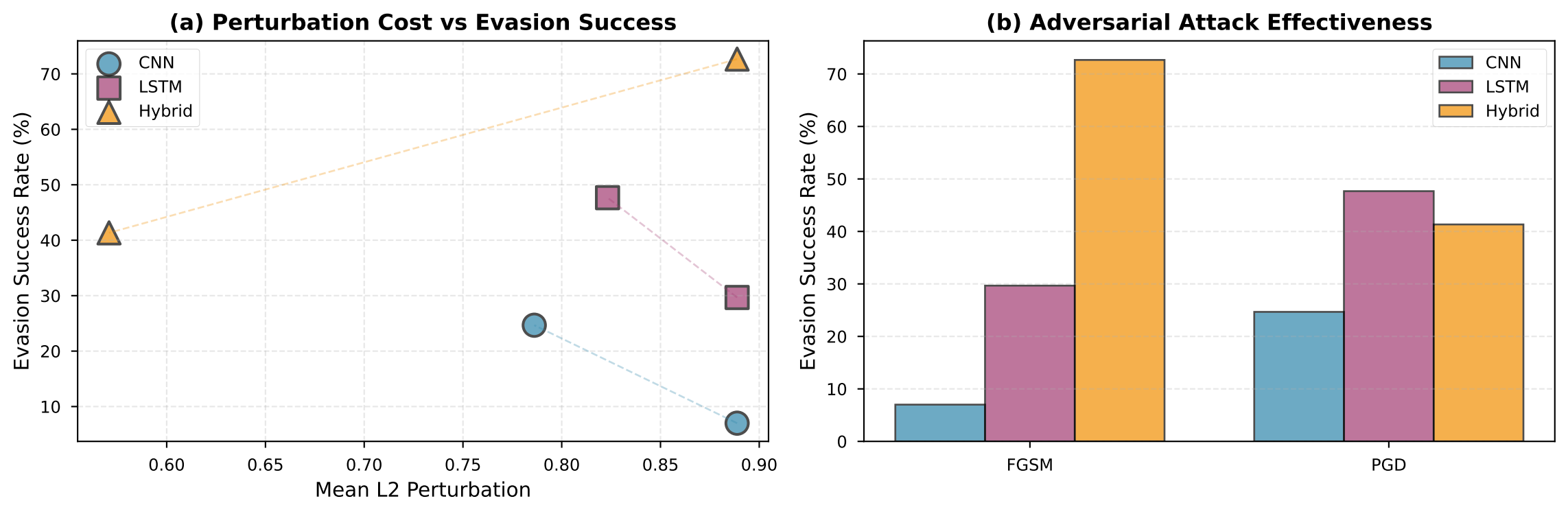
(a) Perturbation Cost vs Evasion Success
CNN
LSTM
Hybrid
Evasion Success Rate (%)
Mean L2 Perturbation
10
20
30
40
50
60
70
0.60
0.65
0.70
0.75
0.80
0.85
0.90
(b) Adversarial Attack Effectiveness
CNN
LSTM
Hybrid
Evasion Success Rate (%)
0
10
20
30
40
50
60
70
FGSM
PGD