systems. We considered that a set of sub-systems are vulnerable in the sense that their controllers may incur random failures or malicious attacks. For the vulnerable subsystems we introduced resilient-safety indices (RSIs) bounding the worst-case impacts of vulnerable systems towards the specified safety constraints. The sign of RSI indicates the contribution of vulnerable sub-system in either satisfying or violating the corresponding safety constraint whereas the magnitude quantifies such contribution. We provided a sufficient condition for the control policies in the non-vulnerable sub-systems so that the safety constraints are satisfied in the presence of failure or attack in the vulnerable sub-systems. We formulated sum-of-squares optimization programs to compute the RSIs and safety-ensuring control policies. Control policy in each sub-system can be computed independently using our proposed algorithm. We presented two special cases for which the RSIs can be found more efficiently. We demonstrated the usefulness of our proposed approach using an example on temperature regulation of interconnected rooms.

REFERENCES

[1] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs for safety critical systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 8, pp. 3861–3876, 2016.

[2] M. H. Cohen and C. Belta, "Approximate optimal control for safety-critical systems with control barrier functions," in *59th IEEE Conference on Decision and Control (CDC)*. IEEE, 2020, pp. 2062–2067.

[3] C. Fan, K. Miller, and S. Mitra, "Fast and guaranteed safe controller synthesis for nonlinear vehicle models," in *International Conference on Computer Aided Verification*. Springer, 2020, pp. 629–652.

[4] 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.

[5] A. Greenberg, "Hackers remotely kill a Jeep on the highway–with me in it," 2015. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[6] X. Xu, "Constrained control of input–output linearizable systems using control sharing barrier functions," *Automatica*, vol. 87, pp. 195–201, 2018.

[7] S. Prajna, A. Jadbabaie, and G. J. Pappas, "A framework for worst-case and stochastic safety verification using barrier certificates," *IEEE Transactions on Automatic Control*, vol. 52, no. 8, pp. 1415–1428, 2007.

[8] F. Björck, M. Henkel, J. Stirna, and J. Zdravkovic, "Cyber resilience–fundamentals for a definition," in *New Contributions in Information Systems and Technologies*. Springer, 2015, pp. 311–316.

[9] Q. Zhu and T. Başar, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 46–65, 2015.

[10] R. Ivanov, M. Pajic, and I. Lee, "Attack-resilient sensor fusion for safety-critical cyber-physical systems," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 15, no. 1, pp. 1–24, 2016.

[11] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic control*, vol. 59, no. 6, pp. 1454–1467, 2014.

[12] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems Magazine*, vol. 21, no. 6, pp. 11–25, 2001.

[13] Y. Zhang and O. Yağan, "Robustness of interdependent cyber-physical systems against cascading failures," *IEEE Transactions on Automatic Control*, vol. 65, no. 2, pp. 711–726, 2019.

[14] C. E. R. Commision, "Report on the grid disturbances on 30th July and 31st July 2012," 2012. [Online]. Available: http://www.cercind.gov.in/2012/orders/Final_Report_Grid_Disturbance.pdf.

[15] A. Nejati, S. Soudjani, and M. Zamani, "Compositional construction of control barrier certificates for large-scale stochastic switched systems," *IEEE Control Systems Letters*, vol. 4, no. 4, pp. 845–850, 2020.

[16] C. Sloth, G. J. Pappas, and R. Wisniewski, "Compositional safety analysis using barrier certificates," in *Proceedings of the 15th ACM International Conference on Hybrid Systems: Computation and Control*, 2012, pp. 15–24.

[17] Z. Lyu, X. Xu, and Y. Hong, "Small-gain theorem for safety verification of interconnected systems," *Automatica*, vol. 139, p. 110178, 2022.

[18] S. Coogan and M. Arcak, "A dissipativity approach to safety verification for interconnected systems," *IEEE Transactions on Automatic Control*, vol. 60, no. 6, pp. 1722–1727, 2014.

[19] H. Yang, B. Jiang, M. Staroswiecki, and Y. Zhang, "Fault recoverability and fault tolerant control for a class of interconnected nonlinear systems," *Automatica*, vol. 54, pp. 49–55, 2015.

[20] H. Yang, C. Zhang, Z. An, and B. Jiang, "Exponential small-gain theorem and fault tolerant safe control of interconnected nonlinear systems," *Automatica*, vol. 115, p. 108866, 2020.

[21] H. Alemzadeh, D. Chen, X. Li, T. Kesavadas, Z. T. Kalbarczyk, and R. K. Iyer, "Targeted attacks on teleoperated surgical robots: Dynamic model-based detection and mitigation," in *46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. IEEE, 2016, pp. 395–406.

[22] K. Koscher, S. Savage, F. Roesner, S. Patel, T. Kohno, A. Czeskis, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," in *IEEE Symposium on Security and Privacy*. IEEE, 2010, pp. 447–462.

[23] E. M. Clarke, "Model checking," in *International Conference on Foundations of Software Technology and Theoretical Computer Science*. Springer, 1997, pp. 54–56.

[24] Z. Manna and A. Pnueli, *Temporal Verification of Reactive Systems: Safety*. Springer Science & Business Media, 2012.

[25] I. M. Mitchell, A. M. Bayen, and C. J. Tomlin, "A time-dependent Hamilton-Jacobi formulation of reachable sets for continuous dynamic games," *IEEE Transactions on Automatic Control*, vol. 50, no. 7, pp. 947–957, 2005.

[26] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, and G. J. Pappas, "Robustness of attack-resilient state estimators," in *ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*. ACM/IEEE, 2014, pp. 163–174.

[27] A. A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems." in *Proceedings of the 3rd Conference on Hot Topics in Security*, vol. 5. USENIX Association, 2008, p. 15.

[28] M. Castro and B. Liskov, "Practical Byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems (TOCS)*, vol. 20, no. 4, pp. 398–461, 2002.

[29] P. E. Veríssimo, N. F. Neves, and M. P. Correia, "Intrusion-tolerant architectures: Concepts and design," in *Architecting Dependable Systems*. Springer, 2003, pp. 3–36.

[30] J. S. Mertoguno, R. M. Craven, M. S. Mickelson, and D. P. Koller, "A physics-based strategy for cyber resilience of CPS," in *Autonomous Systems: Sensors, Processing, and Security for Vehicles and Infrastructure 2019*, vol. 11009. International Society for Optics and Photonics, 2019, p. 110090E.

[31] F. Abdi, C.-Y. Chen, M. Hasan, S. Liu, S. Mohan, and M. Caccamo, "Guaranteed physical security with restart-based design for cyber-physical systems," in *2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS)*. ACM/IEEE, 2018, pp. 10–21.

[32] L. Niu, D. Sahabandu, A. Clark, and P. Radha, "Verifying safety for resilient cyber-physical systems via reactive software restart," in *(accepted) 2022 ACM/IEEE 13th International Conference on Cyber-Physical Systems (ICCPS)*. ACM/IEEE, 2022.

[33] A. J. Gallo, A. Barboni, and T. Parisini, "On detectability of cyber-attacks for large-scale interconnected systems," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 3521–3526, 2020.

[34] V. Powers, "Positive polynomials and sums of squares: Theory and practice," *Real Algebraic Geometry*, vol. 1, pp. 78–149, 2011.

[35] S. Coogan and M. Arcak, "Finite abstraction of mixed monotone systems with discrete and continuous inputs," *Nonlinear Analysis: Hybrid Systems*, vol. 23, pp. 254–271, 2017.

[36] P.-J. Meyer, A. Girard, and E. Witrant, "Compositional abstraction and safety synthesis using overlapping symbolic models," *IEEE Transactions on Automatic Control*, vol. 63, no. 6, pp. 1835–1841, 2017.