Dr Miroslav Pajić

Personal data

Address:
Duke University
Department of Electrical and Computer Engineering
415 Wilkinson Building, 534 Research Dr
Durham, NC 27710, USA

E-mail:
miroslav.pajic@duke.edu

Research or academic title

Associate Professor

Research field/area

High-assurance Cyber-Physical Systems (CPS) with varying levels of autonomy and human interaction, in a range of application domains (e.g., robotics, autonomous vehicles, medical devices and systems); Secure and robust edge-based autonomy; Data- and model-based system design; AI, controls and embedded systems

Education

2012 **Ph.D. in Electrical Engineering**
University of Pennsylvania, Philadelphia, PA
Dissertation title: Closing the Loop: Architectures and Algorithms for Real-Time Control over Wireless Networks
Joseph and Rosaline Wolf Best Dissertation Award

2010 **M.S. in Electrical Engineering**
University of Pennsylvania, Philadelphia, PA

2007 **Magister Scientiae – MSc - El. Eng. (four semesters & thesis-research prerequisite to PhD)**
University of Belgrade - School of Electrical Engineering
Department of Electronics
Thesis title: Multirate digital signal processing for timing synchronization in digital modems design

2003 **Dipl.-Ing. – El. Eng. (ten semesters with diploma work)**
University of Belgrade - School of Electrical Engineering
Department of Electronics
Thesis title: Receiver with coherent detection of PSK signal in power grid
Best Student Award

Employment

July 2020-Present **Dickinson Family Associate Professor**
Duke University, Durham, NC
Department of Electrical and Computer Engineering
Department of Computer Science
Department of Mechanical Engineering and Material Science

Jan. 2018 – June 2020 **Nortel Networks Assistant Professor**
Duke University, Durham, NC
Department of Electrical and Computer Engineering
Department of Computer Science

July 2015 – June 2020 **Assistant Professor**
Duke University, Durham, NC
Department of Electrical and Computer Engineering
Department of Computer Science

Aug. 2014 – June 2015 **Adjunct Assistant Professor**
Duke University, Durham, NC
Department of Electrical and Computer Engineering

Oct. 2012 – **Postdoctoral Researcher**
University of Pennsylvania, Philadelphia, PA

Languages

Serbian, English

Number of citations (excluded self-citations, source: Scopus)

2718

Hirsch index (excluded self-citations, source: Scopus)

27

Other information

2015- Head of Cyber-Physical Systems Laboratory at Duke University, Department of Electrical and Computer Engineering;

2022- Director of Master Studies at Duke University, Department of Electrical and Computer Engineering;

2019 General Chair, NSF CPS PI meeting, Washington DC, November

2014- NSF proposal panels: CPS 2014, 2016, 2018, 2020, CISE 2015, 2018, 2019, SaTC 2017

2015- Reviewer for Canadian funding agencies: NSERC (2019) and Mitacs Accelerate (2017-2018), Technology Foundation STW, Netherlands' research council for the engineering and applied sciences (2015), Research Grants Council (RGC) of Hong Kong (2019)

Journal Editor

- Associate Editor, *ACM Transactions on Cyber-Physical Systems*, 2022-present.
- Associate Editor, *ACM Transactions on Computing for Healthcare* (**ACM HEALTH**), 2018-present.

June 2015	Department of Electrical and Systems Engineering PRECISE (The Penn Research in Embedded Computing and Integrated System) Center
Sept. 2008 – Sept. 2012	**Research Assistant** University of Pennsylvania, Philadelphia, PA Department of Electrical and Systems Engineering
Feb. 2008 – Aug. 2008	**Research Scholar** University of Pennsylvania, Philadelphia, PA Department of Electrical and Systems Engineering
2003-2008	**Teching Assistant** University of Belgrade - School of Electrical Engineering Department of Electronics

Experience in competitive public calls in previous 5 years

Athena

Project name: *AI Institute for Edge Computing Leveraging Next Generation Networks (Athena)*, Award Number: 2112562 **Relevant Project for MCSecurity**

Funding source: National Science Foundation (NSF)

Implementation period: 2021-2026.

Awarded grant amount: 20,000,000.00 USD

Project PI: Yiran Chen

Role of Miroslav Pajic: Co-PI

KEY RESULTS OF Athena:

Conference papers:

1. Khazraei, A., Meng, H., **Pajic, M.**, **Stealthy Perception-based Attacks on Unmanned Aerial Vehicles**, In IEEE International Conference on Robotics and Automation (ICRA), pp. 3346-3352, June 2023, https://doi.org/10.1109/ICRA48891.2023.10160900
2. Naeem, M. A. **Pajic, M.**, **Concentration Phenomenon for Random Dynamical Systems: An Operator Theoretic Approach**, In Proceedings of The 5th Annual Learning for Dynamics and Control Conference (L4DC), PMLR 211:1-12, 2023.
3. Hallyburton, R. S., Zhang, S. Pajic, M. **AVstack: An Open-Source, Reconfigurable Platform for Autonomous Vehicle Development**, In 14th ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), pp. 209–220, May 2023, https://doi.org/10.1145/3576841.3585930

- Guest-editor, *Special Issue on Medical Cyber-Physical Systems, ACM Transactions on Cyber-Physical Systems*, 2016-2017.

4. Khazraei, A., **Pajic, M.**, **Resiliency of Nonlinear Control Systems to Stealthy Sensor Attacks**, In 61st IEEE Conference on Decision and Control (CDC), pp. 7109-7114, Dec. 2022, https://doi.org/10.1109/CDC51059.2022.9992988
5. Hallyburton, S. Khazraei, A., Pajic, M., **Optimal Myopic Attacks on Nonlinear Estimation**, In 61st IEEE Conference on Decision and Control (CDC), pp. 5480-5485, Dec. 2022, https://doi.org/10.1109/CDC51059.2022.9992711

Assured Autonomy

Project name: *AFOSR Center of Excellence in Assured Autonomy in Contested Environments* **Relevant Project for MCSecurity**

Funding source: Air Force Office of Scientific Research (AFOSR)

Implementation period: 2019-2025.

Awarded grant amount: 1,489,759.00 USD

Project PI: Warren Dixon

Role of Miroslav Pajic: Co-PI

KEY RESULTS OF Assured Autonomy

Journal papers:

1. Lesi, V., Jakovljevic, Z., **Pajic, M.**, **Security-Analysis for Distributed IoT-Based Industrial Automation**, IEEE Transactions on Automation Science and Engineering, Vol. 19, No. 4, pp. 3093-3108, October 2022. https://ieeexplore.ieee.org/document/9528498
2. Jakovljevic, Z., Lesi, V., **Pajic, M.**, **Attacks on Distributed Sequential Control in Manufacturing Automation**, IEEE Transactions on Industrial Informatics, Vol. 17, No. 2, pp. 775-786, Feb. 2021, https://ieeexplore.ieee.org/abstract/document/9068503
3. Jovanov, I., **Pajic, M.**, **Relaxing Integrity Requirements for Attack-Resilient Cyber-Physical Systems**, IEEE Transactions on Automatic Control, Vol. 64, No. 12, pp. 4843-4858, December 2019, doi: 10.1109/TAC.2019.2898510
4. Wang, Y., Zarei, M., Bonakdarpour, B., **Pajic, M.**, **Statistical Verification of Hyper-properties for Cyber-Physical Systems**, ACM Trans. Embed. Comput. Syst., Vol. 18(5s), pp. 92:1–92:23, 2019, https://dl.acm.org/doi/10.1145/3358232
5. Zhu, H., Cummings, M. Elfar, M. Wang, Z., **Pajic, M.**, **Operator Strategy Model Development in UAV Hacking Detection**, IEEE Trans. on Human-Machine Systems, Vol. 49, No. 6, pp. 540-549, Dec 2019, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8653416

Conference papers:

6. Khazraei, A., Pfister, H., **Pajic, M.**, **Resiliency of Perception-Based Controllers Against Attacks**, In Proceedings of the 4th Annual Learning for Dynamics and Control Conference (L4DC), PMLR 168:713-725, June 2022 (Spotlight presentation), https://proceedings.mlr.press/v168/khazraei22a/khazraei22a.pdf
7. Khazraei, A., Hallyburton, S., Gao, Q., Wang, Y., **Pajic, M.**, **Learning-Based Vulnerability Analysis of Cyber-Physical Systems**, In 13th ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), pp. 259-269, May 2022, doi: 10.1109/ICCPS54341.2022.00030
8. Sun, S., Zhang, Y., Luo, X., Vlantis, P., **Pajic, M.**, Zavlanos, M., **Formal Verification of Stochastic Systems with ReLU Neural Network Controllers**, In IEEE International Conference on Robotics and Automation (ICRA), pp. 6800-6806, June 2022, doi: 10.1109/ICRA46639.2022.9811866
9. Bozkurt, A. K., Wang, Y., **Pajic, M.**, **Model-Free Learning of Safe yet Effective Controllers**, In 60th IEEE Conference on Decision and Control (CDC), pp. 6560-6565, December 2021, doi: 10.1109/CDC45484.2021.9683634
10. Khazraei, A., **Pajic, M.**, **Perfect Attackability of Linear Dynamical Systems with Bounded Noise**, In 2020 American Control Conference (ACC), pp. 749-754, June 2020, doi: 10.23919/ACC45564.2020.9147833

CAREER

Project name: ***CAREER: Foundations for Secure Control of Cyber-Physical Systems***, Award Number: 652544 **Relevant Project for MCSecurity**

Funding source: National Science Foundation (NSF)

Implementation period: 2017-2024.

Awarded grant amount: 530,339.00 USD

Project PI: Miroslav Pajic

Role of Miroslav Pajic: PI

KEY RESULTS OF CAREER:

Journal papers:

1. Khazraei, A., **Pajic, M.**, **Attack-resilient state estimation with intermittent data authentication,** Automatica, Vol. 138 , art. no. 110035, 2022, https://doi.org/10.1016/j.automatica.2021.110035 **Relevant Publication for MCSecurity**

2. Luo, X., **Pajic, M.**, Zavlanos, M., **An optimal graph-search method for secure state estimation,** Automatica, Vol. 123, art. no. 109323, 2021, https://doi.org/10.1016/j.automatica.2020.109323 Citation Details
3. Jakovljevic, Z., Lesi, V., Mitrovic, S., **Pajic, M.**, **Distributing Sequential Control for Manufacturing Automation Systems**, IEEE Transactions on Control Systems Technology, Vol. 28, No. 4, pp. 1586 – 1594, 2020 https://doi.org/10.1109/TCST.2019.2912776
4. Lesi, V., Jovanov, I., **Pajic, M.**, **Integrating Security in Resource-Constrained Cyber-Physical Systems**, ACM Transactions on Cyber-Physical Systems, Vol. 4, No. 3, art. no. 28, 2020, https://doi.org/10.1145/3380866 **Relevant Publication for MCSecurity**
5. Miao, F., Zhu, Q., **Pajic, M.**, and Pappas, G. J., **A hybrid stochastic game for secure control of cyber-physical systems**, Automatica, Vol. 93, pp. 55-63, 2018, doi: 10.1016/j.automatica.2018.03.012 Citation Details

Conference papers:

6. Hallyburton, S. R., Liu, Y., Cao, Y., Mao, Z. M., **Pajic, M.**, **Security Analysis of Camera-LiDAR Fusion Against Black-Box Attacks on Autonomous Vehicles**, IN 31st USENIX Security Symposium (USENIX Security 2022), pp. 1903-1920, Aug 2022**,** https://www.usenix.org/biblio-12506 **Relevant Publication for MCSecurity**
7. Wang, Y., Zarei, M., Bonakdarpour, B., **Pajic, M.**, **Probabilistic Conformance for Cyber-Physical Systems**, In 12th ACM/IEEE International Conf. on Cyber-Physical Systems (ICCPS), pp. 55-66, May 2021, https://dl.acm.org/doi/10.1145/3450267.3450534
8. Bozkurt, A. K., Wang, Y., **Pajic, M.**, **Secure Planning Against Stealthy Attacks via Model-Free Reinforcement Learning**, IEEE International Conference on Robotics and Automation (ICRA), pp. 10656-10662, May 2021, doi: 10.1109/ICRA48506.2021.9560940
9. Hallyburton, R. S., Khazraei, A., **Pajic, M.**, **Optimal Myopic Attacks on Nonlinear Estimation**, In 2022 IEEE 61st Conference on Decision and Control (CDC), pp. 5480-5485, 2022, https://doi.org/10.1109/CDC51059.2022.9992711
10. Khazraei, A., **Pajic, M.**, **Resiliency of Nonlinear Control Systems to Stealthy Sensor Attacks**, In 2022 IEEE 61st Conference on Decision and Control (CDC), pp. 7109-7114, 2022 https://doi.org/10.1109/CDC51059.2022.9992988 Citation Details

1UH3NS129898-01

Project name: *An Integrated Biomarker Approach to Personalized, Adaptive Deep Brain Stimulation in Parkinson Disease,* Award Number: 1UH3NS129898-01

Funding source: National Institutes of Health (NIH)

Implementation period: 2023-2027.

Awarded grant amount: 4,457,893.00 USD

Project PI: Dennis Turner

Role of Miroslav Pajic: Co-Investigator

KEY RESULTS OF 1UH3NS129898-01:

Journal papers:

1. Schmidt S.L., Chowdhury A.H., Mitchell K.T., Peters J.J., Gao Q., Lee H.J., Genty K., Chow S.C., Grill W.M., **Pajic M.**, Turner D.A., At home adaptive dual target deep brain stimulation in Parkinson's disease with proportional control, Brain, Vol. 147, No. 3 pp. 911-922, Mar. 2024, doi: 10.1093/brain/awad429

Small

Project name: *Transforming Computer Architecture Evaluation with Statistical Model Checking*, Award Number: 2133160

Funding source: National Science Foundation (NSF)

Implementation period: 2021-2024.

Awarded grant amount: 500,000.00 USD

Project PI: Daniel Sorin

Role of Miroslav Pajic: co-PI

KEY RESULTS OF 1UH3NS129898-01:

Conference papers:

1. Dobe, O., Schupp, S., Bartocci, E., Bonakdarpour, B., Legay, A., **Pajic, M.**, Wang, Y., **Lightweight Verification of Hyperproperties**. In: André, É., Sun, J. (eds) Automated Technology for Verification and Analysis. ATVA 2023, Lecture Notes in Computer Science, Vol. 14216, pp 3–25, 2023, Springer, Cham. https://doi.org/10.1007/978-3-031-45332-8_1

Additional 2 publications relevant for MCSecurity (2 are listed as key references 1, 4 and 6 of CAREER)

1. **Pajic, M.**, Lee, I., Pappas, G. J., **Attack-Resilient State Estimation for Noisy Dynamical Systems**, IEEE Transactions on Control of Network Systems, Vol. 4, No. 1, pp. 82 -92, March 2017, doi: 10.1109/TCNS.2016.2607420 **Relevant Publication for MCSecurity**

2. **Pajic, M.**, Weimer, J., Bezzo, N., Sokolsky, O., Pappas, G. J., Lee, I., **Design and Implementation of Attack-Resilient Cyber-Physical Systems: With a Focus on Attack-Resilient State Estimators**, IEEE Control Systems Magazine, Vol. 37, No. 2, pp. 66-81, April 2017, doi: 10.1109/MCS.2016.2643239 **Relevant Publication for MCSecurity**

Additional 2 projects relevant for MCSecurity

2023-2025 **Pajic, M.**, et al.
General Framework for Vulnerability Analysis of Cyber-Physical Systems,
Project funded by Office of Naval Research (ONR)

2015-2020 Lee, I., Pappas, **G., Pajic, M.**, et al.
Synergy: Collaborative: Security and Privacy-Aware Cyber-Physical Systems
Project funded by National Science Foundation (NSF) and Intel Partnership, CPS-Security Program

Products, services related to MCSecurity

1. **AVStack** – An open-source, reconfigurable software platform for AV design, implementation, test, and analysis. https://www.avstack.org/, 2023.
2. **ARSC** – open-source tool for design of *attack-resilient supervisory controllers*, https://gitlab.oit.duke.edu/cpsl/arsc, 2019.
3. **SMCLearning** – Statistical model checker for *deep-neural-network-based cyber-physical systems*, https://gitlab.oit.duke.edu/cpsl/smclearning, 2019.
4. **MPHyper** – Symbolic motion planner for HyperLTL objectives, https://gitlab.oit.duke.edu/cpsl/mp_hyper, 2019.
5. **RESCHU-SA**: An open-source extendable virtual platform for studying the impact that a human-on-the-loop have on security and resiliency of cyber-physical systems with varying levels of autonomy, 2017.