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:** The paper titled "Machine Learning (ML)-assisted Beam Management in millimeter (mm)Wave Distributed Multiple Input Multiple Output (D-MIMO) systems" explores the use of ML techniques in optimizing beam management for mmWave D-MIMO systems. Beam management (BM) is essential for maintaining connectivity between network nodes and user equipment (UEs). In Distributed MIMO systems, multiple access points (APs) coordinated by a central processing unit (CPU) serve UEs, requiring efficient beam selection due to numerous potential beams at mmWave frequencies. The paper investigates how ML can infer the best APs and beams by sounding only a subset of beams. Techniques such as Random Forest, MissForest, and conditional Generative Adversarial Networks are employed to demonstrate performance improvements. Key focus areas include the efficient measurement and reporting of Downlink Reference Signal Received Power (L1-RSRP) by scanning a subset of beams, aligned with 3GPP Release 18 standards. The goal is to predict signal strengths of unscanned beams using state-of-the-art machine learning algorithms.

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 paper, "A Quick Primer on Machine Learning in Wireless Communications" by Faris B. Mismar, serves as a final installment of a series focused on the application of Python to prototype wireless communication systems, particularly MIMO systems for OFDM symbols. It provides readers with insights into how AI and ML are integrated into these systems, complete with code for practical implementation. The primary goal is to enable readers to conduct reproducible simulations using open-source tools, aiding in the exploration of AI and ML applications within the scope of wireless communications. This primer aligns with a graduate course syllabus first introduced in Fall 2022 at The University of Texas at Dallas. The source code, intended for prototyping 4G LTE and 5G systems, is accessible on GitHub and Code Ocean. The primer emphasizes Python due to its simplicity and extensive library support, making it ideal for AI and ML projects. It also includes a comprehensive list of abbreviations for 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 presents AIJack, an open-source library designed to evaluate security and privacy risks in machine learning (ML) models, addressing the growing concerns surrounding the use of big data and AI. AIJack provides various attack and defense methods through a unified API to help understand and mitigate potential ML vulnerabilities, such as data theft and model manipulation. The library is publicly available on GitHub and aims to facilitate simulations by offering attack-defense combinations with simple code integration, using PyTorch and scikit-learn.

The introduction outlines the significance of ML models in applications like image recognition and natural language processing, emphasizing the need to tackle associated security risks. ML models, although improving in accuracy, are vulnerable to attacks such as evasion and poisoning, which can degrade performance. Privacy risks include Model Inversion and Membership Inference Attacks, which compromise sensitive information. The paper highlights privacy protection methods such as differential privacy, homomorphic encryption, and federated learning.

AIJack addresses these concerns by allowing experimentation with attack and defense strategies, thereby simplifying the assessment of ML model vulnerabilities. The package design includes various techniques for federated learning (both horizontal and vertical) and a range of attacks, such as Model Inversion, Poisoning, and Backdoor Attacks, aimed at exploring and countering different threats to ML security and privacy.