# SLR for: My Research

## Paper 1

**Title:** Machine Learning (ML)-assisted Beam Management in millimeter (mm)Wave Distributed Multiple Input Multiple Output (D-MIMO) systems **Authors:** Karthik R M, Dhiraj Nagaraja Hegde, Muris Sarajlic, Abhishek Sarkar **Published:** 2023-12-30T09:24:19Z **Link:** http://arxiv.org/abs/2401.05422v1 **Abstract:** Beam management (BM) protocols are critical for establishing and maintaining connectivity between network radio nodes and User Equipments (UEs). In Distributed Multiple Input Multiple Output systems (D-MIMO), a number of access points (APs), coordinated by a central processing unit (CPU), serves a number of UEs. At mmWave frequencies, the problem of finding the best AP and beam to serve the UEs is challenging due to a large number of beams that need to be sounded with Downlink (DL) reference signals. The objective of this paper is to investigate whether the best AP/beam can be reliably inferred from sounding only a small subset of beams and leveraging AI/ML for inference of best beam/AP. We use Random Forest (RF), MissForest (MF) and conditional Generative Adversarial Networks (c-GAN) for demonstrating the performance benefits of inference. **Overview:** This paper focuses on enhancing beam management (BM) in millimeter-wave Distributed Multiple Input Multiple Output (D-MIMO) systems using machine learning (ML) techniques. In these systems, multiple access points (APs) coordinated by a central processing unit (CPU) serve user equipments (UEs), and efficient beam management is crucial, particularly due to the high number of narrow beams needed at mmWave frequencies. The challenge lies in identifying the best AP and beam direction without resorting to exhaustive sounding of all the beams, which is resource-intensive.

The research aims to determine whether it is possible to infer the best beams or APs by sounding only a subset of beams and using ML algorithms like Random Forest (RF), MissForest (MF), and conditional Generative Adversarial Networks (c-GAN) for inference. By predicting the link quality indicators such as Layer 1 Reference Signal Received Power (L1-RSRP) based on partial data, the system can potentially optimize resource usage. The study ties into ongoing work in the 3GPP Release 18 for improving intra-cell spatial domain DL transmit beam prediction.

---

## Paper 2

**Title:** A Quick Primer on Machine Learning in Wireless Communications **Authors:** Faris B. Mismar **Published:** 2023-12-29T18:04:11Z **Link:** http://arxiv.org/abs/2312.17713v4 **Abstract:** This is our third (and final) issue of the quick primer on the use of Python to build a wireless communications prototype. This prototype simulates multiple-input and multiple-output (MIMO) systems for a single orthogonal frequency division multiplexing (OFDM) symbol. In addition, it shows several artificial intelligence (AI) and machine learning (ML) use cases with code implementation. The intent of this primer is to empower the reader with the means to efficiently create reproducible simulations related to AI and ML in wireless communications. This primer has sprung from a draft aligned with the syllabus of a graduate course (EESC 7v86), which we created to be first taught in Fall 2022. **Overview:** The document entitled "A Quick Primer on Machine Learning in Wireless Communications" by Faris B. Mismar aims to guide readers on using Python to develop a wireless communications prototype, specifically simulating MIMO systems for a single OFDM symbol. It includes AI and ML use cases with code examples to facilitate reproducible simulations in wireless communication domains. This primer, intended to complement a graduate course syllabus, offers open-source tools to efficiently aid in prototyping 4G LTE and 5G systems. The author's source code, available on GitHub and Code Ocean, leverages Python for its simplicity and extensive library support. The primer also lists abbreviations used within the text for ease of reference.

---

## Paper 3

**Title:** AIJack: Let's Hijack AI! Security and Privacy Risk Simulator for Machine Learning **Authors:** Hideaki Takahashi **Published:** 2023-12-29T16:10:30Z **Link:** http://arxiv.org/abs/2312.17667v2 **Abstract:** This paper introduces AIJack, an open-source library designed to assess security and privacy risks associated with the training and deployment of machine learning models. Amid the growing interest in big data and AI, advancements in machine learning research and business are accelerating. However, recent studies reveal potential threats, such as the theft of training data and the manipulation of models by malicious attackers. Therefore, a comprehensive understanding of machine learning's security and privacy vulnerabilities is crucial for the safe integration of machine learning into real-world products. AIJack aims to address this need by providing a library with various attack and defense methods through a unified API. The library is publicly available on GitHub (https://github.com/Koukyosyumei/AIJack). **Overview:** The paper introduces AIJack, an open-source library designed to simulate and analyze security and privacy risks in machine learning (ML) models during training and deployment. Given the rapid growth in AI and big data, the security threats, such as data theft and malicious model manipulations, have become more pronounced. AIJack offers a comprehensive API facilitating various attack and defense methods, aimed at understanding and mitigating security vulnerabilities in ML technologies as they integrate into real-world applications.

Key aspects include defenses against evasion attacks like adversarial examples â€” where models can misinterpret inputs â€” and against poisoning attacks that contaminate training data to lower model accuracy. Privacy is another focal point, as large-scale data collection can lead to breaches. Techniques like model inversion and membership inference pose privacy risks by reconstructing or identifying personal data from models. To counter these, AIJack incorporates privacy protection strategies such as differential privacy and homomorphic encryption.

The software package is built on PyTorch and scikit-learn, allowing easy integration into existing projects. AIJack supports experimentation with a variety of attacks and defenses, providing flexibility in simulations. This includes federated learning methods and various attack models such as model inversion, poisoning, backdoor, and free-rider attacks, making it a versatile tool to assess ML security and privacy challenges.

---