Robust Graph Convolutional Networks via Edge Dithering

Vassilis N. Ioannidis, and Georgios B. Giannakis

- Graph convolutional networks (GCNs) under attack
  - GCNs are vulnerable to adversarial attacks [ZG19]

Q: How to robustify semi-supervised learning (SSL)?

Idea: Use dithering to randomize the edge perturbations
Given the multiple auxiliary graphs, employ an adaptive GCN for SSL

Three modules to process the dithered graphs

Thank you!