Bayesian Node-Based Neural Networks Outperform Deterministic Models Under Adversarial Tabular Shifts

Assignee Research

June 7, 2026

Abstract

This report synthesises findings from 11 peer-reviewed papers addressing the following research question: Can node-based Bayesian neural networks enhance robustness against adversarial perturbations in tabular data more effectively than standard deterministic models under distribution shift. 13 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 3.6/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Tackling covariate shift with node-based Bayesian neural networks. Research question: Can node-based Bayesian neural networks enhance robustness against adversarial perturbations in tabular data more effectively than standard deterministic models under distribution shift?.

2 Methodology

Systematic literature search across multiple databases yielded 11 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 3.6/10.

3 Results

11 papers retrieved. 13 claims extracted; 0 independently verified. Quality review score: 3.6/10.

4 Limitations

This report is a machine-generated literature synthesis and does not constitute original research. Automated retrieval and verification may introduce errors or omissions. Review scores reflect automated assessment, not human peer review. Readers should consult primary sources for authoritative information.

5 Extracted Claims

Claim	Verified	Confidence
The datasets used are CIFAR and TINYIMAGENET, which have corrupted versions of the test set provided by Hendrycks & Diet	×	0.01
The architectures used are VGG16, RESNET18, and PREACTRESNET18.	×	0.03
Three structures of latent variables are tested: in, out, and both.	×	0.07
K $\in${1, 2, 4} Gaussian component(s) are used in the variational posterior.	×	0.03
The optimal performance on ID data is quite similar between different latent architectures.	×	0.04
On OOD, the optimal performance of using both input and output latent variables is similar to using only output latent v	×	0.07
The optimal γ is lower when the model uses both types of latent variables (z, s).	×	0.06
As γ increases, the NLL of noisy labels increases much faster than that of clean labels even when the majority of labels	×	0.03
Higher γ prevents the model from memorizing random labels.	×	0.03
Higher γ leads to improved performance on clean test sets.	×	0.03
The variational entropy decreases over time during training.	×	0.05
The model with higher entropy M32 performs better than the one with lower entropy M16 across all corruption levels.	×	0.03
λ controls the severity of the generated corruptions.	×	0.03

References

- http://arxiv.org/abs/2306.11113v2
- http://arxiv.org/abs/2206.02435v2
- http://arxiv.org/abs/2502.14833v2