Anit Kumar Sahu

Contact Information

5437 Ellsworth Avenue
Pittsburgh, PA 15232

Mobile: +1-412-608-8890
E-mail: anit.sahu@gmail.com
Web: http://anitksahu.github.io

Work Experience

Amazon Alexa AI — Seattle, WA
Senior Applied Scientist — Oct 2020 - Present
Federated Learning

Bosch Center for Artificial Intelligence — Pittsburgh, PA
Machine Learning Research Scientist 2 — Jan 2019 - Oct 2020
Black-Box Adversarial attacks on Neural Networks and defenses for attacks.
One query Universal attacks on Neural networks
Multiplicative Filter Networks

Education

Carnegie Mellon University — Pittsburgh, PA
PhD, Electrical and Computer Engineering — June 2013 - Nov 2018

Indian Institute of Technology, Kharagpur — Kharagpur, India
B.Tech and M.Tech(Dual Degree),
Electronics and Communication Engineering, — Jul 2008 - May 2013
– GPA: 9.28/10.00

Internship Experience

Yahoo! Research: Intern Scientist — Sunnyvale, CA
Supervisor: Narayan Bhamidipati — May 2017 - Aug 2017
Developed a margin management scheme for Real Time Bidding with campaign efficiency management for post install conversions.
Designed a novel state-space approach and short term reward function to learn a deterministic policy using Q-learning.

Bosch RTC[1]: Machine Learning & Control Theory Research Intern Pittsburgh, PA
Supervisor: Jon Francis — May 2016 - Aug 2016
Developed data-driven inference models for the evolution of different environmental modalities with occupancy count as a disturbance.
Designed smart control schema based on the data-driven models to provide for user comfort while keeping the energy constraint in mind.

Research Publications

Journal Papers

J0 A.K. Sahu and S. Kar, Decentralized Zeroth Order Constrained Stochastic Optimization Algorithms: Frank-Wolfe and Variants With Applications to Black-Box Adversarial Attacks, In *Proceedings of the IEEE: Special Issue On Optimization for Dara-driven Learning and Control*, DOI: 10.1109/JPROC.2020.3012609

J1 T. Li, A.K. Sahu, A. Talwalkar and V. Smith, Federated Learning: Challenges, Methods and Future Directions, August 2019, A shorter version will appear in the *Special Issue on Distributed, Streaming Machine Learning* of *IEEE Signal Processing Magazine* 2020

J2 A.K. Sahu, D. Jakovetic, D. Bajovic and S. Kar, Communication-Efficient Distributed Strongly Convex Stochastic Optimization Over Networks: Non-Asymptotic Rates., Under review in *IEEE Transactions on Automatic Control*. Initial Submission: August 2018

J3 A.K. Sahu, D. Jakovetic, D. Bajovic and S. Kar, Communication Efficient Distributed Weighted Non-Linear Least Squares Estimation, *EURASIP Journal on Advances in Signal Processing*, December 2018

[1] Research and Technology Center

J4 A.K. Sahu, D. Jakovetic and S. Kar, $\mathcal{CIRFE}$: A Distributed Random Fields Estimator, *IEEE Transactions on Signal Processing.* Vol:66, Issue 18, pp. 4980-4995.

J5 A.K. Sahu, D. Jakovetic and S. Kar, Communication optimality trade-off for distributed estimation, under review in *Journal of Machine Learning Research.* Initial Submission: January 2018

J6 A.K. Sahu, S. Kar, J.M.F. Moura and H.V. Poor, Distributed Constrained Recursive Nonlinear Least-Squares Estimation : Algorithms and Asymptotics, *IEEE Transactions on Signal and Information Processing over Networks: Special issue on Inference and Learning over Networks.*Vol:2, Issue 4, pp. 426-441, 2016

J7 A.K. Sahu and S. Kar, Recursive Distributed Detection for Composite Hypothesis Testing: Nonlinear Observation Models in Additive Gaussian Noise, *IEEE Transactions on Information Theory*, Vol:63, Issue 8, pp. 4797-4828, 2017.

J8 A.K. Sahu and S. Kar, Distributed Sequential Detection for Gaussian Shift-in-Mean Hypothesis Testing, *IEEE Transactions on Signal Processing.* Vol:64, Issue 1, pp. 89-103, 2016.

Conference Papers

C0 A.K. Sahu, D. Willmott, F. Sheikholeslami, F. Condessa and Z. Kolter, You only query once: Effective black box adversarialattacks with minimal repeated queries, Under review in *AAAI 2021*

C1 S.N. Shukla, A.K. Sahu, D. Willmott and Z. Kolter, Hard Label Black-box Adversarial Attacksin Low Query Budget Regimes, Under review in *AAAI 2021*

C2 T. Li, A.K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar and V. Smith, Federated Optimization in Heterogeneous Networks, In Proceedings of *MLSys 2020.* (An abridged version appeared in *ICML 2019 Adaptive and Multi Task Learning (AMTL) Workshop*)

C3 T. Li, A.K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar and V. Smith, Fed-DANE: A Federated Newton-Type Method, In Proceedings of *53rd Annual Asilomar Conference on Signals, Systems and Computers, 2019, Pacific Grove, CA*

C4 R.Xin, A.K. Sahu, U.A. Khan and S. Kar, Distributed empirical risk minimization over directed graphs, In Proceedings of *53rd Annual Asilomar Conference on Signals, Systems and Computers, 2019, Pacific Grove, CA*

C5 J. Wang, A.K. Sahu, Z. Yang, G. Joshi, S. Kar, MATCHA: Speeding up Decentralized SGD via Matching Decomposition Sampling, In *NeurIPS 2019 Workshop on Federated Learning.*

C6 R.Xin, A.K. Sahu, U.A. Khan and S. Kar, Distributed stochastic optimization with gradient tracking over strongly-connected networks, In Proceedings of *58th IEEE Conference on Decision and Control, CDC 2019*

C7 A.K. Sahu, M. Zaheer and S. Kar, Towards Gradient Free and Projection Free Stochastic Optimization, In Proceedings of *22nd International Conference on Artificial Intelligence and Statistics (AISTATS)* 2019

C8 A.K. Sahu, D. Jakovetic, D. Bajovic and S. Kar, Non-Asymptotic Rates For Communication Efficient Distributed Zeroth Order Strongly Convex Optimization, In Proceedings of *IEEE Global Conference on Signal and Information Processing, GlobalSIP 2018.*

C9 D. Jakovetic, D. Bajovic, A.K. Sahu and S. Kar, Convergence rates for distributed stochastic optimization over random networks, In Proceedings of *57th IEEE Conference on Decision and Control, CDC 2018.*

C10 A.K. Sahu, D. Jakovetic, D. Bajovic and S. Kar, Distributed Zeroth Order Optimization Over Random Networks: A Kiefer-Wolfowitz Stochastic Approximation Approach, In Proceedings of *57th IEEE Conference on Decision and Control, CDC 2018.*

C11 A.K. Sahu, D. Jakovetic and S. Kar, Communication Efficient Distributed Estimation, To appear in *International Symposium on Information Theory, ISIT 2018.*

C12 D. Bajovic, D. Jakovetic, A.K. Sahu, and S. Kar, Large Deviations for Products of Non-i.i.d. Stochastic Matrices with Application to Distributed Detection, To appear in *International Symposium on Information Theory, ISIT 2018*.

C13 Z. Jiang, J, Francis, A.K. Sahu, S. Munir, C. Shelton, A. Rowe and M. Berges, Data-driven Thermal Model Inference with ARMAX, in Smart Environments, based on Normalized Mutual Information, In Proceedings of *American Control Conference, ACC 2018*.

C14 A.K. Sahu, and S. Kar, Dist-Hedge: A partial information setting based distributed non-stochastic sequence prediction algorithm, In Proceedings of *IEEE Global Conference on Signal and Information Processing, GlobalSIP 2017*.

C15 S. Kar, R. Negi, M. Mahzoon and A.K. Sahu, Queue-based Broadcast Gossip Algorithm for Consensus, In Proceedings of *54th Annual Allerton Conference on Communication, Control, and Computing, 2016*.

C16 A.K. Sahu, and S. Kar, Distributed Online Learning: A consensus+innovations approach, In Proceedings of *IEEE Global Conference on Signal and Information Processing, GlobalSIP 2016*.

C17 A.K. Sahu and S. Kar, Distributed Composite Hypothesis Testing : Imperfect Communication, In Proceedings of *International Symposium on Information Theory, ISIT 2016*.

C18 A.K. Sahu and S. Kar, Distributed Generalized Likelihood Ratio Tests : Fundamental Limits and Tradeoffs, In Proceedings of *41st IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2016, Shanghai*.

C19 A.K. Sahu and S. Kar, Distributed Sequential Detection for Gaussian Binary Hypothesis Testing: Heterogeneous Networks, In Proceedings of *Asilomar Conference on Signals, Systems and Computers 2014*.

Patents

P1 Bayesian Optimization based query efficient black box adversarial attacks, S. N. Shukla, A. K. Sahu, D. Willmott, Z. Kolter, US Patent App. No. 16/580587

P2 Efficient Black Box adversarial attacks exploiting input data structure, A. K. Sahu, Z. Kolter, US Patent App. No. 16/580650

P3 Training a machine learning model using a batch based active learning approach, J. Szurley, W. Lin, A. K. Sahu, G. Gupta, US Patent App. No. 16/582928

P4 Improved Adversarial Training Using Meta-Learned Initialization, X. Zhang, A. K. Sahu, Z. Kolter, US Patent App. No. 17/062385

P5 Multiplicative Filter Networks, D. Willmott, A. K. Sahu, R. Fathony, F. Condessa, Z. Kolter, US Patent App. No. 17/034496

P6 System and Method of a Monotone Operator Neural Network, E. Winston, Z. Kolter, A. K. Sahu, US Patent App. No. 16/850816

Academic Achievements Awards and Scholarships

- Best Student Paper Award at the NeurIPS 2019 workshop on Federated Learning.
- Awarded the **A.G. Jordan** award for outstanding PhD thesis and exceptional contribution to CMU and ECE communities.
- Awarded the Carnegie Institute of Technology Dean's Fellowship for the academic session 2013-14.
- Awarded the best M.Tech project award for my Master's Thesis at IIT Kharagpur.
- Letter of commendation from the Dean Undergraduate Studies, IIT Kharagpur for securing a perfect 10.0 GPA in my 9th semester.
- **Jagadish Bose National Science Talent Search**(JBNSTS) scholarship,2008
- Ranked **11th,9th,5th and 1st** in state in Regional Mathematics Olympiad**(RMO)** for four consecutive years from Grade 8 to Grade 11 in the years 2003,2004,2005 and 2006 & participated in Indian National Mathematics Olympiad **(INMO)** 2004,2005,2006 and 2007.