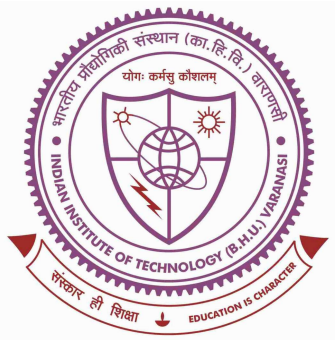
Formulation and detection of false data injection attack in modern smart grid



Thesis submitted in partial fulfillment
for the award of degree

Doctor of Philosophy

by

Debottam Mukherjee

DEPARTMENT OF ELECTRICAL ENGINEERING
Indian Institute of Technology
(Banaras Hindu University)
Varanasi

Roll No: 17081008

2022

Chapter 6

Conclusions and future scopes

6.1 Conclusions

Estimation of the power system operating states is crucial for the grid operator to determine the current grid operation. Critical grid operations like optimal load dispatch, load forecasting, load monitoring, voltage regulation, etc. are inherently dependent on the solutions of the state estimation algorithm. This thesis demonstrates effective attack vector formulation schemes against the linear and nonlinear state estimation algorithms. It can be seen that with an accurate knowledge of line admittances and current grid topology, perfect attack scenarios can be executed.

The conventional attack vector formulation scheme against the linear state estimation algorithm generally encompass the full column space of the topology matrix. It can be seen that attackers with the knowledge of the grid can bypass the BDDs using such aforesaid information. With the aid of the low-rank subspace of the topology matrix along with imposing constraints over the state deviation vector, stealthy attack vectors capable of developing critical scenarios on the grid can be formulated. Such schemes provide better subspace information than the attack vectors defined on the basis of the measurement covariance subspace, hence leading to a higher bypassing probability of the BDDs under limited access to measurement data. With limited access to measurements, an erroneous subspace estimation of the acquired measurements is defined using the state-of-the-art approaches, thus leading to higher residuals and a higher detection probability. The proposed scheme on the other hand is capable of defining an accurate low-rank subspace in presence of noises and outliers as well. Nevertheless, the primary drawback of such an

approach is that the attacker needs to gain access to informations like line admittances, topology configuration of the current grid before launching such an attack. Moreover, it defines a very small non-zero deviation of the estimated states, thus furnishing a minor attack on the grid.

To determine the presence of conventional attacks within the raw measurements at SCADA, this thesis furnishes an effective FDIA detection within the measurements using effective state forecasting driven anomaly detection schemes. With the implementation of nonlinear LSTM structures, an effective state forecasting scheme has been showcased. Such advanced neural network models demonstrate better state forecasting than SVM, ARIMA, and nonlinear MLPs. The aforesaid propositions were validated on the standard IEEE 14-bus test bench. It can be seen that the models demonstrate a scalable, real-time effective state forecasting scheme with a minimal computational burden and performance metrics like RMSE, MSE and MAE. The anomaly detection schemes undertaking the error vector and the error covariance matrix furnishes an efficient determination of the presence of attacks within the raw measurements. The proposed scheme furnishes an efficient performance under varying strength of attack and noise margins. Such schemes may provide the operator with real-time FDIA identification, nevertheless, it comes with their inherent shortcoming. Using such scheme, the operator can not explicitly determine the corresponding locations of intrusions of attack.

To overcome this issue, this thesis also furnishes an effective execution of advanced deep learning structures which work as multilabel classifiers and is capable of determining the presence of attack with their respective points of intrusions within the acquired measurements at SCADA. Moreover, predefined knowledge of statistical information of the power grid and attack vectors are not required for the developed scheme, thus furnishing a model free FDIA detection strategy. Additionally, for an effective model training, only the measurements with their corresponding truth labels are required. The advanced neural network models are capable of working concurrently with the traditional BDDs which can efficiently detect any randomized or unstructured FDIAs. Furthermore, the developed deep learning models does not require any modifications of the conventional BDD, hence demonstrating a cost-effective approach. When tested on large-scale systems, the models demonstrate an effective determination of locations of attack within the raw measurements with high accuracy. The proposed CNN, CNN-LSTM, CNN-BiLSTM

neural networks portray a scalable, real-time multilabel classifier, thus developing an effective FDIA identification scheme. Moreover, the developed models pose a robust FDIA identification scheme under varying noise and attack scenarios.

This thesis primarily demonstrates the effects of FDIAs against the power system state estimators. Most of the literature defines the effect of such attacks when its cyber-physical component is directly attacked. This thesis demonstrates that the protection and control functions that are directly related to the solution of the estimated states may be jeopardised using the proposed attack vector formulation schemes from the control centre like opening the breakers of healthy lines, developing apparent overloading of transmission lines, developing inappropriate control actions etc. The operator may issue a trip command based on the apparent power flows through the transmission lines. On the other hand, FDIAs may also lead to the generation of inappropriate control signals from the control centre. With the possibility of independent and data-driven FDIAs on the automatic voltage control, it can be seen from [263] that the Markov decision process followed by Q learning algorithms can be adopted to define such attacks. The proposed low-rank subspace-based attack vectors may also define a relay malfunction or inappropriate controls as they can effectively bypass the BDDs. To effectively mitigate these effects on the protection and control actions, kernel density estimations are also taken into account that define an advanced BDD with correction coefficients. With sufficient offline data for the normal operation of the protection and the control devices, the proposed neural network schemes can be trained effectively. As the trained neural networks have a minimal computational burden, they can be deployed online for the effective detection of such attacks.

It can be seen from Fig. 6.1 that attacks may also jeopardise the automatic generation control (AGC), load frequency control (LFC) etc. signals at the control centre as they are inherently dependent on the state estimates.

6.2 Future scope

To effectively determine the presence of attacks within the raw measurements using the developed state forecasting scheme, a tighter bound on the detection parameter is one of the key future goals that leads to a higher probability of detection with an effective

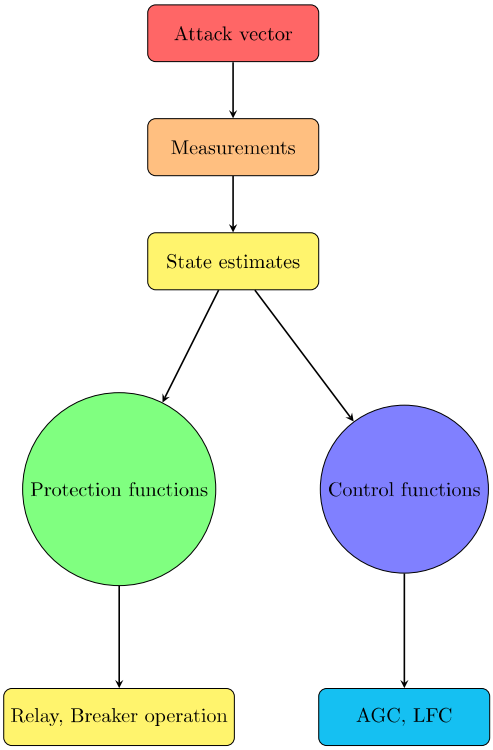


Figure 6.1: Attacks against protection and control actions on the grid

minimisation of the RMSE as the performance index. Future works may include an effective implementation of the proposed approach during contingency scenarios on the grid. Furthermore, this thesis incorporates linear and nonlinear static state estimation techniques for an effective estimation of the operating states. An effective deployment of dynamic state estimation techniques like Kalman filter, recursive least squares etc. may further enhance the accuracy of the state estimation algorithms. It can be seen that conventional attack vector formulation schemes against the linear state estimation algorithms can not guarantee an effective bypassing of the BDDs when the operator implements a dynamic state estimation technique. Hence, modeling of advanced attack vectors against such dynamic state estimation algorithms is one of the key future research prospectives. Additionally, the nonlinear honest Gauss Newton state estimation algorithm undertaken in this thesis is highly sensitive to initialization. Kalman filters define a robust approach against model initialization, hence defining a superior state estimation technique. Moreover, advanced nonlinear scalable neural network models working as multilabel classifiers can be implemented against attack vectors formulated against the nonlinear state estimation algorithm. Furthermore, it is seen that developing attack

vectors against the linear and the nonlinear state estimation algorithm requires adequate system information.. Moreover, modeling of attack vectors using measurement subspace along with reduced access to system measurements is also one of the key future research prospects. Such an approach may lead to stealthy attack vectors with minimal system information. Although this thesis demonstrates an effective low-rank subspace based attack vector formulation scheme against the linear state estimation algorithm, a future possibility of implementing such an approach for nonlinear state estimation algorithm is also one of the potential outcomes.

Digital twin models have recently gained high attention and are designed and formulated based on virtual replicas of the physical power grid. It can easily replicate virtually the characteristics and working patterns of the physical assets in real-time [264]. To monitor the physical assets like distribution transformers, a digital model replicating it can be used to monitor the current and the voltages [265]. Such models are also effectively deployed for the detection of intrusions against industrial control systems [266–268]. Digital twin models can be developed in real-time simulators that can access the system data based on the communication servers and determine any potential attacks. The key challenge is to integrate virtual models of large-scale power sectors with dynamic load changes in the IIOT cloud that can effectively map the physical and cyber components of the grid. The proposed detection schemes in this thesis can be seen to be computationally effective and, hence can be easily deployed in the IIOT cloud infrastructure. After mapping the physical assets with the digital twin, the proposed real-time attack detectors can be easily implemented, thus demonstrating an effective presence and location detection of FDIAs.

Power system restoration can be classified into network reconfiguration and load restoration. It can be seen that during network reconfiguration, the entries of the mapping matrix that depend on line connectivity and network impedances change. This on the other hand ensures that the conventional attack vectors formulated that encompass the entire column space of the mapping matrix would also change. During such network reconfiguration, the low-rank subspace-based data-driven attack vectors would also change due to varying low-rank approximations. Although this thesis has undertaken constant loads during steady-state grid operation, during load restoration the aforementioned attack vectors would not vary significantly as during steady-state line power flows and injections are nearly kept constant. However, if dynamic load restoration is undertaken

followed by an online parameter estimation of the transmission lines from the solution of the state estimates, then the entries of the mapping matrix would vary. This on the other hand would lead to varying attack vectors due to varying column and low-rank subspaces.

The proposed attack detection strategies need to be modified for FDIAs during system restoration. The presence detection model needs to be either trained with state estimation data during system restoration or an effective thresholding should be put in by the operator to efficiently detect the presence of FDIAs. To effectively detect their locations of intrusions, effective training with the state estimation data during system restoration should be used. The trained models could efficiently discriminate between the actual set of state estimates and FDIAs during system restoration using such an approach. This leads to one of the future scopes of this thesis which incorporates expanding the current attack formulation and detection schemes during system restoration.

References

[1] S. G. Mandate, "Standardization mandate to european standardisation organisations (esos) to support european smart grid deployment," *European Commission: Brussels, Belgium*, 2011.

[2] "Country wise ddos attacks," https://securelist.com/ddos-report-q2-2019/91934/., [Online; accessed Jan 27, 2018].

[3] A. Ipakchi and F. Albuyeh, "Grid of the future," *IEEE power and energy magazine*, vol. 7, no. 2, pp. 52–62, 2009.

[4] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—the new and improved power grid: A survey," *IEEE communications surveys & tutorials*, vol. 14, no. 4, pp. 944–980, 2011.

[5] A. Teixeira, H. Sandberg, and K. H. Johansson, "Networked control systems under cyber attacks with applications to power networks," in *Proceedings of the 2010 American Control Conference*. IEEE, 2010, pp. 3690–3696.

[6] G. Dán, H. Sandberg, M. Ekstedt, and G. Björkman, "Challenges in power system information security," *IEEE Security & Privacy Magazine*, vol. 10, no. 4, pp. 62–70, 2012.

[7] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards a framework for cyber attack impact analysis of the electric smart grid," in *2010 First IEEE international conference on smart grid communications*. IEEE, 2010, pp. 244–249.

[8] A. Hahn and M. Govindarasu, "Cyber attack exposure evaluation framework for the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 835–843, 2011.