ECCV'20 ONLINE
23-28 AUGUST 2020

16TH EUROPEAN CONFERENCE ON
COMPUTER VISION

WWW.ECCV2020.EU

SPARK: Spatial-aware Online Incremental Attack Against Visual Tracking

Qing Guo, Xiaofei Xie, Felix Juefei-Xu, Lei Ma,
Zhongguo Li, Wanli Xue, Wei Feng, and Yang Liu

NANYANG TECHNOLOGICAL UNIVERSITY

A New Attack Task Against Visual Object Tracking

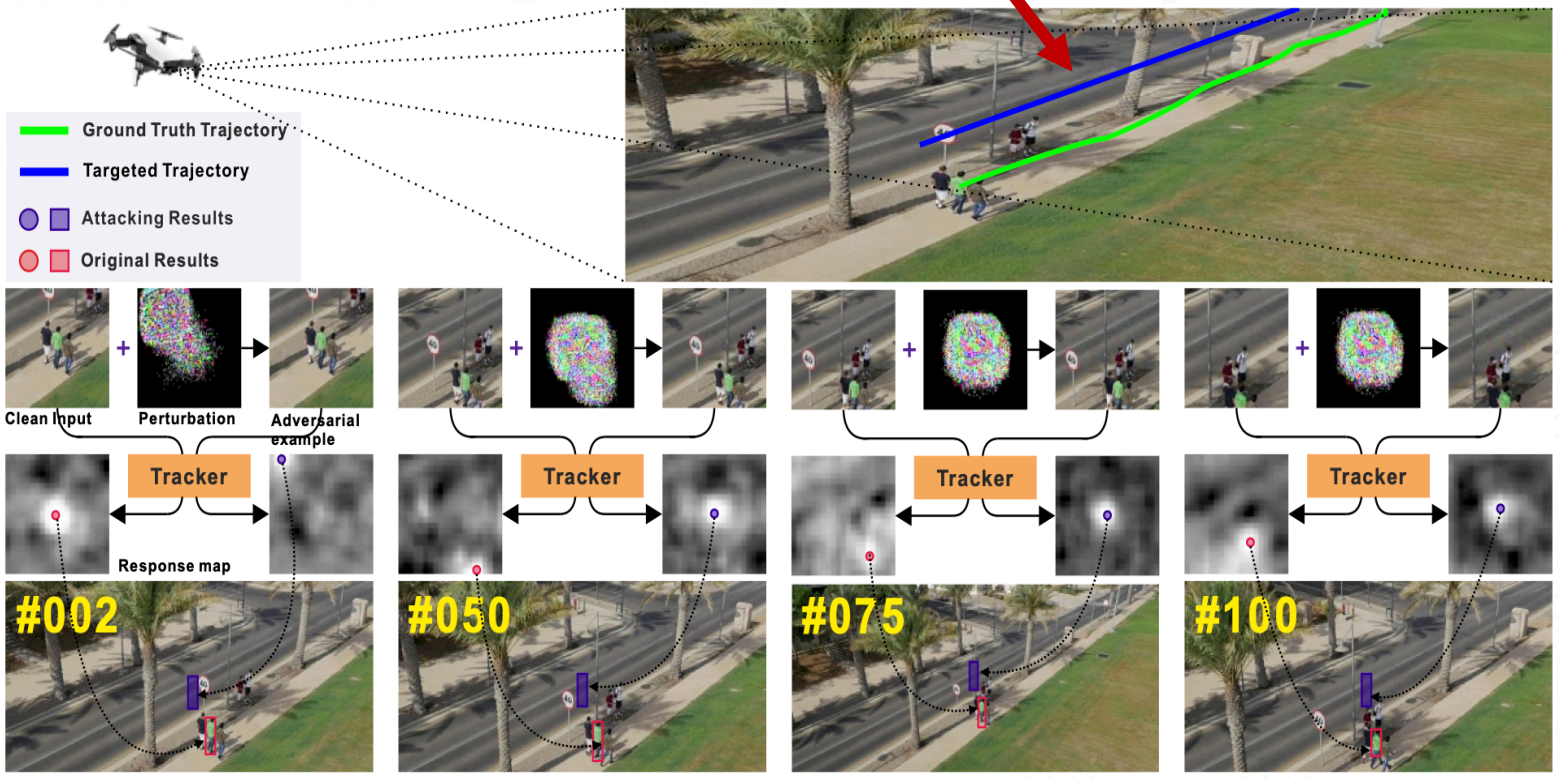
SPARK: Spatial-aware Online Incremental Attack Against Visual Tracking

Motivation

- Adversarial examples (AEs) could mislead trackers embedded in a car or UAV, causing navigation into dangerous environments and even resulting in severe accidents.
- Difference to classification-related AI tasks: online visual tracking mainly focus on the object's moving trajectory instead of its category.
- New challenges to adversarial attack techniques: 1. ***Limited online sequential data***. Attacks can only change the coming frame. 2. ***High efficiency***. Attacks should be efficient to meet the real-time trackers.

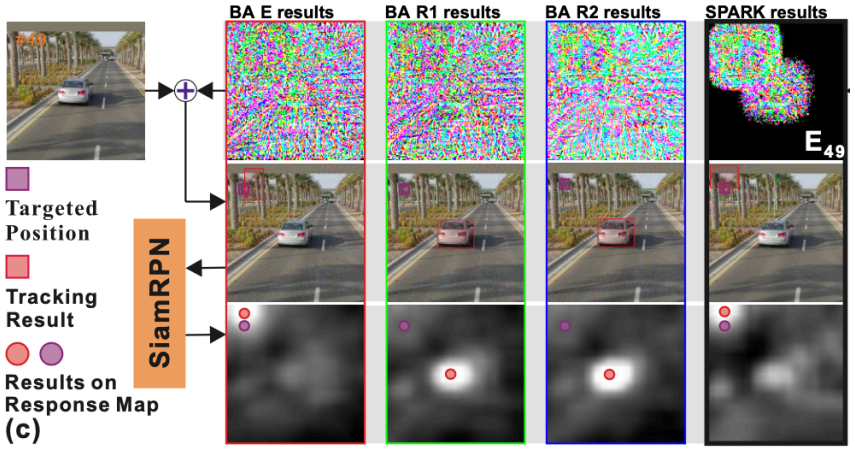
New Task

- Online generating imperceptible perturbations to ***mislead trackers along an incorrect (Untargeted Attack) or specified trajectory (Targeted Attack)***



Spatial-aware Basic Attack: Challenges

SPARK: Spatial-aware Online Incremental Attack Against Visual Tracking



➢ **Basic Untargeted Attack (UA):**

$$\text{minimize} \quad \mathcal{D}(\mathbf{X}_t, \mathbf{X}_t + \mathbf{E}_t)$$

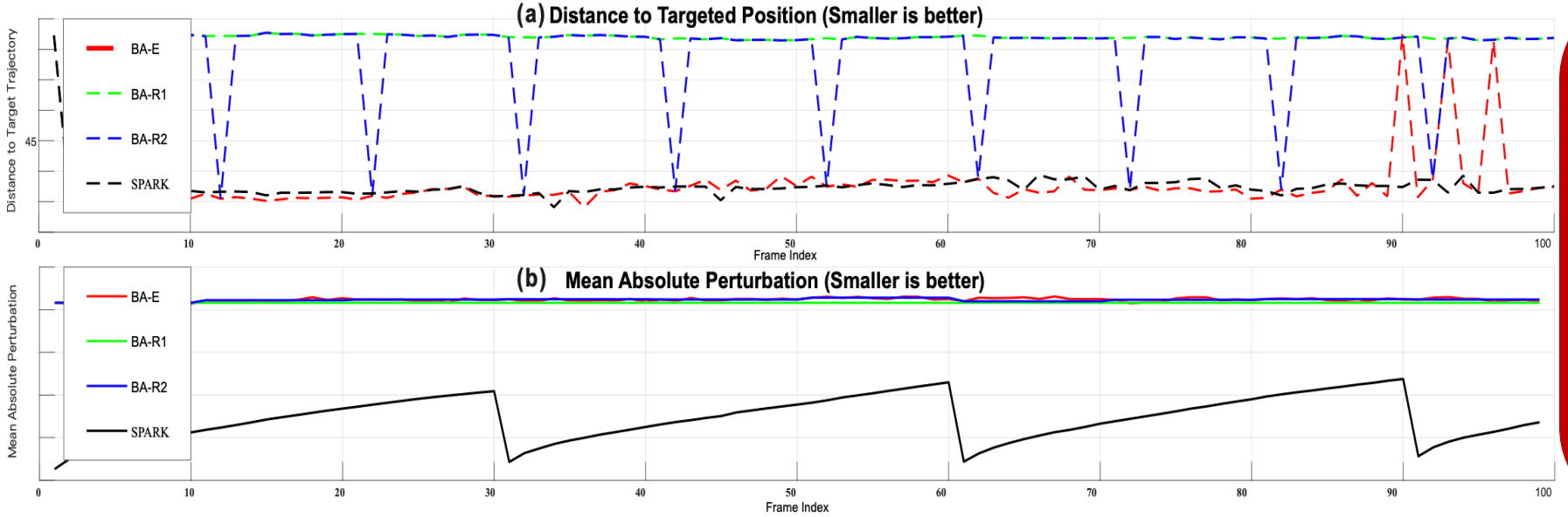
$$\text{subject to} \quad \text{IoU}(OT'(\mathbf{X}_t + \mathbf{E}_t, \mathbf{T}), \mathbf{b}_t^{\text{gt}'}) = 0$$

➢ **Basic Targeted Attack (TA):**

$$\text{minimize} \quad \mathcal{D}(\mathbf{X}_t, \mathbf{X}_t + \mathbf{E}_t)$$

$$\text{subject to} \quad ce(OT'(\mathbf{X}_t + \mathbf{E}_t, \mathbf{T})) = \mathbf{p}_t^{\text{tr}}$$

➢ The ***basic attack (BA)***, i.e., naively adapting existing attacks (e.g., FGSM, BIM, and C&W) to UA&TA against visual tracking, ***shows new challenges***:



- ❖ it is difficult to generate imperceptible perturbations that can transfer across frames
- ❖ real-time trackers require the attack to satisfy a certain level of efficiency.

Spatial-aware Online Incremental Attack

SPARK: Spatial-aware Online Incremental Attack Against Visual Tracking

➢ SPARK Untargeted Attack (UA):

$$\text{minimize} \quad \mathcal{D}(\mathbf{X}_t, \mathbf{X}_t + \mathbf{E}_{t-1} + \epsilon_t)$$

$$\text{subject to} \quad \text{IoU}(OT'(\mathbf{X}_t + \mathbf{E}_{t-1} + \epsilon_t, \mathbf{T}), \mathbf{b}_t^{\text{gt}'}) = 0$$

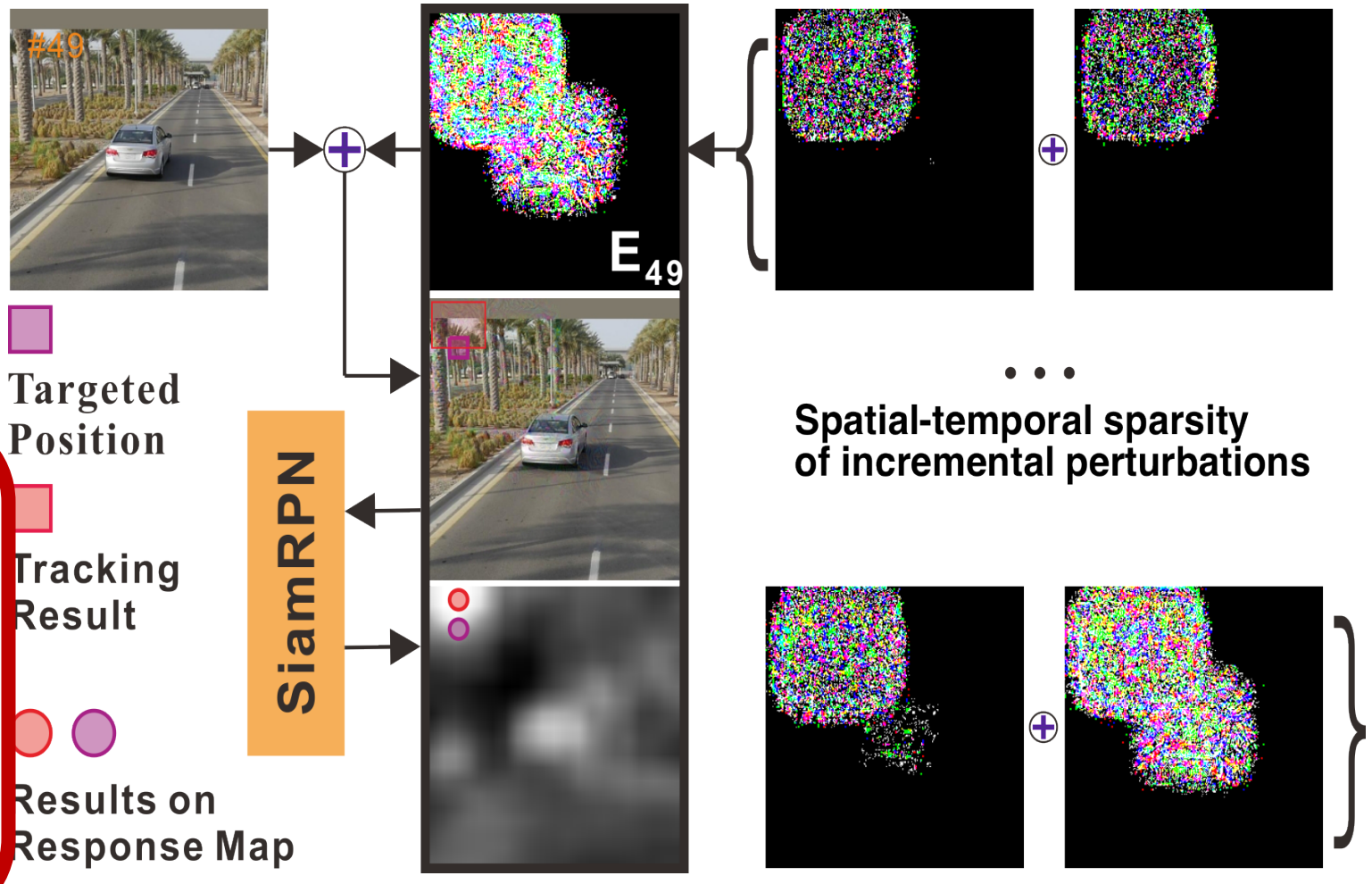
➢ SPARK Targeted Attack (TA):

$$\text{minimize} \quad \mathcal{D}(\mathbf{X}_t, \mathbf{X}_t + \mathbf{E}_{t-1} + \epsilon_t)$$

$$\text{subject to} \quad ce(OT'(\mathbf{X}_t + \mathbf{E}_{t-1} + \epsilon_t, \mathbf{T})) = \mathbf{p}_t^{\text{tr}}$$

➢ Advantages of SPARK:

- ***Spatial-temporal sparsity of incremental perturbations:*** small perturbations with high attack success rates.
- ***Efficient optimization***: attacking with average 2.25 iterations per frame while achieving 78.9% success rate.



Experimental Results

SPARK: Spatial-aware Online Incremental Attack Against Visual Tracking

SiamRPN	Attacks	Untargeted Attack (UA)						Targeted Attack (TA)			
		OTB100			VOT2018			OTB100		VOT2018	
		Org. Prec. (%)	Prec. Drop (%)	MAP	Org. Prec. (%)	Prec. Drop (%)	MAP	Succ. Rate (%)	MAP	Succ. Rate (%)	MAP
AlexNet	FGSM	85.3	8.0	1.24	65.8	13.6	1.24	7.9	1.24	4.3	1.24
	BIM	85.3	72.1	2.17	65.8	57.4	2.28	38.8	2.14	48.5	2.10
	MI-FGSM	85.3	68.4	3.70	65.8	58.2	4.31	41.8	3.18	47.0	3.17
	C&W	85.3	54.2	1.31	65.8	50.6	1.26	25.7	1.27	25.7	1.23
	Wei	85.3	25.9	0.21	65.8	33.6	0.30	16.0	0.27	20.9	0.24
	SPARK	85.3	78.9	1.04	65.8	61.6	1.03	74.6	1.36	78.9	1.38
Mob.	FGSM	86.4	6.7	1.00	69.3	14.1	0.99	7.9	1.00	3.4	0.99
	BIM	86.4	37.8	1.07	69.3	46.2	1.06	30.3	1.06	32.9	1.05
	MI-FGSM	86.4	42.3	1.71	69.3	46.6	1.73	33.5	1.70	32.7	1.71
	C&W	86.4	23.6	1.04	69.3	28.2	1.02	13.7	1.05	8.9	1.01
	Wei	86.4	39.4	0.84	69.3	27.8	0.54	11.3	0.51	7.0	0.53
	SPARK	86.4	54.1	1.66	69.3	55.5	1.25	51.4	1.65	45.5	1.21
Res50	FGSM	87.8	4.5	0.99	72.8	8.1	0.99	7.7	0.92	2.9	0.99
	BIM	87.8	27.0	1.10	72.8	39.1	1.10	17.1	1.09	17.0	1.08
	MI-FGSM	87.8	31.9	1.72	72.8	41.8	1.75	18.8	1.71	19.5	1.72
	C&W	87.8	14.6	1.03	72.8	20.4	1.01	10.0	1.04	5.3	1.01
	Wei	87.8	9.7	0.65	72.8	15.7	0.68	9.7	0.78	4.8	0.69
	SPARK	87.8	29.8	1.67	72.8	54.3	1.26	23.8	1.70	39.5	1.26

SiamRPN	Attacks	Untargeted Attack (UA)						Targeted Attack (TA)			
		UAV123			LaSOT			UAV123		LaSOT	
		Org. Prec.	Prec. Drop	MAP	Org. Prec.	Prec. Drop	MAP	Succ. Rate	MAP	Succ. Rate	MAP
AlexNet	FGSM	76.9	3.7	1.25	43.5	4.0	1.22	3.7	1.25	4.70	1.22
	BIM	76.9	36.4	1.70	43.5	32.0	1.64	28.7	1.75	17.4	1.73
	MI-FGSM	76.9	31.5	2.54	43.5	31.6	2.50	28.3	2.53	17.8	2.46
	C&W	76.9	17.0	1.37	43.5	19.9	1.29	11.0	1.36	8.7	1.28
	Wei	76.9	5.6	0.31	43.5	9.3	0.29	6.8	0.37	6.9	0.31
	SPARK	76.9	43.6	1.13	43.5	38.2	0.93	54.8	1.06	48.9	1.09

- The in-depth evaluation of state-of-the-art trackers ***(i.e., SiamRPN++ with AlexNet, MobileNetv2, and ResNet-50, and SiamDW) on OTB100, VOT2018, UAV123, and LaSOT*** demonstrates the effectiveness and transferability of SPARK in misleading the trackers under both UA and TA with minor perturbations.