Models and Hypotheses

Table 1: Detection models and attack losses. Full details are given in Appendix **??**.

			Attack Losses[c]		
			Targeted		
Detectors	Stages[a]	COCO mAP[b]	Vanishing	Mislabeling	Untargeted[d]
YOLOv3	1	33.7	Object	Class	Class, Box, Object
SSD	1	29.5	Class	Class	Class, Box
RetinaNet	1	36.5	Class	Class	Class, Box
Faster R-CNN	2	37.4	RPN: Object; Det: Class	Det: Class	RPN: Object, Box; Det: Class, Box
Cascade R-CNN	2	40.3	RPN 1: Object; RPNs 2, 3 + Det: Class	RPNs 2, 3: Class; Det: Class	RPN 1: Object, Box; RPNs 2, 3 + Det: Class, Box

[a] In general, 1-stage detectors are quicker whereas 2-stage detectors are more accurate, though the 1-stage RetinaNet aims to be both quick and accurate. In a 2-stage detector, the input image passes through a Region Proposal Network (RPN) stage and a detection (Det) stage.

[b] COCO mean Average Precision (mAP) is the primary metric on the COCO challenge.

[c] The training losses in detectors typically include the box regression loss (Box), the class loss on the 80 COCO labels and/or the background class (Class), and the objectness loss on categorizing an image region as background or object (Object).

[d] Untargeted attack targets all training losses in a model, i.e. the backpropagation loss.

Table 2: Hypothesis testing in the randomized attack (Sections **??** and **??**)

Hypotheses (higher success for)	Accepted (across attacks and models)[a]
1-stage > 2-stage models (YOLOv3, SSD, RetinaNet > Faster R-CNN, Cascade R-CNN)	YOLOv3, SSD > RetinaNet, Faster R-CNN, Cascade R-CNN in vanishing and mislabeling attacks (1-stage RetinaNet is as resilient as 2-stage models)
Targeted > Untargeted attack	YOLOv3 only
Vanishing > Mislabeling attack	All
Larger attack iterations	All
Less confident targets	All
Larger perturb boxes	All except mislabeling attack on Faster R-CNN
Shorter perturb-target distance	All
Less accurate target COCO class	Mixed
Lower target IOU[b] (untargeted attack only)	All
More probable intended class (mislabeling attack only)	Mixed

[a] $p < .05$ for Wald z-test on logistic estimate

[b] intersection-over-union