Adversarial Bounding Box Generation (ABBG) Attack against Visual Object Trackers

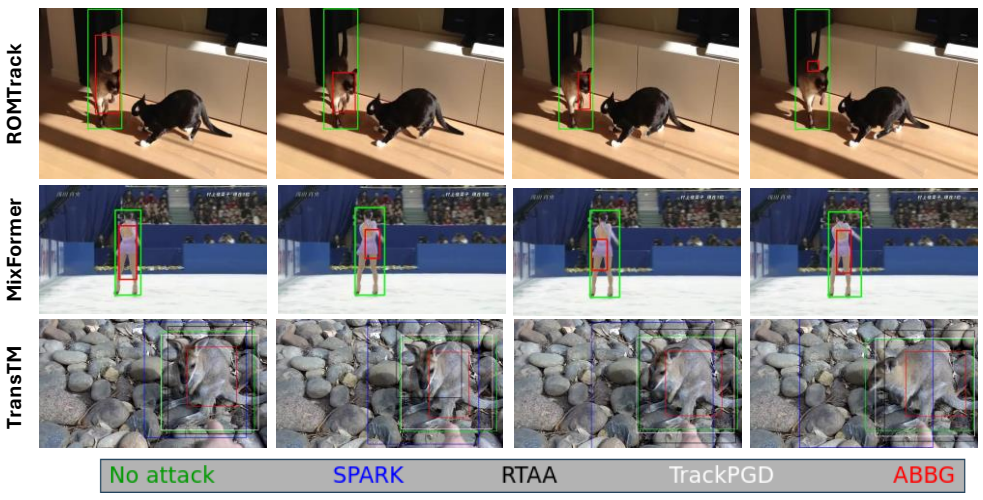
Fatemeh Nourilenjan Nokabadi[1,2,3], Jean-François Lalonde[1,2], Christian Gagné[1,2,3,4]

[1]IID, [2]Université Laval, [3]Mila, [4]Canada CIFAR AI Chair

NEURAL INFORMATION PROCESSING SYSTEMS

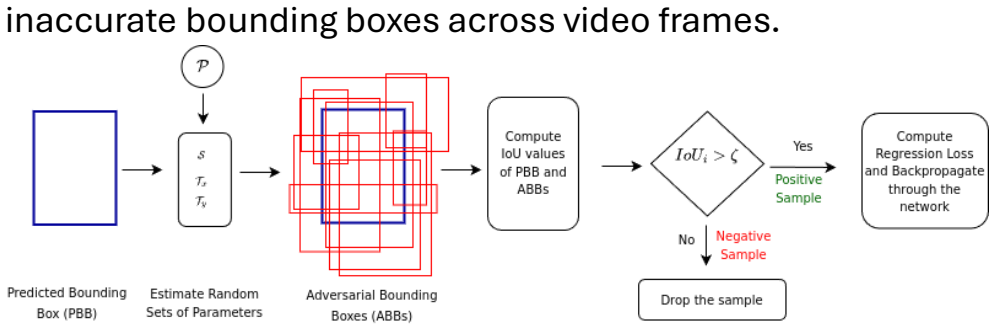
Introduction & Contributions

- The attack proxies are available in some tracking frameworks but are not available in other tracking pipelines.
- AABG attack uses only a single bounding box to challenge the object trackers robustness against adversarial perturbations in a white-box setting.
- AABG attack is ranked first in several tracking datasets per at least one evaluation metric.
- Regarding the sparsity and imperceptibility of perturbations, ABBG is ranked 2nd in comparison to other white box attacks.

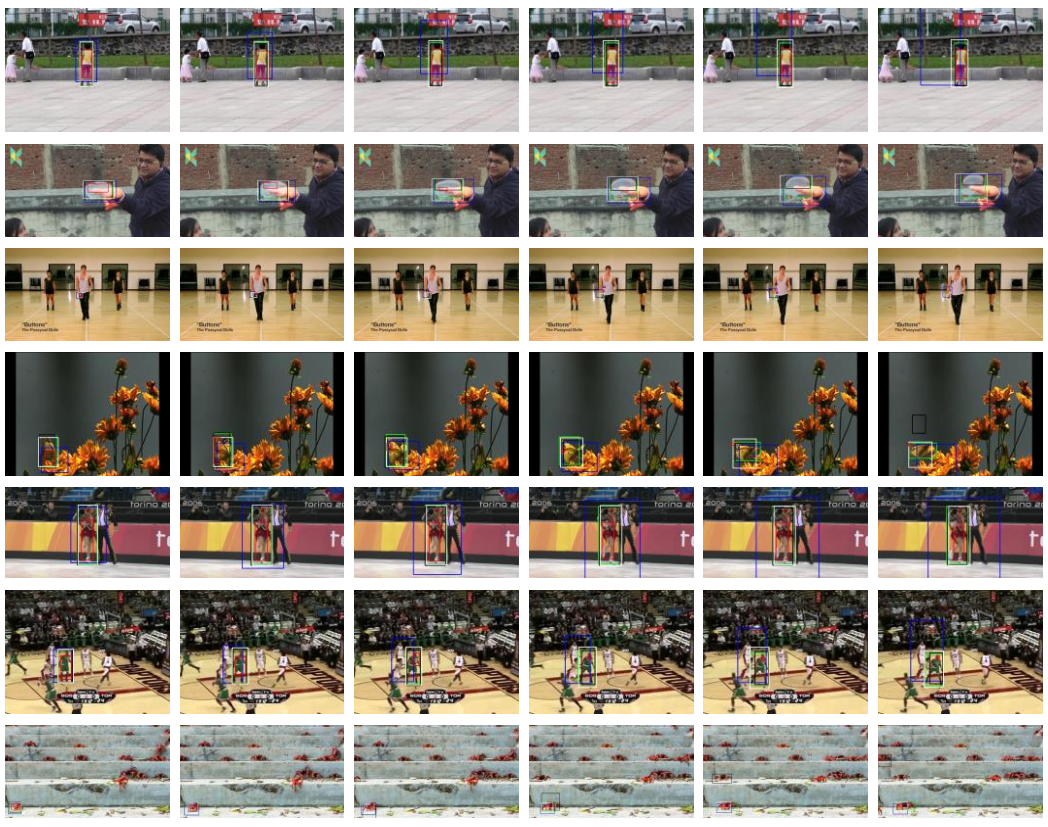


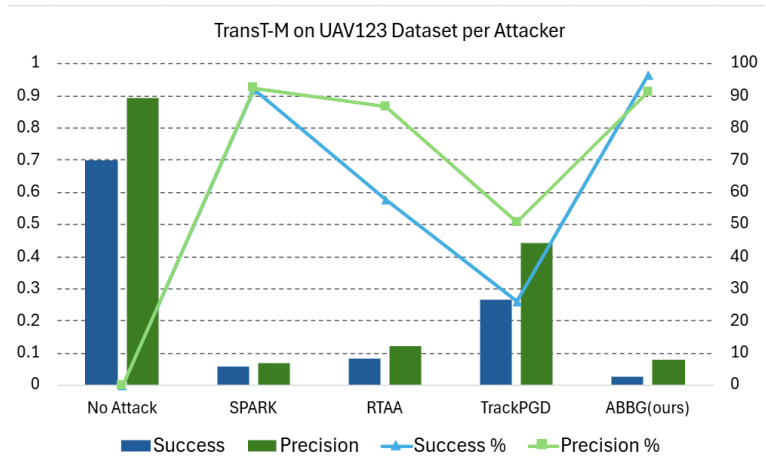
Proposed Method

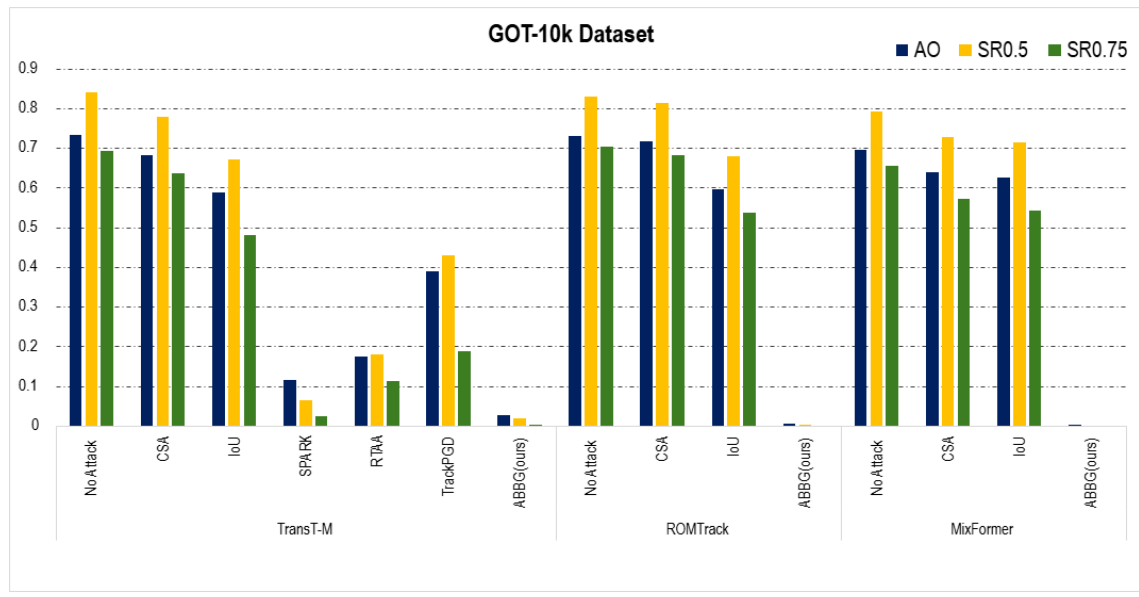
Our goal is to mislead transformer trackers into predicting inaccurate bounding boxes across video frames.



Object Bounding Box Evaluation

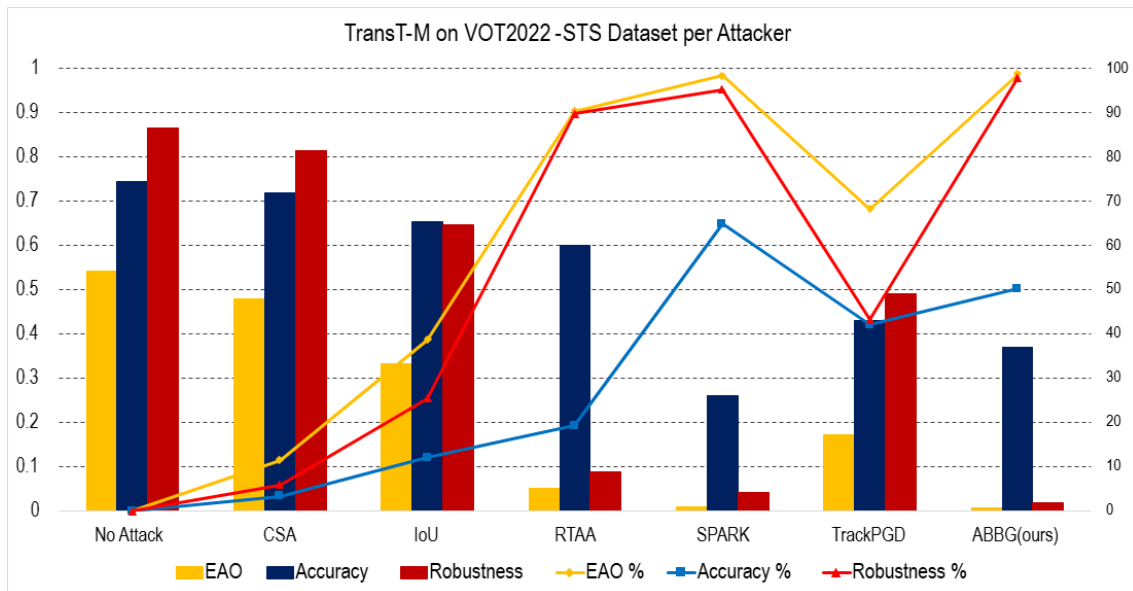






Main Takeaway: Among white-box attacks, ABBG is applicable to all three trackers- TransT-M, ROMTrack, and MixFormer. Beyond this versatility, the ABBG attack causes significant drops in all scores.

Object Binary Mask Evaluation



Main Takeaway: ABBG outperforms other white-box attacks (RTAA, SPARK, and TrackPGD) on the TransT-M tracker, except in accuracy, where it ranks second to SPARK.

Sparsity and Imperceptibility

Tracker	Attacker	L1-Norm ↓	SSIM(%) ↑
TransT-M	SPARK	69.98	94.43
	RTAA	113.48	60.14
	TrackPGD	122.52	64.04
	ABBG (ours)	95.77	89.50

Main Takeaway: ABBG ranks 2nd to SPARK overall but outperforms it in perturbation effectiveness on GOT-10k and VOT2022ST.

Acknowledgments. This work is supported by the DEEL Project CRDPJ 537462-18 funded by the Natural Sciences and Engineering Research Council of Canada (NSERC) and the Consortium for Research and Innovation in Aerospace in Quebec (CRIAQ), together with its industrial partners Thales Canada inc, Bell Textron Canada Limited, CAE inc and Bombardier inc.

Institut intelligence et données · Université Laval · Mila · DEEL DEpendable & Explainable Learning