

# Ipsita Koley, Postdoctoral Researcher at General Electric Aerospace Research, India

✉ ikipsita@gmail.com

☎ +91 9836109083

🌐 LinkedIn

🎓 Google Scholar






## Research Summary

My primary research objective has been designing a holistic secure control framework for safety-critical cyber-physical systems (e.g. for automotive CPSs) that are resource-aware and performance-preserving. The research endeavor spans from vulnerability analysis and theoretical modeling of secure cyber-physical systems (CPSs) to their real-time realization on embedded platforms especially in the automotive domain. The research problems addressed in my doctoral thesis cover 3 prominent areas of automotive CPS security. *Firstly*, we design an *SMT-based CAD framework* for vulnerability assessment of any secure CPS model. The proposed CAD framework synthesizes stealthy false data injection (FDI) attacks that violate the safety and control properties of CPSs (e.g., commonly used automotive control programs like Electronic Stability Program) using counter-example guided abstraction refinement (CEGAR). In follow-up work, we bridge the gap between the theoretical modeling of FDI attacks and modeling the same in the presence of platform-level uncertainties in automotive CPS. Essentially, we analyze the static schedule of CAN messages, utilize the delays induced by jitter, and dynamically synthesize stealthy FDI attacks to optimally degrade the performance of a target control loop at runtime. *Secondly*, for the detection of such stealthy FDIs, we design 2 types of lightweight residue-based attack detectors: a formal methods-based attack detector with varying detection threshold and a learning-based adaptive attack detector. The adaptive detector is developed as a *reinforcement learning agent* in a competitive adversarial environment for detection of FDI attacks (with minimum false alarm) and uses an SMT-based controller for its fast mitigation. *Thirdly*, we also intend to enhance a system's resilience against such attacks. In particular, we explore the effect of performance-aware skipping of certain instances of control task executions on the resilience of any linear dynamical system against FDI attacks. A *Gated Recurrent Unit (GRU)-based attack prediction* and control skipping-based mitigation framework is developed as part of this work. We evaluate the proposed attack injection, detection strategies, and attack-resilient control framework on a real-time hardware-in-loop setup for automotive CPSs. It consists of an *ETAS Labcar real-time PC* connected in a closed loop with industry-scale electronic control units (*Infineon Aurix Tricore and Raptor GCM ECUs*), and *Nvidia Jetson Nano GPUs* (for AI components) via CAN.





## Working Experience

- Mar'24 – till date 📌 **Postdoctoral Researcher** at, General Electric Aerospace Research, India
- Jan'24 – Feb'24 📌 **Program Committee** at, 15th ACM/IEEE International Conference on Cyber-Physical Systems: Poster/Demo
- Jul'18 – Feb'24 📌 **Research Scholar** at, Indian Institute of Technology, Kharagpur  
*My research focus is on exploiting control-theoretic approaches, and learning-based methods to explore vulnerabilities and design lightweight attack detection techniques with formal guarantees for securing real-time cyber-physical systems like automotive.*
- 📌 **Teaching Assistant** at, Indian Institute of Technology, Kharagpur  
*Formal Language and Automata Theory, Foundation of Cyber-Physical Systems, Programming, and Data Structures Lab, Design & Analysis of Algorithms Lab, etc.*
- 📌 **Reviewer** for  
*Euromicro Conference Series on Digital System Design (DSD), ACM Transactions on Cyber-Physical Systems (TCPS), IEEE Transactions on Information Forensics and Security (TIFS), Journal of Cryptographic Engineering (JCEN), International Conference on Security, Privacy, and Applied Cryptographic Engineering (SPACE), International Conference on VLSI Design (VLSID)*
- 📌 **Sub-reviewer** for  
*IEEE Real-Time Systems Symposium (RTSS), Design Automation Conference (DAC), ACM Transactions on Embedded Computing Systems (TECS)*

## Working Experience (continued)

- Jul'18 – Jul'20  **Research Project on Robustness Analysis for Automotive Software System** at, Robert Bosch Engineering and Business Solutions Private Ltd.  
*We have developed a tool using a formal method technique that takes as input vehicle parameters, a maneuver, attack detection rules, and specific performance criteria and generates stealthy deceptive attack vectors that violate the performance criteria by bypassing the detection rules.*
- Jul'16 – Jun'18  **Teaching Assistant** at, Indian Institute of Engineering Science & Technology, Shibpur  
*Database Management Systems, Computer Graphics, Programming and Data Structures Lab, etc.*
- Jan'17 – Jun'18  **Research Project on Mobile Sink-Based Data Collection for Energy Efficient Coordination in Wireless Sensor Network Using Cooperative Game Model** at, Indian Institute of Engineering Science and Technology, Shibpur  
*We addressed the un-proportionate energy consumption in a wireless sensor network and proposed energy-efficient data collection protocol by multiple mobile sinks based on cooperative game theory with non-transferable utility.*
- Jun'14 – Jul'16  **Associate Software Engineer** at, RS Software India Ltd., Kolkata, India  
*Role: Automation Test Engineer*
- Jan'13 – Jun'14  **Assistant System Engineer** at, Tata Consultancy Services Ltd., Pune, India  
*Role: Automation Test Engineer*

## Education

- 2018  **M.Tech in Information Technology** [86.67%]  
*Indian Institute of Engineering Science and Technology, Shibpur*
- 2012  **B.Tech in Computer Science & Engineering** [GPA: 8.84/10]  
*MCKV Institute of Engineering, Howrah*
- 2008  **Class XII, Belur High School (H.S.)** [86%]
- 2006  **Class X, Patha Bhavan, Dankuni** [90%]

## Research Publications

### Journal Articles

- 1 S. Adhikary, **I. Koley**, S. K. Ghosh, S. Ghosh, and S. Dey, "Revisiting dynamic scheduling of control tasks: A performance-aware fine-grained approach," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, (accepted), 2024.
- 2 **I. Koley**, S. Dey, D. Mukhopadhyay, S. Singh, L. Lokesh, and S. V. Ghotgalkar, "Cad support for security and robustness analysis of safety-critical automotive software," *ACM Transactions on Cyber-Physical Systems*, vol. 7, no. 1, pp. 1–26, 2023.
- 3 **I. Koley** and T. Samanta, "Mobile sink based data collection for energy efficient coordination in wireless sensor network using cooperative game model," *Telecommunication Systems*, vol. 71, pp. 377–396, 2019.

### Conference Proceedings

- 1 S. Adhikary, **I. Koley**, S. K. Ghosh, S. Ghosh, and S. Dey, "Revisiting dynamic scheduling of control tasks: A performance-aware fine-grained approach," in *International Conference on Embedded Software (EMSOFT)*, 2024, (accepted).

- 2 **I. Koley**, S. Adhikary, and S. Dey, "Thinking beyond bus-off: Targeted control falsification in can," in *Proceedings of the ACM/IEEE 15th International Conference on Cyber-Physical Systems (with CPS-IoT Week 2024)*, 2024, pp. 33–44.
- 3 B. Anjana, S. Adhikary, **I. Koley**, A. R. Hota, and S. Dey, "Poster: Adaptive protection of power grids against stealthy load alterations," in *Proceedings of the ACM/IEEE 15th International Conference on Cyber-Physical Systems (with CPS-IoT Week 2024)*, 2024, pp. 285–286.
- 4 S. Maiti, B. Anjana, S. Adhikary, **I. Koley**, and S. Dey, "Targeted attack synthesis for smart grid vulnerability analysis," in *Proceedings of the Proceedings of the 30th ACM Conference on Computer and Communications Security (CCS)*, 2023, pp. 1–15.
- 5 **I. Koley**, S. Adhikary, A. Sain, and S. Dey, "Design and deployment of resilient control execution patterns: A prediction, mitigation approach," in *Proceedings of the ACM/IEEE 14th International Conference on Cyber-Physical Systems (with CPS-IoT Week 2023)*, 2023, pp. 166–176.
- 6 **I. Koley**, S. Adhikary, R. Rohit, and S. Dey, "A framework for evaluating connected vehicle security against false data injection attacks," in *2022 25th Euromicro Conference on Digital System Design (DSD)*, IEEE, 2022, pp. 913–920.
- 7 **I. Koley**, S. Adhikary, and S. Dey, "Catch me if you learn: Real-time attack detection and mitigation in learning enabled cps," in *2021 IEEE Real-Time Systems Symposium (RTSS)*, IEEE, 2021, pp. 136–148.
- 8 **I. Koley**, S. K. Ghosh, S. Dey, *et al.*, "Formal synthesis of monitoring and detection systems for secure cps implementations," in *2020 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, IEEE, 2020, pp. 314–317.
- 9 A. Roy, **I. Koley**, S. Adhikary, and S. Dey, "Optimizing rsu placements for securing vehicle platoon against false data injection attacks," in *Proceedings of the ACM/IEEE 14th International Conference on Cyber-Physical Systems (with CPS-IoT Week 2023)*, 2023, pp. 251–252.
- 10 S. Adhikary, **I. Koley**, S. Maity, and S. Dey, "Work-in-progress: Control skipping sequence synthesis to counter schedule-based attacks," in *2022 IEEE Real-Time Systems Symposium (RTSS)*, IEEE, 2022, pp. 491–494.
- 11 P. Kremer, **I. Koley**, S. Dey, and S. Park, "State estimation for attack detection in vehicle platoon using vanet and controller model," in *2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC)*, IEEE, 2020, pp. 1–8.
- 12 S. Adhikary, **I. Koley**, S. K. Ghosh, S. Ghosh, S. Dey, and D. Mukhopadhyay, "Skip to secure: Securing cyber-physical control loops with intentionally skipped executions," in *Proceedings of the 2020 Joint Workshop on CPS&IoT Security and Privacy*, 2020, pp. 81–86.
- 13 A. Bhattacharya, S. Adhikary, **I. Koley**, A. Majumder, and S. Dey, "Adaptive cusum-based residue analysis for stealthy attack detection in cyber-physical systems," in *Proceedings of the ACM/IEEE 14th International Conference on Cyber-Physical Systems (with CPS-IoT Week 2023)*, 2023, pp. 270–271.
- 14 A. Sain, S. Singh, S. Adhikary, **I. Koley**, and S. Dey, "Work-in-progress: Securing safety-critical control tasks with attack-aware multi-rate scheduling," in *2023 IEEE 29th Real-Time and Embedded Technology and Applications Symposium (RTAS)*, IEEE, 2023, pp. 345–348.

## Book Chapters

- 1 S. Dey, **I. Koley**, and S. Adhikary, "Chapter 6: Resource aware synthesis of automotive security primitives," in *Machine Learning and Optimization Techniques for Automotive Cyber-physical Systems*, V. K. Kukkala and S. Pasricha, Eds., Springer, 2023.

## Achievements

---

- 2024 **Winner of 2024 ACM SIGBED Frank Anger Memorial Award**
- 2023 **Invited for a talk on our publication in Academic Research and Careers for Students (ARCS) organized by ACM India**
- 2022 **Secured 1<sup>st</sup> runner-up position in Ph.D. forum** organized by *IEEE WINTECHCON*
- 2018 **Received UGC NET JRF Scholarship.**
- 2015 **Awarded 'Star of the Month' by RS Software India Ltd.**
- 2013 **Awarded 'On Spot Award' by Tata Consultancy Services Ltd.**
- 2011 **Placed 3<sup>rd</sup> in Regional Student Convention**, organized by Computer Society of India, Region II, held at ISI, Kolkata.
- 2008 **Awarded under Scheme of Scholarship for College & University student's reg. of Government of India** on the result of Higher Secondary examination held by WBCHSE.
- 2006 **Awarded under National Merit Scholarship Scheme of Government of India**, for the result of Madhyamik, Examination held by WBBSE.

## Skills & Trainings

---

- Coding **C, C#, Java, VB, Python**
- Tools & Technology **z3, Matlab, ETAS LabCar, IPG CarMaker, Arduino, QTP, Selenium, SQL,VB.Net**
- Certifications **Microsoft Programming in C# (70-483)**
- Workshops **Training on JEE** organized by Globsyn Finishing School,  
**Workshop on Application Of Advance Algorithm** organized by the Department of Information Technology at Indian Institute of Engineering Science and Technology, Shibpur,  
**Summer School on Algorithms and Optimization** at Indian Statistical Institute, Kolkata,  
**Training program on Application Security** at RS Software, Kolkata
- Web Dev **HTML, css.**
- Languages **Bengali, English, Hindi**