Robustifying Predictive Intelligence for A New Spectrum Market

PI: Ruozhou Yu

Assistant Professor, Department of Computer Science

NC State University

AI Empowers Next-Gen Wireless

- AI is empowering our NextG spectrum and wireless systems

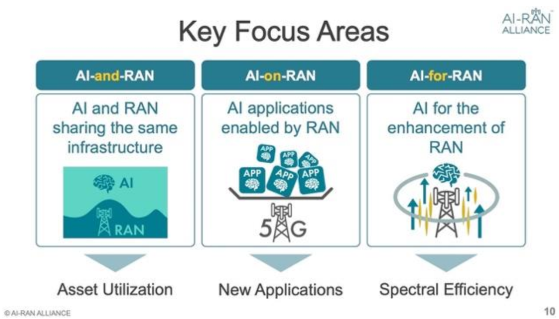
@Tmobile

Huaw

Future Technologies

LLM Application in Wireless Communication Knowledge Management

This paper details the use of RAG to design a Q&A solution for wireless communication know bases and an accompanying evaluation solution.



- But do we trust it yet?

DeepSeek-R1 LLM Fails Over Half of Jailbreak Attacks in Security Analysis

Technology

Deepfake makers can now evade an unusual detection method

Opinion · Chatbots, Robotics & AI

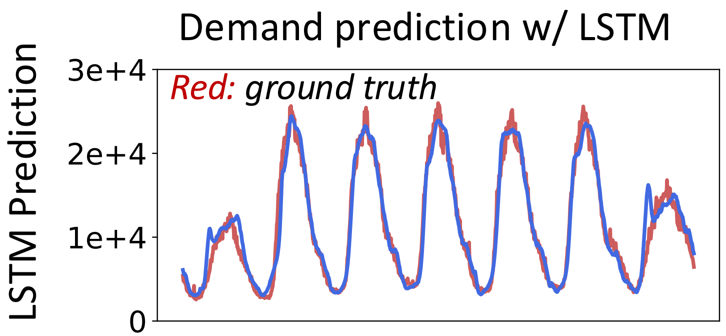
From "Gig" to "Glitch" Economy: Hospitality's New Battle Against AI Hallucinations

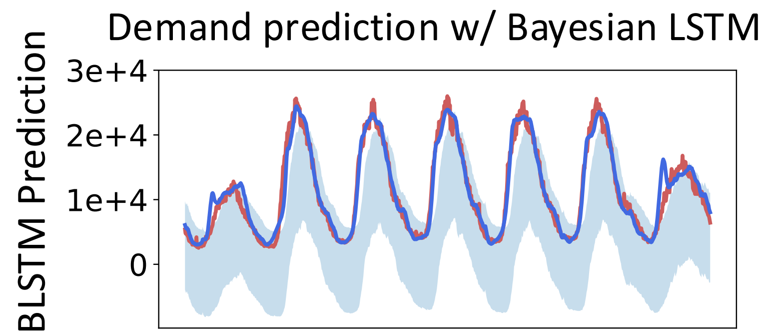
- **Bottomline:** Unsafe and unrobust AI is not ready for wireless.
  - *Risks: infrastructure instability, constraint violation, exploit by malicious user, market manipulation, …*

How This Project Differs from AI Safety Research?

- **Argument:** *Robust AI* does not necessarily make *AI-empowered wireless* sufficiently or more robust.

- **Example:** spectrum allocation based on demand prediction.





Maximum # violated cases: **49.51% - 53.23%**

Maximum # violated cases: **5.67% - 22.26%**

- Apply Bayesian uncertainty quantification and use 95% confidence bound.
  - Reduced violations (underprovisioning) => More robust than LSTM.
  - Violation still larger than estimated risk (95%) => Not robust enough.

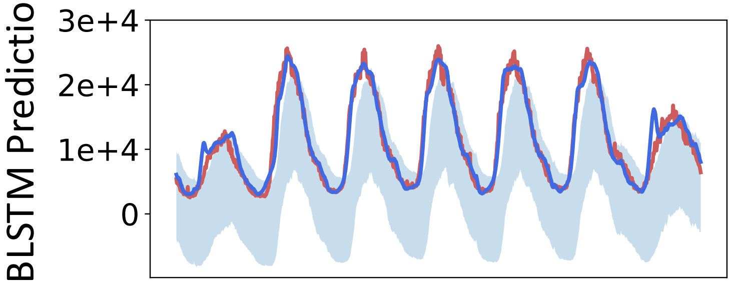
Zhou, Fangtong, and Ruozhou Yu. "Moving Edge for On-Demand Edge Computing: An Uncertainty-aware Approach." *arXiv preprint arXiv:2503.24214* (2025).

Project Goals

❑ **Thrust 1:** Robust AI Algorithms for New Spectrum AI

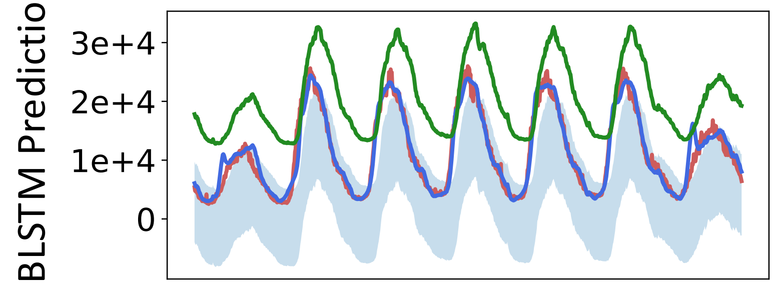
- **Goal:** Certifiable & distributional robustness for dynamic spectrum access
- **Tools:** (1) Bayesian uncertainty quantification, (2) distributionally robust risk, (3) conformal calibration (certifiable statistical guarantee)
- **Preliminary Results:**

Demand prediction w/ Bayesian LSTM



Maximum # violated cases: **5.67% - 22.26%**

BLSTM + Worst-Case CVaR



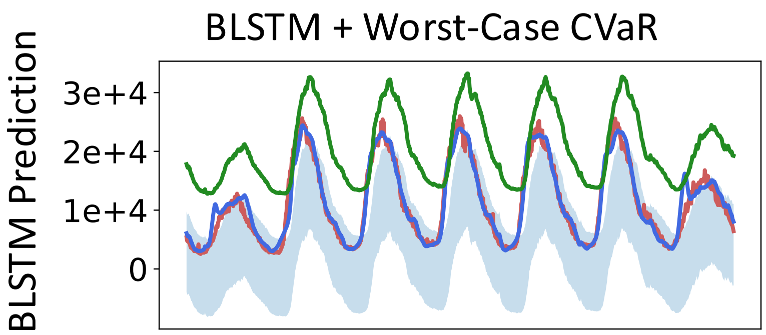
Maximum # violated cases: **0.02% - 9.68%**

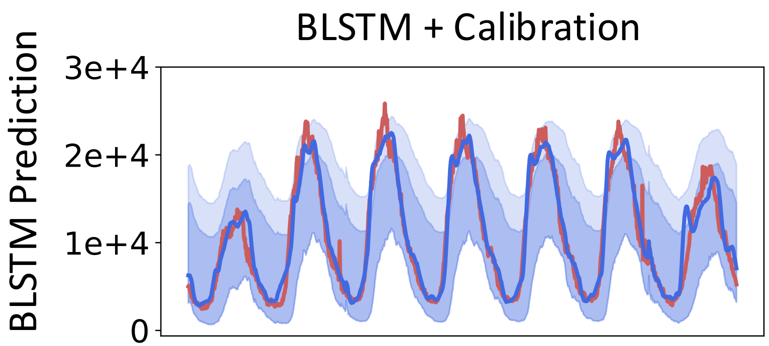
- Apply distributionally robust (CVaR) upper bound on Bayesian posterior.
  - Conservative statistical bound w.r.t. distributional uncertainty.
  - Inefficient, and still not *certifiably* robust.

Zhou, Fangtong, and Ruozhou Yu. "Moving Edge for On-Demand Edge Computing: An Uncertainty-aware Approach." *arXiv preprint arXiv:2503.24214* (2025).

Project Goals

- **Thrust 1:** Robust AI Algorithms for New Spectrum AI
  - **Goal:** Certifiable & distributional robustness for dynamic spectrum access
  - **Tools:** (1) Bayesian uncertainty quantification, (2) distributionally robust risk, (3) conformal calibration (certifiable statistical guarantee)
  - **Preliminary Results:**





Maximum # violated cases: 0.02% - 9.68%

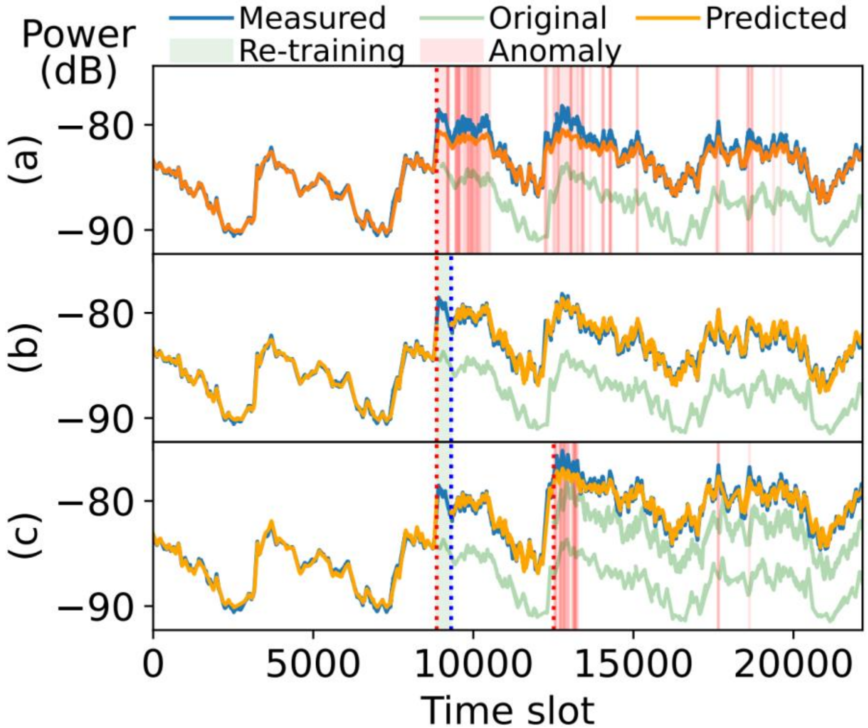
Maximum # violated cases: 2% - ~5%

  - Conformally calibrate Bayesian posterior upper 95%-CI.
    - Nice conformal certifiable robustness.
    - Does not handle well distribution shifts.

Zhou, Fangtong, and Ruozhou Yu. "Moving Edge for On-Demand Edge Computing: An Uncertainty-aware Approach." *arXiv preprint arXiv:2503.24214* (2025).

Project Goals

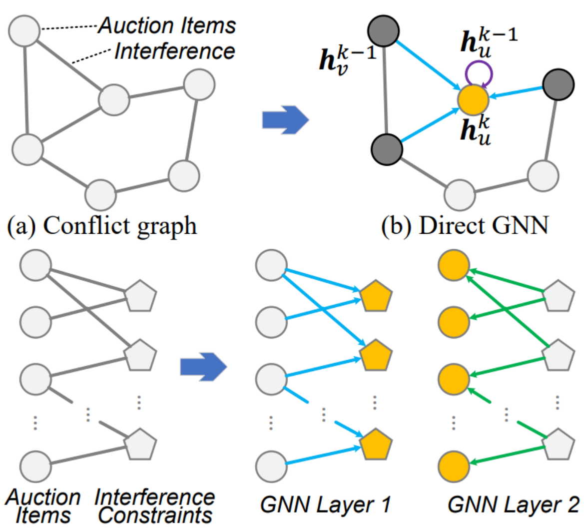
- **Thrust 2:** Robust Spectrum Data for New Spectrum AI

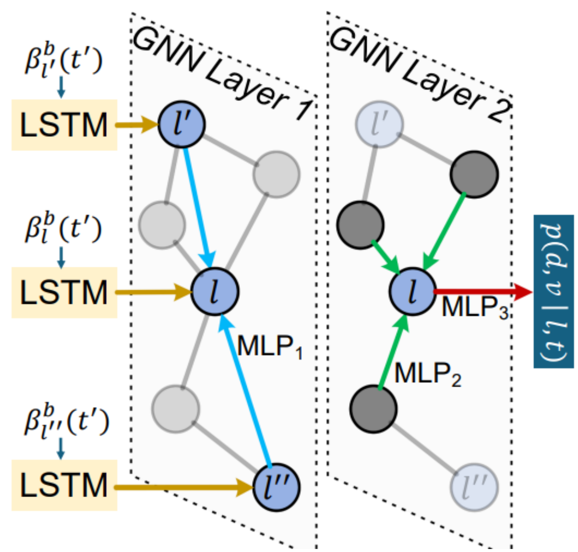


- **Goal:** Obtain trustworthy spectrum data during **spectrum handovers**
- **Tools:** (1) Cryptographic commitments and random sampling, (2) spatio-temporal-spectral learning & federated calibration

Project Goals

- **Thrust 3:** Robust Market Mechanism with New Spectrum AI
  - **Goal:** Design efficient & robust market mechanism in face of AI players
  - **Tools:** learning-based market mechanism design, with provable properties such as truthfulness, individual rationality and budget balance





Zhou, Fangtong, Xiaorui Liu, Ruozhou Yu, and Guoliang Xue. "Traffic Engineering in Large-scale Networks with Generalizable Graph Neural Networks." *arXiv preprint arXiv:2503.24203* (2025).

Thank you very much!

Q&A?

ryu5@ncsu.edu