WiFi User Re-identification: Robustness Comparison Between MLP and MJ-KAN

Hanseon Joo, Geum Vit Dal Yoon*, Eunjii Lee*, Minjong Cheon**
Hanyang Univ., Korea Racing Authority.*, Sejong Univ.**
e-mail:jmj2316@sejong.ac.kr

WiFi 사용자 재식별: MLP vs MJ-KAN 강건성 비교

주한선, 윤금빛달, 이은지*, 전민종**
한양대학교, 한국마사회*, 세종대학교**

Abstract

This study evaluates the adversarial robustness of MLP and MJ-KAN models for WiFi RSSI-based user re-identification. Using the UJI-style fingerprint benchmark, we tested both architectures against white-box attacks including FGSM and PGD. While the MLP achieved a higher clean accuracy of 0.959 compared to 0.917 for MJ-KAN, the MJ-KAN model demonstrated a different robustness profile across various attack strengths. The results highlight a trade-off between utility and robustness that depends on the attack type and modelWhile deep learning-based weather models show great promise, their high computational cost limits academic accessibility. We introduce Sonny, an efficient hierarchical transformer designed for high-performance forecasting within a modest budget. Sonny features a two-stage StepsNet (narrow slow and full-width fast paths) and employs EMA during training to ensure stable medium-range rollouts without extra fine-tuning. On WeatherBench2, Sonny remains competitive with operational systems and outperforms FastNet in tropical regions. Notably, Sonny can be trained to convergence in just 5.5 days on a single NVIDIA A40 GPU, offering a scalable solution for resource-constrained research.

1. Introduction

For decades, the cornerstone of meteorological science has been Numerical Weather Prediction (NWP) systems. These models rely on the integration of complex partial differential equations to simulate the physical laws governing atmospheric dynamics. While NWP has provided a robust framework for global forecasting, it is increasingly constrained by the immense computational resources required for high-resolution simulations and the inherent difficulties in accurately parameterizing sub-grid scale physical processes. As the demand for more precise and timely climate projections grows, the limitations of these traditional physics-based approaches—specifically their high latency and massive energy consumption—have become more pronounced.

Using a standard UJI-style RSSI fingerprint dataset, we evaluate both models against white-box attacks, including the Fast Gradient Sign Method (FGSM) and seven-step Projected Gradient Descent (PGD). By also including a random noise baseline matched in L-infinity magnitude, we isolate the sensitivity of these models to structured corruption versus gradient-based attacks. Our findings highlight a utility-robustness trade-off, where the choice between MLP and MJ-KAN may depend on the specific attack strength and the desired balance between clean accuracy and adversarial stability.

2. Materials and Methods

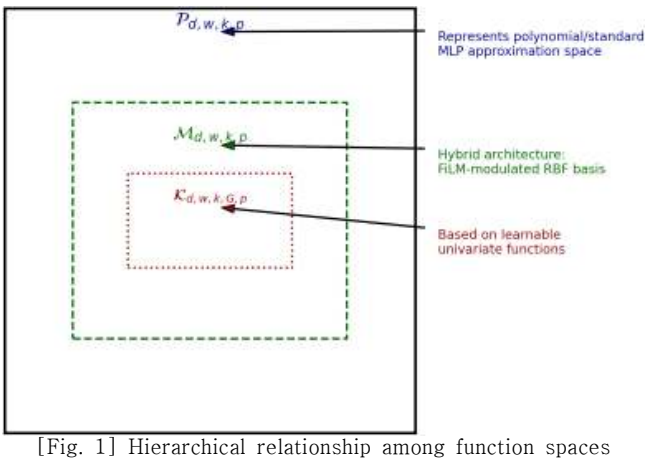
2.1 Dataset Description

The research utilizes a dataset based on UJI-style RSSI fingerprints. The primary data is sourced from a file named TrainingData.csv, specifically focusing on entries where the user ID is greater than zero. Each sample

consists of 520 Wireless Access Point (WAP) RSSI features. In cases where a signal is not detected, a model value of −105 dBm is assigned to represent the missing feature [2].

2.2 MJKAN

The MJKAN model is a hybrid neural network architecture designed to combine the mathematical power of Kolmogorov−Arnold Networks with the practical efficiency of traditional Multilayer Perceptrons. It functions by decomposing complex, high−dimensional data into simpler, one−dimensional transformations through a process called radial basis expansion. To ensure the model remains fast and easy to train, it incorporates a modulation mechanism inspired by feature−wise linear modulation. This technique allows the network to learn how to scale and shift these nonlinear signals dynamically, effectively reintroducing the efficiency of linear weights without losing expressive power. As a result, MJKAN is particularly effective for complex function modeling and general classification tasks. Furthermore, the architecture is uniquely interpretable, as its mathematical structure allows researchers to clearly see and extract the specific contribution each input feature makes to the final decision [3].



[Fig. 1] Hierarchical relationship among function spaces among MLP, MJKAN, and KAN

3. Results

The experimental evaluation reveals distinct performance characteristics for both models. In clean testing, the MLP architecture achieves a superior accuracy of 0.959, whereas the MJ−KAN model reaches 0.917. This indicates that the MLP provides higher utility under normal operating conditions.

However, the vulnerability to adversarial attacks varies by model type and the magnitude of the perturbation. At a low perturbation level of zero point one, the MJ−KAN demonstrates better resistance to the Fast Gradient Sign Method (FGSM) with an attack success rate of 0.31, compared to 0.34 for the MLP. This gap remains evident at a perturbation level of zero point five, where the MJ−KAN maintains a success rate of 0.74 against FGSM, while the MLP rises to 0.83. Even at a high perturbation level of one point zero, the MJ−KAN shows a lower attack success rate of 0.81 for FGSM, whereas the MLP reaches 0.91.

Despite these differences, the iterative Projected Gradient Descent (PGD) attack consistently outperforms FGSM across both models. At the highest tested perturbation level of one point zero, PGD achieves an attack success rate of 0.97 for the MLP and 0.98 for the MJ−KAN. These results highlight a utility−robustness trade−off, showing that while the MLP is more accurate initially, the MJ−KAN offers a different robustness profile depending on the attack strength. Finally, these evaluations characterize the mathematical fragility of the learned scores rather than physical spoofing of WiFi channels.

4. Conclusion

This study demonstrates that while the MLP architecture provides superior accuracy on clean WiFi RSSI data, the MJ−KAN model exhibits a distinct robustness profile when subjected to adversarial perturbations. The results highlight a fundamental trade−off between model utility and its stability against gradient−based attacks. Iterative attacks were found to be consistently more effective at compromising both models compared to single−step methods, revealing the inherent mathematical fragility of learned feature scores.

Furthermore, the comparison with random noise isolates how these architectures respond to structured versus unstructured feature corruption. Ultimately, this research emphasizes that the choice of architecture for

WiFi-based identity inference should not rely solely on accuracy but must consider the specific balance between raw performance and defensive strength against potential feature-space manipulations</source-footnote>. These findings characterize the internal vulnerability of neural scoring systems rather than physical spoofing of the wireless environment.

References

[1] Wei, Z., Chen, W., Ning, S., Lin, W., Li, N., Lian, B., ... & Zhao, J. (2025). A survey on WiFi-based human identification: Scenarios, challenges, and current solutions. ACM Transactions on Sensor Networks, 21(1), 1-32.

[2] Conte, S., & Hall, R. (1988). A measure of execution path complexity. Communications of the ACM, 31(2), 188-200.

[3] Joo, H., Choi, H., Lee, O., & Cheon, M. (2025). Bridging KAN and MLP: MJKAN, a hybrid architecture with both efficiency and expressiveness. ICT Express.