Review of: "Generative Artificial Intelligence Using Machine Learning on Wireless Ad Hoc Networks"

Zakwan Al-Arnaout[1]

1 American University of Middle East

Potential competing interests: No potential competing interests to declare.

This paper presents an interesting approach to using Generative Artificial Intelligence (GenAI) and Machine Learning (ML) techniques in optimizing wireless Ad Hoc networks, specifically through the application of neural networks like the Multilayer Perceptron (MLP) and Radial Basis Function (RBF). While the topic is timely and relevant, there are several areas where the paper could be improved, both in content and structure.

Strengths

1- Relevant Topic: The application of GenAI and ML to wireless networks is a contemporary and important research area, especially with the increasing reliance on wireless communication and the growing complexity of network infrastructures.

2- Clear Objectives: The paper sets clear objectives in terms of improving wireless Ad Hoc network performance and reducing blind spots through the application of ML techniques.

3- Use of Neural Networks: The choice of MLP and RBF as methods to optimize network parameters is appropriate, given their strengths in pattern recognition and data fitting.

Areas for Improvement

1- Clarity and Language:

1.a- The paper often uses overly complex language, which can make it difficult to follow. For example, sentences like "Given this situation that arises with access to data in wireless networks, we have given ourselves the task of using GAI" could be simplified for clarity.

1.b- The terminology is sometimes inconsistent or vague. For instance, the term "Generative Artificial Intelligence" is used broadly without a clear definition or distinction from other AI techniques, which could confuse readers unfamiliar with the nuances.

2- Technical Detail:

2.a- The methodology section lacks sufficient technical detail, particularly in describing how the MLP and RBF models are trained and validated. For instance, there is no discussion of the dataset size, training duration, or specific hyperparameters used, which are crucial for replicability and understanding the results.

2.b- The normalization equation provided is a standard min-max normalization, but the paper does not explain why this particular normalization technique was chosen or how it impacts the performance of the neural networks.

2.c- Illogical or Misleading Points:

- Dead Spots Leading to Unwanted Intrusion: The claim that dead spots or areas with weak signals could "allow unwanted intruders to access the wireless network" is illogical. In fact, dead spots would typically mean no signal, making it difficult for anyone, including intruders, to access the network in those areas. Weak signals could make the network more vulnerable, but the dead spots themselves wouldn't necessarily increase the risk of intrusion.
- Direct Link Between Dead Spots and Malware Infections: The statement that dead spots would lead to network infections like worms, trojans, or rumors is not directly logical. Malware infections are typically the result of compromised devices or vulnerabilities within the network, not necessarily because of dead spots or weak signals. The connection between network coverage issues and the spread of malware is not directly clear.

2.d- The figures are just cited without any discussions.

2.e- The related work does not provide any studies using Radial Basis Function (RBF) that the author is going to use. Moreover, the author is not providing a criticism for the related works to show the gap this article is going to overcome.