systems: a network based approach." Ph.D. dissertation, Centre Telematics Inf. Technol., Univ. Twente, Enschede, The Netherlands, 2014.

[2] Langner, Ralph. "Stuxnet: Dissecting a cyberwarfare weapon." IEEE Security and Privacy 9, no. 3 (2011): 49-51.

[3] Cheung, Steven, Bruno Dutertre, Martin Fong, Ulf Lindqvist, Keith Skinner, and Alfonso Valdes. "Using model-based intrusion detection for SCADA networks." In Proceedings of the SCADA security scientific symposium, vol. 46, pp. 1-12. 2007.

[4] Valdes, Alfonso, and Steven Cheung. "Communication pattern anomaly detection in process control systems." In Technologies for Homeland Security, 2009. HST'09. IEEE Conference on, pp. 22-29. IEEE, 2009.

[5] Rrushi, Julian, and Kyoung-Don Kang. "Detecting anomalies in process control networks." In International Conference on Critical Infrastructure Protection, pp. 151-165. Springer, Berlin, Heidelberg, 2009.

[6] Ten, Chee-Wooi, Govindarasu Manimaran, and Chen-Ching Liu. "Cybersecurity for critical infrastructures: Attack and defense modeling." IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans 40, no. 4 (2010): 853-865.

[7] Morris, Thomas, and Wei Gao. "Industrial control system traffic data sets for intrusion detection research." In International Conference on Critical Infrastructure Protection, pp. 65-78. Springer, Berlin, Heidelberg, 2014.

[8] Bailey, David, and Edwin Wright. Practical SCADA for industry. Elsevier, 2003.

[9] Foundations, Critical. "Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection." Washington, D.C., (1997).

[10] Krutz, Ronald L. Securing SCADA systems. John Wiley and Sons, 2005.

[11] Slay, Jill, and Michael Miller. "Lessons learned from the maroochy water breach." In International Conference on Critical Infrastructure Protection, pp. 73-82. Springer, Boston, MA, 2007.

[12] USNR Commission. "Potential Vulnerability of Plant Computer Network to Worm Infection." NRC Information Notice 14 (2003): 2003.

[13] Falliere, Nicolas, Liam O. Murchu, and Eric Chien. "W32. stuxnet dossier." White paper, Symantec Corp., Security Response 5, no. 6 (2011): 29.

[14] Koehrsen, Will. Feature Selector, (2018), https://github.com/WillKoehrsen/feature-selector. (Access date: 5 May, 2019)

[15] Baker, Stewart Abercrombie, Natalia Filipiak, and Katrina Timlin. In the dark: crucial industries confront cyber attacks. McAfee, Incorporated, 2011.

[16] ICS CERT. Monthly Monitor October December, 2012.

[17] Yang, Dayu, Alexander Usynin, and J. Wesley Hines. "Anomaly-based intrusion detection for SCADA systems." In 5th intl. topical meeting on nuclear plant instrumentation, control and human machine interface technologies (npic&hmit 05), pp. 12-16. 2006.

[18] Majdalawieh, Munir, Francesco Parisi-Presicce, and Duminda Wijesekera. "DNPSec: Distributed network protocol version 3 (DNP3) security framework." In Advances in Computer, Information, and Systems Sciences, and Engineering, pp. 227-234. Springer, Dordrecht, 2007.

[19] East, Samuel, Jonathan Butts, Mauricio Papa, and Sujeet Shenoi. "A Taxonomy of Attacks on the DNP3 Protocol." In International Conference on Critical Infrastructure Protection, pp. 67-81. Springer, Berlin, Heidelberg, 2009.

[20] Drury, Bill. Control techniques drives and controls handbook. No. 35. IET, 2001.

[21] Smith, Rebecca. "Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say." The Wall Street Journal, https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110 (Access date: 1 May, 2019)

[22] Mohurle, Savita, and Manisha Patil. "A brief study of Wannacry Threat: Ransomware Attack 2017" International Journal of Advanced Research in Computer Science 8, no. 5 (2017).

[23] Djidjev, Hristo, Gary Sandine, Curtis Storlie, and Scott Vander Wiel. "Graph based statistical analysis of network traffic." In Proceedings of the Ninth Workshop on Mining and Learning with Graphs. 2011.

[24] Collins, M. Patrick, and Michael K. Reiter. "Hit-list worm detection and bot identification in large networks using protocol graphs." In International Workshop on Recent Advances in Intrusion Detection, pp. 276-295. Springer, Berlin, Heidelberg, 2007.

[25] Iliofotou, Marios, Michalis Faloutsos, and Michael Mitzenmacher. "Exploiting dynamicity in graph-based traffic analysis: techniques and applications." In Proceedings of the 5th international conference on Emerging networking experiments and technologies, pp. 241-252. ACM, 2009.

[26] Iliofotou, Marios, Prashanth Pappu, Michalis Faloutsos, Michael Mitzenmacher, Sumeet Singh, and George Varghese. "Network traffic analysis using traffic dispersion graphs (TDGs): techniques and hardware implementation." (2007).

[27] "Graph-based anomaly detection." In Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining, pp. 631-636. ACM, 2003.

 