Table 6. Exponential Cost Resource Allocation ($\lambda = 0.53$)

Nodes	C	$maxA$	$\frac{C}{maxA}$	A	$V(\%)$	R
WS	3.25	4.64	0.70	0.561	63.8	2.074
WebS	6.84	4.64	1.474	2.060	9.24	0.632
SCADA1	12.52	4.64	2.70	3.278	5.68	0.711
SCADA2	11.06	4.64	2.38	3.029	6.0	0.663
RTU1	11.18	4.64	2.41	3.051	5.97	0.667
RTU2	11.01	4.64	2.37	3.020	6.01	0.662

[4] S. Ullah, S. Shetty, and A. Hassanzadeh, "Towards modeling attacker's opportunity for improving cyber resilience in energy delivery systems," in *2018 Resilience Week (RWS)*. IEEE, 2018, pp. 100–107.

[5] M. Rezvani, V. Sekulic, A. Ignjatovic, E. Bertino, and S. Jha, "Interdependent security risk analysis of hosts and flows," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 11, pp. 2325–2339, 2015.

[6] Y. Zhang, L. Gu, X. Liao, H. Jin, D. Zeng, and B. B. Zhou, "Frank: A fast node ranking approach in large-scale networks," *IEEE Network*, vol. 31, no. 1, pp. 36–43, 2017.

[7] X. Ou and A. Singhal, *Quantitative security risk assessment of enterprise networks*. Springer, 2011.

[8] M. Alhomidi and M. Reed, "Attack graph-based risk assessment and optimisation approach," *International Journal of Network Security & Its Applications*, vol. 6, no. 3, p. 31, 2014.

[9] C. Suh-Lee and J. Jo, "Quantifying security risk by measuring network risk conditions," in *Computer and Information Science (ICIS), 2015 IEEE/ACIS 14th International Conference on*. IEEE, 2015, pp. 9–14.

[10] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Inclusion of scada cyber vulnerability in power system reliability assessment considering optimal resources allocation," *IEEE Transactions on Power Systems*, vol. 31, no. 6, pp. 4379–4394, 2016.

[11] K. Hasan, S. Shetty, A. Hassanzadeh, M. B. Salem, and J. Chen, "Modeling cost of countermeasures in software defined networking-enabled energy delivery systems," in *2018 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2018, pp. 1–9.

[12] K. Hasan, S. Shetty, A. Hassanzadeh, M. B. Salem *et al.*, "Self-healing cyber resilient framework for software defined networking-enabled energy delivery system," in *2018 IEEE Conference on Control Technology and Applications (CCTA)*. IEEE, 2018, pp. 1692–1697.

[13] X. Ou, S. Govindavajhala, and A. W. Appel, "Mulval: A logic-based network security analyzer." in *USENIX Security Symposium*, vol. 8. Baltimore, MD, 2005.

[14] M. Frigault, L. Wang, S. Jajodia, and A. Singhal, "Measuring the overall network security by combining cvss scores based on attack graphs and bayesian networks," in *Network Security Metrics*. Springer, 2017, pp. 1–23.

[15] P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," *IEEE Security & Privacy*, vol. 4, no. 6, 2006.

[16] K. Hasan, S. Shetty, S. Ullah, A. Hassanzadeh, and E. Hadar, "Towards optimal cyber defense remediation in energy delivery systems," in *2019 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2019, pp. 1–7.

[17] K. Hasan, S. Shetty, A. Hassanzadeh, and S. Ullah, "Towards optimal cyber defense remediation in cyber physical systems by balancing operational resilience and strategic risk," in *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)*. IEEE, 2019, pp. 1–8.

[18] A. Hassanzadeh and R. Burkett, "Samiit: Spiral attack model in iiot mapping security alerts to attack life cycle phases," in *ICS & SCADA Cyber Security Research,2018 5th International Symposium for*. BCS, 2018, pp. 11–20.

[19] T. G. Lewis, *Network science: Theory and applications*. John Wiley & Sons, 2011.

[20] M. Touhiduzzaman, A. Hahn, and A. Srivastava, "Arcades: Analysis of risk from cyber attack against defensive strategies for power grid," *IET Cyber-Physical Systems: Theory & Applications*, 2018.

[21] S. Wang, "Optimal level and allocation of cybersecurity spending: Model and formula," 2017.