NetRadar: Enabling Robust Carpet Bombing DDoS Detection

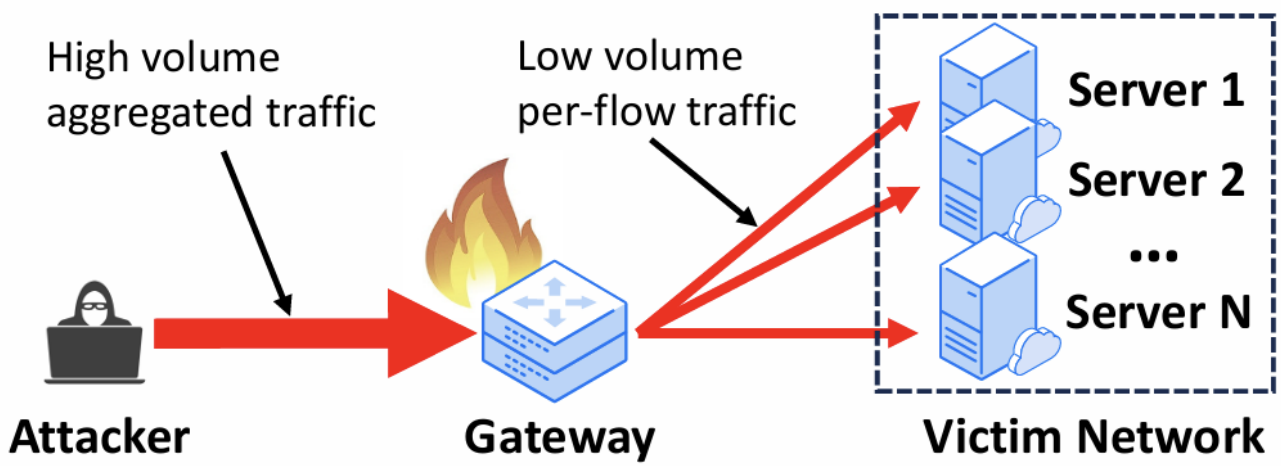
Junchen Pan, Lei Zhang, Xiaoyong Si, Jie Zhang,

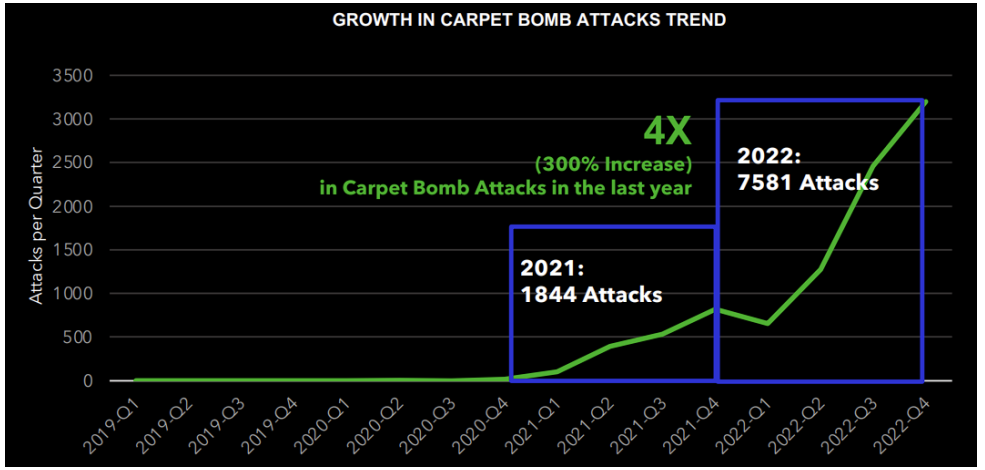
Xinggong Zhang, Yong Cui

Tencent 腾讯

Carpet Bombing DDoS

- Characteristics: Distribute and Aggregate
  - Malicious traffic is distributed to a large number of victim servers and aggregates at the gateway, cutting off the victim network.





An increasingly severe threat in recent years

Challenge in Carpet Bombing Detection

- Low-Rate Application-Layer Carpet Bombing

Appears benign in terms of both traffic volume and semantics.

Challenge in Carpet Bombing Detection

- Low-Rate Application-Layer Carpet Bombing

Appears benign in terms of both traffic volume and semantics.

- Dynamic Attack Behavior
  - Each time interval, attacker may select victim combinations and redistribute DDoS budget.

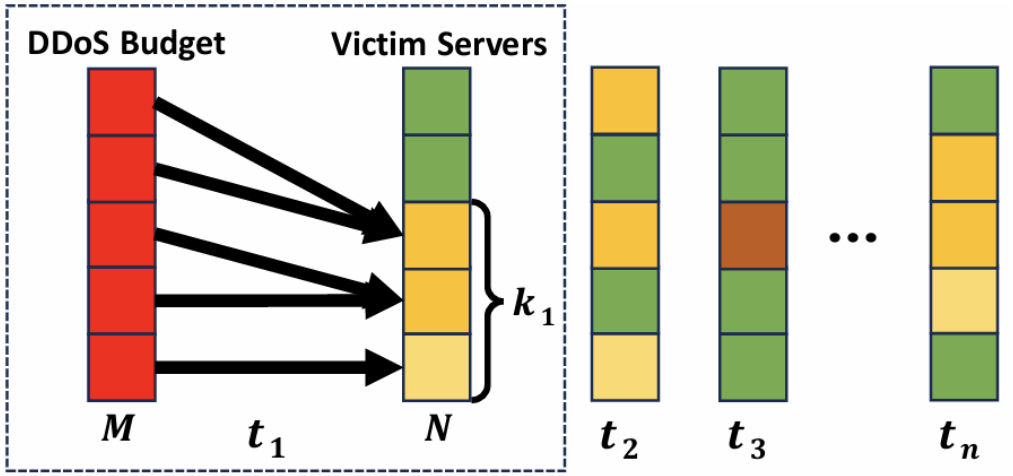


Fig. 2: Carpet Bombing Attacker Behavior

Expanded feature space greatly complicates detection

Key Ideas

- **Assistance from Victim Servers**
  - Effective Server-Only Features
    - Decrypted Payload, Request Pattern, URL, etc.
  - Available Resource for Server Monitoring
    - Carpet Bombing Distributed Nature -> Low Per-Server Volume

Key Ideas

- **Assistance from Victim Servers**
  - Effective Server-Only Features
    - Decrypted Payload, Request Pattern, URL, etc.
  - Available Resource for Server Monitoring
    - Carpet Bombing Distributed Nature -> Low Per-Server Volume
- **Similarity between Malicious Flows**
  - Coordinated Malicious Behavior as Indicator
    - Attack Launched with Botnets and Automatic Scripts

NetRadar Overview

- Server-Gateway Cooperation Architecture
  - Feature Gathering
    - Gateway-collected Traffic Feat & Server-collected Server Feat
    - Gathered at the Gateway
  - Centralized Analysis
    - Full Feat of all servers
    - Analyzed holistically

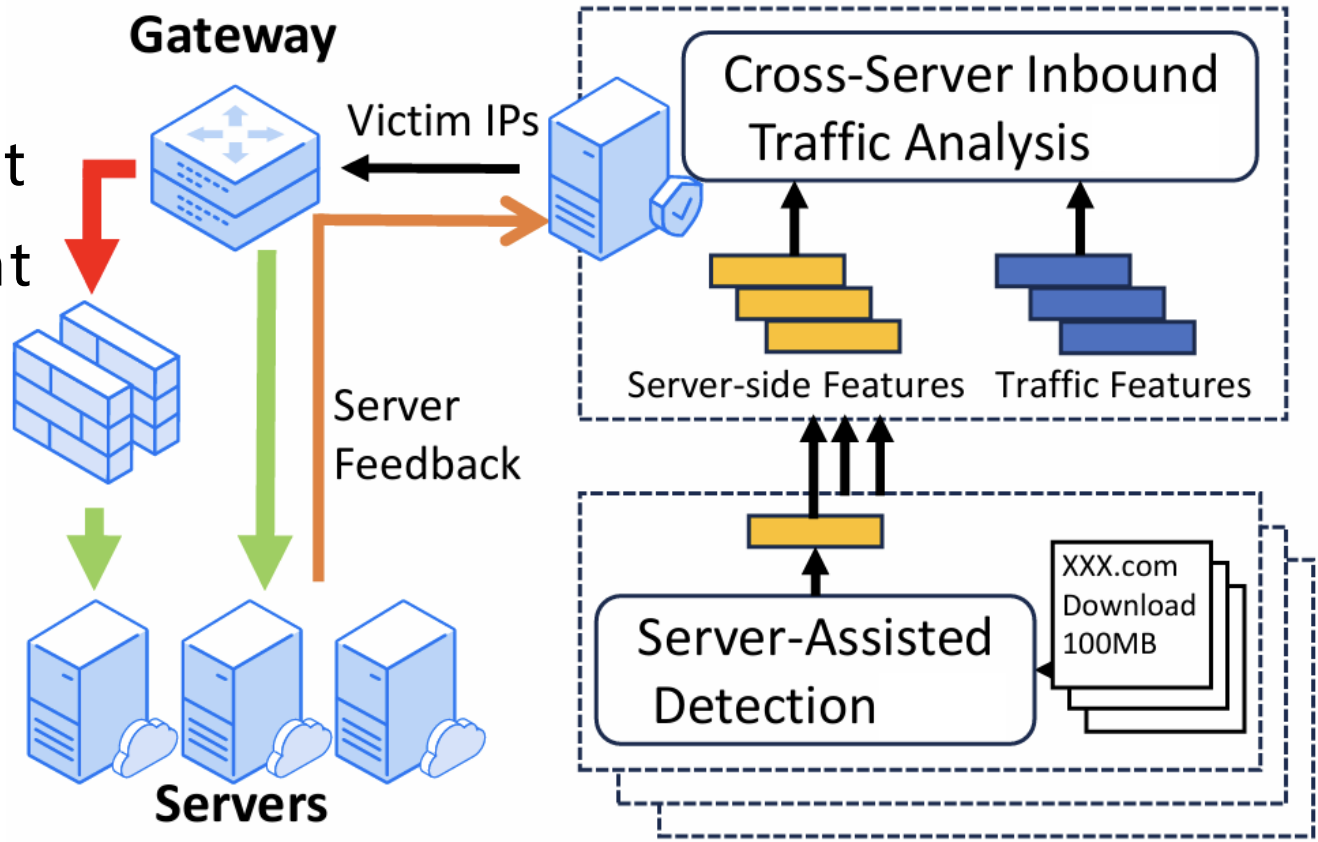


Fig. 3: NetRadar Architecture

Server-Assisted Detection

- General Server-side Features
  - Resource Hit Frequency
  - Active Resource Size

Widely available & Effective.

Server-Assisted Detection

- General Server-side Features
  - Resource Hit Frequency
  - Active Resource Size

Widely available & Effective.

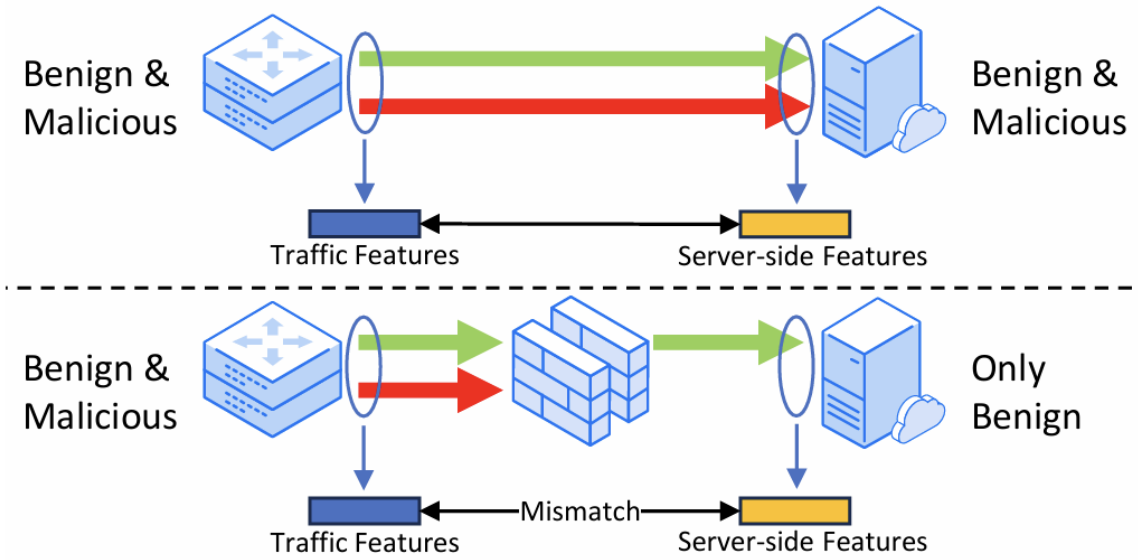


Fig. 4: Feature Mismatch when DDoS Mitigation is On

- Robust Server-Assisted Model
  - Robust Model Training with Random Erasing

Handles all possible states with different valid ratios of server-side features.

Cross-Server Inbound Traffic Analysis

- Cross-Server Analysis.
  - Analyze traffic to multiple servers simultaneously to reveal similarity.
- Scalability Issue.
  - Multiple Input at Once -> Prohibitively High Model Complexity

Cross-Server Inbound Traffic Analysis

- Cross-Server Analysis.
  - Analyze traffic to multiple servers simultaneously to reveal similarity.
- Scalability Issue.
  - Multiple Input at Once -> Prohibitively High Model Complexity
- Observation: Features of Multiple Servers as A Set.

Similarity matters!
The order of features can be ignored in analysis

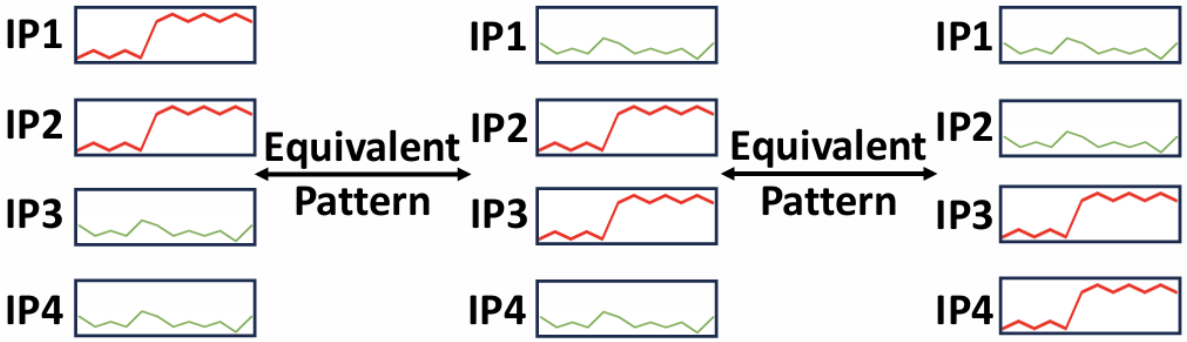
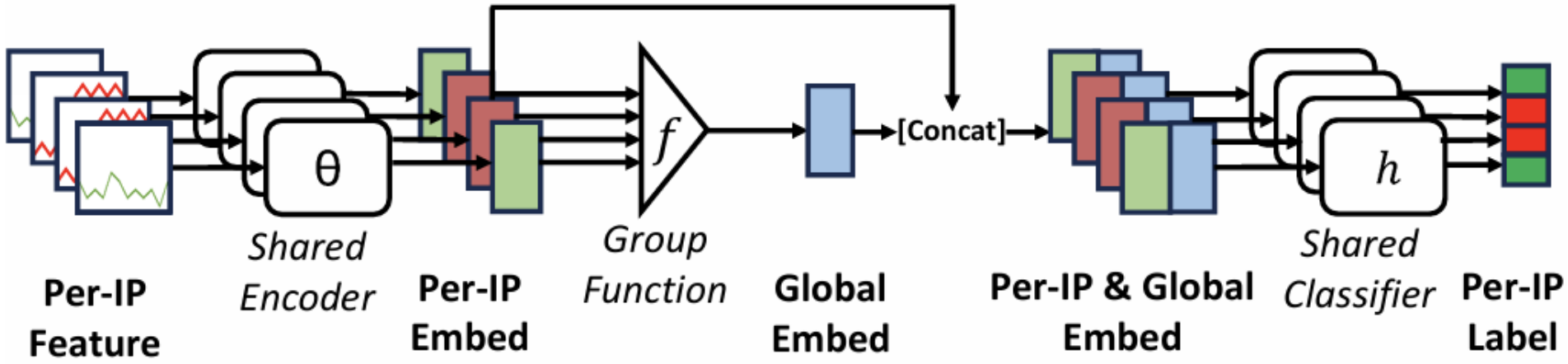


Fig. 5: Example of Equivalent Carpet Bombing Patterns

Cross-Server Inbound Traffic Analysis

- Permutation-Equivariant Model Structure
  - Neural Network for Set-Structured Data, from PointNet[1]



Consistent results for different input orders! Highly scalable!

[1] [2017][CVPR] PointNet: Deep Learning on Point Sets for 3D Classification and Segmentation

Cross-Server Inbound Traffic Analysis

- Group Function for Carpet Bombing Detection
  - Prior: Overall Property.
    - MAX, MIN, AVG, etc.
  - Ours: Similarity Analyze.
    - Sort-based Group Function

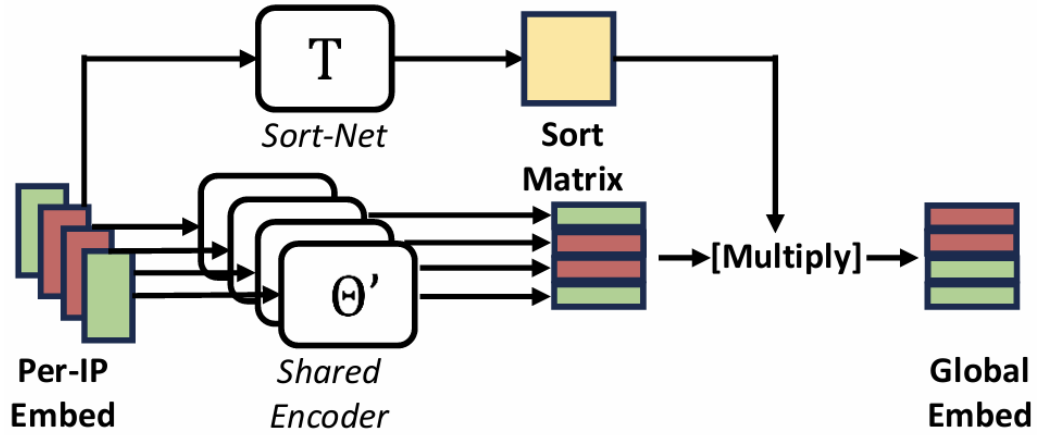


Fig. 7: Sort-based Group Function

$$L_{sort} = \|I - AA^T\|^2 + \lambda(\Sigma \frac{(sum(a_i) - \max(a_i))}{\max(a_i)}) \quad (2)$$

Sort-Net Loss Function

Preserve per-flow features in global embed for similarity analysis

Evaluation – End-to-End Performance

- Dynamic Low & High-Rate Carpet bombing
  - Real-World (Tencent) & Simulated Dataset (CIC-IDS-{2017,2018})

TABLE I: Detection Accuracy of NetRadar and Baselines in Different Carpet Bombing Detection Tasks.

Attack Traffic	Volumetric DDoS			Low-rate HTTP			Synchronous Download		
Metric	Accuracy	Precision	Recall	Accuracy	Precision	Recall	Accuracy	Precision	Recall
Lemon	99.28%	99.64%	99.61%	53.04%	53.41%	81.32%	54.23%	52.55%	86.47%
Kitsune	99.95%	99.99%	99.95%	63.22%	34.70%	52.66%	89.86%	96.07%	72.36%
Flowlens	99.99%	99.99%	99.99%	92.90%	94.92%	93.69%	90.31%	93.37%	83.57%
Whisper	99.69%	99.81%	99.86%	92.77%	95.34%	90.18%	86.63%	84.14%	85.18%
NetRadar	99.79%	99.83%	99.95%	96.28%	96.98%	96.06%	94.78%	96.38%	93.70%

Better than SOTA, achieving over 94% ACC in all scenarios.

Evaluation – Detection Robustness

- Extreme Covert Low-Rate Carpet Bombing
  - Malicious traffic throughput ratio of 1/1 to 1/16. (By modifying victim server num & per-server attack throughput)

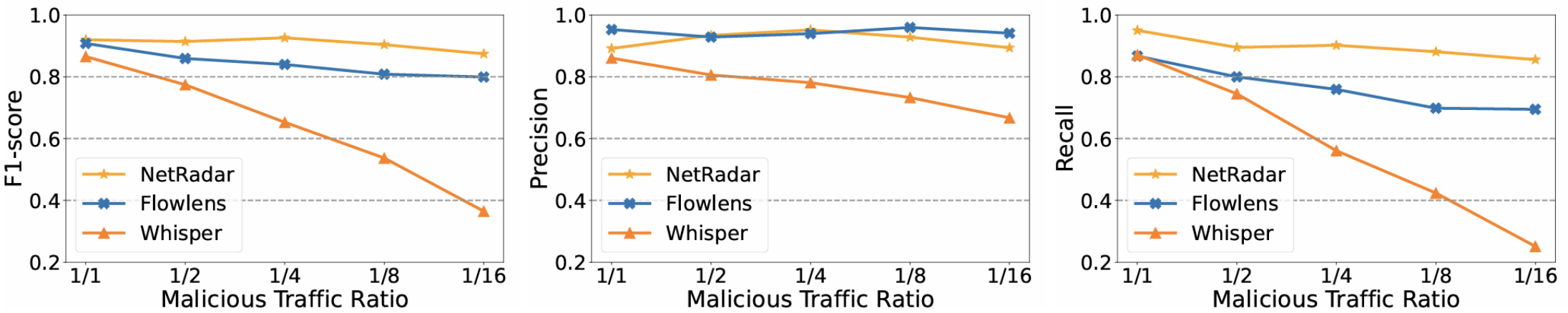


Fig. 8: Detection Robustness Test with Different Malicious Traffic Ratio Dataset

Identify 85% victim even if malicious volume <= 10% total volume.

Evaluation – Deep Dive

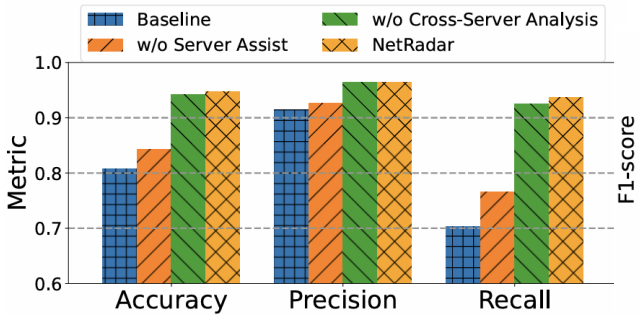


Fig. 9: Ablation Test on NetRadar

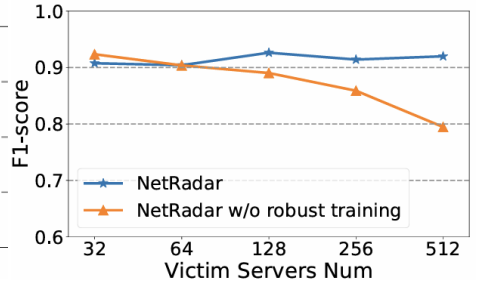


Fig. 12: Random Erase Test

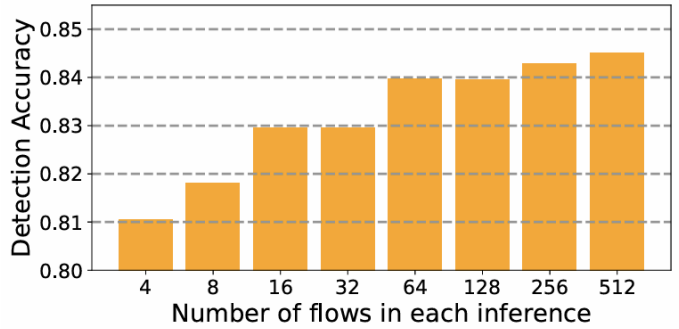


Fig. 11: The Impact of Inference Subnet Size

TABLE II: Group Function Comparison

Group Function	DeepSets	PointNet	NetRadar
Accuracy	86.86%	85.98%	94.78%

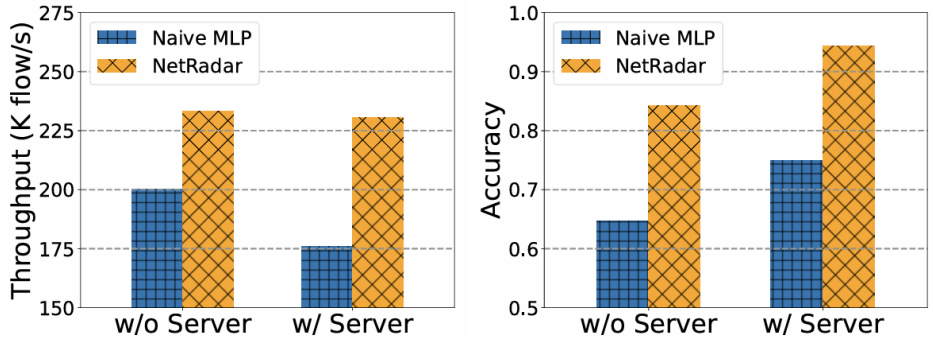


Fig. 10: Cross-Server Analysis Efficiency

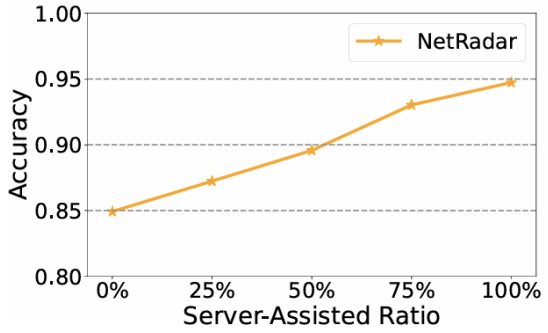


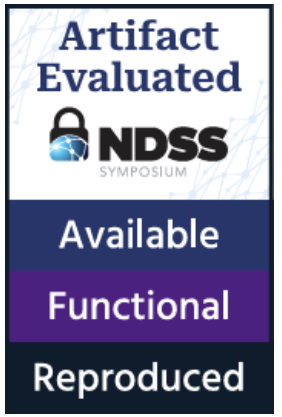
Fig. 13: Incremental Deploy Test

64-flow-input for sufficient ACC

Comprehensive component test

Support incremental deployment

Conclusion



- Key Ideas
  - Assistance from Victim Servers.
  - Similarity between Malicious Flows.
- NetRadar
  - Server-Gateway Cooperation Architecture.
  - Server-Assisted Detection & Cross-Server Inbound Traffic Analysis.
  - Accurate and Robust Carpet Bombing DDoS Detection.
- Artifact Available
  - Codes，Dataset，Script for Main Experiment

Thank You!

NetRadar: Enabling Robust Carpet Bombing DDoS Detection

Junchen Pan , Lei Zhang, Xiaoyong Si, Jie Zhang,

Xinggong Zhang, Yong Cui

pjc21@mails.tsinghua.edu.cn