic analysis techniques, attackers can reveal consumers' activities even if the data is encrypted. To address this issues, we propose a privacy-preserving data collection scheme for efficient AMI networks. The proposed scheme allows irregular data collection to reduce the communication overhead while ensuring the correctness of the aggregated data at all times. In addition, the proposed scheme can resist traffic analysis attacks and achieve satisfactory protection against collusion attacks. Secondly, existing schemes consider only single-recipient AMI network model while in a competitive electricity market, multi-entities, e.g., distribution network operators and electricity suppliers, need to collect power consumption data of different sets of users. In this case, access control to aggregated power consumption data is needed. To address this issue, we propose a privacy-preserving data collection and access control scheme for multi-recipient AMI networks. In the proposed scheme, no entity should have access to individual users' data to preserve users' privacy. In addition, each entity should access only the aggregated data intended to it and cannot access the data intended for other competitors. Thirdly, most of the existing schemes does not consider the multi-dimensional nature of power consumption and multi-subset aggregation in which the utility should be able to obtain the number of consumers whose consumption lies within a specific consumption range, and the overall consumption of each set of users. To address this issue, we propose an efficient and privacy-preserving multi-dimensional multi-subset data aggregation scheme for AMI network. With the proposed scheme, the utility can obtain the total power consumption of each subset in each dimension as well as the number of users of each subset in each dimension. In addition, the proposed scheme can resist collusion attacks in which external adversaries and internal attackers may collude to learn the power consumption of individual users. Moreover, it allows advanced dynamic billing in which electricity prices are different based on based on power consumption type. Lastly, in addition to the aforementioned data collection and access control schemes that consider the smart grid uplink communications, i.e., data sent by SMs to grid operators and electricity suppliers, we also investigate in the last part of the dissertation secure multicast communications for the smart grid downlink, i.e. communications sent by grid operators or electricity suppliers to a group of users. In order to enable the grid operators and the electricity suppliers to communicate securely with users who subscribe in a certain plan and/or reside in a specific area, secure data multicast is required. However, IEEE 802.11 protocol, which is the underlying protocol for AMI networks, does not support multicast communication. In order to address this issue, we propose a novel multi-authority attribute based signcryption scheme that can be used to secure the SG downlink multicast communications. The proposed scheme ensures message confidentiality, i.e., only no one can decrypt the multicasted messages except the intended users and allows users to authenticate the senders and ensures non-repudiation.