TASAR: Transfer-based Attack on Skeletal Action Recognition

Yunfeng Diao, Baiqi Wu†, Ruixuan Zhang, Ajian Liu, Xiaoshuai Hao, Xingxing Wei, Meng Wang, He Wang†

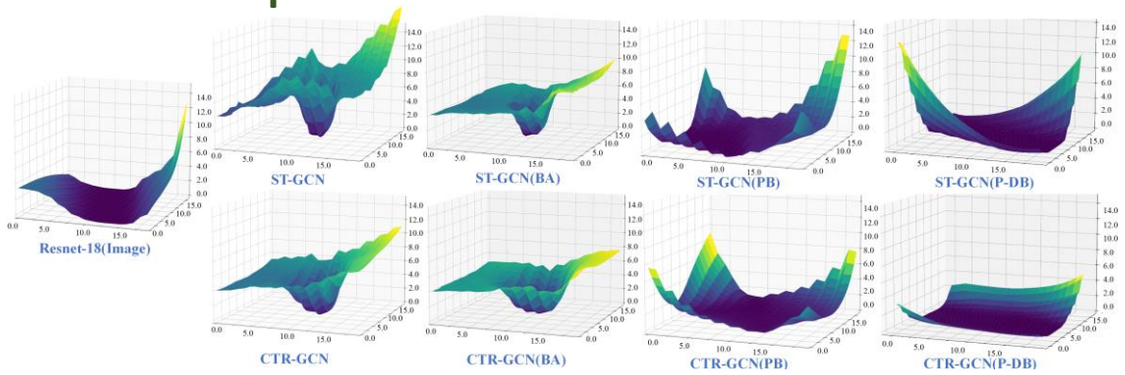
UNIVERSITY COLLEGE LONDON

What Happened in the Skeletal Action Recognition (SAR)?

SAR (important topic) classifiers are susceptible to white-box adversarial attack.

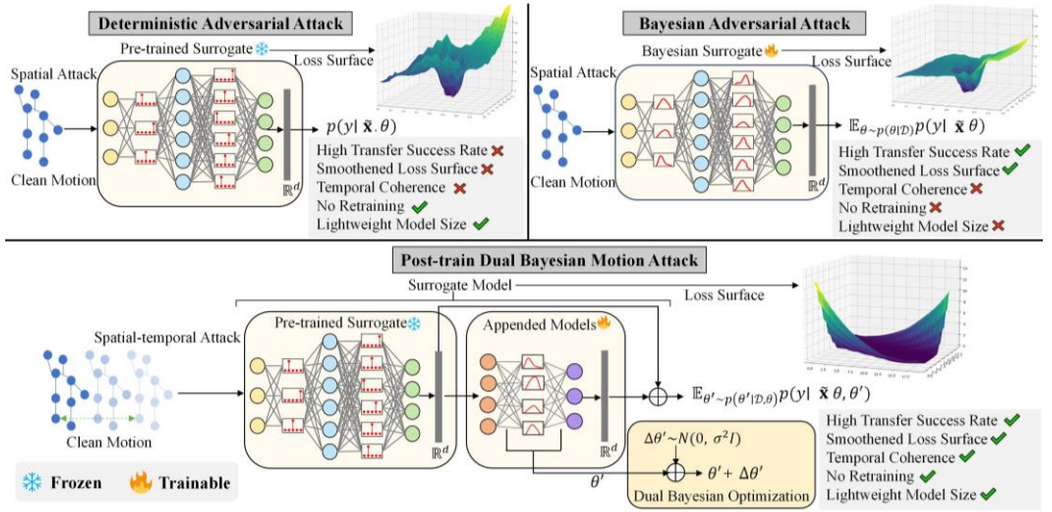
However, transfer-based attack on SAR classifiers is generally poor and unreliable.

The Loss Landscape of SAR Classifiers.



- **Sharper Loss Surface:** Models trained on SAR exhibit a much sharper loss landscape than those trained on images, resulting in reduced transferability.
- **Limited Adversarial Transfer:** Adversarial examples confined to these steep regions seldom transfer across SAR models.

The Post-Train Dual Bayesian Optimization Strategy



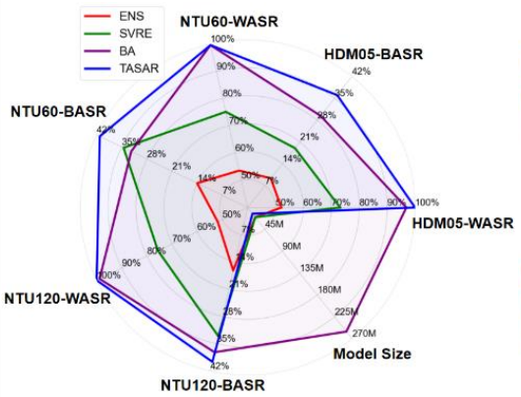
- **Post-train Bayesian:** Appending a tiny Bayesian component behind pre-trained surrogate.
- **Dual Bayesian Strategy:** Learning a **smoother** posterior for appended models.
- **Temporal Gradient:** Consider temporal gradient in a Bayesian manner.

Experiments

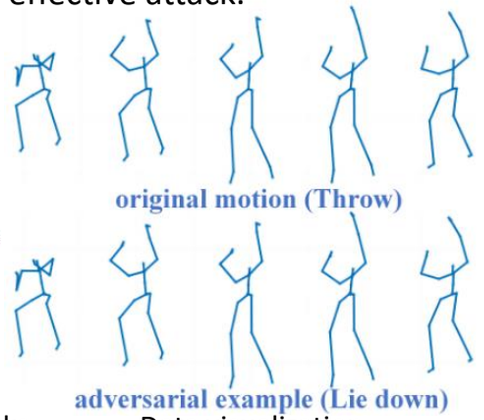
The attack success rate of transfer-based attacks

Surrogate	Method	Dataset: NTU60 Target Models STGCN	2sAGCN	MSG3D	CTRGCN	FRHEAD	SFormer	Ave	Dataset: NTU120 Target Models STGCN	2sAGCN	MSG3D	CTRGCN	FRHEAD	SFormer	Ave
STGCN	IFGSM	99.26	11.76	8.33	14.22	16.42	15.44	13.23	96.81	8.82	7.10	13.97	16.42	24.75	14.21
	MI	**100.00**	17.76	27.20	14.95	26.59	11.76	19.65	99.63	18.75	**28.18**	15.07	20.22	23.03	21.05
	SMART	93.28	5.62	2.19	6.88	7.19	10.08	6.39	94.06	8.28	7.66	11.09	10.16	16.12	10.66
	CIASA	**100.00**	3.43	3.43	7.60	9.80	8.33	6.52	**100.00**	4.16	4.41	9.07	8.08	14.95	8.13
	MIG	99.50	25.49	39.60	19.80	36.50	**18.14**	27.91	98.01	17.45	23.01	15.22	**23.76**	21.53	20.19
	DIM	77.97	20.54	34.03	12.13	28.83	13.11	21.73	75.61	10.76	12.25	12.75	16.21	23.01	15.00
	TASAR	99.29	**42.55**	**64.60**	**20.33**	**49.41**	17.22	**38.82**	99.26	**19.60**	19.37	**15.28**	22.79	**25.24**	**20.46**
MSG3D	IFGSM	25.49	22.79	**100.00**	20.10	24.75	16.66	21.96	26.96	16.42	**100.00**	15.20	18.38	27.20	20.83
	MI	22.42	13.72	**100.00**	14.83	20.22	12.25	16.69	25.49	12.25	**100.00**	14.46	16.78	22.30	18.26
	SMART	21.66	8.96	**100.00**	12.50	13.54	12.09	13.75	31.25	13.96	**100.00**	16.04	17.92	23.38	20.51
	CIASA	17.40	5.88	**100.00**	11.27	11.51	11.76	11.56	22.79	5.88	**100.00**	11.03	12.50	19.11	14.26
	MIG	31.92	39.65	**100.00**	24.44	36.15	23.06	31.04	32.17	27.22	**100.00**	23.27	31.18	33.54	29.48
	DIM	28.58	47.27	**100.00**	17.82	35.27	17.69	29.33	30.94	38.24	**100.00**	19.43	30.19	29.82	29.72
	TASAR	**48.87**	**51.18**	99.61	**41.49**	**40.14**	**23.90**	**41.11**	**41.16**	**47.28**	**100.00**	**28.83**	**40.60**	**40.37**	**39.65**
CTRGCN	IFGSM	27.45	16.54	13.72	95.22	44.97	20.71	24.68	33.33	14.95	14.33	97.30	31.00	31.49	25.02
	MI	25.36	23.52	36.51	99.02	51.34	19.85	31.32	30.14	19.73	29.16	99.26	29.16	28.30	27.30
	SMART	15.00	5.00	4.69	99.69	15.31	9.27	9.85	19.75	5.84	4.63	99.60	9.27	17.13	11.32
	CIASA	14.70	4.65	5.88	**99.75**	15.93	9.31	10.09	19.60	5.88	4.65	**99.75**	10.53	16.91	11.51
	MIG	28.86	35.34	48.19	93.55	53.46	21.04	37.38	30.94	24.75	32.67	94.18	34.03	29.45	30.37
	DIM	23.01	14.97	15.59	53.16	34.71	17.51	21.16	29.51	19.49	24.87	62.31	25.37	23.63	24.57
	TASAR	**33.76**	**52.31**	**66.74**	97.06	**58.32**	**21.07**	**46.44**	**33.59**	**26.22**	**33.82**	92.89	**35.78**	**32.84**	**32.45**
STFormer	IFGSM	23.03	15.19	11.27	14.95	16.42	13.48	15.72	26.26	13.97	12.99	15.44	20.83	24.50	19.00
	MI	18.13	12.29	19.36	12.25	19.36	10.78	15.36	26.22	21.07	32.35	15.20	22.54	23.77	23.53
	SMART	21.77	6.04	6.04	11.29	10.08	10.88	11.02	23.79	9.27	4.43	9.27	12.90	21.37	13.51
	CIASA	18.62	6.37	5.39	10.54	10.78	10.78	10.41	24.01	10.53	6.61	11.03	15.19	22.30	14.95
	MIG	22.31	21.44	18.89	16.77	23.44	16.77	19.94	30.54	20.32	21.88	16.46	21.25	24.87	22.55
	DIM	23.39	33.04	32.67	15.47	28.71	14.72	24.67	29.82	15.84	14.72	13.99	19.05	24.50	19.65
	TASAR	**26.44**	**54.32**	**42.78**	**16.35**	**37.98**	**18.38**	**32.71**	**34.61**	**34.61**	**46.63**	**19.71**	**32.21**	**26.92**	**32.45**

Our approach achieves the most effective attack.



Compared to ensemble&Bayesian attacks



Data visualization

RobustBenchHAR

The first large-scale robust SAR benchmark, comprising **7 SAR models**, **10 attack methods**, **3 SAR datasets** and **2 defense models**.

Paper, code, checkpoints and data are all available:

https://github.com/yunfengdiao/Skeleton-Robustness-Benchmark

[1] Yunfeng Diao,Baiqi Wu, Ruixuan Zhang et al, TASAR, ICLR'2025