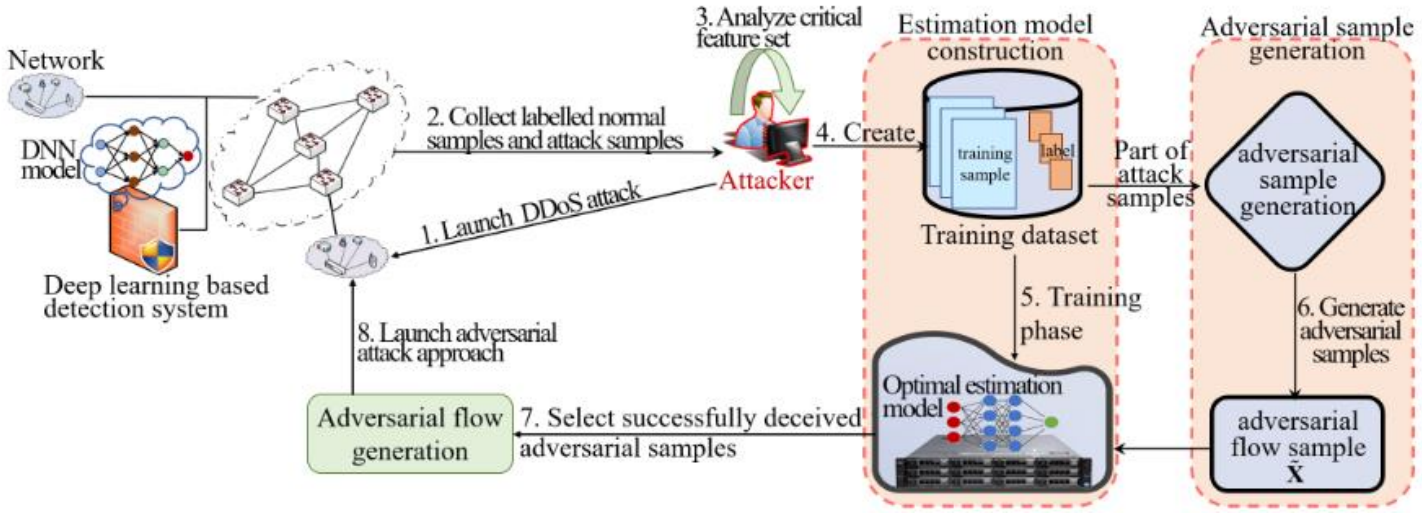
Robustness on Deep Learning based DDoS Detection: An Adversarial Study

Hui SHAO, Jianjun LI, Wei RUAN, Jing LAI

Frontiers of Computer Science, DOI: 10.1007/s11704-026-51877-4

Problems & Ideas

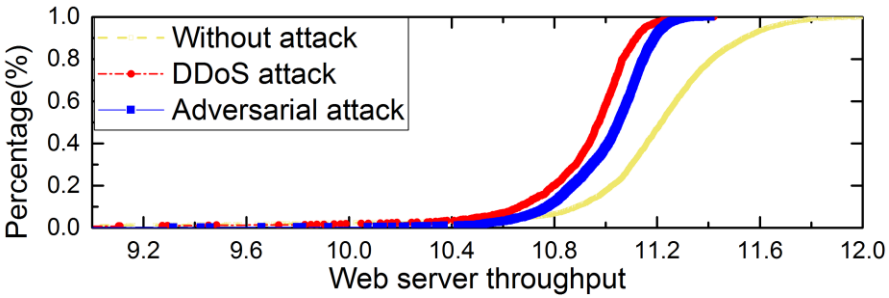
- Problems of adversarial approaches for Deep Learning based DDoS Detection:
  - Assume prior knowledge about the detection model.
  - Focus solely on classification evasion without network protocol constraints.
- Ideas: Reduce the detection accuracy of deep learning based detection systems by deceiving their built-in deep learning based detection models while maintaining DDoS attack effect.

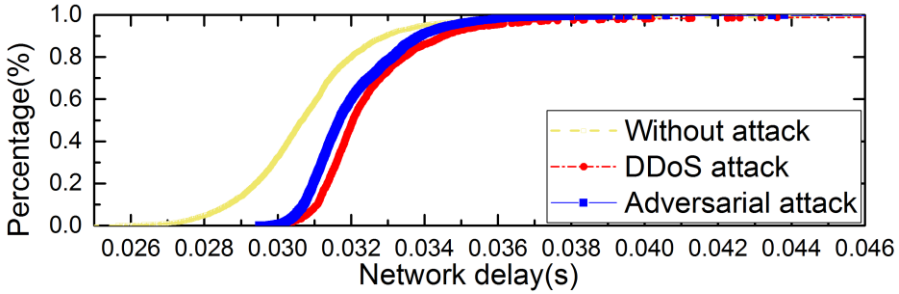


The principles of adversarial attack approach against deep learning based DDoS detection system.

Main Contributions

- Contributions:
  - We explore a feasible adversarial attack approach against deep learning based DDoS detection systems when the detail of input features and detection model remains unknown.
  - We provide the corresponding defense method for preventing the proposed adversarial attack approach
  - We conduct and evaluate the proposed adversarial approach and its defense method based on a real-world network topology and dataset.





the proposed adversarial approach is capable of reducing the detection accuracy markedly and the defense method is effective in mitigating the negative impact of the adversarial samples