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.

[9] Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and evaluation of security threats on the communication networks in the smart grid," in *2010-Milcom 2010 Military Communications Conference*. IEEE, 2010, pp. 1830–1835.

[10] S. Gong, Z. Zhang, H. Li, and A. D. Dimitrovski, "Time stamp attack in smart grid: Physical mechanism and damage analysis," *arXiv preprint arXiv:1201.2578*, 2012.

[11] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time synchronization attack in smart grid-part i: Impact and analysis," *arXiv preprint arXiv:1204.0459*, 2012.

[12] Z. Zhang, S. Gong, H. Li, and C. Pei, "Time stamp attack on wide area monitoring system in smart grid," *arXiv preprint arXiv:1102.1408*, 2011.

[13] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 667–674, 2011.

[14] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security & Privacy*, vol. 8, no. 1, pp. 81–85, 2010.

[15] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," in *IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004.* IEEE, 2004, pp. 259–271.

[16] K. Wang, M. Du, S. Maharjan, and Y. Sun, "Strategic honeypot game model for distributed denial of service attacks in the smart grid," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2474–2482, 2017.

[17] K. I. Sgouras, A. D. Birda, and D. P. Labridis, "Cyber attack impact on critical smart grid infrastructures," in *ISGT 2014*, 2014, pp. 1–5.

[18] A. Huseinović, S. Mrdović, K. Bicakci, and S. Uludag, "A survey of denial-of-service attacks and solutions in the smart grid," *IEEE Access*, vol. 8, pp. 177 447–177 470, 2020.

[19] D. Acarali, K. R. Rao, M. Rajarajan, D. Chema, and M. Ginzburg, "Modelling smart grid it-ot dependencies for ddos impact propagation," *Computers & Security*, vol. 112, p. 102528, 2022.

[20] S. Ali and Y. Li, "Learning multilevel auto-encoders for ddos attack detection in smart grid network," *IEEE Access*, vol. 7, pp. 108 647–108 659, 2019.

[21] R. C. Diovu and J. T. Agee, "A cloud-based openflow firewall for mitigation against ddos attacks in smart grid ami networks," in *2017 IEEE PES PowerAfrica*, 2017, pp. 28–33.

[22] D. Du, X. Li, W. Li, R. Chen, M. Fei, and L. Wu, "Admm-based distributed state estimation of smart grid under data deception and denial of service attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1698–1711, 2019.

[23] M. M. Pour, A. Anzalchi, and A. Sarwat, "A review on cyber security issues and mitigation methods in smart grid systems," in *SoutheastCon 2017*, 2017, pp. 1–4.

[24] M. Qasaimeh, R. Turab, and R. S. Al-Qassas, "Authentication techniques in smart grid: a systematic review," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 17, no. 3, pp. 1584–1594, 2019.

[25] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, "Cyber-security in smart grid: Survey and challenges," *Computers & Electrical Engineering*, vol. 67, pp. 469–482, 2018.

[26] E. N. Yılmaz, H. H. Sayan, F. Üstünsoy, S. Gönen, and G. Karacayılmaz, "Cyber security analysis of dos and mitm attacks against plcs used in smart grids," in *7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG), Istanbul, Turkey*, vol. 36, 2019, p. 40.

[27] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer networks*, vol. 169, p. 107094, 2020.

[28] S. Kulkarni, R. Rahul, R. Shreyas, S. Nagasundari, and P. B. Honnavalli, "Mitm intrusion analysis for advanced metering infrastructure communication in a smart grid

environment," in *International Conference on Computational Intelligence, Security and Internet of Things*. Springer, 2020, pp. 256–267.

[29] J. Zhao, J. Wang, and L. Yin, "Detection and control against replay attacks in smart grid," in *2016 12th International Conference on Computational Intelligence and Security (CIS)*. IEEE, 2016, pp. 624–627.

[30] T.-T. Tran, O.-S. Shin, and J.-H. Lee, "Detection of replay attacks in smart grid systems," in *2013 international conference on computing, management and telecommunications (ComManTel)*. IEEE, 2013, pp. 298–302.

[31] T. Irita and T. Namerikawa, "Detection of replay attack on smart grid with code signal and bargaining game," in *2017 American Control Conference (ACC)*. IEEE, 2017, pp. 2112–2117.

[32] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An efficient merkle-tree-based authentication scheme for smart grid," *IEEE Systems Journal*, vol. 8, no. 2, pp. 655–663, 2013.

[33] Z. A. Baig and A.-R. Amoudi, "An analysis of smart grid attacks and countermeasures." *J. Commun.*, vol. 8, no. 8, pp. 473–479, 2013.

[34] A. Abdelwahab, W. Lucia, and A. Youssef, "Set-theoretic control for active detection of replay attacks with applications to smart grid," in *2020 IEEE Conference on Control Technology and Applications (CCTA)*. IEEE, 2020, pp. 1004–1009.

[35] L. Pavithra and D. Rekha, "Prevention of replay attack for isolated smart grid," in *Next Generation Information Processing System*. Springer, 2021, pp. 251–258.

[36] P. Pradhan, K. Nagananda, P. Venkitasubramaniam, S. Kishore, and R. S. Blum, "Gps spoofing attack characterization and detection in smart grids," in *2016 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2016, pp. 391–395.

[37] Y. Fan, Z. Zhang, M. Trinkle, A. D. Dimitrovski, J. B. Song, and H. Li, "A cross-layer defense mechanism against gps spoofing attacks on pmus in smart grids," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 2659–2668, 2014.

[38] P. Risbud, N. Gatsis, and A. Taha, "Vulnerability analysis of smart grids to gps spoofing," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3535–3548, 2018.

[39] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 87–98, 2013.

[40] A. Xue, F. Xu, J. H. Chow, S. Leng, H. Kong, J. Xu, and T. Bi, "Data-driven detection for gps spoofing attack using phasor measurements in smart grid," *International Journal of Electrical Power & Energy Systems*, vol. 129, p. 106883, 2021.

[41] S. Gong, Z. Zhang, M. Trinkle, A. D. Dimitrovski, and H. Li, "Gps spoofing based time stamp attack on real time wide area monitoring in smart grid," in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2012, pp. 300–305.

[42] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011.

[43] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. CRC press, 2004.

[44] A. Monticelli, "Electric power system state estimation," *Proceedings of the IEEE*, vol. 88, no. 2, pp. 262–282, 2000.

[45] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 659–666, 2011.

[46] K. G. Boroojeni, M. H. Amini, and S. Iyengar, "Overview of the security and privacy issues in smart grids," in *Smart grids: security and privacy issues*. Springer, 2017, pp. 1–16.

[47] A. G. Delavar, M. Nejadkheirallah, and M. Motalleb, "A new scheduling algorithm for dynamic task and fault tolerant in heterogeneous grid systems using genetic algorithm," in *2010 3rd International Conference on Computer Science and Information Technology*, vol. 9. IEEE, 2010, pp. 408–412.

[48] S. Akhlaghi, N. Zhou, and Z. Huang, "Adaptive adjustment of noise covariance in kalman filter for dynamic state estimation," in *2017 IEEE power & energy society general meeting*. IEEE, 2017, pp. 1–5.

[49] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *2012 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2012, pp. 3153–3158.

[50] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1665–1676, 2014.

[51] X. Liu, Z. Bao, D. Lu, and Z. Li, "Modeling of local false data injection attacks with reduced network information," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1686–1696, 2015.

[52] Z.-H. Yu and W.-L. Chin, "Blind false data injection attack using pca approximation method in smart grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 3, pp. 1219–1226, 2015.

[53] J. Kim, L. Tong, and R. J. Thomas, "Subspace methods for data attack on state estimation: A data driven approach," *IEEE Transactions on Signal Processing*, vol. 63, no. 5, pp. 1102–1114, 2014.

[54] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *2012 IEEE Global Communications Conference (GLOBECOM)*, 2012, pp. 3153–3158.

[55] X. Liu and Z. Li, "False data attacks against ac state estimation with incomplete network information," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2239–2248, 2017.

[56] Y. Li and Y. Wang, "False data injection attacks with incomplete network topology information in smart grid," *IEEE Access*, vol. 7, pp. 3656–3664, 2019.

[57] M. A. Rahman and M. Alam, "Imperfect nonlinear false data injection attack against largest normalized residual test," in *2019 IEEE Power Energy Society General Meeting (PESGM)*, 2019, pp. 1–5.

[58] D. Deka, R. Baldick, and S. Vishwanath, "Data attack on strategic buses in the power grid: Design and protection," in *2014 IEEE PES General Meeting— Conference & Exposition*. IEEE, 2014, pp. 1–5.

[59] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *2010 First IEEE International Conference on Smart Grid Communications*. IEEE, 2010, pp. 226–231.

[60] L. Jia, R. J. Thomas, and L. Tong, "Malicious data attack on real-time electricity market," in *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2011, pp. 5952–5955.

[61] L. Jia, R. J. Thomas, and L. Tong, "Impacts of malicious data on real-time price of electricity market operations," in *2012 45th Hawaii International Conference on System Sciences*. IEEE, 2012, pp. 1907–1914.

[62] M. Esmalifalak, H. Nguyen, R. Zheng, L. Xie, L. Song, and Z. Han, "A stealthy attack against electricity market using independent component analysis," *IEEE Systems Journal*, vol. 12, no. 1, pp. 297–307, 2018.

[63] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 160–169, 2013.

[64] Q. Zhang, F. Li, Q. Shi, K. Tomsovic, J. Sun, and L. Ren, "Profit-oriented false data injection on electricity market: Reviews, analyses, and insights," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 9, pp. 5876–5886, 2020.

[65] J. Cao, D. Wang, Z. Qu, M. Cui, P. Xu, K. Xue, and K. Hu, "A novel false data injection attack detection model of the cyber-physical power system," *IEEE Access*, vol. 8, pp. 95 109–95 125, 2020.

[66] T. O. Olowu, S. Dharmasena, H. Jafari, and A. Sarwat, "Investigation of false data injection attacks on smart inverter settings," in *2020 IEEE CyberPELS (CyberPELS)*. IEEE, 2020, pp. 1–6.

[67] M. M. Roomi, P. P. Biswas, D. Mashima, Y. Fan, and E.-C. Chang, "False data injection cyber range of modernized substation system," in *2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2020, pp. 1–7.

[68] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 382–390, 2011.

[69] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1731–1738, 2012.

[70] Y. Xiang, Z. Ding, Y. Zhang, and L. Wang, "Power system reliability evaluation considering load redistribution attacks," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 889–901, 2016.

[71] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2016.

[72] M. Giannini, "Improving cyber-security of power system state estimators," 2014.

[73] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks against nonlinear state estimation in smart power grids," in *2013 IEEE Power & Energy Society General Meeting*, 2013, pp. 1–5.

[74] J. Nayak and I. Al-Anbagi, "Modelling false data injection attacks against nonlinear state estimation in ac power systems," in *2020 8th International Conference on Smart Grid (icSmartGrid)*, 2020, pp. 37–42.

[75] Y. Sun, W.-T. Li, W. Song, and C. Yuen, "False data injection attacks with local topology information against linear state estimation," in *2015 IEEE Innovative Smart Grid Technologies - Asia (ISGT ASIA)*, 2015, pp. 1–5.

[76] M. Ashrafuzzaman, Y. Chakhchoukh, A. A. Jillepalli, P. T. Tosic, D. C. de Leon, F. T. Sheldon, and B. K. Johnson, "Detecting stealthy false data injection attacks in power grids using deep learning," in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, 2018, pp. 219–225.

[77] X. Li and K. W. Hedman, "Enhancing power system cyber-security with systematic two-stage detection strategy," *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 1549–1561, 2019.

[78] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, pp. 1–29, 2016.

[79] J. E. Sullivan and D. Kamensky, "How cyber-attacks in ukraine show the vulnerability of the us power grid," *The Electricity Journal*, vol. 30, no. 3, pp. 30–35, 2017.

[80] Y. Guo, C.-W. Ten, and P. Jirutitijaroen, "Online data validation for distribution operations against cybertampering," *IEEE Transactions on Power Systems*, vol. 29, no. 2, pp. 550–560, 2013.

[81] S. Mehrdad, S. Mousavian, G. Madraki, and Y. Dvorkin, "Cyber-physical resilience of electrical power systems against malicious attacks: A review," *Current Sustainable/Renewable Energy Reports*, vol. 5, no. 1, pp. 14–22, 2018.

[82] X. Zhang, X. Yang, J. Lin, and W. Yu, "On false data injection attacks against the dynamic microgrid partition in the smart grid," in *2015 IEEE International Conference on Communications (ICC)*. IEEE, 2015, pp. 7222–7227.

[83] B. K. Sethi, D. Mukherjee, D. Singh, R. K. Misra, and S. Mohanty, "Smart home energy management system under false data injection attack," *International Transactions on Electrical Energy Systems*, vol. 30, no. 7, p. e12411, 2020.

[84] S. Mousavian, J. Valenzuela, and J. Wang, "Real-time data reassurance in electrical power systems based on artificial neural networks," *Electric Power Systems Research*, vol. 96, pp. 285–295, 2013.

[85] A. S. Mohamed, M. F. M. Arani, A. A. Jahromi, and D. Kundur, "False data injection attacks against synchronization systems in microgrids," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4471–4483, 2021.

[86] N. Nikmehr and S. M. Moghadam, "Game-theoretic cybersecurity analysis for false data injection attack on networked microgrids." *IET Cyper-Phys. Syst.: Theory & Appl.*, vol. 4, no. 4, pp. 365–373, 2019.

[87] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 3, pp. 717–729, 2014.

[88] J. Kim, L. Tong, and R. J. Thomas, "Subspace methods for data attack on state estimation: A data driven approach," *IEEE Transactions on Signal Processing*, vol. 63, no. 5, pp. 1102–1114, 2015.

[89] A. Anwar and A. N. Mahmood, "Stealthy and blind false injection attacks on scada ems in the presence of gross errors," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*, 2016, pp. 1–5.

[90] B. K. Sethi, A. Singh, S. Mohanty, D. Singh, and R. K. Misra, "Game theoretic smart residential buildings energy management system under false data injection attack," *IEEE Internet of Things Journal*, pp. 1–1, 2022.

[91] F. Wen and W. Liu, "An efficient data-driven false data injection attack in smart grids," in *2018 IEEE 23rd International Conference on Digital Signal Processing (DSP)*, 2018, pp. 1–5.

[92] X. Liu, Z. Bao, D. Lu, and Z. Li, "Modeling of local false data injection attacks with reduced network information," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1686–1696, 2015.

[93] X. Fu, G. Chen, and D. Yang, "Local false data injection attack theory considering isolation physical-protection in power systems," *IEEE Access*, vol. 8, pp. 103 285–103 290, 2020.

[94] Q. Wang, W. Tai, Y. Tang, and M. Ni, "Review of the false data injection attack against the cyber-physical power system," *IET Cyber-Physical Systems: Theory & Applications*, vol. 4, no. 2, pp. 101–107, 2019.

[95] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *First Workshop on Secure Control Systems (SCS), Stockholm, 2010*, 2010.

[96] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *2010 first IEEE international conference on smart grid communications*. IEEE, 2010, pp. 214–219.

[97] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 326–333, 2011.

[98] M. M. Roomi, S. M. S. Hussain, D. Mashima, E.-C. Chang, and T. S. Ustun, "Analysis of false data injection attacks against automated control for parallel generators in iec 61850-based smart grid systems," *IEEE Systems Journal*, pp. 1–12, 2023.

[99] M. Kabir-Querrec, S. Mocanu, J.-M. Thiriet, and E. Savary, "A test bed dedicated to the study of vulnerabilities in iec 61850 power utility automation networks," in *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 2016, pp. 1–4.

[100] R. Macwan, C. Drew, P. Panumpabi, A. Valdes, N. Vaidya, P. Sauer, and D. Ishchenko, "Collaborative defense against data injection attack in iec61850 based smart substations," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*. IEEE, 2016, pp. 1–5.

[101] R. Tan, H. H. Nguyen, E. Y. Foo, D. K. Yau, Z. Kalbarczyk, R. K. Iyer, and H. B. Gooi, "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 7, pp. 1609–1624, 2017.

[102] A. Abbaspour, A. Sargolzaei, P. Forouzannezhad, K. K. Yen, and A. I. Sarwat, "Resilient control design for load frequency control system under false data injection attacks," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 9, pp. 7951–7962, 2019.

[103] M. Li and Y. Chen, "Wide-area robust sliding mode controller for power systems with false data injection attacks," *IEEE Transactions on Smart Grid*, vol. 11, no. 2, pp. 922–930, 2019.

[104] A. Anwar, A. Mahmood, B. Ray, M. A. Mahmud, and Z. Tari, "Machine learning to ensure data integrity in power system topological network database," *Electronics*, vol. 9, no. 4, p. 693, 2020.

[105] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645–658, 2011.

[106] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1644–1652, 2014.

[107] M. Ganjkhani, S. N. Fallah, S. Badakhshan, S. Shamshirband, and K.-w. Chau, "A novel detection algorithm to identify false data injection attacks on power system state estimation," *Energies*, vol. 12, no. 11, p. 2209, 2019.

[108] D. Mukherjee, S. Chakraborty, R. Banerjee, and J. Bhunia, "A novel real-time false data detection strategy for smart grid," in *2021 IEEE 9th Region 10 Humanitarian Technology Conference (R10-HTC)*, 2021, pp. 1–6.

[109] D. Mukherjee and S. Chakraborty, "Real-time identification of false data injection attack in smart grid," in *2021 IEEE Region 10 Symposium (TENSYMP)*, 2021, pp. 1–6.

[110] A. Kumar, N. Saxena, and B. J. Choi, "Machine learning algorithm for detection of false data injection attack in power system," in *2021 International Conference on Information Networking (ICOIN)*, 2021, pp. 385–390.

[111] K. Huang, Z. Xiang, W. Deng, C. Yang, and Z. Wang, "False data injection attacks detection in smart grid: A structural sparse matrix separation method," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 3, pp. 2545–2558, 2021.

[112] S. Bi and Y. J. Zhang, "Defending mechanisms against false-data injection attacks in the power system state estimation," in *2011 IEEE GLOBECOM Workshops (GC Wkshps)*. IEEE, 2011, pp. 1162–1167.

[113] C. Pei, Y. Xiao, W. Liang, and X. Han, "Pmu placement protection against coordinated false data injection attacks in smart grid," *IEEE transactions on industry applications*, vol. 56, no. 4, pp. 4381–4393, 2020.

[114] Q. Yang, L. Jiang, W. Hao, B. Zhou, P. Yang, and Z. Lv, "Pmu placement in electric transmission networks for reliable state estimation against false data injection attacks," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1978–1986, 2017.

[115] J. Bae, "Cost-effective placement of phasor measurement units to defend against false data injection attacks on power grid," *Energies*, vol. 13, no. 15, p. 3862, 2020.

[116] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 3, pp. 717–729, 2013.

[117] Q. Yang, D. An, R. Min, W. Yu, X. Yang, and W. Zhao, "On optimal pmu placement-based defense against data integrity attacks in smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 7, pp. 1735–1750, 2017.

[118] C. Pei, Y. Xiao, W. Liang, and X. Han, "Pmu placement protection against coordinated false data injection attacks in smart grid," *IEEE Transactions on Industry Applications*, vol. 56, no. 4, pp. 4381–4393, 2020.

[119] H. Zhang, S. Wang, Y. Pei, Y. Li, G. Wang, and T. Lu, "Optimal configuration of pmu based on false data injection," in *2018 International Conference on Power System Technology (POWERCON)*, 2018, pp. 3016–3022.

[120] P. K. Jena, S. Ghosh, and E. Koley, "An optimal pmu placement scheme for detection of malicious attacks in smart grid," in *2021 4th Biennial International Conference on Nascent Technologies in Engineering (ICNTE)*, 2021, pp. 1–6.

[121] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," in *Preprints of the first workshop on secure control systems, CPSWEEK*, vol. 2010. Stockholm, Sweden, 2010.

[122] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in ac state estimation," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2476–2483, 2015.

[123] B. Li, R. Lu, G. Xiao, T. Li, and K.-K. R. Choo, "Detection of false data injection attacks on smart grids: A resilience-enhanced scheme," *IEEE Transactions on Power Systems*, pp. 1–1, 2021.

[124] E. Drayer and T. Routtenberg, "Detection of false data injection attacks in power systems with graph fourier transform," in *2018 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, 2018, pp. 890–894.

[125] E. Drayer and T. Routtenberg, "Detection of false data injection attacks in smart grids based on graph signal processing," *IEEE Systems Journal*, vol. 14, no. 2, pp. 1886–1896, 2020.

[126] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1216–1227, 2014.

[127] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1389–1407, 2017.

[128] D. Mukherjee, S. Chakraborty, R. Banerjee, J. Bhunia, and P. Kumar Guchhait, "A novel deep learning framework to identify false data injection attack in power sector," in *TENCON 2021 - 2021 IEEE Region 10 Conference (TENCON)*, 2021, pp. 278–283.

[129] D. Mukherjee, S. Chakraborty, R. Banerjee, J. Bhunia, and P. K. Guchhait, "Deep learning based real-time detection of false data injection attacks in power grids," in *2021 22nd International Middle East Power Systems Conference (MEPCON)*, 2021, pp. 124–130.

[130] B. Li, T. Ding, C. Huang, J. Zhao, Y. Yang, and Y. Chen, "Detecting false data injection attacks against power system state estimation with fast go-decomposition

approach," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 5, pp. 2892–2904, 2018.

[131] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Limiting false data attacks on power system state estimation," in *2010 44th Annual Conference on Information Sciences and Systems (CISS)*. IEEE, 2010, pp. 1–6.

[132] W. Xu, M. Wang, and A. Tang, "On state estimation with bad data detection," in *2011 50th IEEE Conference on Decision and Control and European Control Conference*. IEEE, 2011, pp. 5989–5994.

[133] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "On malicious data attacks on power system state estimation," in *45th International Universities Power Engineering Conference UPEC2010*, 2010, pp. 1–6.

[134] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *2010 first IEEE international conference on smart grid communications*. IEEE, 2010, pp. 220–225.

[135] Y. Huang, H. Li, K. A. Campbell, and Z. Han, "Defending false data injection attack on smart grid network using adaptive cusum test," in *2011 45th Annual Conference on Information Sciences and Systems*. IEEE, 2011, pp. 1–6.

[136] V. Obrien, R. D. Trevizan, and V. S. Rao, "Detecting false data injection attacks to battery state estimation using cumulative sum algorithm," in *2021 North American Power Symposium (NAPS)*. IEEE, 2021, pp. 01–06.

[137] V. Obrien, V. Rao, and R. D. Trevizan, "Detection of false data injection attacks in battery stacks using physics-based modeling and cumulative sum algorithm," in *2022 IEEE Power and Energy Conference at Illinois (PECI)*. IEEE, 2022, pp. 1–8.

[138] S. Li, Y. Yılmaz, and X. Wang, "Quickest detection of false data injection attack in wide-area smart grids," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 2725–2735, 2014.

[139] K. L. Morrow, E. Heine, K. M. Rogers, R. B. Bobba, and T. J. Overbye, "Topology perturbation for detecting malicious data injection," in *2012 45th Hawaii International Conference on System Sciences*. IEEE, 2012, pp. 2104–2113.

[140] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, 2016.

[141] B. Li, G. Xiao, R. Lu, R. Deng, and H. Bao, "On feasibility and limitations of detecting false data injection attacks on power grid state estimation using d-facts devices," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 854–864, 2019.

[142] F. Pasqualetti, R. Carli, and F. Bullo, "A distributed method for state estimation and false data detection in power networks," in *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2011, pp. 469–474.

[143] H. Hashimoto and T. Hayakawa, "Distributed cyber attack detection for power network systems," in *2011 50th IEEE Conference on Decision and Control and European Control Conference*. IEEE, 2011, pp. 5820–5824.

[144] D. Zhang, W. Yu, and R. Hardy, "A distributed network-sensor based intrusion detection framework in enterprise networks," in *2011-MILCOM 2011 Military Communications Conference*. IEEE, 2011, pp. 1195–1200.

[145] M. Dehghani, T. Niknam, M. Ghiasi, P. Siano, H. Haes Alhelou, and A. Al-Hinai, "Fourier singular values-based false data injection attack detection in ac smartgrids," *Applied Sciences*, vol. 11, no. 12, p. 5706, 2021.

[146] H. Moayyed, M. Mohammadpourfard, C. Konstantinou, A. Moradzadeh, B. Mohammadi-Ivatloo, and A. Pedro Aguiar, "Image processing based approach for false data injection attacks detection in power systems," *IEEE Access*, pp. 1–1, 2021.

[147] Y. Wang, M. M. Amin, J. Fu, and H. B. Moussa, "A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids," *IEEE Access*, vol. 5, pp. 26 022–26 033, 2017.

[148] D. Mukherjee, S. Chakraborty, and S. Ghosh, "Deep learning-based multilabel classification for locational detection of false data injection attack in smart grids," *Electrical Engineering*, pp. 1–24, 2021.

[149] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645–658, 2011.

[150] R. C. B. Hink, J. M. Beaver, M. A. Buckner, T. Morris, U. Adhikari, and S. Pan, "Machine learning for power system disturbance and cyber-attack discrimination," in *2014 7th International symposium on resilient control systems (ISRCS)*. IEEE, 2014, pp. 1–8.

[151] S. Pan, T. Morris, and U. Adhikari, "Developing a hybrid intrusion detection system using data mining for power systems," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 3104–3113, 2015.

[152] J. Landford, R. Meier, R. Barella, X. Zhao, E. Cotilla-Sanchez, R. B. Bass, and S. Wallace, "Fast sequence component analysis for attack detection in synchrophasor networks," *arXiv preprint arXiv:1509.05086*, 2015.

[153] S. Nath, I. Akingeneye, J. Wu, and Z. Han, "Quickest detection of false data injection attacks in smart grid with dynamic models," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, pp. 1–1, 2019.

[154] O. Boyaci, A. Umunnakwe, A. Sahu, M. R. Narimani, M. Ismail, K. R. Davis, and E. Serpedin, "Graph neural networks based detection of stealth false data injection attacks in smart grids," *IEEE Systems Journal*, pp. 1–12, 2021.

[155] J. Zhao, G. Zhang, M. La Scala, Z. Y. Dong, C. Chen, and J. Wang, "Short-term state forecasting-aided method for detection of smart grid general false data injection attacks," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1580–1590, 2017.

[156] J. Zhao, G. Zhang, Z. Y. Dong, and K. P. Wong, "Forecasting-aided imperfect false data injection attacks against power system nonlinear state estimation," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 6–8, 2016.

[157] A. S. Musleh, G. Chen, Z. Y. Dong, C. Wang, and S. Chen, "Online characterization and detection of false data injection attacks in wide-area monitoring systems," *IEEE Transactions on Power Systems*, pp. 1–1, 2021.

[158] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE transactions on neural networks and learning systems*, vol. 27, no. 8, pp. 1773–1786, 2015.

[159] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical dc microgrids," *IEEE Transactions on industrial informatics*, vol. 13, no. 5, pp. 2693–2703, 2017.

[160] S. K. Singh, K. Khanna, R. Bose, B. K. Panigrahi, and A. Joshi, "Joint-transformation-based detection of false data injection attacks in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 1, pp. 89–97, 2017.

[161] R. Xu, R. Wang, Z. Guan, L. Wu, J. Wu, and X. Du, "Achieving efficient detection against false data injection attacks in smart grid," *IEEE Access*, vol. 5, pp. 13 787–13 798, 2017.

[162] J. Zhao, G. Zhang, M. La Scala, Z. Y. Dong, C. Chen, and J. Wang, "Short-term state forecasting-aided method for detection of smart grid general false data injection attacks," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1580–1590, 2015.

[163] K. Khanna, B. K. Panigrahi, and A. Joshi, "Ai-based approach to identify compromised meters in data integrity attacks on smart grid," *IET Generation, Transmission & Distribution*, vol. 12, no. 5, pp. 1052–1066, 2017.

[164] U. Adhikari, T. H. Morris, and S. Pan, "Applying non-nested generalized exemplars classification for cyber-power event and intrusion detection," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 3928–3941, 2016.

[165] M. Zhang, C. Shen, N. He, S. Han, Q. Li, Q. Wang, and X. Guan, "False data injection attacks against smart gird state estimation: Construction, detection and defense," *Science China Technological Sciences*, vol. 62, no. 12, pp. 2077–2087, 2019.

[166] B. Li, T. Ding, C. Huang, J. Zhao, Y. Yang, and Y. Chen, "Detecting false data injection attacks against power system state estimation with fast go-decomposition approach," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 5, pp. 2892–2904, 2019.

[167] M. I. Oozeer and S. Haykin, "Cognitive dynamic system for control and cyber-attack detection in smart grid," *IEEE Access*, vol. 7, pp. 78 320–78 335, 2019.

[168] A. Ayad, H. E. Z. Farag, A. Youssef, and E. F. El-Saadany, "Detection of false data injection attacks in smart grids using recurrent neural networks," in *2018 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2018, pp. 1–5.

[169] Q. Deng and J. Sun, "False data injection attack detection in a power grid using rnn," in *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, 2018, pp. 5983–5988.

[170] H. Salehghaffari and F. Khorrami, "Resilient power grid state estimation under false data injection attacks," in *2018 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2018, pp. 1–5.

[171] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "False data injection attacks targeting dc model-based state estimation," in *2017 IEEE Power & Energy Society General Meeting*, 2017, pp. 1–5.

[172] A. Sayghe, O. M. Anubi, and C. Konstantinou, "Adversarial examples on power systems state estimation," in *2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2020, pp. 1–5.

[173] B. M. R. Amin, S. Taghizadeh, S. Maric, M. J. Hossain, and R. Abbas, "Smart grid security enhancement by using belief propagation," *IEEE Systems Journal*, vol. 15, no. 2, pp. 2046–2057, 2021.

[174] Y. Li and Y. Wang, "False data injection attacks with incomplete network topology information in smart grid," *IEEE Access*, vol. 7, pp. 3656–3664, 2018.

[175] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1665–1676, 2014.

[176] Y. Zhou, J. Cisneros-Saldana, and L. Xie, "False analog data injection attack towards topology errors: Formulation and feasibility analysis," in *2018 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2018, pp. 1–5.

[177] Z. Qin and Y. Lai, "Detection and localization of coordinated state-and-topology false data injection attack by multi-modal learning," *Journal of Electrical Engineering & Technology*, pp. 1–14, 2022.

[178] S. Aoufi, A. Derhab, and M. Guerroumi, "Survey of false data injection in smart power grid: Attacks, countermeasures and challenges," *Journal of Information Security and Applications*, vol. 54, p. 102518, 2020.

[179] G. Hug and J. A. Giampapa, "Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on smart grid*, vol. 3, no. 3, pp. 1362–1370, 2012.

[180] C. Liu, H. Liang, and T. Chen, "Network parameter coordinated false data injection attacks against power system ac state estimation," *IEEE Transactions on Smart Grid*, vol. 12, no. 2, pp. 1626–1639, 2021.

[181] M. Jorjani, H. Seifi, and A. Y. Varjani, "A graph theory-based approach to detect false data injection attacks in power system ac state estimation," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 4, pp. 2465–2475, 2020.

[182] M. Du, G. Pierrou, X. Wang, and M. Kassouf, "Targeted false data injection attacks against ac state estimation without network parameters," *IEEE Transactions on Smart Grid*, vol. 12, no. 6, pp. 5349–5361, 2021.

[183] S. Bi and Y. J. Zhang, "False-data injection attack to control real-time price in electricity market," in *2013 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2013, pp. 772–777.

[184] J. Lin, W. Yu, and X. Yang, "On false data injection attack against multistep electricity price in electricity market in smart grid," in *2013 IEEE Global Communications Conference (GLOBECOM)*, 2013, pp. 760–765.

[185] A. Tajer, "False data injection attacks in electricity markets by limited adversaries: Stochastic robustness," *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 128–138, 2017.

[186] H. Ye, Y. Ge, X. Liu, and Z. Li, "Transmission line rating attack in two-settlement electricity markets," *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1346–1355, 2016.

[187] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Generalized fdia-based cyber topology attack with application to the australian electricity market trading mechanism," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 3820–3829, 2018.

[188] M. I. Reddy, R. Saha, and S. K. Valluru, "Modelling financially motivated cyber attacks on electricity markets using mixed integer linear programming," in *2020 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS)*, 2020, pp. 1–6.

[189] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1731–1738, 2012.

[190] Q. Yang, R. Min, D. An, W. Yu, and X. Yang, "Towards optimal pmu placement against data integrity attacks in smart grid," in *2016 Annual Conference on Information Science and Systems (CISS)*, 2016, pp. 54–58.

[191] M. M. Aboelwafa, K. G. Seddik, M. H. Eldefrawy, Y. Gadallah, and M. Gidlund, "A machine-learning-based technique for false data injection attacks detection in industrial iot," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8462–8471, 2020.

[192] A. Sayghe, Y. Hu, I. Zografopoulos, X. Liu, R. G. Dutta, Y. Jin, and C. Konstantinou, "Survey of machine learning methods for detecting false data injection attacks in power systems," *IET Smart Grid*, vol. 3, no. 5, pp. 581–595, 2020.

[193] A. Pinceti, L. Sankar, and O. Kosut, "Load redistribution attack detection using machine learning: A data-driven approach," in *2018 IEEE Power & Energy Society General Meeting (PESGM)*, 2018, pp. 1–5.

[194] C. Yang, Y. Wang, Y. Zhou, J. Ruan, W. Liu *et al.*, "False data injection attacks detection in power system using machine learning method," *Journal of Computer and Communications*, vol. 6, no. 11, p. 276, 2018.

[195] J. James, Y. Hou, and V. O. Li, "Online false data injection attack detection with wavelet transform and deep neural networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 3271–3280, 2018.

[196] A. Parizad and C. Hatziadoniu, "Semi-supervised false data detection using gated recurrent units and threshold scoring algorithm," in *2021 IEEE Power & Energy Society General Meeting (PESGM)*, 2021, pp. 01–05.

[197] M. Dehghani, A. Kavousi-Fard, M. Dabbaghjamanesh, and O. Avatefipour, "Deep learning based method for false data injection attack detection in ac smart islands," *IET Generation, Transmission & Distribution*, vol. 14, no. 24, pp. 5756–5765, 2020.

[198] Y. Ding, K. Ma, T. Pu, X. Wang, R. Li, and D. Zhang, "A deep learning-based classification scheme for false data injection attack detection in power system," *Electronics*, vol. 10, no. 12, p. 1459, 2021.

[199] Y. Zhang, J. Wang, and B. Chen, "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 623–634, 2020.

[200] F. Almutairy, L. Scekic, R. Elmoudi, and S. Wshah, "Accurate detection of false data injection attacks in renewable power systems using deep learning," *IEEE Access*, vol. 9, pp. 135 774–135 789, 2021.

[201] L. Yang, Y. Zhai, and Z. Li, "Deep learning for online ac false data injection attack detection in smart grids: An approach using lstm-autoencoder," *Journal of Network and Computer Applications*, vol. 193, p. 103178, 2021.

[202] X. Niu, J. Li, J. Sun, and K. Tomsovic, "Dynamic detection of false data injection attack in smart grid using deep learning," in *2019 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2019, pp. 1–6.

[203] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Processing Letters*, vol. 22, no. 10, pp. 1652–1656, 2015.

[204] R. Xu, R. Wang, Z. Guan, L. Wu, J. Wu, and X. Du, "Achieving efficient detection against false data injection attacks in smart grid," *IEEE Access*, vol. 5, pp. 13 787–13 798, 2017.

[205] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505–2516, 2017.

[206] D. Ye and T.-Y. Zhang, "Summation detector for false data-injection attack in cyber-physical systems," *IEEE Transactions on Cybernetics*, vol. 50, no. 6, pp. 2338–2345, 2020.

[207] E. Farantatos, G. K. Stefopoulos, G. J. Cokkinides, and A. Meliopoulos, "Pmu-based dynamic state estimation for electric power systems," in *2009 IEEE Power & Energy Society General Meeting*. IEEE, 2009, pp. 1–8.

[208] Y. Chakhchoukh, V. Vittal, and G. T. Heydt, "Pmu based state estimation by integrating correlation," *IEEE Transactions on Power Systems*, vol. 29, no. 2, pp. 617–626, 2013.

[209] J. Zhao, G. Zhang, K. Das, G. N. Korres, N. M. Manousakis, A. K. Sinha, and Z. He, "Power system real-time monitoring by using pmu-based robust state estimation method," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 300–309, 2015.

[210] Y.-F. Huang, S. Werner, J. Huang, N. Kashyap, and V. Gupta, "State estimation in electric power grids: Meeting new challenges presented by the requirements of the future grid," *IEEE Signal Processing Magazine*, vol. 29, no. 5, pp. 33–43, 2012.

[211] A. Gomez-Exposito, A. Abur, A. de la Villa Jaen, and C. Gomez-Quiles, "A multi-level state estimation paradigm for smart grids," *Proceedings of the IEEE*, vol. 99, no. 6, pp. 952–976, 2011.

[212] G. N. Korres and N. M. Manousakis, "State estimation and bad data processing for systems including pmu and scada measurements," *Electric Power Systems Research*, vol. 81, no. 7, pp. 1514–1524, 2011.

[213] S. Chakrabarti, E. Kyriakides, G. Ledwich, and A. Ghosh, "Inclusion of pmu current phasor measurements in a power system state estimator," *IET generation, transmission & distribution*, vol. 4, no. 10, pp. 1104–1115, 2010.

[214] C. Bruno, C. Candia, L. Franchi, G. Giannuzzi, M. Pozzi, R. Zaottini, and M. Zaramella, "Possibility of enhancing classical weighted least squares state estimation with linear pmu measurements," in *2009 IEEE Bucharest PowerTech*. IEEE, 2009, pp. 1–6.

[215] H. Zhao, "A new state estimation model of utilizing pmu measurements," in *2006 International Conference on Power System Technology*. IEEE, 2006, pp. 1–5.

[216] F. Chen, X. Han, Z. Pan, and L. Han, "State estimation model and algorithm including pmu," in *2008 Third International Conference on Electric Utility Deregulation and Restructuring and Power Technologies*. IEEE, 2008, pp. 1097–1102.

[217] H. Xue, Q.-q. Jia, N. Wang, Z.-q. Bo, H.-t. Wang, and H.-x. Ma, "A dynamic state estimation method with pmu and scada measurement for power systems," in *2007 International Power Engineering Conference (IPEC 2007)*. IEEE, 2007, pp. 848–853.

[218] A. Jain and N. Shivakumar, "Impact of pmu in dynamic state estimation of power systems," in *2008 40th North American Power Symposium*. IEEE, 2008, pp. 1–8.

[219] L. Zhao and A. Abur, "Multi area state estimation using synchronized phasor measurements," *IEEE Transactions on Power Systems*, vol. 20, no. 2, pp. 611–617, 2005.

[220] M. Zhou, V. A. Centeno, J. S. Thorp, and A. G. Phadke, "An alternative for including phasor measurements in state estimators," *IEEE transactions on power systems*, vol. 21, no. 4, pp. 1930–1937, 2006.

[221] W. Jiang, V. Vittal, and G. T. Heydt, "A distributed state estimator utilizing synchronized phasor measurements," *IEEE Transactions on Power Systems*, vol. 22, no. 2, pp. 563–571, 2007.

[222] M. Laouamer, R. Mohammedi, A. Kouzou, and A. Tlemçani, "Optimal placement of pmus in algerian network using genetic algorithm," in *2018 15th International Multi-Conference on Systems, Signals Devices (SSD)*, 2018, pp. 947–951.

[223] T. A. Alexopoulos, G. N. Korres, and N. M. Manousakis, "Complementarity reformulations for false data injection attacks on pmu-only state estimation," *Electric Power Systems Research*, vol. 189, p. 106796, 2020.

[224] N. R. Shivakumar and A. Jain, "A review of power system dynamic state estimation techniques," in *2008 Joint International Conference on Power System Technology and IEEE Power India Conference*, 2008, pp. 1–6.

[225] J. Zhang, G. Welch, G. Bishop, and Z. Huang, "A two-stage kalman filter approach for robust and real-time power system state estimation," *IEEE Transactions on Sustainable Energy*, vol. 5, no. 2, pp. 629–636, 2014.

[226] A. Monticelli, *State estimation in electric power systems: a generalized approach*. Springer Science & Business Media, 2012.

[227] K. C. Sou, H. Sandberg, and K. H. Johansson, "Electric power network security analysis via minimum cut relaxation," in *2011 50th IEEE Conference on Decision and Control and European Control Conference*. IEEE, 2011, pp. 4054–4059.

[228] M. Mohammadpourfard, A. Khalili, I. Genc, and C. Konstantinou, "Cyber-resilient smart cities: Detection of malicious attacks in smart grids," *Sustainable Cities and Society*, vol. 75, p. 103116, 2021.

[229] L. Zhang, V. Kekatos, and G. B. Giannakis, "Scalable electric vehicle charging protocols," *IEEE Transactions on Power Systems*, vol. 32, no. 2, pp. 1451–1462, 2016.

[230] P. L. Bhattar, N. M. Pindoriya, and A. Sharma, "Impact of brute force based false data injection attack on distribution system state estimation," in *TENCON 2021 - 2021 IEEE Region 10 Conference (TENCON)*, 2021, pp. 562–567.

[231] S. Bi and Y. J. Zhang, "Using covert topological information for defense against malicious attacks on dc state estimation," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 7, pp. 1471–1485, 2014.

[232] A. Anwar, A. N. Mahmood, and Z. Tari, "Identification of vulnerable node clusters against false data injection attack in an ami based smart grid," *Information Systems*, vol. 53, pp. 201–212, 2015.

[233] F. Mohammadi, "Emerging challenges in smart grid cybersecurity enhancement: A review," *Energies*, vol. 14, no. 5, p. 1380, 2021.

[234] S. Obata, K. Kobayashi, and Y. Yamashita, "Sensor scheduling-based detection of false data injection attacks in power system state estimation," in *2021 IEEE International Conference on Consumer Electronics (ICCE)*, 2021, pp. 1–4.

[235] X. Lu, J. Jing, and Y. Wu, "False data injection attack location detection based on classification method in smart grid," in *2020 2nd International Conference on Artificial Intelligence and Advanced Manufacture (AIAM)*, 2020, pp. 133–136.

[236] J. Tian, B. Wang, T. Li, F. Shang, K. Cao, and R. Guo, "Total: Optimal protection strategy against perfect and imperfect false data injection attacks on power grid cyber–physical systems," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 1001–1015, 2021.

[237] J. Kim and L. Tong, "On phasor measurement unit placement against state and topology attacks," in *2013 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2013, pp. 396–401.

[238] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1244–1253, 2013.

[239] G. Strang, *Linear algebra and learning from data*. Wellesley-Cambridge Press Cambridge, 2019.

[240] P. Drineas, R. Kannan, and M. W. Mahoney, "Fast Monte Carlo algorithms for matrices III: Computing a compressed approximate matrix decomposition," *SIAM Journal on Computing*, vol. 36, no. 1, pp. 184–206, 2006.

[241] S. L. Brunton and J. N. Kutz, *Data-driven science and engineering: Machine learning, dynamical systems, and control*. Cambridge University Press, 2019.

[242] P. Drineas, R. Kannan, and M. W. Mahoney, "Fast monte carlo algorithms for matrices i: Approximating matrix multiplication," *SIAM Journal on Computing*, vol. 36, no. 1, pp. 132–157, 2006.

[243] P. Drineas, R. Kannan, and M. W. Mahoney, "Fast monte carlo algorithms for matrices ii: Computing a low-rank approximation to a matrix," *SIAM Journal on computing*, vol. 36, no. 1, pp. 158–183, 2006.

[244] P. Drineas, A. M. Frieze, R. Kannan, S. S. Vempala, and V. Vinay, "Clustering in large graphs and matrices." in *SODA*, vol. 99. Citeseer, 1999, pp. 291–299.

[245] T. Zhou and D. Tao, "Godec: Randomized low-rank & sparse matrix decomposition in noisy case," in *Proceedings of the 28th International Conference on Machine Learning, ICML 2011*, 2011.

[246] D. Mukherjee, S. Chakraborty, P. K. Guchhait, and J. Bhunia, "Application of machine learning for speed and torque prediction of pms motor in electric vehicles," in *2020 IEEE 1st International Conference for Convergence in Engineering (ICCE)*, 2020, pp. 129–133.

[247] I. Goodfellow, Y. Bengio, A. Courville, and Y. Bengio, *Deep learning*. MIT press Cambridge, 2016, vol. 1, no. 2.

[248] R. Zhao, R. Yan, J. Wang, and K. Mao, "Learning to monitor machine health with convolutional bi-directional lstm networks," *Sensors*, vol. 17, no. 2, p. 273, 2017.

[249] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016, pp. 770–778.

[250] L. Wei, D. Gao, and C. Luo, "False data injection attacks detection with deep belief networks in smart grid," in *2018 Chinese Automation Congress (CAC)*, 2018, pp. 2621–2625.

[251] Q. Pu, H. Qin, H. Han, Y. Xia, Z. Li, K. Xie, and W. Wang, "Detection mechanism of fdi attack feature based on deep learning," in *2018 IEEE SmartWorld,*

Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), 2018, pp. 1761–1765.

[252] D. Bose, C. K. Chanda, and A. Chakrabarti, "Vulnerability assessment of a power transmission network employing complex network theory in a resilience framework," *Microsystem Technologies*, pp. 1–9, 2020.

[253] L. Van der Maaten and G. Hinton, "Visualizing data using t-sne." *Journal of machine learning research*, vol. 9, no. 11, 2008.

[254] D. Mukherjee, S. Chakraborty, and S. Ghosh, "Power system state forecasting using machine learning techniques," *Electrical Engineering*, pp. 1–23, 2021.

[255] M. M. N. Aboelwafa, K. G. Seddik, M. H. Eldefrawy, Y. Gadallah, and M. Gidlund, "A machine-learning-based technique for false data injection attacks detection in industrial iot," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8462–8471, 2020.

[256] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1644–1652, 2017.

[257] J. Zhang, "Quickest detection of time-varying false data injection attacks in dynamic smart grids," in *ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2019, pp. 2432–2436.

[258] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2218–2234, 2020.

[259] H. Shi, L. Xie, and L. Peng, "Detection of false data injection attacks in smart grid based on a new dimensionality-reduction method," *Computers & Electrical Engineering*, vol. 91, p. 107058, 2021.

[260] F. ALmutairy, R. Shadid, and S. Wshah, "Identification and correction of false data injection attacks against ac state estimation using deep learning," in *2020 IEEE Power Energy Society General Meeting (PESGM)*, 2020, pp. 1–5.

[261] X. Huang, Z. Qin, M. Xie, H. Liu, and L. Meng, "Defense of massive false data injection attack via sparse attack points considering uncertain topological changes," *Journal of Modern Power Systems and Clean Energy*, pp. 1–11, 2021.

[262] S. Tufail, S. Batool, and A. I. Sarwat, "False data injection impact analysis in ai-based smart grid," in *SoutheastCon 2021*, 2021, pp. 01–07.

[263] Y. Chen, S. Huang, F. Liu, Z. Wang, and X. Sun, "Evaluation of reinforcement learning-based false data injection attack to automatic voltage control," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2158–2169, 2018.

[264] B. Ashtari Talkhestani, T. Jung, B. Lindemann, N. Sahlab, N. Jazdi, W. Schloegl, and M. Weyrich, "An architecture of an intelligent digital twin in a cyber-physical production system," *at-Automatisierungstechnik*, vol. 67, no. 9, pp. 762–782, 2019.

[265] P. Moutis and O. Alizadeh-Mousavi, "Digital twin of distribution power transformer for real-time monitoring of medium voltage from low voltage measurements," *IEEE Transactions on Power Delivery*, vol. 36, no. 4, pp. 1952–1963, 2020.

[266] M. Zhou, J. Yan, and D. Feng, "Digital twin framework and its application to power grid online analysis," *CSEE Journal of Power and Energy Systems*, vol. 5, no. 3, pp. 391–398, 2019.

[267] C. Gehrmann and M. Gunnarsson, "A digital twin based industrial automation and control system security architecture," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 669–680, 2019.

[268] F. Akbarian, E. Fitzgerald, and M. Kihl, "Intrusion detection in digital twins for industrial control systems," in *2020 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*. IEEE, 2020, pp. 1–6.

List of Publications

The publications originating from this thesis are:

1. Real-time identification of false data injection attack in smart grid. (to be communicated)

2. Deep learning-based identification of false data injection attacks on modern smart grids. (to be communicated)

3. Mukherjee, D. (2022). A novel strategy for locational detection of false data injection attack. Sustainable Energy, Grids and Networks, 31, 100702.

4. Mukherjee, D. (2022). Data-Driven False Data Injection Attack: A Low-Rank Approach. IEEE Transactions on Smart Grid, 13(3), 2479-2482.

5. Mukherjee, D., Ghosh, S., & Misra, R. K. (2022). A Novel False Data Injection Attack Formulation Based on CUR Low-Rank Decomposition Method. IEEE Transactions on Smart Grid.

The relavent publications during doctoral degree:

1. Mukherjee, D. (2022). A novel strategy for locational detection of false data injection attack. Sustainable Energy, Grids and Networks, 31, 100702.

2. Mukherjee, D. (2022). Data-Driven False Data Injection Attack: A Low-Rank Approach. IEEE Transactions on Smart Grid, 13(3), 2479-2482.

3. Mukherjee, D., Ghosh, S., & Misra, R. K. (2022). A Novel False Data Injection Attack Formulation Based on CUR Low-Rank Decomposition Method. IEEE Transactions on Smart Grid.