phdprimehelp@gmail.com
+91-97 91 62 64 69

Ph.D. Research Proposal

Doctoral Program in "Department Name"

Defend against Cybersecurity Attacks and Distributed State Estimation for SmartGrid Power Systems via Secure Intelligence Schemes

by

<Name of the Candidate>

<Reg. No of the Candidate>

<Supervisor Name>

<Date of Submission (DD MM 20YY>

I. INTRODUCTION / BACKGROUND

Smart Grids (SGs) are designed to meet energy requirements in the presence of large human population, increased consumerism, and multiple challenges of power industries. However, SGs are vulnerable to many security threats such as blind false data injection attack, false data injection attack, denial of service attack and so on [1]. The security provision and attack detection are performed by graph analysis, machine learning approaches, etc. In these approaches, state estimation play vital role and it is challenging process. Three phase particle swarm optimization algorithm was presented to estimate the state variables [2]. This method performs state estimation is centralized manner which increases complexity and overhead in the system. Supervised machine learning algorithm (SVM classifier) was proposed with genetic algorithm (GA) based attack detection in smart grid [3]. In this method, the complexity of the system is increased since the state estimation is performed in centralized manner. This method is also not able to detect compromised meter in the system. In host based monitoring system, attack detection was performed by set of specified rules and compromised PMU detection was carried out by majority voting. But the system complexity and detection time increases with increase in number of rules specified. Attack detection by majority voting is not efficient. Kalman filter was utilized for state estimation and chi-square method and cosine similarity tests were performed for attack detection [5]. Kalman filter is not suitable for linear system and similarity measurement based attack detection is not efficient. Recursive systematic convolutional code (RSC) and Kalman filter were utilized to enhance protection in smart grid system [6]. Involvement of Kalman filter limits the performance in non-linear system and in uncertainties.

Euclidean distance metric and Markov chain model were used for sate estimation based attack detection [8]. This method requires additional trusted buses and determining Euclidean distance for all historical data increases complexity of the system. Robust principle component analysis (RPCA) method was employed to perform attack detection with entry wise constraints [9]. Here the time consumption for state estimation and attack detection high due to centralized estimation. State estimation through extended Kalman filter was improved by employing PSO

algorithm for probability detection [10]. Security was provided to most vulnerable nodes detected by constriction factor PSO algorithm [11]. In this approach, all other nodes are not secured and authentication based on one time signature is not efficient. An adaptive CUSUM method was presented for false data detection process [14]. However, the compromised nodes are not identified in this method. Game theoretic approaches also play vital role in false data attack detection [15]. In false data attack detection, spying concept was utilized in smart meters [13]. Here, the smart meters are vulnerable o attacks since the secret which can be easily cracked by attacker is used for authentication. In wide-area detection sequential detector [14] which increases time consumption due to centralized manner is utilized. Source authentication based on received signal was performed by mathematical morphology [16]. However, this method is only able to identify the source of measurement and not able to secure the measurement. Elliptic curve cryptography (ECC) based key distribution was utilized to improve security in smart grids [19].

1.1 Research Outline & Scope

False data injection (FDI) attacks are a major security threat to smart grid (SG) communication systems. In FDI attacks, attacker has the ability of modifying the measurements transmitted by smart grid entities such as smart meters, buses etc. Further other cyber security attacks introduce more threats such as replay and masquerade.

1.2 Research Objectives

Primarily, this research work has the objective of protecting smartgrid environment against vulnerable attacks. Further, this work has the following sub-objectives as,

- To provide more efficient electricity transmission
- To support for quick restoration of electricity after power disturbances
- To support for large scale secure renewable energy environment

II. RESEARCH GAPS

2.1 Common Problem Statement

An unwanted consequence of this standardized communication over ethernet is increased viability to cyber threats. Especially of Replay and masquerade attacks are, especially, of concern due to their imminent impact on the operation. While detecting replay attacks is easier, since the original messages are used for the attack, masquerade attack messages may be difficult to distinguish from original ones. Furthermore, inadequate mitigation approaches may be tricked by the hackers and the system starts the attacker as the authentic sender and discards original messages from authentic sources. It is vital to develop an approach that incorporates message authentication. In this fashion, when the hackers modify the message contents to by-pass security systems, the tampering can be detected, and the messages will be discarded.

2.2 Problem Definition

In this paper [16] concentrates on false data injection attack in advanced metering infrastructure in smart grids. Here the nodes are clustered into most, moderate, and least vulnerable clusters by constriction factor particle swarm optimization (CS-PSO) algorithm. In this approach, nodes with same level vulnerabilities are grouped into same clusters. To protect the vulnerable nodes, authentication and different intrusion prevention systems are used. The authentication process is carried out by one time signature based multicast authentication method. The most vulnerable nodes are equipped with intrusion detection system.

Problems

- Providing security to vulnerable nodes is not efficient since moderately vulnerable nodes also affected by attackers
- One time signature based authentication is not able to ensure high authenticity

Proposed Solutions

- Here security is provided for all measurements by PRINCE algorithm
- SwA based authentication is efficient and highly secured

In this paper, a new method [17] is presented to ensure security against cyber-attacks in smart grid systems. The analytical technique utilizes Markov chain model and Euclidean distance

metric for attack detection. In this method, initially a set of smart meters are considered as critical meters and optimal PMU placement process is performed. The state estimation process is carried out by Markov chain model. In addition, a set of trusted buses are incorporated in the system in order to detect the injected data. Euclidean distance between trusted bus measurement and all historic data is performed to improve attack detection accuracy.

Problems

- In this method, computation of Euclidean distance between trusted bus measurement and all historical data increases complexity of the system
- This method requires additional trusted buses in the system and detection of critical meters is not efficient

Proposed Solutions

- Proposed work improves security by PRINCE algorithm, CNN classifier, and SwAscheme without increase in time consumption and complexity

This paper utilizes chi-square method [18] and cosine similarity for false data injection attack in smart grid system. In this method, the measurements are acquired from supervisory control and data acquisition (SCADA) using sensors. Here sate estimation is performed by Kalman filter using sensor measurements. In attack detection, chi-square test is carried out to measure the deviation in estimated value (by Kalman filter) and original measurement (sensor measurement). And cosine similarity matching approach is involved to measure the similarity between estimated value and original measurement by sensors. Based on similarity level, the false data injection attack is detected.

Problems

- Kalman filter based state estimation is not suitable for non-linear system
- Involvement of similarity measurement alone in attack detection is not efficient since similarity can be affected by other factors

Proposed Solutions

- Involvement of SSO based state estimation resolves the Kalman filter problem
- Attack detection by CNN algorithm considers significant metrics to improve accuracy

In [19], false data injection attack carried out by compromised phasor measurement unit (PMU) is detected with the support of host monitors. In state estimation, four rules are specified to detect anomaly measurements. These rules are represented by binary variables in host monitors. Based on specified rules, false data injection attack is detected. In compromised PMU detection, majority voting method is incorporated. Here, a PMU is considered as compromised PMU if majority of host monitors reports that the PMU is malicious. Otherwise, the PMU is considered as normal PMU.

Problems

- Accuracy of attack detection is improved with increase in number of rules specified. However, increasing number of rules results in higher complexity and time consumption
- Compromised PMU detection based on majority rule limits the detection accuracy since it is not ensured that all host monitors are trust worthy.

Proposed Solutions

- Attack detection and compromised RTU detection by CNN algorithm minimizes time consumption and complexity

In this paper [20] author attempts to utilize the hybrid particle swarm optimization (HPSO) algorithm for state estimation in smart grid system. In this paper, HPSO algorithm is utilized to develop a distributed state estimation system in smart grids. Here, the PSO algorithm is improved by incorporating tournament selection process. This process is inspired from genetic algorithm and combined with PSO algorithm.

Problems

- Here distributed state estimation is performed in each sensor and smart meters etc. increases complexity and overhead in the system

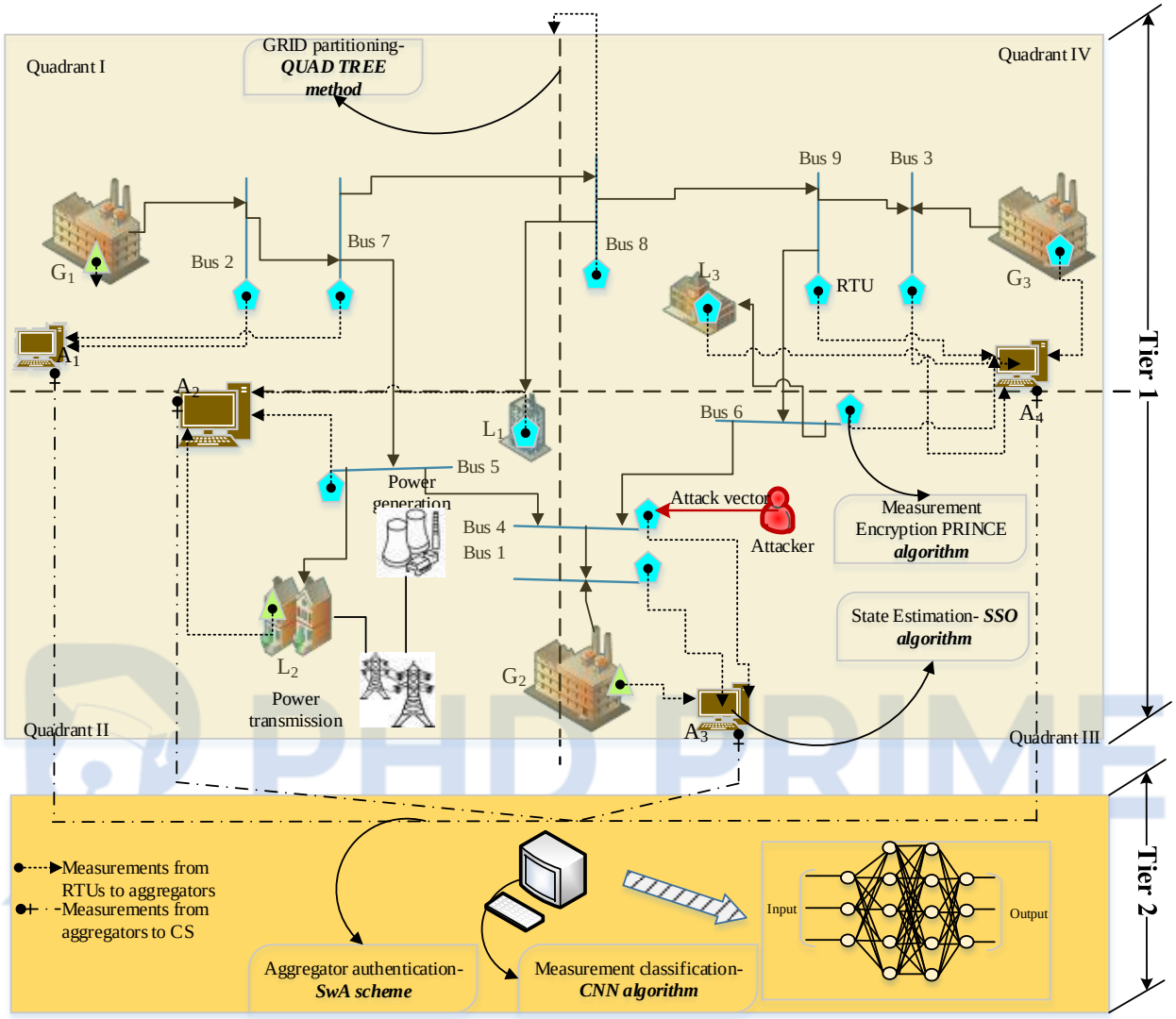
Proposed Solutions

- Distributed state estimation is performed at aggregators which minimizes overhead at RTUs

III. RESEARCH CONTRIBUTIONS

To overwhelm above mentioned problems, this research work focused on improving security in smart grids through efficient state estimation and attack detection processes. The proposed two-tier smart grid architecture is comprised with following entities: power generators, buses, loads, remote terminal units (RTUs), aggregators, and control server.

SYSTEM ARCHITECTURE



Here the first tier consists of RTUs which transmits the measurements from power grids and aggregators. Here the aggregators are employed to perform distributed state estimation. In second tier, centralized control server is involved to detect compromised RTU in an efficient manner. Initially, the overall area is partitioned into four sections by Quad Tree method. In each section, an aggregator which is static in position is incorporated. RTU collects measurements from power grids and encrypt the measurement by using novel PRINCE algorithm. Then encrypted measurements are transmitted aggregators. In aggregator, Shuffled Shepherd Optimization (SSO) algorithm is employed to perform state estimation. Aggregators are also responsible for determining similarity level between measurements obtained from RTU and

estimated measurement. Then, the estimated states, similarity level, and error level are transmitted to control server. In control server, aggregators are authenticated by novel Schedule with Authentication scheme. After successful authentication, all measurements are received by control server. In control server, the measurements are classified into normal and malicious by Convolutional Neural Network (CNN) classifier based on significant metrics.

Performance Evaluation

Finally, our proposed work is evaluated based on following performance metrics,

- Voltage magnitude vs. Bus Number
- Estimation error and detector output vs. Bus Number
- Number of protected measurements vs. Bus Number
- Detection probability vs. Bus Number
- Successful detection rate vs. Simulation Time
- Detection delay vs. Simulation Time

IV. RESEARCH NOVELTIES

- Topology errors and wrong switch statuses detection. Minimizing small errors found in measurements
- Analyzing measurements redundancy for estimating network parameters. Managing missing and delayed measurements through providing estimation for unmonitored parts of the system
- Compromised meters in the system are identified effectually by analyzing received SG information of each meter. For compromised meter detection, CNN algorithm is employed in control server.

V. PREVIOUS WORKS & LIMITATIONS

Paper 1

Title: Cyber Security Analysis and Protection of Wireless Sensor Networks for Smart Grid Monitoring

Concept

This paper analysis the security of wireless sensor networks in smart grid monitoring. Then ECC based secure broadcast authentication is proposed to ensure security in the smart grid system. The proposed authentication process is involved with following phases: initialization phase, and packet pre-processing phase.

Paper 2

Title: Anonymous ECC-Based Self-Certified Key Distribution Scheme for Smart Grid

Concept

This paper explains the application of ECC algorithm in smart grids to enhance security level in the system. Based on ECC algorithm, this paper presents anonymous ECC-based self-certified key distribution mechanism. Through this mechanism, the key distribution overhead is minimized without loss in security level. The overall process is comprised with system setup phase, registration phase, authentication and key agreement phase.

Paper 3

Title: Graph-based Cyber Security Analysis of State Estimation in Smart Power Grid

Concept

In this paper, state estimation process in power grid is carried out by graph-based analysis. Here a graph is extracted for a power grid consists of generators, buses, loads, transmission lines. Then the false data is injected on the constructed graph of power grid. Attack detection is carried out by maximum matching algorithm, commodity flow maximization algorithm, tree pruning algorithm, and minimum S-cut algorithm.

Paper 4

Title: A Novel Approach for Mitigation of Replay and Masquerade Attacks in Smartgrids Using IEC 61850 Standard

Concept

This paper analyses replay and masquerade attacks on IEC 61850 GOOSE messages and develops a solution to mitigate both of those. To detect modified messages, two distinct authentication mechanisms are utilized: RSA since it is the algorithm stipulated in IEC 62351-6 and Elliptic Curve Digital Signature Algorithm (ECDSA) due to its widespread use in smartgrid cybersecurity solutions.

Paper 5

Title: Scheduling and Provision of Secondary Frequency Reserves by Aggregations of Commercial Buildings

Concept

In this paper, we follow up on a recently proposed framework for scheduling and provision of secondary frequency control (SFC) reserves within a building aggregation. We extend this framework with a new reserve scheduling formulation, which is based on a combination of robust and stochastic optimization, to allocate reserve capacities among buildings. The HVAC system set points are determined by a model predictive controller, the frequency signal is tracked by heat pump (HP) control with virtually no occupant discomfort, and the tracking quality is evaluated using a dynamic HP model.

Paper 6

Title: Machine Learning Methods for Attack Detection in the Smart Grid

Concept

In this paper, false data injection attack detection is carried out by machine learning approaches. In this paper, perceptron, K-nearest neighbor approach, SVM, and sparse logistic regression methods are involved in supervised machine learning category. The classification

rules are determined by fusion methods such as ensemble learning for decision level fusion, and multiple kernel learning for feature level fusion.

Paper 7

Title: Bi-level modelling of false data injection attacks on security constrained optimal power flow

Concept

In this paper, the vulnerability of smart grid is evaluated by launching false data injection attack. Here the attack launching problem is modeled as bi level modeling optimization problem which aims to find minimal set of sensors required to launch false data injection attack. This approach suggests that securing this minimal set of sensors leads to improve security of the smart grid system.

Paper 8

Title: Data Injection Attacks on Smart Grids with Multiple Adversaries: A Game-Theoretic Perspective

Concept

This paper proposes two game theoretic approaches for false data injection attack detection. In first, a Stackelberg game model is proposed for attack detection in which the defender is act as leader. In this approach, the equilibrium is determined by a distributed learning algorithm. In second proposed model, defender is not able to act as leader (i.e.) the defender is not able to anticipate the actions of adversaries. To this end, hybrid satisfaction equilibrium-Nash equilibrium algorithm is proposed.

Paper 9

Title: A Constrained Optimization Approach to Dynamic State Estimation for Power Systems including PMU Measurements

Concept

In this paper, state estimation methods involved in remote terminal units (RTUs) and PMU are evaluated.to state estimation schemes such as extended Kalman filter and PSO algorithm based state estimation are presented. Here PMU measurements are treated as inequality constraints of the states with the help of statistical criterion. Then, the extended Kalman filter algorithm is modified in order to tolerate practical issues of missing measurements. In modified extended Kalman filter, PSO algorithm is combined to find probability function.

Paper 10

Title: Blind False Data Injection Attack Using PCA Approximation Method in Smart Grid

Concept

This paper presents a false data injection attack in the smart grids named as blind false data injection attack. The attack is launched by PCA approximation method. In this type of attack, the attacker doesn't have the entire knowledge about system topology and transmission line admittances. Here the attacker is not able to know about the Jacobian matrix and distribution of state variables

Paper 11

Title: Feature Selection Based Detection of Covert Cyber Deception Assaults in Smart Grid Communications Networks Using Machine Learning

Concept

This paper focused on detection of covert cyber assault which is a type of false data injection attack in smart grids. The attack detection is performed in state estimator and bad data detector by using supervised machine learning algorithm. Initially, attack is launched by altering the measurements aggregated by sensors in smart grids. The measurements are collected over a period and used to train classifier. Optimal features are selected by genetic algorithm (GA) and attack detection is performed by support vector machine (SVM) classifier.

Limitations

- This method is not suitable for compromised meter detection since it only detects affected measurements
- Centralized state estimation increases complexity and overhead in the system

Paper 12

Title: Quickest Detection of False Data Injection Attack in Wide-Area Smart Grids

Concept

In false data injection attack detection, sequential detector is presented which performs based on generalized likelihood ratio. This method is able to handle variety of attacking strategies and load situations in power systems. In addition, sequential detector using adaptive sampling technique called as level triggered sampling method is employed for wide-area monitoring.

Limitations

- Here both detectors are performed in centralized manner which increases the system complexity

Paper 13

Title: A Collaborative Intrusion Detection Mechanism against False Data Injection Attack in Advanced Metering Infrastructure

Concept

A collaborative intrusion detection mechanism is presented in this paper for false data injection attack detection. In this approach, a spying domain concept is utilized to protect data in smart meters. This approach requires following constraints: secret information, event log, and spying domain. Here the attackers also classified into innocent attackers, skilled attackers, and powerful attackers.

Limitations

- This method requires secret information to be shared in advance. However, if the secret information is known to attacker then that attacker is easily compromise the node

Paper 14

Title: Real-Time Detection of False Data Injection in Smart Grid Networks: An Adaptive CUSUM Method and Analysis

Concept

In this paper Markov chain based analytical model and CUSUM based attack detection model are introduced. To improve CUSUM method in terms of delay and accuracy, an adaptive CUSUM method is presented in this paper. This proposed method is recursive in nature and each recursion is comprised with two major interleaved tests such as i) unknown variable solver based on Rao test, and ii) multithread CUSUM test.

Limitations

- This method is not able to detect compromised node in the system

Paper 15

Title: A Measurement Source Authentication Methodology for Power System Cyber Security Enhancement

Concept

In this paper, a mathematical morphology (MM) method is proposed to defend against major attacks in the smart grid system. In this method, the power system measurements are decomposed to obtain intrinsic component. Then based on intrinsic components, the time-frequency sparsity mapping is established. The signals are correlated by random forest classifier based on time-frequency mapping. With this information the source of each measurement is then authenticated.

Limitations

- This method is only able to identify the source of the measurement and not able to secure the measurement.

BIBLIOGRAPHY

Daojing He, Sammy Chan, and Mohsen Guizani, "Cyber Security Analysis and Protection of Wireless Sensor Networks for Smart Grid Monitoring", IEEE Wireless Communications, pp. 2-7, 2016.

Dariush Abbasinezhad-Mood, Morteza Nikooghadam, "Anonymous ECC-Based Self-Certified Key Distribution Scheme for Smart Grid", IEEE Transactions on Industrial Electronics, Vol. 65, Issue. 10, pp. 7996-8004, 2018.

Suzhi Bi and Ying Jun (Angela) Zhang, "Graph-based Cyber Security Analysis of State Estimation in Smart Power Grid', IEEE Communications Magazine, pp. 176-183, 2017.

Ustun, Taha Selim & Farooq, Shaik & Hussain, Suhail. (2019). A Novel Approach for Mitigation of Replay and Masquerade Attacks in Smartgrids using IEC 61850 Standard. IEEE Access.

Vrettos, Evangelos & Andersson, Göran. (2015). Scheduling and Provision of Secondary Frequency Reserves by Aggregations of Commercial Buildings. IEEE Transactions on Sustainable Energy. 7. 1-15.

Mete Ozay, Inaki Esnaola, Fatos T. Yarman Vural, Sanjeev R. Kulkarni, and H. Vincent Poor, "Machine Learning Methods for Attack Detection in the Smart Grid", IEEE Transactions on Neural Networks and Learning Systems, Vol. 27, Issue.8, 2016.

Kush Khanna, Bijaya Ketan Panigrahi, and Anupam Joshi, "Bi-level modelling of false data injection attacks on security constrained optimal power flow", IET Generation, Transmission & Distribution, Vol. 11, Issue. 14, pp. 3586-3593, 2017.

Anibal Sanjab, and Walid Saad, "Data Injection Attacks on Smart Grids with Multiple Adversaries: A Game-Theoretic Perspective", IEEE Transactions on Smart Grid, Vol. 7, Issue. 4, pp. 2038-2049, 2016.

Liang Hu, Zidong Wang, Izaz Rahman and Xiaohui Liu, "A Constrained Optimization Approach to Dynamic State Estimation for Power Systems including PMU Measurements", IEEE Transactions on Control Systems Technology, Vol. 24, Issue. 2, 2016.

Zong-Han Yu and Wen-Long Chin, "Blind False Data Injection Attack Using PCA Approximation Method in Smart Grid", IEEE Transactions on Smart Grid, Vol. 6, Issue. 3, pp. 1219-1226.

Saeed Ahmed, Youngdoo Lee, Seung Ho Hyun, and Insoo Koo, "Feature Selection_Based Detection of Covert Cyber Deception Assaults in Smart Grid Communications Networks Using Machine Learning", IEEE Access, Vol. 6, pp. 27518-27529.

Shang Li, Yasin Yılmaz, and Xiaodong Wang, "Quickest Detection of False Data Injection Attack in Wide-Area Smart Grids", IEEE Transactions on Smart Grid, Vol. 6, Issue. 6, pp. 2725-2735, 2015

Xiaoxue Liu, Peidong Zhu, Yan Zhang, and Kan Chen, "A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure", IEEE Transactions on Smart Grid, Vol. 6, Issue. 5, pp. 2435-2443, 2015.

Yi Huang, Jin Tang, Yu Cheng, Husheng Li, Kristy A. Campbell, and Zhu Han, "Real-Time Detection of False Data Injection in Smart Grid Networks: An Adaptive CUSUM Method and Analysis", IEEE Systems Journal, Vol. 10, Issue. 2, pp. 532-543, 2016.

Yi Yi Cui, Feifei Bai, Yong Liu, and Yilu Liu, "A Measurement Source Authentication Methodology for Power System Cyber Security Enhancement", IEEE Transactions on Smart Grid, Vol. 9, Issue. 4, pp. 3914-3916, 2018.

Adnan Anwar, Abdun Naser Mahmood, and Zahir Tari, "Identification of Vulnerable Node Clusters against False Data Injection Attack in an AMI based Smart Grid", Information Systems, Elsevier, Vol. 53, pp. 201-212, 2015.

Hadis Karimipour, and Venkata Dinavahi, "Robust Massively Parallel Dynamic State Estimation of Power Systems Against Cyber-Attack", IEEE Access, Vol. 6, pp. 2984-2995.

Danda B. Rawat, and Chandra Bajracharya, "Detection of False Data Injection Attacks in Smart Grid Communication Systems", IEEE Signal Processing Letters, Vol. 22, Issue. 10, pp. 1652-1656.

Li, B., Lu, R., Wang, W., & Choo, K.-K. R., "Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system", Journal of Parallel and Distributed Computing, Vol. 103, pp.32-41.

Sara Nanchian, Ankur Majumdar, and Bikash C. Pal, "Three-Phase State Estimation Using Hybrid Particle Swarm Optimization", IEEE Transactions on Smart Grid, Vol. 8, Issue. 3, pp. 1035-1045, 2017.