CYBER-PHYSICAL SECURITY OF SMART GRID AND ADVANCED METERING INFRASTRUCTURE

SANDEEP KUMAR SINGH

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY DELHI
OCTOBER 2018

CYBER-PHYSICAL SECURITY OF SMART GRID AND ADVANCED METERING INFRASTRUCTURE

by

SANDEEP KUMAR SINGH

DEPARTMENT OF ELECTRICAL ENGINEERING

Submitted

in fulfillment of the requirements of the degree of Doctor of Philosophy

to the

INDIAN INSTITUTE OF TECHNOLOGY DELHI

OCTOBER 2018

Certificate

This is to certify that the thesis entitled **"Cyber-Physical Security of Smart Grid and Advanced Metering Infrastructure"** being submitted by **Mr. Sandeep Kumar Singh** to the Department of Electrical Engineering, Indian Institute of Technology Delhi, for the award of the degree of **Doctor of Philosophy** is the record of bonafide research work carried out by him under my supervision. In my opinion, the thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted either in part or in full to any other University or Institute for the award of any degree or diploma.

Dr. Ranjan Bose
Professor
Department of Electrical Engineering
Indian Institute of Technology Delhi
New Delhi, India-110016

Date:
Place: New Delhi

Dr. Anupam Joshi
Professor
Department of Computer Science and Electrical Engineering
University of Maryland, Baltimore County
Baltimore, MD 21250, United States

Date:
Place:

Acknowledgements

First of all, I would like to take this opportunity to express my gratitude to my supervisor, Prof. Ranjan Bose, for his constant support, guidance and motivation during the period of my Ph.D that helped me to develop my research work. I am also thankful to my co-supervisor, Prof. Anupam Joshi, for many useful interactions and for their comments and suggestions on my research work.

I would like to thank my student research committee members Prof. Shankar Prakriya, Prof. Manav Bhatnagar and Prof. Kolin Paul for their critical but constructive comments and suggestion on my research work. A special thanks goes to Prof. Bijaya Ketan Panigrahi of Department of Electrical Engineering, and fellow research scholar Kush Khanna for a lot of insightful discussions during the problems solved jointly.

I would like to thank all members of the Center of Excellence in Cyber Systems and Information Assurance lab. I am also thankful to my friends Amit Agrawal, Bipin Patel, Sasi Vinay Pechetti and Kirti Kant Sharma for their support, friendship and advices.

Most importantly, I would like to thank my parants for their support, care and motivation throughout my life. I wholeheartedly thank to my wife for her love and support during the final year of my Ph.D.

Sandeep Kumar Singh

Dedicated to my parents
Mr. Shiv Singh and Mrs. Vimla
and
my lovely wife
Mrs. Shalloo Yadav

Abstract

The power grid has become an essential part of the present-day society. People's day-to-day life will be affected dramatically without a reliable and stable power grid. Therefore, nations have been modernising their existing power system into the smart grid with advanced information system and communication technologies. The control and operation of the smart grid relies on complex cyberspace of communication and information technologies, computers, and software. Due to the integration and dependency on cyber infrastructure, the possibilities of cyber-physical threats also increases. Cyber attack is one of the key threat in the smart grid system. Advanced Metering Infrastructure (AMI) play an important role in the smart grid. AMI has modernized the electricity metering system by replacing mechanical and digital meters with smart meters. While some security mechanism has been developed for cyber threats in smart meters, they are not sufficient to prevent attacks. So there is a need of strong defence mechanism to detect cyber threats in smart meters.

In this thesis, we investigate cyber-physical security challenges in smart grid and AMI; and propose several defence algorithms for detecting cyber attacks. Our work includes three parts.

In the first part of the thesis, we address the cyber-physical security of the smart grid. We present a method to detect a relatively new type of cyber-attack called false data injection (FDI) attacks in smart grid. The FDI attacks are one of the most thoroughly researched cyber-attacks. Intelligently crafted, it can cause false estimation of states, which seriously affects the entire power system operation. We have introduced the state estimation process, bad data detection method and the formulation of FDI attacks. To detect FDI attacks, we propose a transformation-based method

by transforming the measurement variation, which enhances the resolution (scaling) of the probability distribution function, thereby, increasing the detection probability. In the proposed method, the probability distribution of measurement variations is obtained from the histogram plot of measurement variations. The chosen transformation techniques are computationally efficient and detect the FDI attacks without burdening the state estimation process. The proposed method is tested using IEEE 14 bus system considering attack on different state variables. The performance of the proposed transformation-based scheme is also tested under different topologies.

In the second part of the thesis, we address the problem of cyber-physical security of AMI. AMI, one of the prime components of the smart grid, has many benefits like the demand response and load management. Electricity theft is a key concern in AMI security since smart meters used in AMI are vulnerable to cyber-attacks. In the light of this problem, we have proposed a statistical distance based electricity theft detection scheme to detect theft attacks by tracking the dynamics of consumption variations of the consumers. Different statistical distances are used to compute the distance between probability distributions obtained from the consumption data. When electricity theft attacks are launched against AMI, the probability distribution of the consumption data deviates from historical consumption, thus leading to a larger statistical distance. To test the performance of the proposed method, we have used real smart meters consumption data. A wide range of attack patterns is generated using synthetic attack dataset. Extensive experiments on real dataset show the effectiveness of the proposed method.

In the third part of the thesis, we address the issue of large dimensional AMI data. Smart meters send consumption measurement data to the control center at predefined time intervals. Hence, large dimensional data is stored at the control center. To handle this large sized data, we have applied Principal Component Analysis (PCA) to the large dimensional AMI data, computed different Principal components (PCs) and transformed the data to the low dimensional AMI data. The first PC retains the maximum variance, the second PC retains the second largest variance and so on. To detect the electricity theft attacks, we propose three different detection methodologies. In the first method, we reconstruct the consumption data using PCs and compute Kullback-Leibler distance. In the second method, we propose an anomaly score based electricity

theft detection in which anomaly score at each time step is computed and threshold based detection is made. In the third method, we propose Mahalanobis distance based electricity theft detection. In this method, we project the AMI data on the PCs space and compute Mahalanobis distance of the test data from the historical data set. We have classified the testing data as malicious or true based on the computed Mahalanobis distance. We have tested the proposed detection methods for different attack scenarios using real smart meter data. The performance of the proposed schemes are compared with the existing SVM based theft detector.

सार

पावर ग्रिड आज के समाज का एक अनिवार्य हिस्सा बन गया है। लोगो का दिन-प्रतिदिन का जीवन एक भरोसेमंद और स्थिर पावर ग्रिड के बिना नाटकीय रूप से प्रभावित होगा। इसलिए, राष्ट्र उन्नत सूचना प्रणाली और संचार प्रौद्योगिकियों के साथ स्मार्ट ग्रिड में अपनी मौजूदा पावर सिस्टम का आधुनिकीकरण कर रहे हैं। स्मार्ट ग्रिड का नियंत्रण और संचालन संचार और सूचना प्रौद्योगिकी, कंप्यूटर और सॉफ्टवेयर के जटिल साइबर स्पेस पर निर्भर करता है। साइबरइनफ्रास्ट्रक्चर पर एकीकरण और निर्भरता के कारण, साइबर-भौतिक खतरों की संभावनाएं भी बढ़ जाती हैं। स्मार्ट ग्रिड सिस्टम में साइबर हमला महत्वपूर्ण खतरा है। उन्नत मीटरींग इंफ्रास्ट्रक्चर (एएमआई) स्मार्ट ग्रिड में एक महत्वपूर्ण भूमिका निभाते हैं। एएमआई ने यांत्रिक और डिजिटल मीटर की जगह स्मार्ट मीटर का उपयोग कर के बिजली मीटरिंग प्रणाली का आधुनिकीकरण किया है। जबकि स्मार्ट मीटर में साइबर खतरों के लिए कुछ सुरक्षा तंत्र विकसित किए गए हैं, वे हमलों को रोकने के लिए पर्याप्त नहीं हैं। इसलिए स्मार्ट मीटर में साइबर खतरों का पता लगाने के लिए मजबूत रक्षा तंत्र की आवश्यकता है।

इस थीसिस में, हम स्मार्ट ग्रिड और एएमआई में साइबर-भौतिक सुरक्षा चुनौतियों की जांच करते हैं; और साइबर हमलों का पता लगाने के लिए कई रक्षा एल्गोरिदम प्रस्तावित करते है। हमारे काम में तीन हिस्से शामिल हैं।

थीसिस के पहले भाग में, हम स्मार्ट ग्रिड की साइबर-भौतिक सुरक्षा को संबोधित करते हैं। हम स्मार्ट ग्रिड में झूठे डेटा इंजेक्शन (एफडीआई) हमलों नामक एक अपेक्षाकृत नए प्रकार के साइबर हमले का पता लगाने के लिए एक विधि प्रस्तुत करते हैं। एफडीआई हमले सबसे अच्छी तरह से शोध किए गए साइबर हमलों में से एक हैं। समझदारी से तैयार की गई, यह स्टेट्स के झूठे अनुमान का कारण बन सकती है, जो पूरे पावर सिस्टम ऑपरेशन को गंभीरता से प्रभावित करती है। हमने स्टेट्स अनुमान प्रक्रिया, खराब डेटा पहचान विधि और एफडीआई हमलों के निर्माण की शुरुआत की है। एफडीआई हमलों का पता लगाने के लिए, हम माप भिन्नता को बदलकर एक परिवर्तन-आधारित विधि का प्रस्ताव देते हैं, जो प्रोबेबिलिटी डिस्ट्रीब्यूशन फंक्शन के रिज़ॉल्यूशन (स्केलिंग) को बढ़ाता है, जिससे पता लगाने की संभावना बढ़ जाती है। प्रस्तावित विधि में, मापन भिन्नता का प्रोबेबिलिटी डिस्ट्रीब्यूशन फंक्शन मापन भिन्नता के हिस्टोग्राम से प्राप्त किया जाता है। चयनित परिवर्तन तकनीक कम्प्यूटेशनल रूप

से कुशल हैं और स्टेट्स अनुमान प्रक्रिया को बोझ किए बिना एफडीआई हमलों का पता लगाती हैं। विभिन्न स्टेट्स पर हमले पर विचार करते हुए आईईईई 14 बस प्रणाली का उपयोग करके प्रस्तावित विधि का परीक्षण किया जाता है। प्रस्तावित परिवर्तन-आधारित योजना का प्रदर्शन विभिन्न टोपोलॉजीज के तहत भी किया जाता है।

थीसिस के दूसरे भाग में, हम एएमआई की साइबर-भौतिक सुरक्षा की समस्या का समाधान करते हैं। स्मार्ट ग्रिड के प्रमुख घटकों में से एक एएमआई में मांग प्रतिक्रिया और लोड प्रबंधन जैसे कई फायदे हैं। एएमआई सुरक्षा में विद्युत चोरी एक महत्वपूर्ण चिंता है क्योंकि एएमआई में इस्तेमाल होने वाले स्मार्ट मीटर साइबर हमलों के लिए कमजोर हैं। इस समस्या के प्रकाश में, हमने उपभोक्ताओं की खपत भिन्नताओं की गतिशीलता को ट्रैक करके चोरी हमलों का पता लगाने के लिए एक सांख्यिकीय दूरी आधारित बिजली चोरी पहचान योजना का प्रस्ताव दिया है। कंसम्पशन डेटा से प्राप्त प्रोबेबिलिटी डिस्ट्रीब्यूशन के बीच की दूरी की गणना करने के लिए विभिन्न सांख्यिकीय दूरी का उपयोग किया जाता है। जब एएमआई के खिलाफ बिजली चोरी हमले शुरू किए जाते हैं, कंसम्पशन डेटा का प्रोबेबिलिटी डिस्ट्रीब्यूशन ऐतिहासिक कंसम्पशन से विचलित हो जाता है, इस प्रकार एक बड़ी सांख्यिकीय दूरी की ओर अग्रसर होता है। प्रस्तावित विधि के प्रदर्शन का परीक्षण करने के लिए, हमने वास्तविक स्मार्ट मीटर कंसम्पशन डेटा का उपयोग किया है। सिंथेटिक अटैक डेटासेट का उपयोग करके अटैक पैटर्न की एक विस्तृत श्रृंखला उत्पन्न होती है। वास्तविक डेटासेट पर व्यापक प्रयोग प्रस्तावित विधि की प्रभावशीलता दिखाते हैं।

थीसिस के तीसरे हिस्से में, हम बड़े आयामी एएमआई डेटा के मुद्दे को संबोधित करते हैं। स्मार्ट मीटर पूर्ववर्ती समय अंतराल पर नियंत्रण केंद्र में कंसम्पशन माप डेटा भेजते हैं। इसलिए, नियंत्रण केंद्र पर बड़े आयामी डेटा संग्रहीत किया जाता है। इस बड़े आकार के डेटा को संभालने के लिए, हमने प्रिंसिपल कंपोनेंट एनालिसिस (पीसीए) को बड़े आयामी एएमआई डेटा पर लागू किया है, विभिन्न प्रिंसिपल घटकों (पीसी) की गणना की और डेटा को कम आयामी एएमआई डेटा में बदल दिया। पहला पीसी अधिकतम वैरिअन्स बरकरार रखता है, दूसरा पीसी दूसरा सबसे बड़ा वैरिअन्स बरकरार रखता है। बिजली चोरी हमलों का पता लगाने के लिए, हम तीन अलग-अलग पहचान पद्धतियों का प्रस्ताव देते हैं। पहली विधि में, हम पीसी का उपयोग कर कंसम्पशन डेटा का पुनर्निर्माण करते हैं और कुल्बैक-लीबलर दूरी की गणना करते हैं। दूसरी विधि में, हम एक एनोमली स्कोर आधारित विद्युत चोरी का पता लगाने का प्रस्ताव करते हैं

जिसमें प्रत्येक समय चरण में एनोमली स्कोर गणना की जाती है और थ्रेसहोल्ड आधारित पहचान की जाती है। तीसरी विधि में, हम महालानोबिस दूरी आधारित बिजली चोरी पहचान का प्रस्ताव देते हैं। इस विधि में, हम पीसी स्पेस पर एएमआई डेटा प्रोजेक्ट करते हैं और ऐतिहासिक डेटा सेट से परीक्षण डेटा की महलानोबिस दूरी की गणना करते हैं। हमने गणना डेटा को गणना की गई महलानोबिस दूरी के आधार पर असत्य या सत्य डेटा के रूप में देखा है। हमने वास्तविक स्मार्ट मीटर डेटा का उपयोग करके विभिन्न हमले परिदृश्यों के लिए प्रस्तावित पहचान विधियों का परीक्षण किया है। प्रस्तावित योजनाओं का प्रदर्शन मौजूदा एसवीएम आधारित चोरी डिटेक्टर के साथ तुलना की जाती है।

Table of Contents

List of Figures

List of Tables

List of Algorithms

List of Abbreviations

AMI	Advanced metering infrastructure
CBD	Cumulative distribution function based distance
CDF	Cumulative distribution function
DR	Detection rate
EE	External entity
EMS	Energy management system
FDI	False data injection
FPR	False positive rate
GA	Genetic algorithm
GLRT	Generalized likelihood test
HD	Hellinger distance
IoT	Internet of Things
ISSDA	Irish Social Science Data Archive
JSD	Jensen-Shannon distance
KLD	Kullback-Leibler distance
LSE	Linear system of equations
MITM	Man in the middle
NN	Neural network
NTL	Non technical loss
NYISO	New York independent system operator
PC	Principal component
PCA	Principal component analysis
PMU	Phasor measurement unit
P2P	Peer to peer
RFID	Radio frequency identification

ROC	Receiver operating characteristic
RTU	Remote terminal unit
SCADA	Supervisory control and data acquisition
SE	State estimation
SVM	Support vector machine
TL	Technical loss
WLS	Weighted least square