Biologically Inspired Hierarchical Cyber-Physical Multi-agent Distributed Control Framework for Sustainable Smart Grids

Abstract

It is well known that information will play an important role in enhancing emerging power system operation.However, questions naturally arise as to when the increased data-dependence may be considered excessive. Two practical considerations emerge: 1) communications and computational overhead, in which redundant and irrelevant information acquisition and use results in heavy computational burden with limited performance return, and 2) increasing risks of cyber attack whereby indiscriminate cyber-dependence and -connectivity increases attack scope and impact. In this chapter, we present a hierarchical cyber-physical framework of power system operation based on flocking theory in the context of the smart grid stability problem. We study strategies to harness an appropriate degree of cyber technology by effectively leveraging physical couplings. Our formulation enables the identification of large-scale distributed control strategies for robust power grid operation. Furthermore, our formulation also enables a novel witness-based cyber-physical protocol whereby physical coherence is leveraged to probe and identify phasor measurement unit data corruption and estimate the true information values for attack mitigation.

Keywords

Power System, Smart Grid, Power Grid, Control Framework, Lead Agent

References

1. NERC CIP standards, http://www.nerc.com
2. Reliability considerations from the integration of smart grid. North American Electric Reliability Corporation (2010)Google Scholar
3. Roadmap to achieve energy delivery system cyber security. Energy Sector Control Systems Working Group (ESCSWG) (2011)Google Scholar
4. Intelligrid program: 2012 annual review. Electric Power Research Institute (EPRI) (2013)Google Scholar
5. Smart grids and renewables: A guide for effective deployment. International Renewable Energy Agency (IRENA) (2013)Google Scholar
6. How much electricity does an american home use? (2014), http://www.eia.gov/tools/faqs/faq.cfm?id=97&t=3
7. Adeodu, O., Chmielewski, D.: Design of massive energy storage systems within electric transmission networks. In: 2013 AIChE Annual Meeting, San Francisco, CA (2013)Google Scholar
8. Almond, S.J., Baird, S., Flynn, B.F., Hawkins, D.J., Mackrell, A.J.: Integrated protection and control communications outwith the substation: Cyber security challenges. In: Proc. IET 9th International Conference on Developments in Power System Protection, pp. 698–701 (2008)Google Scholar

9. Amin, S., Cárdenas, A.A., Sastry, S.S.: Safe and secure networked control systems under denial-of-service attacks. In: Majumdar, R., Tabuada, P. (eds.) HSCC 2009. LNCS, vol. 5469, pp. 31–45. Springer, Heidelberg (2009)CrossRefGoogle Scholar
10. Amin, S.M.: Energy infrastructure defense systems. Proceedings of the IEEE 93(5), 861–875 (2005)CrossRef Google Scholar
11. Amina, M., Stringer, J.: The electric power grid: Today and tomorrow. MRS Bulletin 33, 399–407 (2008)CrossRef Google Scholar
12. Ananad, M., Cronin, E., Sherr, M., Blaze, M., Ives, Z., Lee, I.: Security challenges in next generation cyber physical systems. In: Proc. Beyond SCADA: Cyber Physical Systems Meeting (HCSS-NEC4CPS), Pittsburgh, Pennsylvania (2006)Google Scholar
13. Athay, T., Podmore, R., Virmani, S.: A practical method for the direct analysis of transient stability. IEEE Transactions on Power Apparatus and Systems PAS-98, 573–587 (1979)CrossRef Google Scholar
14. Bakken, D.E., Hauser, C.H., Gjermundrod, H., Bose, A.: Toward more flexible and robust data delivery for monitoring and control of the electric power grid. Technical Report EECS-GS-009, Washington State University, Pullman, Washington (2007)Google Scholar
15. Bergen, A.R., Vittal, V.: Power Systems Analysis. Prentice Hall (1999)Google Scholar
16. Bobba, R., Khurana, H., AlTurki, M., Ashraf, F.: PBES: A policy based encryption system with application to date sharing in the power grid. In: Proc. ACM Sympoisum of Information, Computer and Communications Security, ASIACCS 2009, pp. 262–275 (2009)Google Scholar
17. Bobba, R., Rogers, K.M., Wang, Q., Khurana, H., Nahrstedt, K., Overbye, T.J.: Detecting false data injection attacks on DC state estimation. In: Proc. First Workshop on Secure Control Systems, Stockholm, Sweden (2010)Google Scholar
18. Byres, E., Chauvin, B., Hoffman, J., Kube, N.: The special needs of SCADA/PCN firewalls: Architectures and test results. In: Proc. 10th IEEE Conference on Emerging Technologies and Factor Automation, vol. 2, pp. 877–884 (2005)Google Scholar
19. C1 Working Group Members of Power System Relaying Committee: Cyber security issues for protective relays. In: Proc. IEEE Power Engineering Society General Meeting, pp. 1–8 (2007)Google Scholar
20. Cárdenas, A.A., Amin, S., Sastry, S.: Research challenges for the security of control systems. In: Proc. 3rd USENIX Conference on Hot Topics in Security, p. Article 6 (2008)Google Scholar
21. Cárdenas, A.A., Amin, S., Sastry, S.: Secure control: Towards survivable cyber-physical systems. In: Proc. 28th International Conference on Distributed Computing Systems Workshops, pp. 495–500 (2008)Google Scholar
22. Cárdenas, A.A., Amin, S., Sastry, S.: Secure control: Towards survivable cyber-physical systems. In: Proc. First International Workshop on Cyber-Physical Systems (2008)Google Scholar
23. Cárdenas, A.A., Roosta, T., Taban, G., Sastry, S.: Cyber security basic defenses and attack trends. In: Franceschetti, G., Grossi, M. (eds.) Homeland Security Technology Challenges, ch. 4, pp. 73–101. Artech House (2008)Google Scholar

24. Cleveland, F.M.: Cyber security issues for advanced meter infrastructure (AMI). In: Proc. IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century, pp. 1–5 (2008)Google Scholar
25. Constable, G., Somerville, B.: A Century of Innovation: Twenty Engineering Achievements That Transformed Our Lives. Joseph Henry Press, Washington, DC (2003)Google Scholar
26. Conte de Leon, D., Alves-Foss, J., Krings, A., Oman, P.: Modeling complex control systems to identify remotely accessible devices vulnerable to cyber attack. In: Proc. First Workshop on Scientific Aspects of Cyber Terrorism, Washington, D.C. (2002)Google Scholar
27. Dán, G., Sandberg, H.: Stealth attacks and protection schemes for state estimators in power systems. In: Proc. First IEEE International Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, MD, pp. 214–219 (2010)Google Scholar
28. Dán, G., Sandberg, H., Ekstedt, M., Björkman, G.: Challenges in power system information security. IEEE Security & Privacy 10(4), 62–70 (2012)CrossRef Google Scholar
29. Darby, J., Phelan, J., Sholander, P., Smith, B., Walter, A., Wyss, G.: Evidence-based techniques for evaluating cyber protection systems for critical infrastructures. In: Proc. IEEE Military Communications Conference, pp. 1–10 (2006)Google Scholar
30. Davis, C.M., Tate, J.E., Okhravi, H., Grier, C., Overbye, T.J., Nicol, D.: SCADA cyber security testbed development. In: Proc. 38th North American Power Symposium, pp. 483–488 (2006)Google Scholar
31. Dawson, R., Boyd, C., Dawson, E., Manuel Gonzàlez Nieto, J.: SKMA – A key management architecture for SCADA systems. In: Proc. Fourth Australasian Workshops on Grid Computing and E-Research, vol. 54, pp. 183–192 (2006)Google Scholar
32. Depoy, J., Phelan, J., Sholander, P., Smith, B., Varnado, G.B., Wyss, G.: Risk assessment for physical and cyber attacks on critical infrastructures. In: Proc. IEEE Military Communications Conference, vol. 3, pp. 1961–1969 (2005)Google Scholar
33. Dondossola, G., Garrone, F., Szanto, J.: Supporting cyber risk assessment of power control systems with experimental data. In: Proc. IEEE Power Systems Conference and Exposition, pp. 1–3 (2009)Google Scholar
34. Dörfler, F., Bullo, F.: Synchronization and transient stability in power networks and non-uniform kuramoto oscillators. In: Proc. American Control Conference, pp. 930–937 (2010)Google Scholar
35. Draney, B., Cambell, S., Walter, H.: NERSC cyber security challenges that require doe development and support. Technical Report LBNL–62284, Ernest Orlando Lawrence Berkeley National Laboratory, Berkeley, California (2007)Google Scholar
36. Dudenhoeffer, D.D., Permann, M.R., Woolsey, S., Timpany, R., Miller, C., McDermott, A., Manic, M.: Interdependency modeling and emergency response. In: Proc. 2007 Summer Computer Simulation Conference, pp. 1230–1237 (2007)Google Scholar
37. Eberle, W., Holder, L.: Insider threat detection using graph-based approaches. In: Proc. Cybersecurity Applications and Technology Conference for Homeland Security, pp. 237–241 (2009)Google Scholar

38. Edwards, D., Srivastava, S.K., Cartes, D.A., Simmons, S., Wilde, N.: Implementation and validation of a mult-level security model architecture. In: Proc. International Conference on Intelligent Systems Applications to Power Systems, pp. 1–4 (2007)Google Scholar
39. Ekstedt, M., Sommestad, T.: Enterprise architecture models for cyber security analysis. In: Proc. IEEE Power Systems Conference and Exposition, pp. 1–6 (2009)Google Scholar
40. Falliere, N., Murchu, L., Chien, E.: W32.stuxnet dossier, version 1.3. Symantec (2010)Google Scholar
41. Farris, J.F., Nicol, D.M.: Evaulation of secure peer-to-peer overlay routing for survivable SCADA systems. In: Proc. 36th Conference on Winter Simulation, pp. 300–308 (2004)Google Scholar
42. Fernandez, E.B., Wu, J., Larrondo-Petrie, M.M., Shao, Y.: On building secure SCADA systems using security patterns. In: Proc. 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies (2009)Google Scholar
43. Fleury, T., Khurana, H., Welch, V.: Towards a taxonomy of attacks against energy control systems. In: Second Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection (2008)Google Scholar
44. Flick, T., Morehouse, J.: Securing the Smart Grid: Next Generation Power Grid Security. Syngress (2011)Google Scholar
45. Gellings, C.: The Smart Grid: Enabling Energy Efficiency and Demand Response. Fairmont Press (2009)Google Scholar
46. Giani, A., Karsai, G., Roosta, T., Shah, A., Sinopoli, B., Wiley, J.: A testbed for secure and robust SCADA systems. SIGBED Review 5(2), Article No. 4 (2008)Google Scholar
47. Gilchrist, G.: Secure authentication for DNP3. In: Proc. IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century, pp. 1–3 (2008)Google Scholar
48. Gonen, T.: Electric Power Distribution System Engineering. Mcgraw-Hill College (1985)Google Scholar
49. Grid, N.: Operating the electricity transmission networks in 2020 (2011)Google Scholar
50. GridWise Alliance: GridWise(TM) accelerates efforts to develop a smart grid in the U.S. In: GridWeek, Washington DC, MD (2007)Google Scholar
51. Grochocki, D., Huh, J., Berthier, R., Bobba, R., Sanders, W., Cardenas, A., Jetcheva, J.: AMI threats, intrusion detection requirements and deployment recommendations. In: Proc. Third IEEE International Conference on Smart Grid Communications (SmartGridComm), Tainan, pp. 395–400 (2012)Google Scholar
52. The Cyber Security Coordination Task Group: Smart Grid Cyber Security Strategy and Requirements. National Institute of Standards and Technology Google Scholar

53. Hadeli, H., Schierholz, R., Braendle, M., Tuduce, C.: Generating configuration for missing traffic detector and security measures in industrial control systems based on

the system description files. In: Proc. IEEE Conference on Technologies for Homeland Security, pp. 503–510 (2009)Google Scholar
54. HadjSaid, N., Tranchita, C., Rozel, B., Viziteu, M., Caire, R.: Modeling cyber and physical interdependencies – application in ICT and power grids. In: Proc. IEEE Power Systems Conference and Exposition, pp. 1–6 (2009)Google Scholar
55. Hasan, R., Bobba, R., Khurana, H.: Analyzing NASPInet data flows. In: Proc. IEEE Power Systems Conference and Exposition, pp. 1–6 (2009)Google Scholar
56. Holcomb, J.: Auditing cyber security configuration for control system applications. In: Proc. IEEE Conference on Technologies for Homeland Security, pp. 7–13 (2009)Google Scholar
57. Holstein, D.K., Diaz, J.: Cyber security management for utility operations. In: Proc. 39th Annual Hawaii International Conference on Systems Sciences, vol. 10, p. 241c (2006)Google Scholar
58. Hughes, T.: Networks of Power: Electrification in Western Society, 1880-1930. JHU Press (1993)Google Scholar
59. Hull, J., Khurana, H., Markham, T., Staggs, K.: Staying in control: Cyber security and the modern electric grid. IEEE Power & Energy Magazine 10(1), 41–48 (2012)CrossRef Google Scholar
60. Jones, P.: The role of new technologies: A power engineering equipment supply base perspective. In: Grid Policy Workshop, Paris, France (2010)Google Scholar
61. Kang, D.J., Kim, H.M.: A method for determination of key period using QoS function. In: Proc. Future Generation Communication and Networking, vol. 2, pp. 532–535 (2007)Google Scholar
62. Kang, D.J., Kim, H.M.: A proposal for key policy of symmetric encryption application to cyber security of KEPCO SCADA network. In: Proc. Future Generation Communication and Networking, vol. 2, pp. 609–613 (2007)Google Scholar
63. Khaitan, S., McCalley, S.: Cyber physical system approach for design of power grids: A survey. In: Proc. IEEE Power & Energy Society General Meeting, Vancouver, BC, pp. 1–5 (2013)Google Scholar
64. Khaitan, S., McCalley, S.: Design techniques and applications of cyber physical systems: A survey. IEEE Systems Journal (2014)Google Scholar
65. Khalil, H.: Nonlinear Systems. Prentice-Hall (2002)Google Scholar
66. Khurana, H., Hadley, M., Lu, N., Frincke, D.: Smart-grid security issues. IEEE Security Privacy 8(1), 81–85 (2009)CrossRefGoogle Scholar
67. Khurana, H., Khan, M.M.H., Welch, V.: Leveraging computational grid technologies for building a secure and manageable power grid. In: Proc. Hawaii International Conference on System Sciences, pp. 115–124 (2007)Google Scholar
68. Khurana, H., Koleva, R., Basney, J.: Performance of cryptographic protocols for high-performance high-bandwidth and high-latency grid systems. In: Proc. Third IEEE International Conference on e-Science and Grid Computing, pp. 431–439 (2007)Google Scholar
69. Kim, H.M., Kang, D.J., Kim, T.H.: Flexible key distribution for SCADA network using multi-agent system. In: Proc. ECSIS Syposium on Bio-inspired, Learning, and Intelligent Systems for Security, pp. 29–34 (2007)Google Scholar

70. Klein, S.A.: An open source IEC-61850 toolkit for utility automation and wind power applications. In: Proc. IEEE/PES Transmission and Distribution Conference and Exposition, pp. 1–4 (2008)Google Scholar
71. Klein, S.A.: A secure IEC-61850 toolkit for utility automation. In: Proc. Cybersecurity Applications and Technology Conference for Homeland Security, pp. 245–250 (2009)Google Scholar
72. Kosut, O., Jia, L., Thomas, R.J., Tong, L.: Limiting false data attacks on power system state estimation. In: Proc. 44th Annual Conference on Information Sciences and Systems (CISS), Princeton, NJ, pp. 1–6 (2010)Google Scholar
73. Kosut, O., Jia, L., Thomas, R.J., Tong, L.: Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures. In: Proc. First IEEE International Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, MD, pp. 220–225 (2010)Google Scholar
74. Kundur, D.: Cyber-physical security of the smart grid. Lecture conducted from University of Toronto, Toronto, Canada (2013)Google Scholar
75. Kundur, D., Feng, X., Liu, S., Zourntos, T., Butler-Purry, K.: Towards a framework for cyber attack impact analysis of the electric smart grid. In: Proc. IEEE International Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, Maryland, pp. 244–249 (2010)Google Scholar
76. Kundur, D., Feng, X., Mashayekh, S., Liu, S., Zourntos, T., Butler-Purry, K.: Towards modeling the impact of cyber attacks on a smart grid. International Journal of Security and Networks 6(1), 2–13 (2011)CrossRef Google Scholar
77. Kundur, P.: Power System Stability and Control. McGraw-Hill Professional (1994)Google Scholar
78. Kundur, P.: Power System Stability and Control. McGraw-Hill (1994)Google Scholar
79. Kundur, P., Paserba, J., Ajjarapu, V., Andersson, G., Bose, A., Canizares, C., Hatziargyriou, N., Hill, D., Stankovic, A., Taylor, C., Cutsem, T., Vittal, V.: Definition and classification of power system stability: Ieee/cigre joint task force on stability terms and definitions. IEEE Transactions on Power Systems 19, 1387–1401 (2004)CrossRef Google Scholar
80. Lin, H., Sambamoorthy, S., Shukla, S., Thorp, J., Mili, L.: Power system and communicaiton network co-simulation for smart grid applications. In: Proc. IEEE PES Conference on Innovative Smart Grid Technologies (ISGT), Anaheim, California, pp. 1–6 (2011)Google Scholar
81. Liu, C.C., Ten, C.W., Govindarasu, M.: Cybersecurity of SCADA systems: Vulnerability assessment and mitigation. In: Proc. IEEE Power Systems Conference and Exposition, pp. 1–3 (2009)Google Scholar
82. Liu, S., Liu, X., El-Saddik, A.: Denial-of-service (DoS) attacks on load frequency control in smart grids. In: Proc. IEEE PES Innovative Smart Grid Technologies (ISGT), Washington DC, MD, pp. 1–6 (2013)Google Scholar
83. Liu, Y., Ning, P., Reiter, M.: Generalized false data injection attacks against state estimation in electric power grids. ACM Transactions on Information and System Security (TISSEC) 14(1) (2011)Google Scholar
84. Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. In: Proc. 16th ACM Conference on Computer and Communications Security, Chicago, IL, pp. 21–32 (2009)Google Scholar

85. Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. ACM Transactions on Information and System Security (2011) (to appear)Google Scholar
86. Mander, T., Nabhani, F., Wang, L., Cheung, R.: Integrated network security protocol layer for open-access power distribution systems. In: Proc. IEEE Power Engineering Society General Meeting, pp. 1–8 (2007)Google Scholar
87. McDaniel, P., McLaughlin, S.: Security and privacy challenges in the smart grid. IEEE Security Privacy 7(3), 75–77 (2009)CrossRef Google Scholar
88. McMillin, B.: Complexities of information security in cyber-physical power systems. In: Proc. IEEE Power Systems Conference and Exposition, pp. 1–2 (2009)Google Scholar
89. McMillin, B., Gill, C., Crow, M.L., Liu, F., Niehaus, D., Potthast, A., Tauritz, D.: Cyber-physical systems distributed control: The advanced electric power grid. In: Proc. National Workshop on Beyond SCADA: Networked Embedded Control for Critical Physical Systems, HCSS:NEC4CPS (2006)Google Scholar
90. McQueen, M.A., Boyer, W.F.: Deception used for cyber defense of control systems. In: Proc. 2nd Conference on Human System Interactions, pp. 624–631 (2009)Google Scholar
91. McQueen, M.A., Boyer, W.F., Flynn, M.A., Beitel, G.A.: Quantitative cyber risk reduction estimation methodology for small SCADA control system. In: Proc. 39th Annual Hawaii International Conference on Systems Sciences, vol. 9, pp. 226–236 (2006)Google Scholar
92. Meyer, C.D.: Matrix Analysis and Applied Linear Algebra. SIAM (2001)Google Scholar
93. Mohsenian-Rad, A., Leon-Garcia, A.: Distributed internet-based load altering attacks against smart power grids. IEEE Transactions on Smart Grid 2(4), 667–674 (2011)CrossRef Google Scholar
94. Moslehi, K., Kumar, R.: A reliability perspective of the smart grid. IEEE Transactions on Smart Grid 1(1), 57–64 (2010)CrossRefGoogle Scholar
95. Olfati-Saber, R.: Flocking for multi-agent dynamic systems: Algorithms and theory. IEEE Transactions on Automatic Control 51(3), 401–420 (2006)CrossRef MathSciNet Google Scholar
96. Olfati-Saber, R., Fax, J., Murray, R.: Consensus and cooperation in networked multi-agent systems. Proceedings of the IEEE 95(1), 215–233 (2007)CrossRef Google Scholar
97. Patel, S.C., Bhatt, G.D., Graham, J.H.: Improving the cyber security of SCADA communication networks. Communications of the ACM 52(7), 139–142 (2009)CrossRef Google Scholar
98. Piètre-Cambacédès, L., Sitbon, P.: Cryptographic key management for SCADA systems – issues and perspectives. In: Proc. International Conference on Information Security and Assurance, pp. 156–161 (2008)Google Scholar
99. Reynolds, C.: Flocks, herds, and schools: a distributed behavioral model. Computer Graphics 21(4), 25–34 (1987)CrossRef Google Scholar
100. Risley, A., Carson, K.: Low- or no-cost cybersecurity solutions for defending the electric power system against electronic intrusions. Schweitzer Engineering Laboratories, Inc. (2006)Google Scholar

101. Rozel, B., Viziteu, M., Caire, R., Hadjsaid, N., Rognon, J.P.: Towards a common model for studying critical infrastructure interdependencies. In: Proc. IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, Pennsylvania, pp. 1–6 (2008)Google Scholar
102. Sauer, P., Pai, M.: Power System Dynamics and Stability. Prentice Hall (1997)Google Scholar
103. Sioshansi, F.: Smart Grid: Integrating Renewable, Distributed & Efficient Energy. Academic Press (2011)Google Scholar
104. Sologar, A., Moll, J.: Developing a comprehensive substation cyber security and data management solution. In: Proc. IEEE/PES Transmission and Distribution Conference and Exposition, pp. 1–7 (2008)Google Scholar
105. Sou, K., Sandberg, H.: Detection and identification of data attacks in power system. In: American Control Conference (ACC), Montreal, QC, pp. 3651–3656 (2012)Google Scholar
106. Stamp, J., McIntyre, A., Ricardson, B.: Reliability impacts from cyber attack on electric power systems. In: Proc. IEEE Power Systems Conference and Exposition, pp. 1–8 (2009)Google Scholar
107. Takano, M.: Sustainable cyber security for utility facilities control system based on defense-in-depth concept. In: Proc. SICE Annual Conference, pp. 2910–2913 (2007)Google Scholar
108. Tan, H.: Security analysis of a cyber-physical system. Master's thesis, University of Missouri-Rolla (2007)Google Scholar
109. Tang, H., McMillin, B.: Security property violation in CPS through timing. In: Proc. 28th International Conference on Distributed Computing Systems Workshops, pp. 519–524 (2008)Google Scholar
110. Ten, C.W., Liu, C.C., Govindarasu, M.: Vulnerability assessment of cybersecurity for SCADA systems using attack trees. In: Proc. IEEE Power Engineering Society General Meeting, pp. 1–8 (2007)Google Scholar
111. Ton, D.: DOE's perspectives on smart grid technology, challenges, & research opportunities. In: UCLA Engineering SmartGrid Seminar, Los Angeles, CA (2009)Google Scholar
112. Tuzzo, S.: A PlugN'Play platform independent solution that eliminates unauthorized access without the use of passwords or encryption keys. In: Proc. IEEE Conference on Technologies for Homeland Security, pp. 79–85 (2008)Google Scholar
113. Vijayan, J.: Stuxnet renews power grid security concerns. Computerworld (2010)Google Scholar
114. Wang, Y., Chu, B.T.: sSCADA: Securing SCADA infrastructure communications (2004), http://eprint.iacr.org/2004/265.pdf
115. Wei, J., Kundur, D.: A multi-flock approach to rapid dynamic generator coherency identification. In: Proc. IEEE Power & Energy Society General Meeting, Vancouver, Canada, pp. 1–5 (2013)Google Scholar
116. Wei, J., Kundur, D., Zourntos, T.: On the use of cyber-physical hierarchy for smart grid security and efficient control. In: Proc. IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Montreal, Canada (2012)Google Scholar

117. Wei, J., Kundur, D., Zourntos, T., Butler-Purry, K.: A flocking-based dynamical systems paradigm for smart power system analysis. In: Proc. IEEE Power & Energy Society General Meeting, San Diego, California (2012)Google Scholar
118. West, A.: Securing DNP3 and Modbus with AGA12-2J. In: Proc. IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century, pp. 1–4 (2008)Google Scholar
119. Xiangjun, Z.: Context information-based cyber security defense of protection system. IEEE Transactions on Power Delivery 22(3), 1477–1481 (2007)CrossRef Google Scholar
120. Xiao, K., Chen, N., Ren, S., Shen, L., Sun, X., Kwiat, K., Macalik, M.: A workflow-based non-intrusive approach for enhancing the survivability of critical infrastructures in cyber environment. In: Proc. Third International Workshop on Software Engineering for Secure Systems (2007)Google Scholar
121. Xie, L., Mo, Y., Sinopoli, B.: False data injection attacks in electricity markets. In: Proc. IEEE International Conference on Smart Grid Communications, Tainan, Taiwan, pp. 226–231 (2010)Google Scholar
122. Yamada, T., Maruyama, T.: Study on a security framework for a plant level network. In: Proc. 2006 SICE-ICASE International Joint Conference, Bexco, Busan Korea, pp. 1063–1066 (2006)Google Scholar