Jairo A. Giraldo, Ph.D.

CONTACT INFORMATION

50 S. Central Campus Drive., Room 2110
Department of Electrical and Computer Engineering,
University of Utah,
Salt Lake City, 84112

Voice: 301-820-1345
E-mail: jairo.giraldo@utah.edu

RESEARCH INTERESTS

My research interests are centered around control and cyber-security of critical infrastructures with emphasis in attack detection, identification, and mitigation to make systems more resilient and robust to cyber threats. I am interested in power and energy systems applications, particularly in power distribution systems and microgrids with high penetration of DERs. I am also interested on distributed control of multi-agent systems with applications in autonomous vehicles and the smart grid.

CURRENT POSITION

University of Utah Salt Lake City, USA

Research Assistant Professor July, 2020 -

- **Affiliation:** U-Smart: Utah Smart Energy Laboratory, Department of Electrical and Computer Engineering.
- **Research:** Cyber-physical systems control and security, Resilience analysis of the power grid using tools from control theory, optimization, and machine learning.

EDUCATION

University of the Andes Bogota, Colombia

Ph.D., Electrical Engineering *August 2015*

- Advisors: Nicanor Quijano, Alvaro Cárdenas

M.S., Electronic Engineering *March 2012*

National University of Colombia Manizales, Colombia

B.Sc. Major: Electronic Engineering *February 2010*

HONORS AND AWARDS

- Best presentation in session award, American Control Conference 2014
- Colciencias Scholarship for doctoral studies, 2013

RESEARCH EXPERIENCE

University of Utah Salt Lake City, USA

Postdoctoral Research Associate August, 2019 - June 2020

- **Affiliation:** U-Smart: Utah Smart Energy Laboratory, Department of Electrical and Computer Engineering.
- **Research:** Security and Resilience analysis of the power grid using tools from control theory, optimization, and machine learning.

University of Texas at Dallas Dallas, USA

Postdoctoral Research Associate December, 2015 - July 2019

- **Affiliation:** Cyber-Physical Systems Security and Privacy Lab (CyPhy-SP), Department of Computer Science in the Erik Jonsson School of Engineering.
- **Research:** Analysis of security and privacy in cyber-physical systems using different tools from optimization and control theory such as system modeling, estimation, detection, stochastic control, and hybrid systems, to make CPS more robust and resilient to cyber-attacks. Applications in smart grids, vehicular platooning, UAVs, and industrial control systems.

National Institute of Standards & Technology (NIST) Gaithersburg, USA

Research Visitor June, 2016 - August, 2016

- **Affiliation:** Networked Control Systems Group
- **Research:** Vulnerability analysis and developing of anomaly detection strategies for the Tennessee Eastman Testbed using nonlinear system modeling and estimation.

Singapore University of Technology and Design (SUTD) Singapore

Research Visitor September, 2015 - November, 2015

- **Affiliation:** iTrust: Center for Research in Cyber-Security
- **Research:** Development of novel attack detection strategies in the Secure Water Test-bed (SWaT) using system modeling, Kalman filters, and the correlation between different control loops.

Massachusetts Institute of Technology (MIT) Cambridge, USA

Visiting Scholar February, 2015 - June, 2015

- **Affiliation:** Resilient Infrastructure Network Lab, Department of Civil and Environmental Engineering.
- **Research:** Design of robust and distributed control strategies for the smart grid in the presence of attacks over networked systems.

University of Texas at Dallas Dallas, USA

Visiting Scholar January, 2014 - December, 2014

- **Affiliation:** Cyber Security Research and Education Institute, Department of Computer Science in the Erik Jonsson School of Engineering.
- **Research:** Analysis of security and privacy in the smart grid, with applications in anomaly detection and attack attenuation in real-time pricing. Design of anomaly detection strategies to limit the impact of stealthy attacks for industrial control systems.

University of the Andes Bogota, Colombia

Graduate Research Assistant *January, 2012 - August 2015*

- **Affiliation:** Research Group in Production Automation (GIAP), Department of Electrical and Electronic Engineering.
- **Research:** Development of new control strategies for the frequency synchronization of smart grids with distributed generation, taking into consideration communication constraints and cyber-security.

Research Assistant *January, 2010 - January 2012*

- **Research**: Design and implementation of mine detection devices for humanitarian demining, Dispatch of Distributed Generation, Networked control systems.

Invited Talks

- *Cyber-Physical Systems Security: Threats and Solutions*
  University of Utah, ECE Seminar
  January 30,2022.
- *Attack Detection and Mitigation in Industrial Control Systems*
  ABB US Corporate Research Center,
  August 5, 2016.

- *Attacks and Detection in Cyber-Physical Systems*
  The Advanced Digital Sciences Center (ADSC) in Singapore
  November 19, 2015.
- *Synchronization in the Smart Grid with Communication Constraints. Linear and Non-linear Approaches*
  Ohio State University. Department of Electrical and Computer Engineering.
  August 5, 2014.

Grants

- NSF I-CORPS, PI: Jairo Giraldo ($6,000).

Technical Services

- **Reviewer**: Automatica, Journal of Cyber-Physical Systems, IEEE Trans. Smart Grid, IEEE Design & Test, IEEE Trans. Automatic Control, IEEE Internet Computing, Journal of Mathematical Physics, American Control Conference, IEEE Conference on Decision and Control, European Control Conference, ICCPS, IEEE Colombian Conference on Automatic Control, GameSec, SciSec, AISec, International Journal of Cooperative Information Systems, International Journal of Electrical Power and Energy Systems, IEEE Multiconference Systems and Control, Congreso Latinoamericano de Control Automatico .
- **Invited Session Chair:** American Control Conference, Milwaukee, 2018.
- **Guest Editor:** MDPI Journal, *Information*. Special Issue: Cyber-Physical Systems Security and Resilience, 2021.
- **Program Committee:** ISGT NA 2022 (IEEE 13th Conference on Innovative Smart Grid Technologies, North America).
- **Program Committee:** AIoTS 2022 (4th International Workshop on Artificial Intelligence and Industrial Internet-of-Things Security)
- **Program Committee:** CIMSS 2022 (2nd International Workshop on Critical Infrastructure and Manufacturing System Security).
- **Program Committee:** CRITIS 2021 (The 16th International Conference on Critical Information Infrastructures Security)
- **Program Committee:** CIMSS 2021 (1st International Workshop on Critical Infrastructure and Manufacturing System Security).

Publications

Journal Papers

1. A. Palomino, J. Giraldo, M. Parvania, Graph-Based Interdependent Cyber-Physical Risk Analysis of Power Distribution Networks, "Submitted to IEEE Transactions on Power Deliver", 2022.
2. J. Giraldo, M. El Hariri, M. Parvania, Decentralized Moving Target Defense for Microgrid Protection Against False-Data Injection Attacks, "Submitted to IEEE Transactions on Smart Grids",2022.
3. J. Giraldo, A. Cardenas, R. Sanfelice, An Observer-based Moving Target Defense Against Sensor Attacks in Control Systems, "Submitted to Nonlinear Analysis: Hybrid Systems", 2022.
4. J. Giraldo, M. El Hariri, M. Parvania, "Moving Target Defense for Cyber-Physical Systems Using IoT-Enabled Data Replication", IEEE Transactions in Internet of Things, 2022.
5. M. Khan, J. Giraldo, M. Parvania, " Attack Detection in Power Distribution Systems Using a Cyber-Physical Real-Time Reference Model", IEEE Transactions on Smart Grid, 13(2), 2021.

6. G. Diaz-Garcia, G. Narvaez, LF. Giraldo, J. Giraldo, A. Cardenas, Resilient Structural Sparsity in the Design of Consensus Networks, "IEEE Transactions on Cybernetics", 2021.
7. M. Ganjkhani, M. Gilanifar, J. Giraldo, M. Parvania, "Integrated Cyber and Physical Anomaly Location and Classification in Power Distribution Systems", IEEE Transactions on Industrial Informatics,17(10), 7040-7049, 2021.
8. C. Oroza, J. Giraldo, M. Parvania, T. Watteyne, " Wireless-Sensor Network Topology Optimization in Complex Terrain: A Bayesian Approach", IEEE Internet of Things Journal, 8(24), pp, 17429-17435, 2021.
9. M. Khan, A. Palomino, J. Brugman, J. Giraldo, S. Kasera, M. Parvania, "The Cyberphysical Power System Resilience Testbed: Architecture and Applications", IEEE Computer, 53(5), 2020, pp. 44-54.
10. J. Giraldo, E. Mojica-Nava and N. Quijano, "Synchronization of Directed-Coupled Kuramoto Oscillators with Sampled Information and a Virtual Leader", International Journal of Control, 2019, 92(11), pp. 2591-2607.
11. J. Giraldo, D. Urbina, A. Cárdenas, J. Valente, Mustafa Faisal, N. Tippenhauer, J. Ruths, R. Candell, H. Sandberg, "A Survey of Process-Aware Attack Detection in Cyber-Physical Systems", ACM Computing Surveys, vol. 51(4), 2018.
12. AFM. Piedrahita, V. Gaur, J. Giraldo, A. Cardenas, SJ. Rueda, "Virtual Incident Response Functions in Control Systems", Computer Networks, 135(1), 2018, pp. 174-159
13. AFM. Piedrahita, V. Gaur, J. Giraldo, A. Cardenas, SJ. Rueda, "Leveraging Software-Defined Networking for Incident Response in Industrial Control Systems", IEEE Software, 35(1), 2018, pp. 44-50.
14. J. Giraldo, E. Sarkar, A. Cardenas, M. Maniatakos, M. Kantarcioglu, " Security and Privacy in Cyber-Physical Systems: A Survey of Surveys", IEEE Design & Test, 34(4), 2017, pp. 7-17.
15. J. Giraldo, A. Cárdenas and N. Quijano, "Integrity Attacks on Real-Time Pricing in Smart Grids: Impact and Countermeasures ", IEEE Transactions on Smart Grids, 8(5), 2017, pp. 2249 - 2257.
16. C. Barreto, J. Giraldo, A. Cárdenas, E. Mojica-Nava, and N. Quijano, "Control Systems for the Power Grid and their Resiliency to Attacks", IEEE Security and Privacy Magazine, 12(6), 2014, pp. 15-23.
17. J. Giraldo, E.Mojica-Nava, and N. Quijano. "Synchronization of isolated microgrids with a communication infrastructure using energy storage systems". International Journal of Electrical Power & Energy Systems, 63(0), 2014, pp. 71 - 82.

Book Chapter

1. J. Giraldo, A. Cardenas, "Moving Target Defense for Attack Mitigation in Multi-vehicle Systems", Proactive and Dynamic Network Defense, Springer International Publishing, 2019, pp. 163-190.
2. L. Combita, J. Giraldo, A. Cárdenas, N. Quijano, "DDDAS for Attack Detection and Isolation of Control Systems", Handbook of Dynamic Data Driven Applications Systems, pp. 407-422, Springer, 2018.
3. J. Giraldo, N. Quijano and K. Passino, "Honey Bee Social Foraging Algorithm for Resource Allocation", Springer Handbook of Computational Intelligence, Springer Berlin Heidelberg, 2015, pp. 1361-1376.

Conference Presentations and Miscellaneous

1. J. Giraldo, M. Parvania, "IoT-Enabled Decentralized Moving Target Defense for Enhancing Privacy in Microgrid Control", Accepted IEEE Innovative Smart Grid Technologies North America, 2022.
2. A. Zambrano, A. Palacio, L. Burbano, A. Nino, LF. Giraldo, M. Soto, J. Giraldo, A. Cardenas, "You Make Me Tremble: A First Look at Attacks Against Structural Control Systems", In Proceedings of the ACM Conference on Computer and Communications Security (CCS 2021), pp. 1320-1337, 2021.
3. J. Giraldo, D. Urbina, C.Y. Tang, A. Cardenas, "The More the Merrier: Adding Hidden Measurements to Secure Industrial Control Systems", in Proceedings of the 7th Symposium on Hot Topics in the Science of Security, 2020, pp 1-10.
4. J. Giraldo, S.H. Kafash, J. Ruths, A. Cardenas, ''DARIA: Designing Actuators to Resist Arbitrary Attacks Against Cyber-Physical Systems", in Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P), 2020, pp. 339-353.
5. R. Quinonez, J. Giraldo, L. Salazar, A. Cardenas, Z. Lin, "SAVIOR: Securing Autonomous Vehicles with Robust Physical Invariants", in Proceedings of the USENIX Security Conference, 2020.
6. R. Quinonez, L. Salazar, J. Giraldo, A. Cardenas, "Dynamic Sensor Processing for Securing Unmanned Vehicles", in Proceedings of the International Conference on Dynamic Data Driven Application Systems, 2020, pp 253-261.
7. J. Giraldo, A. Cárdenas, M. Kantarcioglu, Jonathan Katz, " Adversarial Classification Under Differential Privacy", To appear on the Network and Distributed System Security Symposium (NDSS), 2020.
8. J. Giraldo, A. Cardenas, R. Sanfelice, "A Moving Target Defense to Reveal Cyber-Attacks in CPS And Minimize Their Impact " In Proceedings of the American Control Conference (ACC), 2019, pp. 391-396.
9. J. Giraldo, D. Urbina, A. Cárdenas, N. Tippenhauer, " Hide and Seek: An Architecture for Improving Attack-Visibility in Industrial Control Systems", in Proceedings of the Applied Cryptography and Network Security Conference, pp. 175-195, 2019.
10. SH Kafash, J. Giraldo, C Murguia, A. Cardenas. J. Ruths, "Constraining Attacker Capabilities Through Actuator Saturation", 2018 American Control Conference, 2018, pp. 986-991.
11. J. Giraldo, A. Cárdenas, M. Kantarcioglu, "Security and privacy trade-offs in CPS by leveraging inherent differential privacy", in Proceedings of the Conference on Control Technologies and Applications (CCTA 2017), pp 1313-1318, 2017.
12. J. Giraldo, A. Cárdenas, M. Kantarcioglu, "Leveraging Unique CPS Properties to Design Better Privacy-Enhancing Algorithms", in Proceedings of the Hot Topics in Science of Security: Symposium and Bootcamp, pp 1-12, 2017.
13. J. Giraldo, A. Cárdenas, M. Kantarcioglu, "Security vs. Privacy: How Integrity Attacks can be Masked by the Noise of Differential Privacy", in Proceedings of the American Control Conference (ACC 2017), 2017.
14. D. Urbina, J. Giraldo, A. Cárdenas, J. Valente, Mustafa Faisal, N. Tippenhauer, J. Ruths, Richard Candell, Henrik Sandberg, "Survey and New Directions for Physics-Based Attack Deteciton in Control Systems", Technical NIST Report, NIST GCR 16-010, 2016
15. D. Urbina, J. Giraldo, A. Cárdenas, N. Tippenhauer, J. Ruths, J. Valente, Mustafa Faisal, Richard Candell, Henrik Sandberg, " Limiting the Impact of Stealthy Attacks on Industrial Control Systems", in the Proceedings of the ACM Conference on Computer and Communications Security, 2016, pp. 1092-1105.

16. D. Urbina, J. Giraldo, N. Tippenhauer, A. Cárdenas, "Attacking Fieldbus Communications in ICS: Applications to the SWaT Test-bed", in Proceedings of the Singapore Cyber-security Conference, 2016, pp. 75-89.
17. F. Combita, J. Giraldo, A. Cárdenas, N. Quijano, "Response and Reconfiguration in Cyber-physical Control Systems: A survey", in Proceedings of the 2nd Colombian Conference on Automatic Control, 2015, pp. 1-6.
18. D. Shelar, J. Giraldo, S. Amin, "A Decentralized Strategy for Electricity Distribution Network Control in the face of DER Disruptions", In proceedings of the 54th Conference on Decision and Control (CDC 2015), Osaka, Japan 2015, pp. 6934-6939.
19. J. Giraldo, A. Cárdenas, N. Quijano, "Attenuating the Impact of Integrity Attacks on Real-Time Pricing in Smart Grids", arXiv preprint, arXiv:1410.5111,2014.
20. J. Giraldo, A. Cárdenas, E. Mojica-Nava, N. Quijano, R. Dong, "Delay and Sampling Independence of a Consensus Algorithm and its Application to Smart Grid Privacy", in Proceedings of the 53rd Conference on Decision and Control (CDC 2014), Los Angeles, CA, 2014, pp. 1389-1394.
21. J. Giraldo, E. Mojica-Nava and N. Quijano, "Tracking of Kuramoto Oscillators with Input Saturation and Applications in Smart Grids", in Proceedings of the 2014 American Control Conference, Portland, OR, 2014, pp. 2656-2661.
22. J. Giraldo, E. Mojica-Nava and N. Quijano, "Synchronization of Dynamical Networks with a Communication Infrastructure: A Smart Grid Application", in Proceedings of the 52nd Conference on Decision and Control (CDC 2013), Florence, Italy, 2013, pp. 4638-4643.
23. J. Giraldo, E. Mojica-Nava and N. Quijano, "Synchronization of Dynamical Networks Under Sampling", in Proceedings of the European Control Conference, Switzerland, 2013, pp. 3839-3844.
24. J. Giraldo and N. Quijano, "Delay Independent Evolutionary Dynamics for Resource Allocation with Asynchronous Distributed Sensors", in Proceedings of the 3rd IFAC Workshop on Distributed Estimation and Control in Networked Systems, 2012, pp. 121-126.
25. J. Giraldo and N. Quijano, "Current Results and Research Trend in Networked Control Systems", IEEE Colombian Conference on Automatic Control, 2011, pp. 1-6.