In-Network Probabilistic Monitoring Primitives under the Influence of Adversarial Network Inputs

[1] **Harish S A**[*], [1] K Shiv Kumar[*], [1]Anibrata Majee, [1]Amogh Bedarakota, [1] Praveen Tammana,

[3] Pravien Govindan Kannan, [2] Rinku Shah

[1] IIT Hyderabad
India

[2] IIIT Delhi
India

[3] IBM Research
India

30th June 2023

7th Asia-Pacific Workshop on Networking (APNET 2023)

Fast control loop systems

Monitoring and Debugging

FlowRadar [NSDI'16] | **LossRadar** [CoNEXT'16] | **Dapper** [SOSR'17] | **ConQuest** [CoNEXT'19] | **SpiderMon** [SOSR'20] | **Continuous In-network RTT Monitoring** [SIGCOMM'22]

Load Balancing and Caching

HULA [SOSR'16] | **SilkRoad** [SIGCOMM'17] | **NetCache** [SOSP'17]

Routing

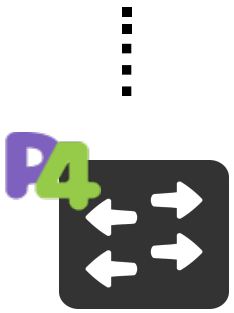
Blink [NSDI'19] | **Contra** [NSDI'20] | **RouteScout** [SOSR'21]

Security

Nethcf [ICNP'19] | **Poise** [USENIX Security'20] | **NetWarden** [USENIX Security'20] | **Jaqen** [USENIX Security'21]

In-network monitoring primitives

Q: Is a flow new or old? **FlowRadar** [NSDI'16]
Q: How many times has a key been accessed? **NetCache** [SOSP'17]



Monitoring and Debugging | Routing | Caching | Security | Load Balancing | ...

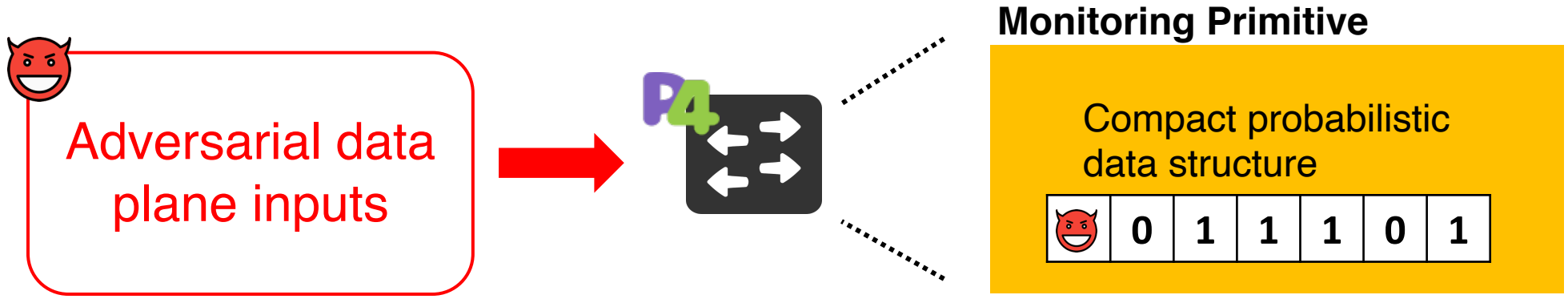
Compact probabilistic data structures!

Bloom filters (BFs), Count Minimum Sketches (CMS), Inverted Bloom Lookup Tables (IBLTs)….

Impact of attacks on probabilistic monitoring primitives

Corruption of network statistics, Denial of service, Performance degradation

…



Pollute the bloom filters and sketches through targeted attacks!

In this work….

Question

What are the negative impacts of polluting compact probabilistic data structures that drive in-network monitoring primitives?

Key contribution

Empirically gauge the impact of bloom filter pollution attacks on *FlowRadar*[1]

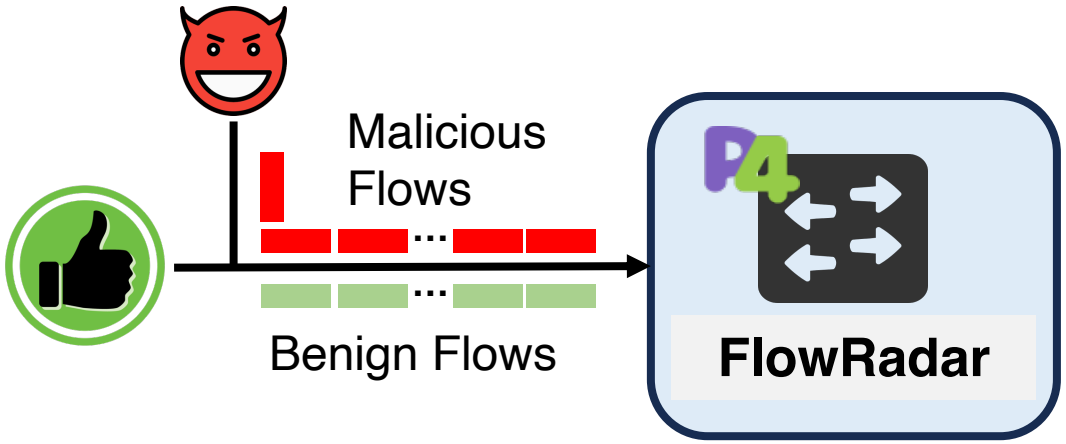
[1]Li, Y., Miao, R., Kim, C., & Yu, M. (2016). Flowradar: A better netflow for data centers. In 13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16) (pp. 311-324).

Our approach

Define threat model

Adversarial privileges? Adversarial objectives?

Craft malicious flows



FlowRadar system affected?

Yes ☹

Is it bad?

Yes ☹

How bad are the effects?

Threat model

Bloom filter size | Type of hash function | Number of hash functions

Chosen Insertion Adversary (CIA)

Query only Adversary (QOA)

Malicious flow

Malicious flow

1	0 1	0	0	0 1	0	1	0	0	1	0	0

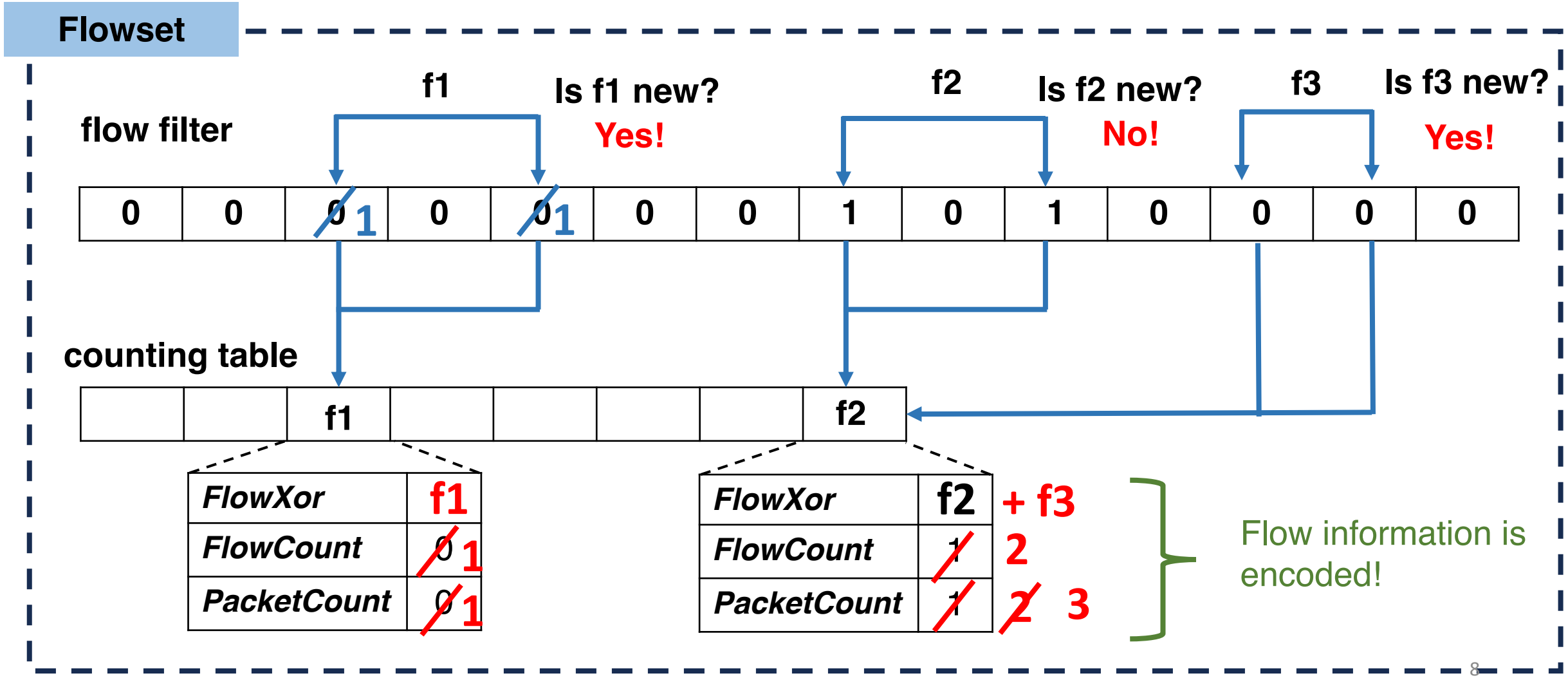
Benign new flow

False positive!

Statistics behind the BF polluted affected!

Bloom filters in FlowRadar

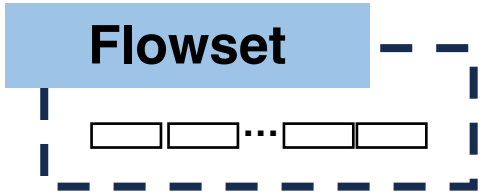
Network monitoring system that maintains flows and their counters



FlowRadar decode operations

Single Decode (SD) — Extract decodable flows

Input



Process

1. Find “pure cells”
2. Extract decodable flows

Output

Flow IDs

Counter Decode (CD) — Extract packet counts

Input

Flow IDs

Process

1. Represent as linear equations
2. Solve using approximations

Output

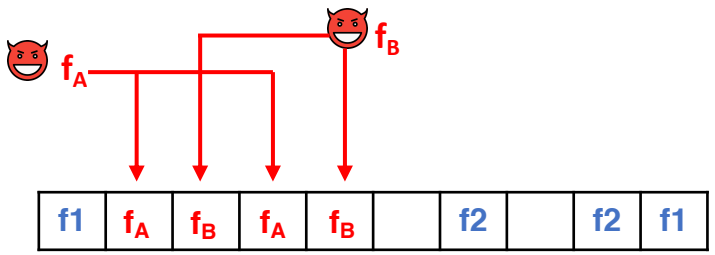
Packet counts!

Crafting Malicious flows

① Generate flow IDs ② Interlace generated flows among benign flows

Chosen Insertion Adversary (CIA)

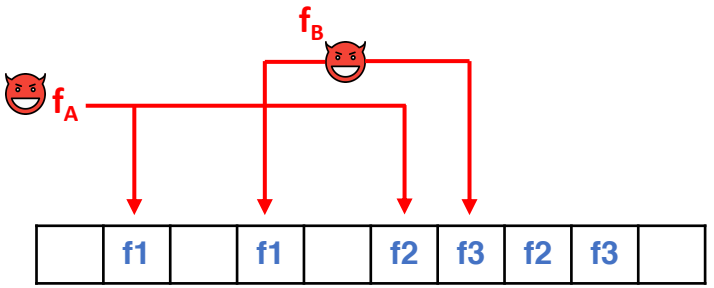
Flow IDs do not collide amongst themselves in the flowset's flowfilter



Flow filter

Query only Adversary (QOA)

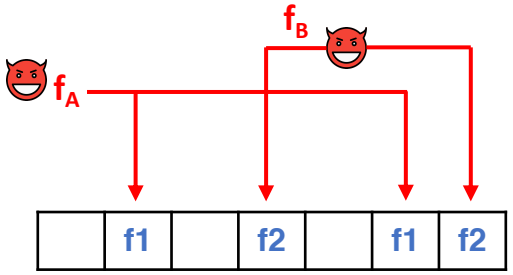
Flow IDs map to already set locations in the flowset's flowfilter



Flow filter

Subset

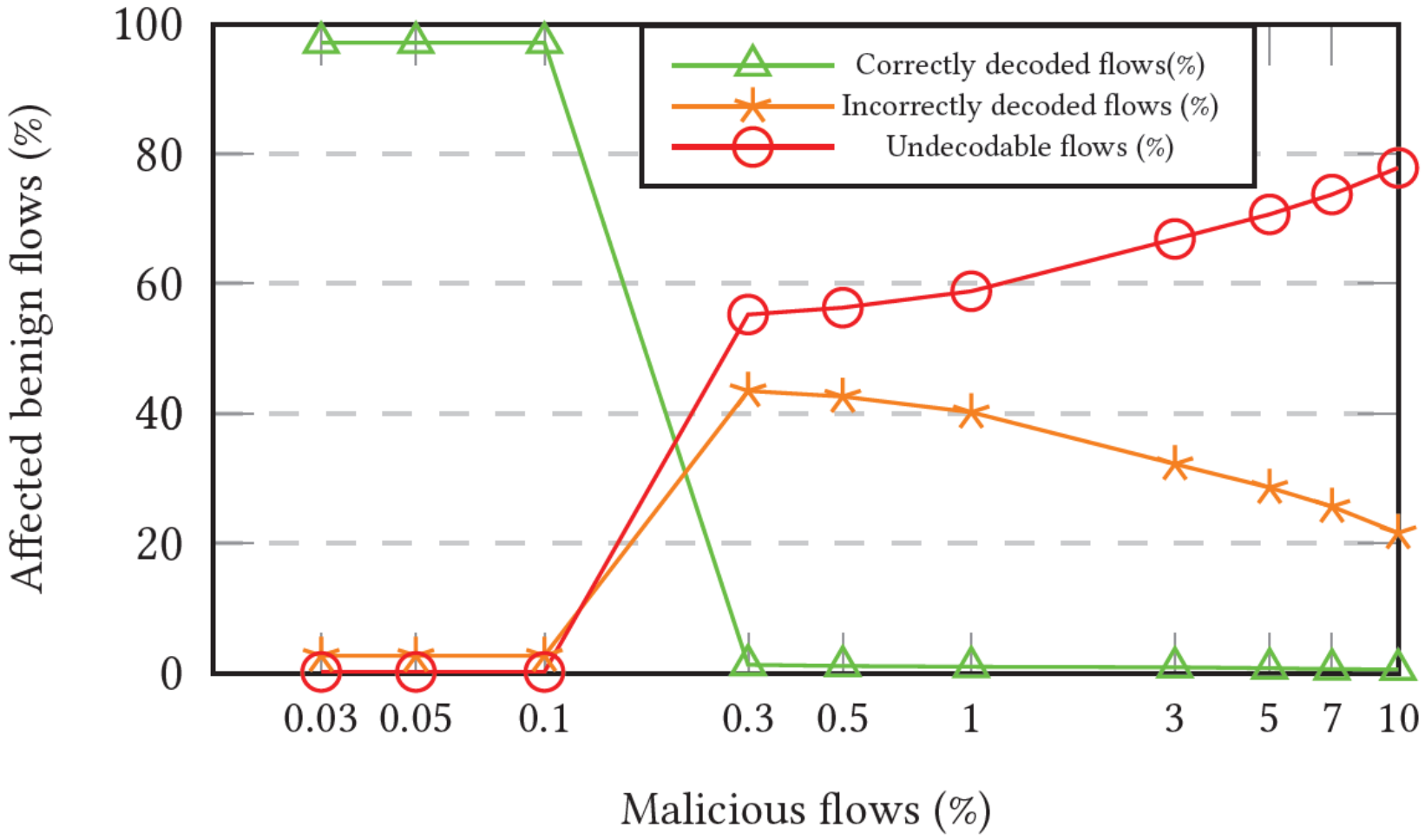
Flow IDs are identical to benign flows



Flow filter

Results: CIA & QoA

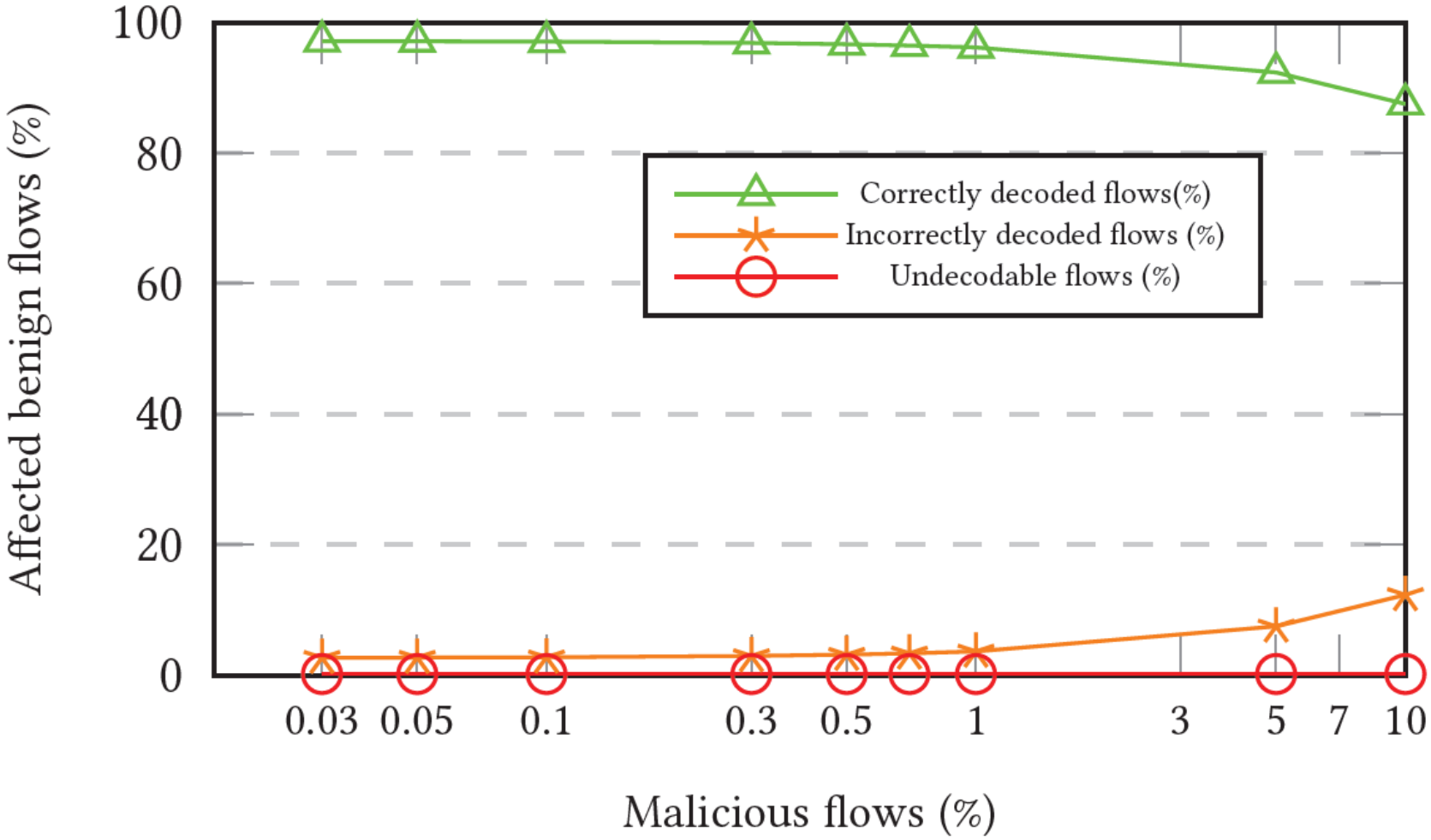
Correctly decoded flows | **Incorrectly decoded flows** | **Undecodable flows**



~0.3% malicious flows, disrupt almost 99% of benign flows

Bang for his buck!

Results: Subset



The effects of subset strategy are subdued

Reason: only packet counts affected

Summary and Future work

- We empirically gauged the impact of polluting attack on FlowRadar
- An adversary can corrupt the traffic statistics with only a few crafted malicious flows
- **Future work:**
  - Extend our analysis to other fast control loop systems (e.g., RouteScout)
  - Develop detection and defence mechanisms

In-Network Probabilistic Monitoring Primitives under the Influence of Adversarial Network Inputs

[1] **Harish S A**[*], [1] K Shiv Kumar[*], [1]Anibrata Majee, [1]Amogh Bedarakota, [1] Praveen Tammana, [3] Pravien Govindan Kannan, [2] Rinku Shah

Thank You

CS21RESCH11009@iith.ac.in

30th June 2023

7th Asia-Pacific Workshop on Networking (APNET 2023)