Can DBNNs Robust to Environmental Noise for Resource-constrained Scenarios?

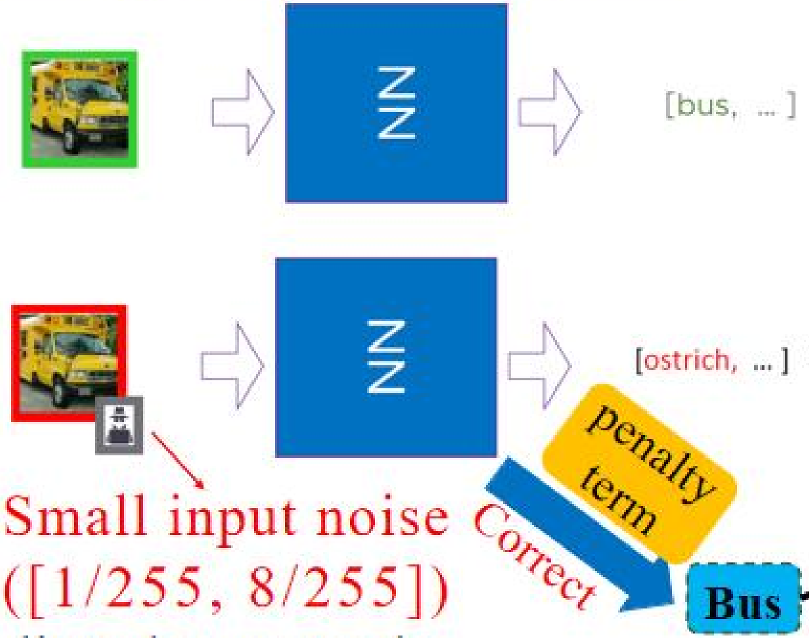
Wendong Zheng[1], Junyang Chen[2,*], Husheng Guo[1] and Wenjian Wang[1,*]

1. Shanxi University

2. Shenzhen University

Background – Environmental Noise Robustness

What is Environmental Noise Robustness?



- Small input noise ([1/255, 8/255]) disturbance to the DBNNs.

Research Significance

> ➢ The safety-critical tasks (e.g., B-ultrasound-assisted diagnostic) affected by environmental noise due to patient movement artifact, which pose significant challenges for DBNNs to perform robust inference.

- We can observe that the DBNN is not robust!
- We can get a robust decision of DBNNs by using the penalty loss function to defense environmental noise.

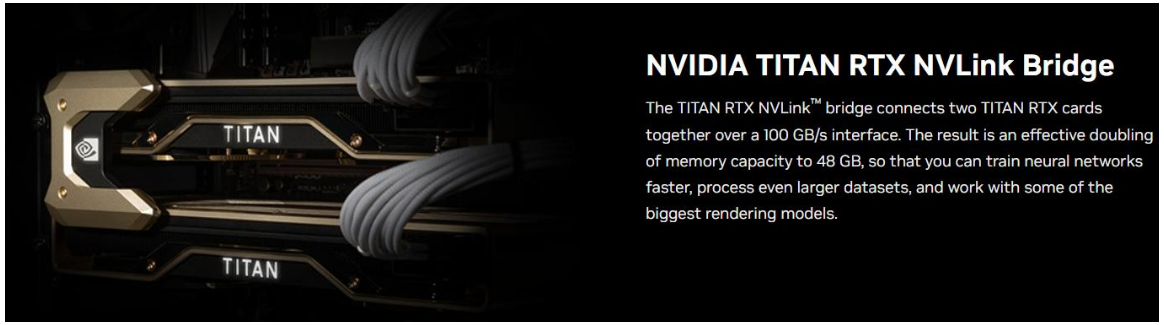
Background – High efficient DBNNs

Advantages of DBNNs

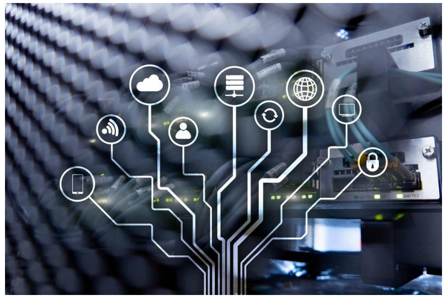
- DBNNs with low power consumption and binary weight/activations have met the performance of the best modern DNNs (i.e., ResNet34) on the several image classification tasks.

	DBNN-based models	DNN-based models
Network Structure	XNOR, bitcount computational operations	Deep convolutional structure（e.g., ResNet18,ResNet34）
Complexity	Binary weight/activation matrix (i.e., Excitation :1, inhibition : -1)	Large scale floating point computation (i.e., float 64)
Performance	Low test accuracy	High test accuracy

- High performance device, such as RTX TITAN:

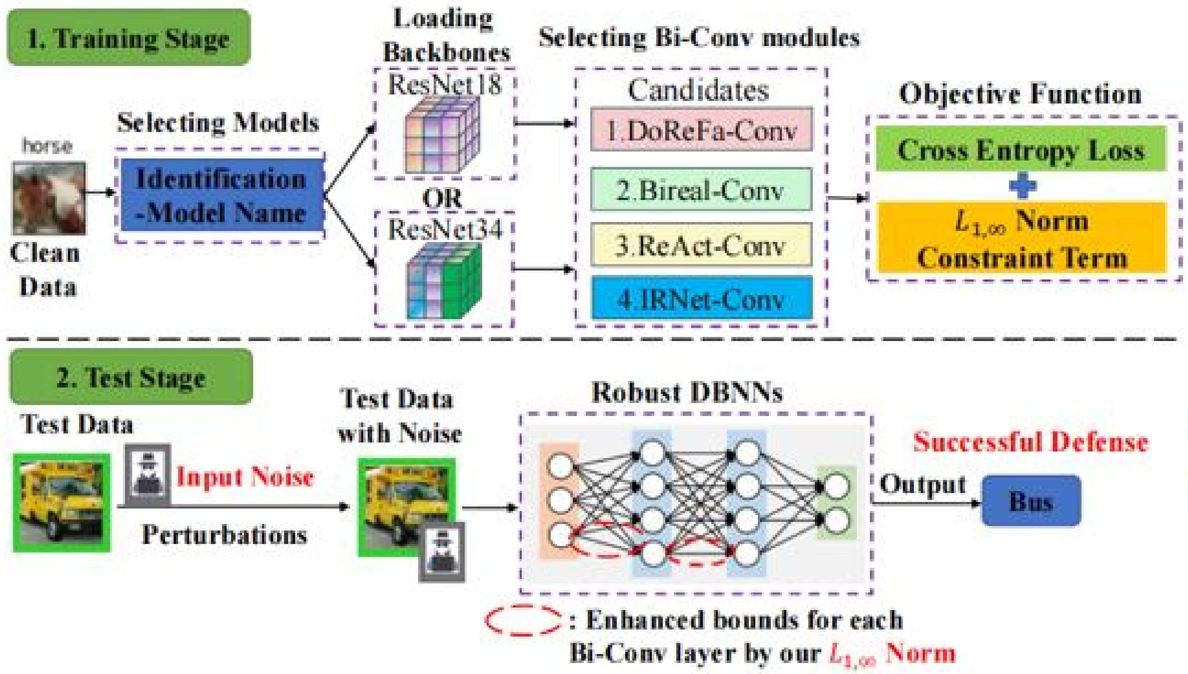


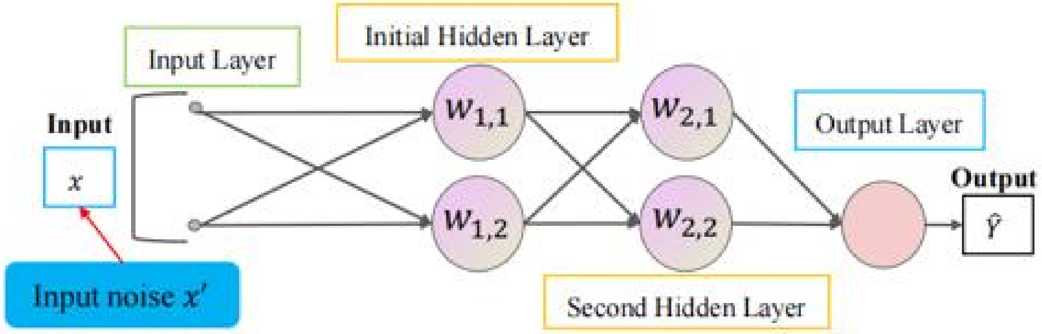
- Edge devices with limited GPU resources, such as mobile phone:



Method-Overview

- The Overview of our proposed framework and description of variables is as follows:





Method

Theoretical results

➢ The robustness of DBNNs and tightness under environmental noise is as follows:

Upper bound

Theorem 4.2. *For L-layer DBNNs against noise perturbations, we can derive the upper bound of robustness for the discrepancy between two classification outcomes (i.e., C_1 and C_2) as follows:*

$$F_{W_b}^{C_1}(\hat{x}) - F_{W_b}^{C_2}(x) \le \left(\prod_{l=1}^{L-1} \alpha_l \beta_l\right) \cdot \|W_{b;C_1}^L - W_{b;C_2}^L\|_1 \cdot \prod_{l=1}^{L-1} \|(W_b^{L-l})^T\|_{1,\infty} \prod_{M=2}^{N} \|(W_b^M)^T\|_{1,\infty} \|\hat{h}_B^{M-1} - h_B^{M-1}\|_\infty ,$$

Tightness

Corollary 4.3. *According to Eqn.12 and Eqn.15, we can determine the tightness ratio of Q binary convolution layers between our study and previous work (i.e., LCR) (Shang et al., 2022) under noise perturbation as follows:*

$$\frac{\prod_{j=1}^{Q} \|w_b^j\|_{1,\infty}}{\prod_{j=1}^{Q} L_{lip}^j} \le \frac{k \cdot \sqrt{n}}{\|W_b^j\|_2 \cdot (\gamma^{j-Q})^2} \cdot \max \frac{\|x\|_\infty}{\|x\|_1} . \quad (16)$$

Summary

- ☐ In particular, the weight is a key variable in the update process that is easy to control and understanding during the training phase.

Method-training algorithm

- Robust training for DBNNs by using our targeted objective function is as follows:

Objective function

$$\mathcal{L}_p = \delta * \prod_{j=1}^{Q} \alpha \| W_b^j \|_{1,\infty} , \qquad (18)$$

Given a classification-based objective function $\mathcal{L}_{total}$, we design a robustness loss function inside $\mathcal{L}_{total}$ through $L_{1,\infty}$-norm constrain as

$$\mathcal{L}_{total} = \mathcal{L}_{mlc}(X, Y) + \mathcal{L}_p , \qquad (19)$$

where $\mathcal{L}_{mlc}(X, Y)$ is the traditional cross-entropy loss function for multiple classification tasks. Here, the X denotes the input image signal and Y denotes the target label. Fur-

Experimental Setups

Execution Environment

- OS: Linux Ubuntu 18.04
- GPU: A800 * 1 & RTX 3090 * 1
- Software of IDE: Anaconda3, Spyder 5.2
- Programming language: Python 3.9, PyTorch 1.13

Environmental Noise with SNR

- Noise randomly applied to pixels at random locations with middle Signal to Noise Ratio (SNR) levels.
- The environmental noise perturbations on each test sample is ε = [1/255, 8/255] both on CIFAR-10 CIFAR-100 tasks.

Experimental Results

1. Main Results

Table 2. Robustness comparison between our approach and popular BNN-based methods against environmental noise on the CIFAR-10 and CIFAR-100 datasets. Here, ↑ denotes the proposed method can improve the robustness of the existing BNN-based methods.

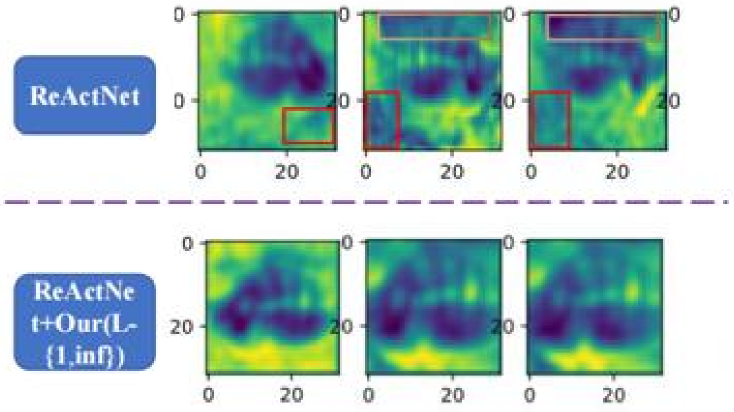
Datasets	Scenarios	Backbones	Methods								
			FP32 (clean)	DoReFa	DoReFa+our	BiReal	Bireal+our	ReAct	ReAct+our	IRNet	IRNet+our
CIFAR-10	With Noise	ResNet18	94.82	91.55	92.27↑	91.20	93.21↑	91.40	93.04↑	91.41	**93.64**↑
		ResNet34	94.17	85.16	87.04↑	87.80	**90.13**↑	87.87	89.00↑	87.88	88.31↑
CIFAR-100	With Noise	ResNet18	72.61	65.15	67.21↑	65.35	68.84↑	66.01	68.26↑	65.24	**70.04**↑
		ResNet34	71.52	60.37	61.16↑	63.76	**64.69**↑	60.48	63.81↑	60.61	61.71↑

Table 3. Robustness comparison between our strategy and three Binary Convolution structure against environmental noise on the bio-electricity series classification task.

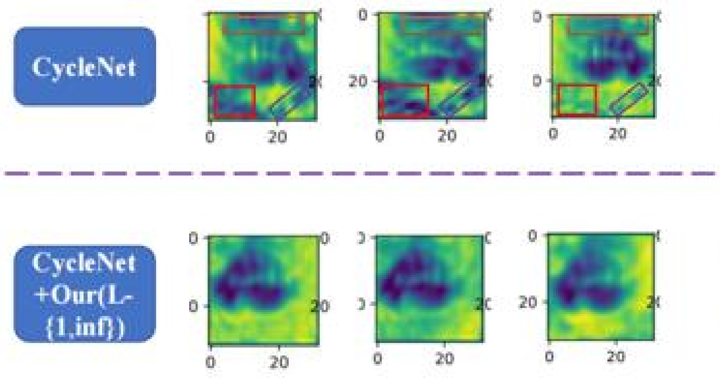
Performance	Methods						
	FP32(**clean**)	IRConv	IRConv+our	BirealConv	BirealConv+our	AdaBinConv	AdaBinConv+our
Test Acc. with Noise	97.1	87.21	**88.36**↑	88.66	**89.51**↑	93.13	**93.72**↑

Experimental Results

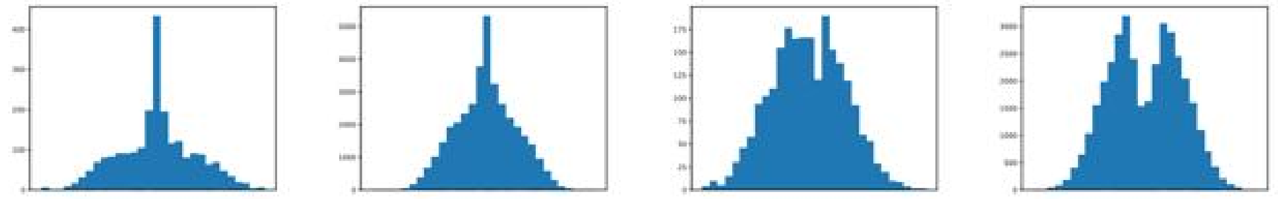
2. Visualization results



(a) ReActNet V.S. ReActNet+our

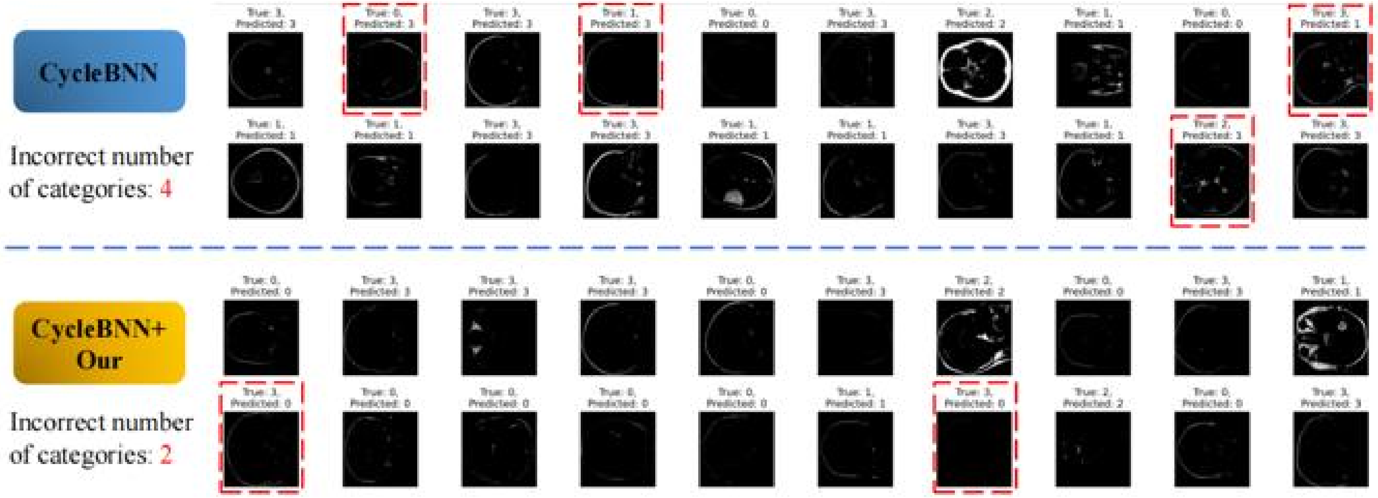


(b) CycleNet V.S. CycleNet+our



(a) IRNet layer1 conv2 (b) IRNet layer3 conv2 (c) Our+IRNet layer1 conv2 (d) Our+IRNet layer3 conv2

Figure 7. The distributions of learnable parameters in two binary convolution layers are compared on the CIFAR-10 by using our method and IRNet.



Conclusion

◆Summary highlights conclusion:

- Based on our theoretical findings, targeted objective function that penalizes the binary weights of DBNNs during the training process.
- Our proposed bounds more compact than state-of-the-art baselines.

Thank you very much for your patience, if you have any questions please do not hesitate to contact me via the email (wendongz@sxu.edu.cn).

SHANXI UNIVERSITY 1902

SCHOOL OF COMPUTER & INFORMATION TECHNOLOGY

深圳大学
SHENZHEN UNIVERSITY