Collaboration! Towards Robust Neural Methods for Routing Problems

Jianan Zhou[1], Yaoxin Wu[2], Zhiguang Cao[3], Wen Song[4], Jie Zhang[1], Zhiqi Shen[1]

[1]Nanyang Technological University [2]Eindhoven University of Technology [3]Singapore Management University [4]Shandong University

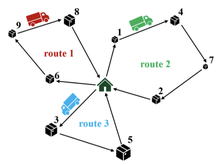
TLDR

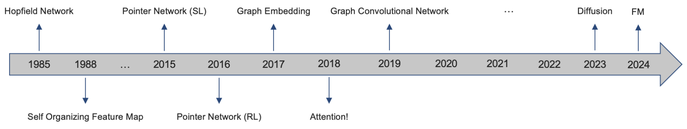
Improving the generalization of neural combinatorial solvers through the lens of adversarial robustness.

Introduction

Routing Problems

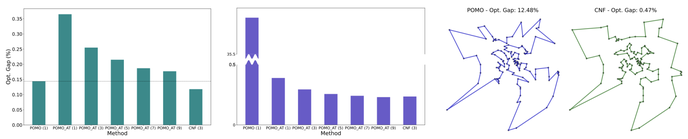
- A class of NP-hard combinatorial optimization problems
- Find an optimal solution that satisfies all constraints
- Exact solvers (e.g., Gurobi)
- Heuristic solvers (e.g., LKH3)
- Neural solvers





Are NCO Solvers Robust?

- DNNs suffer from adversarial robustness issues → How about NCO solvers?



(a) Performance on Clean Instances

(b) Performance on Adversarial Instances

(c) Illustration of Robustness Issue

Preliminary

Adversarial Training

$$\min_{\theta} \mathbb{E}_{(x,y)\sim\mathcal{D}}[\ell(y, f_\theta(\tilde{x}))], \text{ with } \tilde{x} = \arg\max_{\tilde{x}_i \in \mathcal{N}_\epsilon[x]} [\ell(y, f_\theta(\tilde{x}_i))]$$

Attacker - Attribute Perturbation

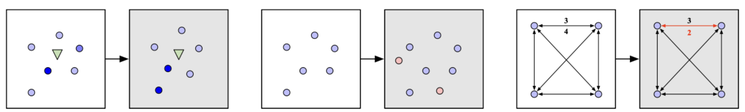
- Perturb node coordinates, node demands, …

Attacker - Node Insertion

- Needs the optimal solution to $\tilde{x}$
- Maximally diverge the model prediction from the derived optimal solution

Attacker - No-Worse Theoretical Optimum

- Enlarge the feasible region (e.g., by relaxing constraints)
- Ensure $c(\tilde{x}) \leq c(x) \leq c(x|\theta) < c(\tilde{x}|\theta)$

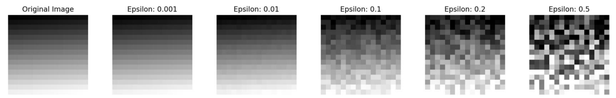


Takeaway

Free the attacker!

- Attack as a way of generating "hard" COP instances
- All generated "adversarial" instance can be valid COP instances
- Do not constrain the attacker's strength within a small range

Vision



Language

Original:	*The quick brown fox jumps over the lazy dog*
Character-level:	*The quikc brown fox jumps oevr the lazy dog*
Word-level:	*The swift brunet fox leaps above the sluggish canine*
Sentence-level:	*A speedy auburn animal vaults past a drowsy hound*
Semantic shift:	*Fast chestnut critter bounds near inert beast*

Leverage the model capacity!

- No free lunch theorem of ML
- No single model performs best across all possible tasks
- One only outperforms others when tailored to a specific task

Methodology

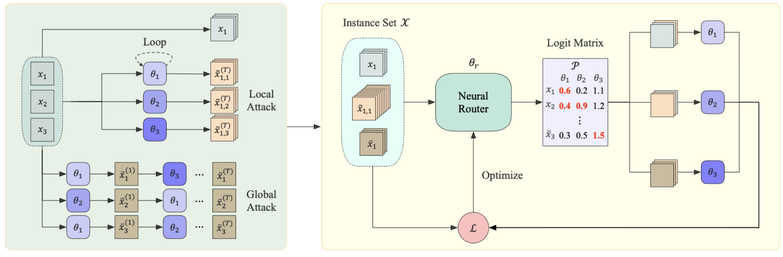


Figure 2: The overview of CNF. Suppose we train $M = 3$ models ($\Theta = \{\theta_1, \theta_2, \theta_3\}$) on a batch ($B = 3$) of clean instances. The inner maximization generates local ($\tilde{x}$) and global ($\bar{x}$) adversarial instances within T steps. In the outer minimization, a neural router θ_r is jointly trained to distribute instances to the M models for training. Specifically, based on the logit matrix $\mathcal{P}$ predicted by the neural router, each model selects the instances with Top$\mathcal{K}$-largest logits (e.g., red ones). The neural router is optimized to maximize the improvement of collaborative performance after each training step of Θ. For simplicity, we omit the superscripts of instances in the outer minimization.

Collaborative Neural Framework

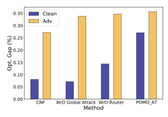
- Ensemble-based adversarial training
- Inner Maximization - Instance Generation
  - Clean instance
  - Local adversarial instance
  - Global adversarial instance
- Outer Minimization - Policy Optimization
  - An attention-based neural router trained with RL
  - Reward: the performance improvement
  - Alternative: Population-based RL (Poppy)

Experiment

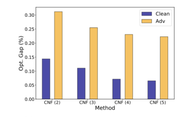
		$n = 100$						$n = 200$					
		Uniform (100)		Fixed Adv. (100)		Adv. (100)		Uniform (200)		Fixed Adv. (200)		Adv. (200)	
		Gap	Time	Gap	Time	Gap	Time	Gap	Time	Gap	Time	Gap	Time
TSP	Concorde	0.000%	0.3m	0.000%	0.3m	–	–	0.000%	0.6m	0.000%	0.6m	–	–
	LKH3	0.000%	1.3m	0.002%	2.1m	–	–	0.000%	3.9m	0.005%	5.8m	–	–
	POMO (1)	0.144%	0.1m	35.803%	0.1m	35.803%	0.1m	0.736%	0.5m	63.477%	0.5m	63.477%	0.5m
	POMO_AT (1)	0.365%	0.1m	0.390%	0.1m	0.330%	0.1m	2.151%	0.5m	1.248%	0.5m	1.154%	0.5m
	POMO_AT (3)	0.255%	0.3m	0.295%	0.3m	0.243%	0.3m	1.884%	1.5m	1.090%	1.5m	1.011%	1.5m
	POMO_HAC (3)	0.135%	0.3m	0.344%	0.3m	0.316%	0.3m	0.683%	1.5m	1.308%	1.5m	1.273%	1.5m
	POMO_DivTrain (3)	0.255%	0.3m	0.297%	0.3m	0.254%	0.3m	1.875%	1.5m	1.093%	1.5m	1.026%	1.5m
	CNF_Greedy (3)	0.187%	0.3m	0.314%	0.3m	0.280%	0.3m	0.868%	1.5m	1.108%	1.5m	1.096%	1.5m
	CNF(3)	**0.118%**	0.3m	**0.236%**	0.3m	**0.217%**	0.3m	**0.614%**	1.5m	**0.954%**	1.5m	**0.952%**	1.5m
CVRP	HGS	0.000%	6.6m	0.000%	14.6m	–	–	0.000%	0.4h	0.000%	1.2h	–	–
	LKH3	0.538%	18.1m	0.344%	23.0m	–	–	1.116%	0.5h	0.761%	0.6h	–	–
	POMO (1)	1.209%	0.1m	3.983%	0.1m	3.983%	0.1m	2.122%	0.6m	16.173%	0.8m	16.173%	0.8m
	POMO_AT (1)	1.456%	0.1m	0.882%	0.1m	0.935%	0.1m	3.249%	0.6m	1.384%	0.6m	1.435%	0.6m
	POMO_AT (3)	1.256%	0.3m	0.767%	0.3m	0.809%	0.3m	2.919%	1.8m	1.253%	1.8m	1.296%	1.8m
	POMO_HAC (3)	1.085%	0.3m	0.829%	0.3m	0.848%	0.3m	1.974%	1.8m	1.374%	1.8m	1.367%	1.8m
	POMO_DivTrain (3)	1.254%	0.3m	0.754%	0.3m	0.809%	0.3m	2.946%	1.8m	1.220%	1.8m	1.302%	1.8m
	CNF_Greedy (3)	1.112%	0.3m	0.785%	0.3m	0.821%	0.3m	**1.969%**	1.8m	1.316%	1.8m	1.353%	1.8m
	CNF(3)	**1.073%**	0.3m	**0.730%**	0.3m	**0.769%**	0.3m	2.031%	1.8m	**1.193%**	1.8m	**1.198%**	1.8m

– For traditional methods, *Adv.* is not shown since the test adversarial dataset is different for each neural method.

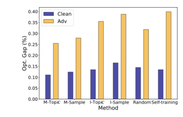
Ablation Study



(a) Ablation study on Components

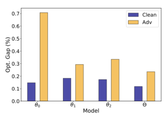


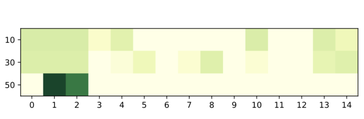
(b) Ablation study on Hyperparameters



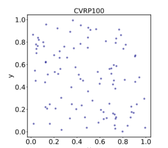
(c) Ablation study on Routing Strategies

Analysis

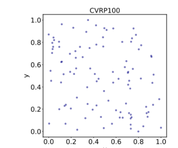




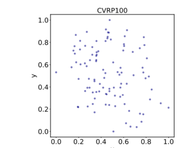
Visualization



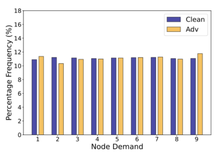
(a) Clean Instances



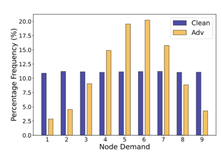
(b) Adversarial Instances (Weak)



(c) Adversarial Instances (Strong)



(d) Adversarial Instances (Weak)



(e) Adversarial Instances (Strong)

Contacts & Links

- Email: jianan004@e.ntu.edu.sg
- Links of Homepage, Paper, and Code:

The 38th Annual Conference on Neural Information Processing Systems (NeurIPS 2024)