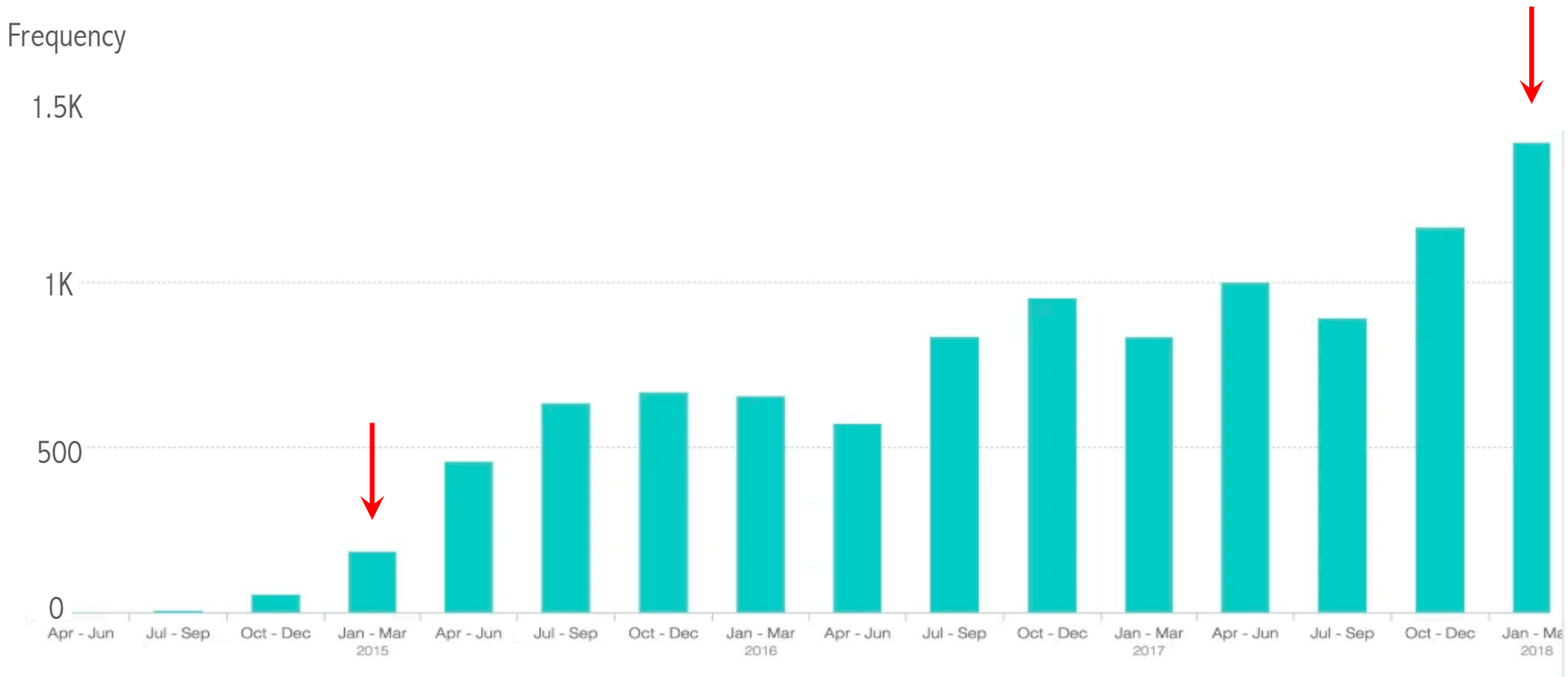
PERSIA: a PuzzlE-based InteReSt FloodIng Attack Countermeasure

Reza Tourani, George Torres, Satyajayant Misra

SAINT LOUIS UNIVERSITY
EST. 1818

ICN '20, September 2020, Virtual Event, Canada

Infusion of smart devices at the edge and memcached systems are major contributors of recent DDoS attacks.

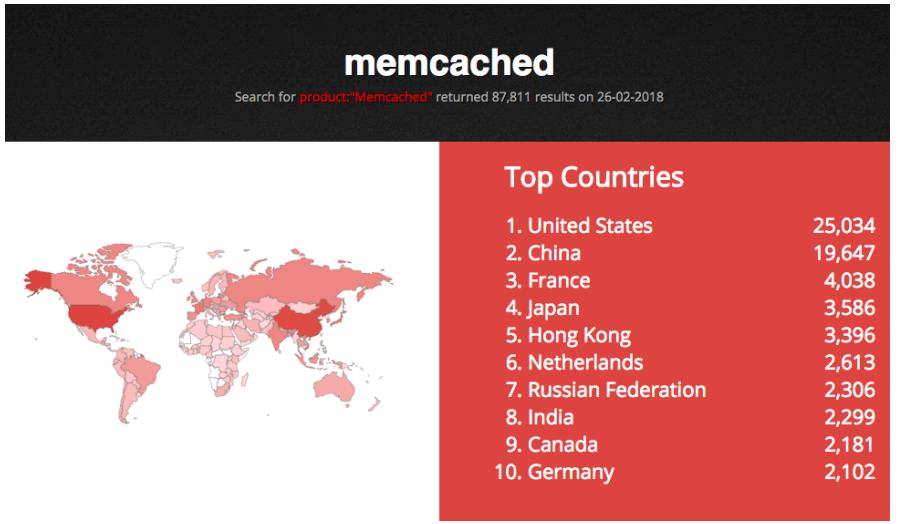


https://www.netscout.com/blog/asert/1-terabit-ddos-attacks-become-reality-reflecting-five-years
https://arstechnica.com/information-technology/2018/02/in-the-wild-ddoses-use-new-way-to-achieve-unthinkable-sizes/

Infusion of smart devices at the edge and memcached systems are major contributors of recent DDoS attacks.

Protocol	Banners	Devices Identified	
HTTPS	342,015	271,471	(79.4%)
FTP	318,688	144,322	(45.1%)
Telnet	472,725	103,924	(22.0%)
CWMP	505,977	35,163	(7.0%)
SSH	148,640	8,107	(5.5%)
Total	1,788,045	587,743	(31.5%)

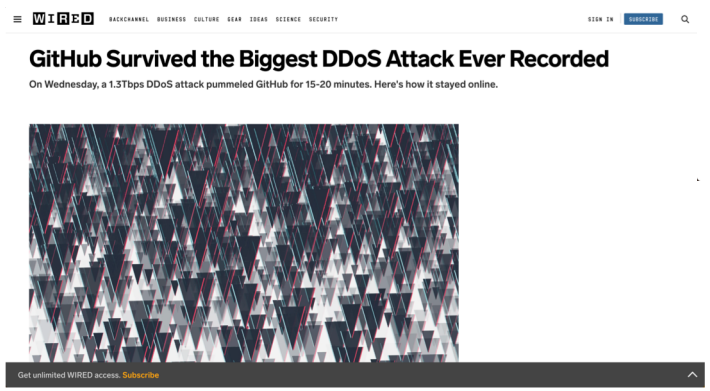
Table 2: **Devices Identified** — We identified device type, model, and/or vendor for 31.5% of active scan banners. Protocol banners varied drastically in device identifiability, with HTTPS certificates being most descriptive, and SSH prompts being the least. [Antonakakis, USENIX'17]



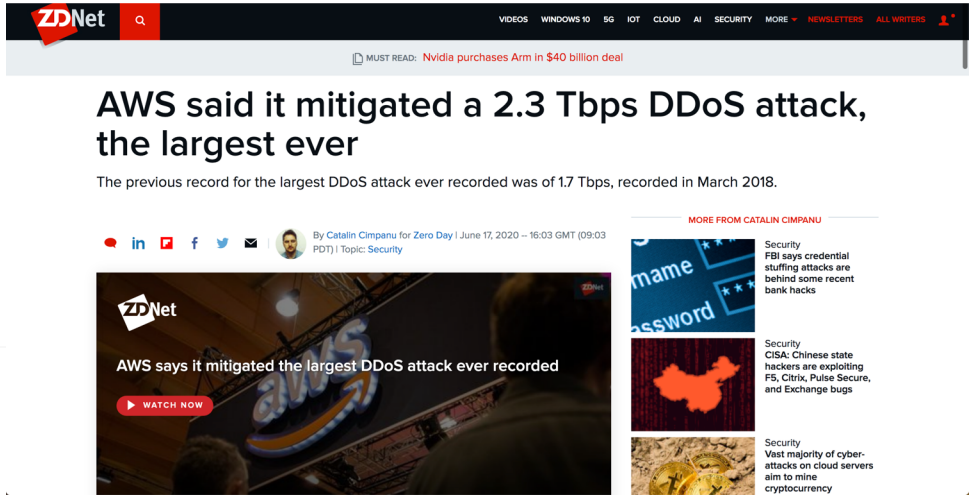
https://www.netscout.com/blog/asert/1-terabit-ddos-attacks-become-reality-reflecting-five-years
https://arstechnica.com/information-technology/2018/02/in-the-wild-ddoses-use-new-way-to-achieve-unthinkable-sizes/

The intensity and frequency of Distributed Denial of Service (DDoS) attacks are increasing.

In 2016, the Dyn DDoS attack set a record at 1.2Tbps from 600,000 compromised devices.



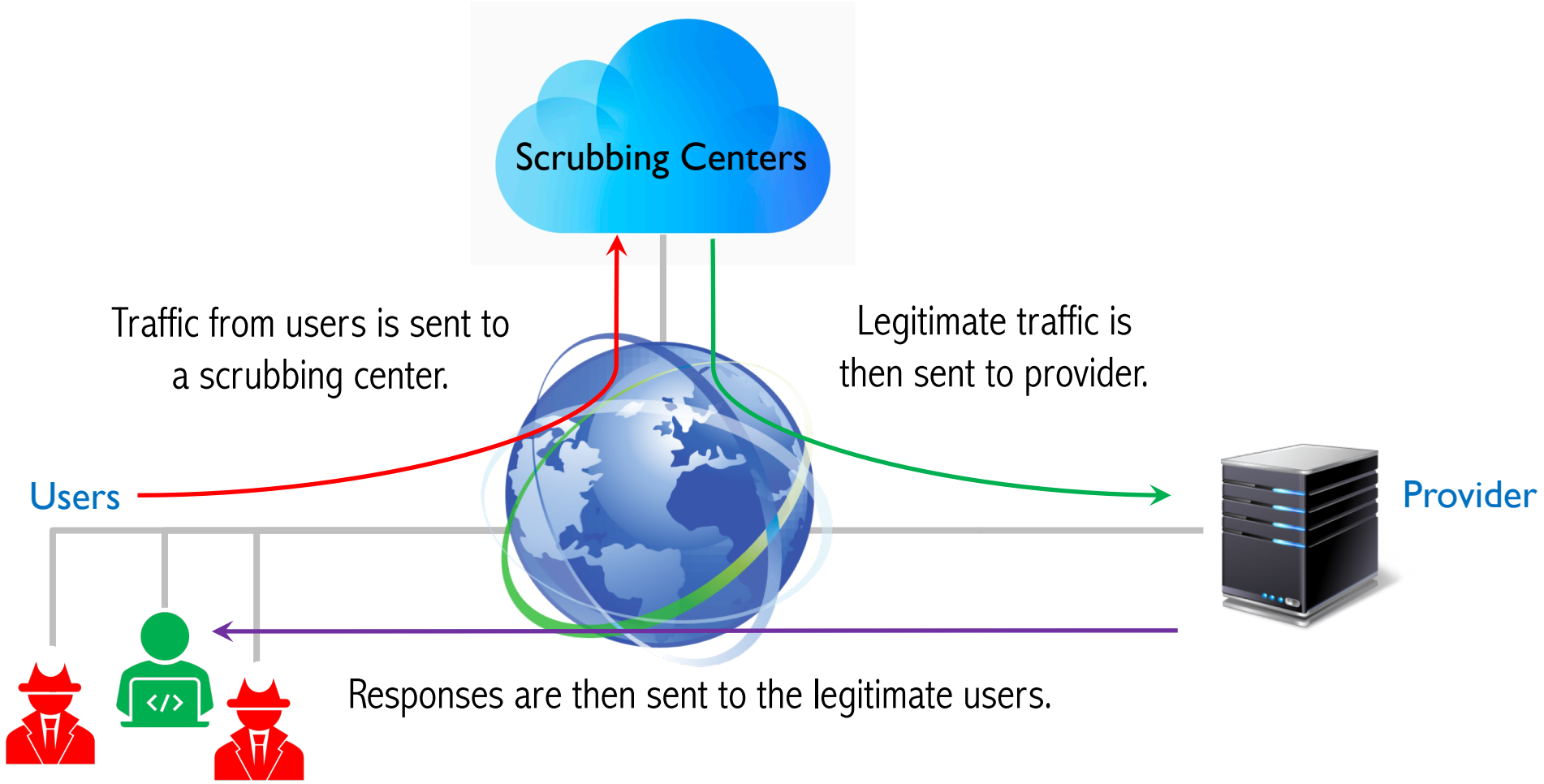
In 2018, a DDoS attack with intensity of 1.3Tbps pummeled GitHub for 15-20 minutes. Akamai Prolexic for mitigation.



In 2020, AWS reported a 2.3Tbps DDoS attack using hijacked CLDAP web servers, which was mitigated by AWS Shield service.

https://www.wired.com/story/github-ddos-memcached/
https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet
https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/

Scrubbing service is a common DDoS mitigation technique.



Denial of Service Attacks in Named-Data Networking

Interest Flooding Attack (IFA)

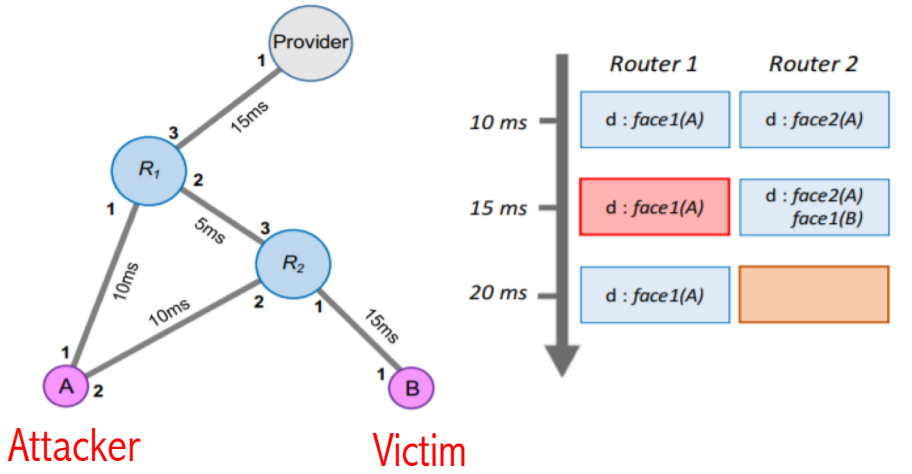
Attackers overwhelm network resource using volumetric malicious traffic (non-existent content).

Pending Interest Table		
Name	Incoming Faces	Lifetime
Netflix/2020/OdGurd.avi	1,2	1 seconds
Youtube/somevideo.m33	2	5 seconds
⋮	⋮	⋮

Implicit Denial of Service (iDoS)

Attackers craft multicast requests, which along aggregation and loop prevention blocks content delivery to victim.

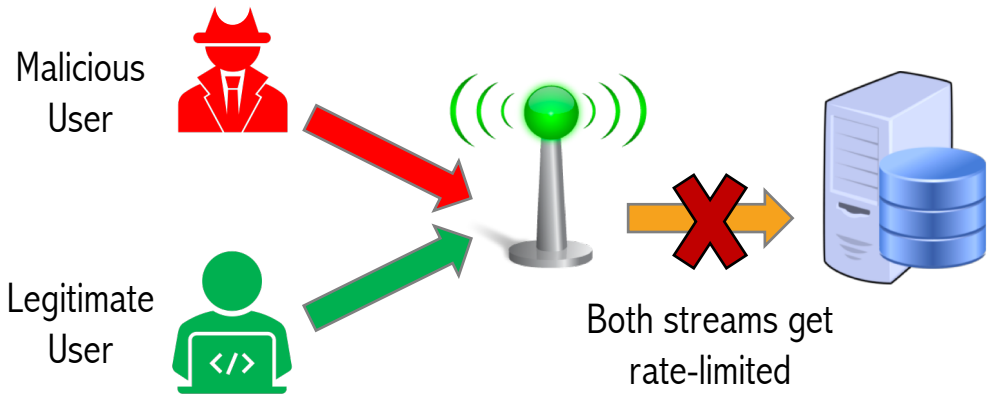
[Panwar, ICC'18]



Rate limiting is the dominating IFA mitigation technique.

Mechanism	Target	Objective	Content Type	Technique
Afanasyev [1]	Router	Mitigation	Non-Existent	Rate Limiting & Per-face Fairness
Gasti [14]	Router/Provider	Mitigation	All Content	Rate Limiting & Per-face Statistics
Compagno [9]	Router	Mitigation	Non-Existent	Rate Limiting & Per-face Statistics
Dai [10]	Router	Mitigation	Non-Existent	Rate Limiting & PIT Size Monitoring
Wang [40]	Router	Mitigation	Non-Existent	Fuzzy Logic Detection & Rate Limiting
Nguyen [25]	Router	Mitigation	Non-Existent	Statistical Hypotheses Testing Theory
Wang [39]	Router	Mitigation	Non-Existent	Self Routing for Suspicious Requests
Li [20]	Provider	Prevention	Dynamic	Per Request Proof-of-Work

Rate Limiting



Negatively Impacts on users' Quality-of-Experience.

Interest

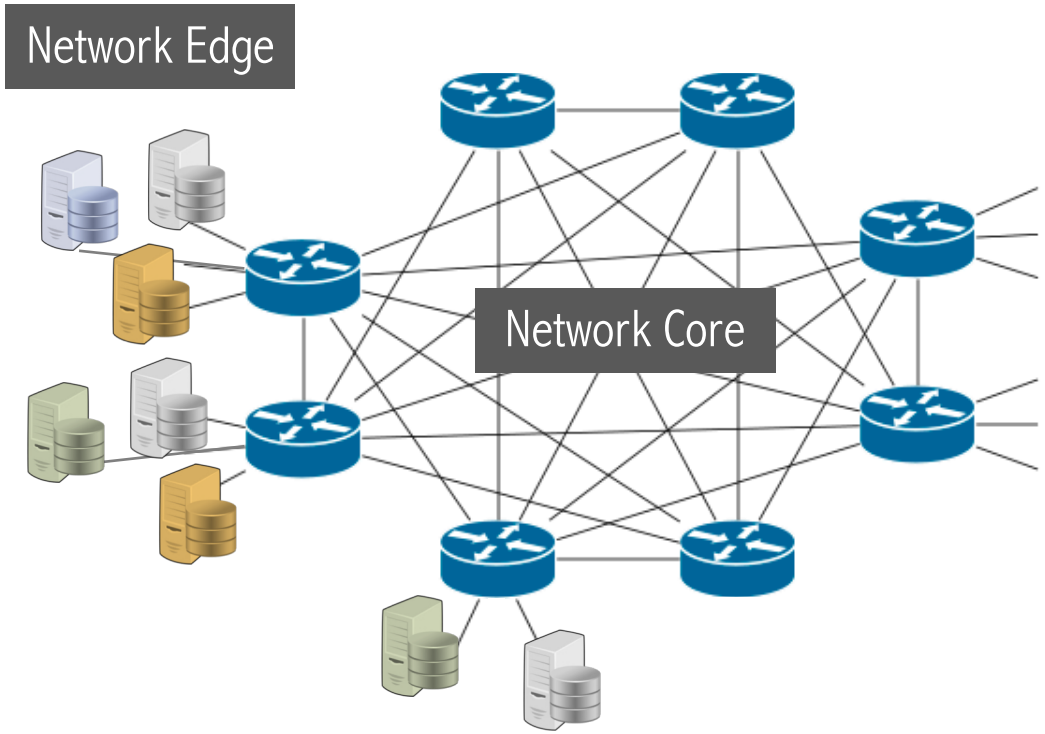
Name
Netflix/2020/OldGuard.avi/face256/face258

Undermines content caching and aggregation.
Contradicts NDN's content name immutability.

PERSIA is an ISP-based countermeasure that employs independent prevention and mitigation mechanisms.

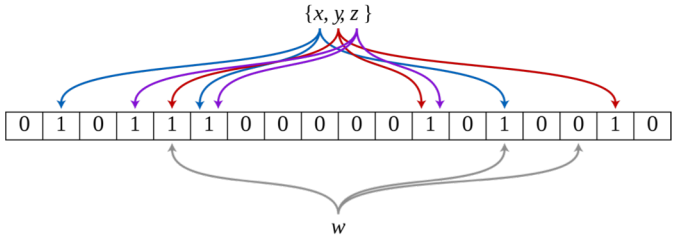
Edge-centric Prevention Mechanism

Proof of Work
Token-based Communication



Dynamic in-network Mitigation Mechanism

Decoupling Interests from PIT
Bloom Filter



In prevention phase, users solve computational puzzles and generate tokens for communication.

PERSIA uses Lagrange polynomial interpolation as its plug & play PoW mechanism.

A Lagrange's polynomial of degree n ($F_n(x)$) taking on the values $f(x_0), \ldots, f(x_n)$ for the points $x_0, \ldots, x_n$ is given by,

$$F_n(x) = f(x_0)\frac{(x-x_1)(x-x_2)\ldots(x-x_n)}{(x_0-x_1)(x_0-x_2)\ldots(x_0-x_n)} + \ldots + f(x_n)\frac{(x-x_0)(x-x_1)\ldots(x-x_{n-1})}{(x_n-x_0)(x_n-x_1)\ldots(x_n-x_{n-1})}.$$

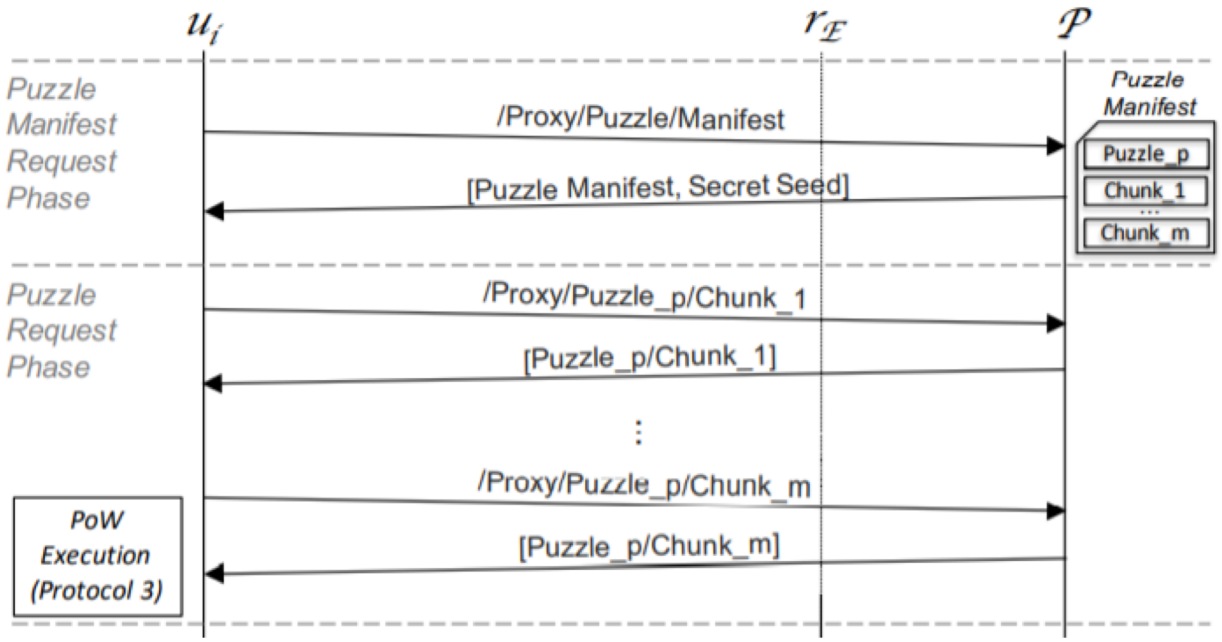
The i^{th} fractional term (Lagrangian coefficient) in $F_n(0)$ is represented as, $\lambda_i = \Pi_{0\le j(\neq i)\le n}\frac{x_j}{x_j-x_i}$ resulting in $a_0 = F_n(0) = f(x_0)\lambda_0 + f(x_1)\lambda_1 + \ldots + f(x_n)\lambda_n$. □

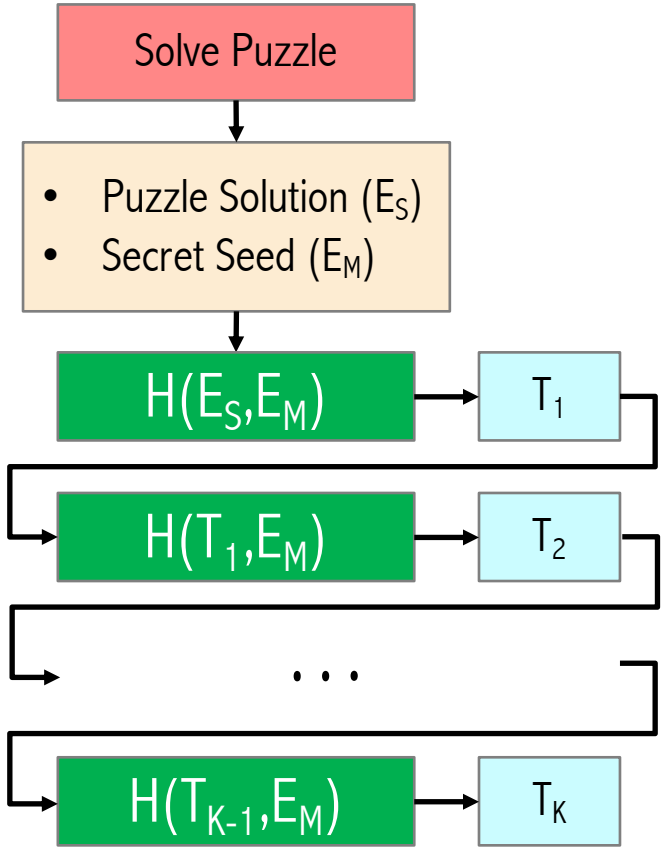
Users include their tokens in their requests to prove the work.

Interest

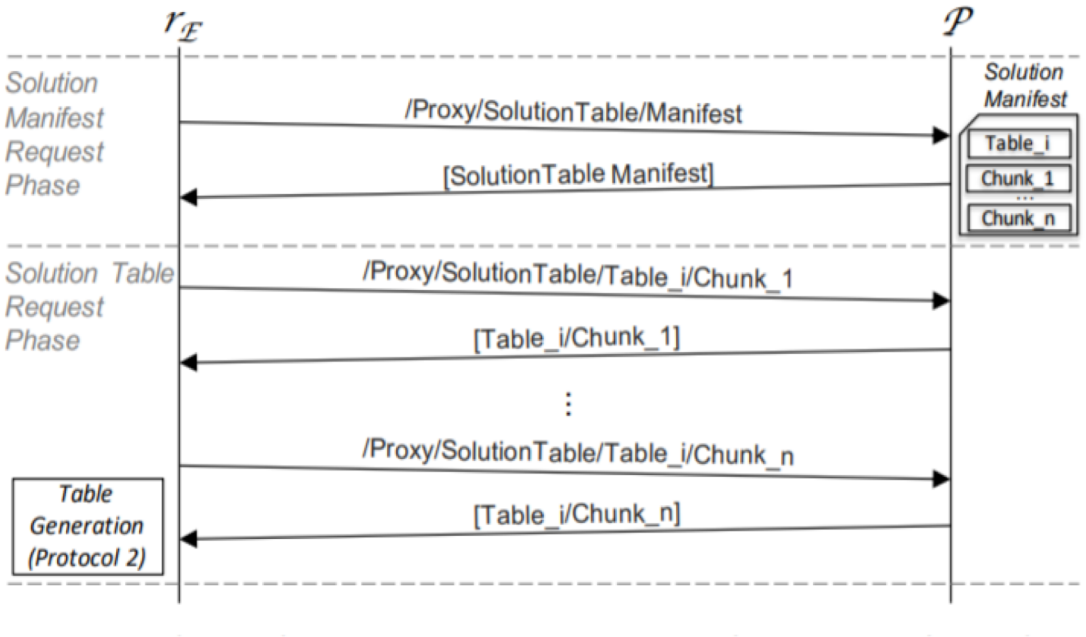
Name	Token
Netflix/2020/OldGuard.avi	T1

Users obtain puzzles from the proxy, solve the puzzles, and generate the token chains.





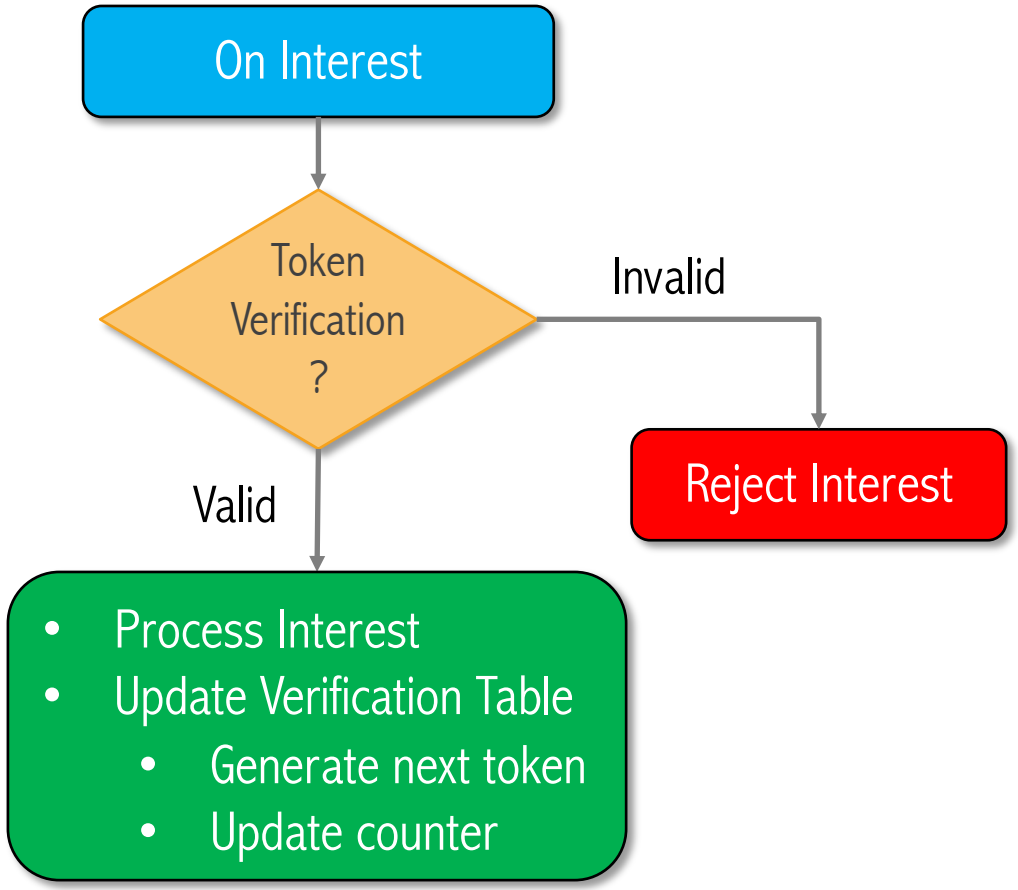
Edge Routers obtain the list of puzzles, their solutions, and seed from the proxy to build verification table.



	Solution	Seed	T_j	Limit	Counter
Puzzle1	562…	3737…	T_1	1000	0
Puzzle2	841…	4544…	T_1	1000	0
Puzzle3	544…	7873…	T_1	1000	0

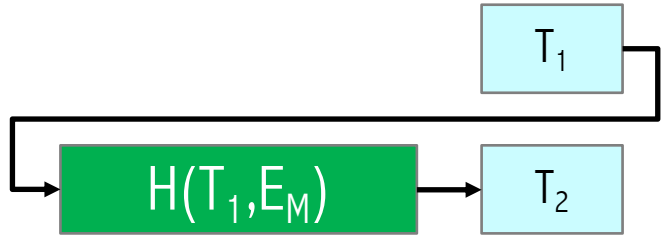
<Puzzle Solution, Secret Seed , Next Token, Token Limit, Token Counter>

Edge router validates the users' token, updates its validation table with next token, if token was valid.



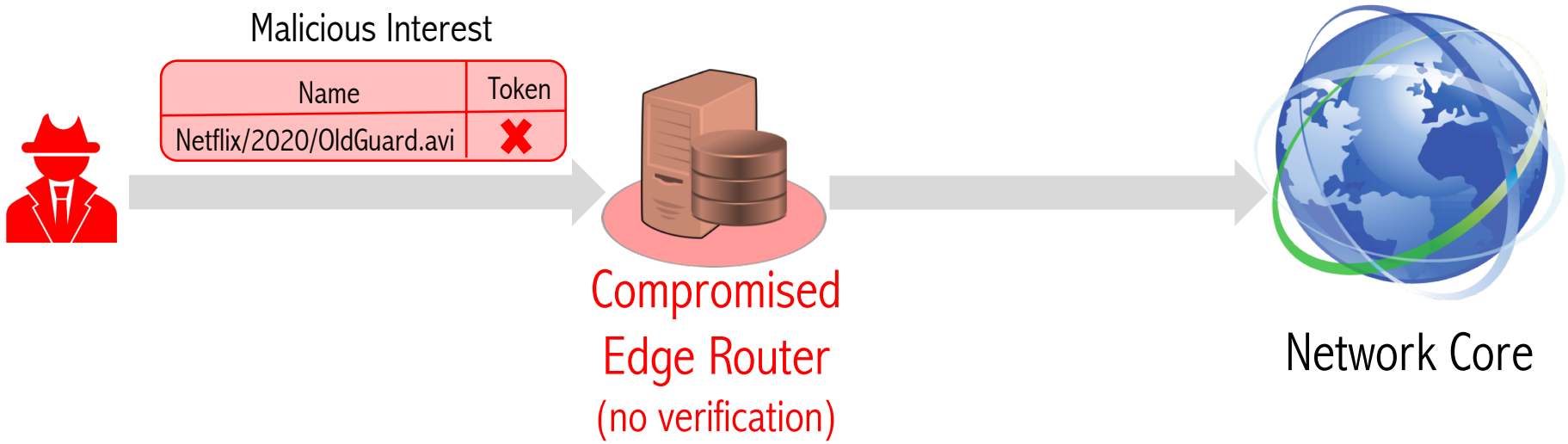
	Solution	Seed	Tj	Limit	Counter
Puzzle1	5462…	3737…	T1	1000	0

Update token value and increment counter.



	Solution	Seed	Tj	Limit	Counter
Puzzle1	5462…	3737…	T2	1000	1

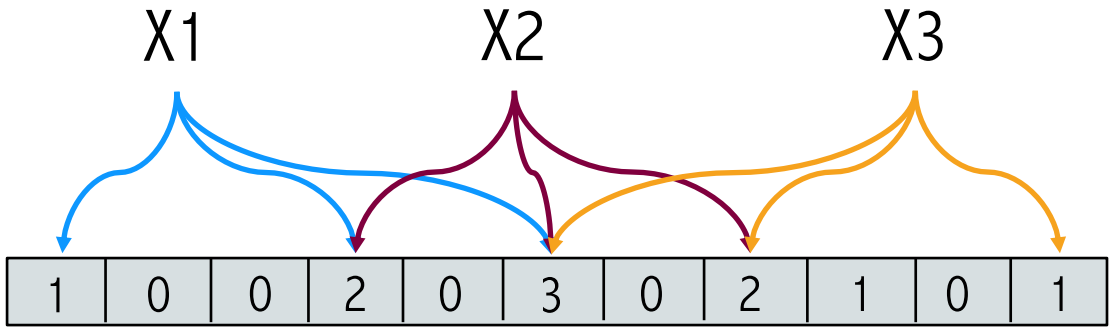
PERSIA's Bloom Filter-Assist mitigation strategy runs on core routers, **independent** of it prevention mechanism.



Each core router **autonomously** deploys BFA, which works **irrespective** of the data name.

	Loss Rate	Status
Interface 1	28%	Normal
Interface 2	12%	Normal
Interface 3	75%	Under attack

BFA detects attacks by monitoring the loss rate of interest from incoming interfaces.

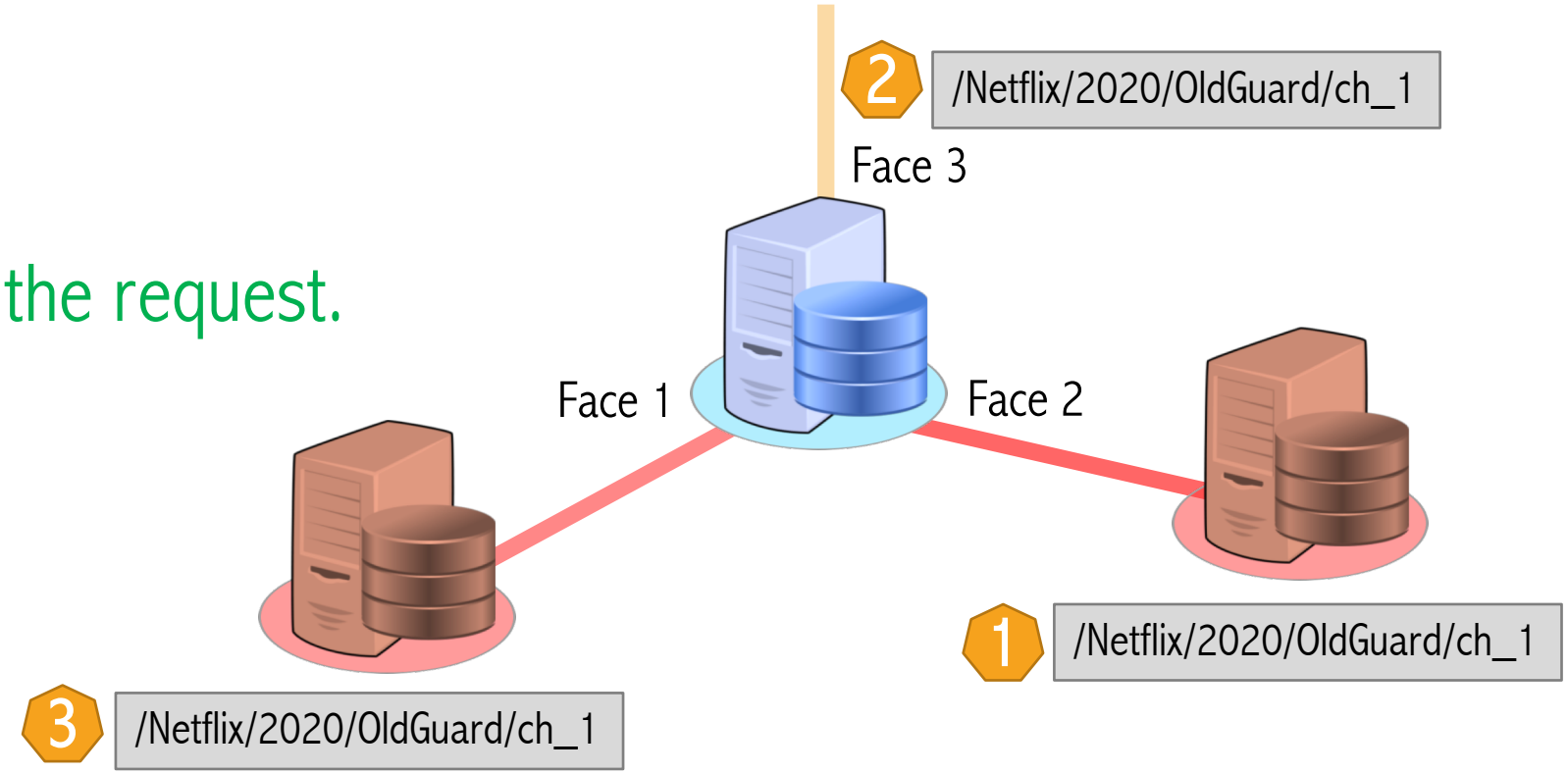


BFA uses a counting bloom filter (CBF) to store suspicious Interests.

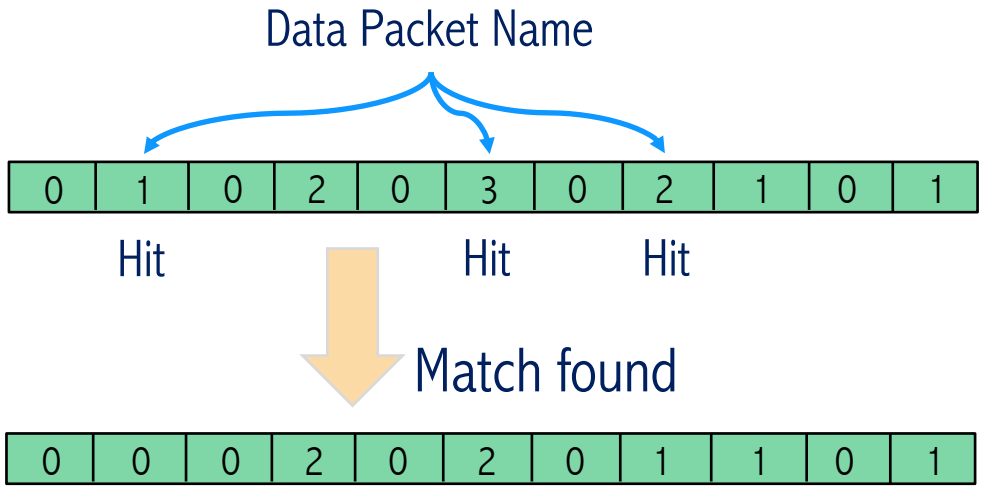
BFA strategy enables request aggregation even when a subset of faces use CBF.

Aggregation Conditions:

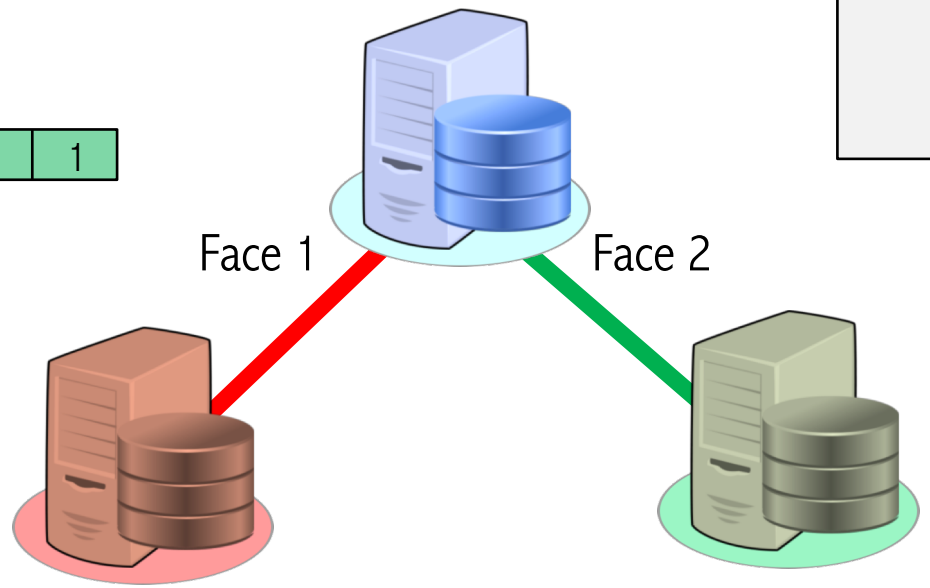
1. Existing PIT entry.
2. Another CBF indexes the request.



On receiving data, BFA strategy lookup the data name on CBFs of faces and the PIT for data forwarding.



Pending Interest Table		
Name	Incoming Faces	Lifetime
⋮	⋮	⋮



Attack Model

Attackers, requesting data without solving puzzles or using invalid tokens for content retrieval.

Attackers, intercepting and hijacking users' tokens to use themselves (replay attack).

Malicious users, colluding with users/attackers by sharing puzzles' solutions, tokens, and credentials.

Compromised infrastructure (malicious routers) forwarding Interests without validating the tokens.

Puzzle Complexity and Solvability.
Attacks on Proxies.

Attack categorization for simulation purposes.

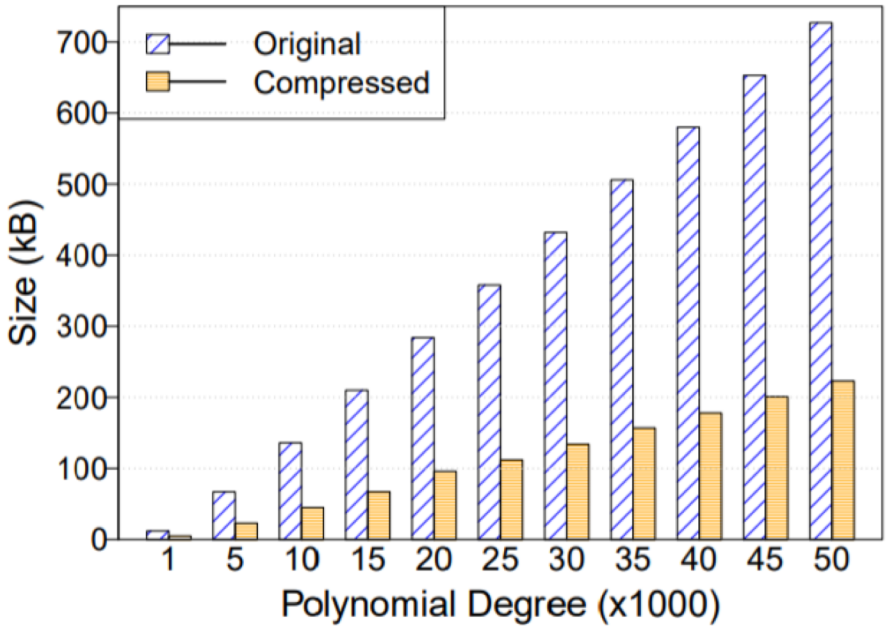
A1	Request content either without tokens or with fake tokens.
A2	The malicious users who share their puzzles' solutions and secret seeds with others. Replay attack and Token hijacking.
A3	Compromised Routers.

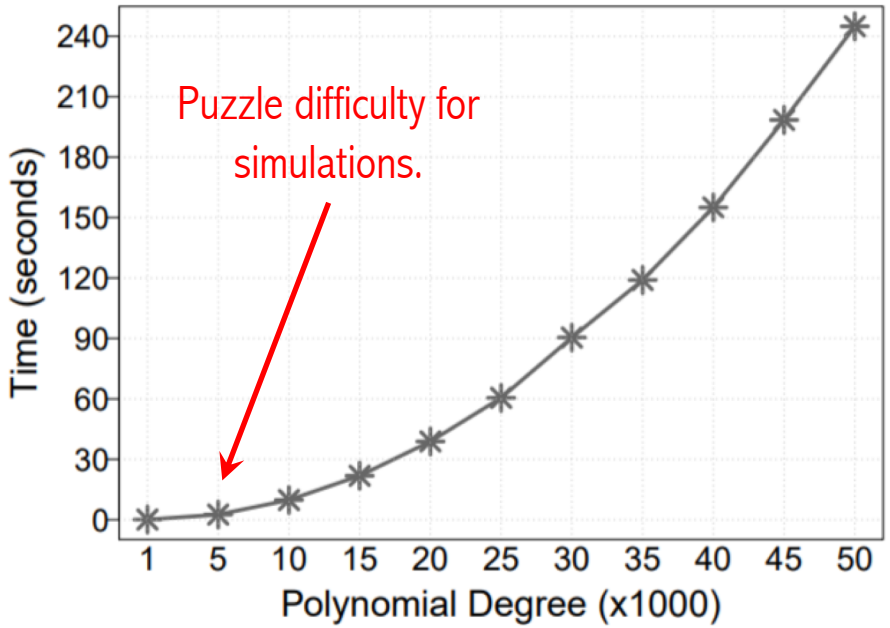
Simulation Setup

	Ebone	Telstra	AT&T
Core Routers	134	295	550
Edge Routers	28 (7)	46 (12)	71 (18)
Providers	10	10	10
Proxies	5	5	5
Legitimate Users	47	98	147
Attackers	53	102	153

- Users' request rates: uniformly at random from U[20, 30] Interests/sec.
- Attackers request rates: uniformly at random from U[50, 100] Interests/sec.
- Attackers request unique, non-existent content.
- Duration: 2500 Seconds.
- Averaged over 5 random runs.

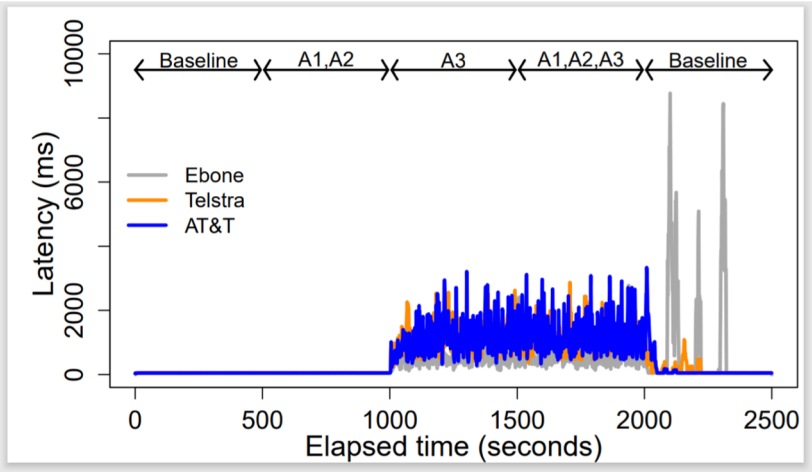
Puzzle solving complexity and size



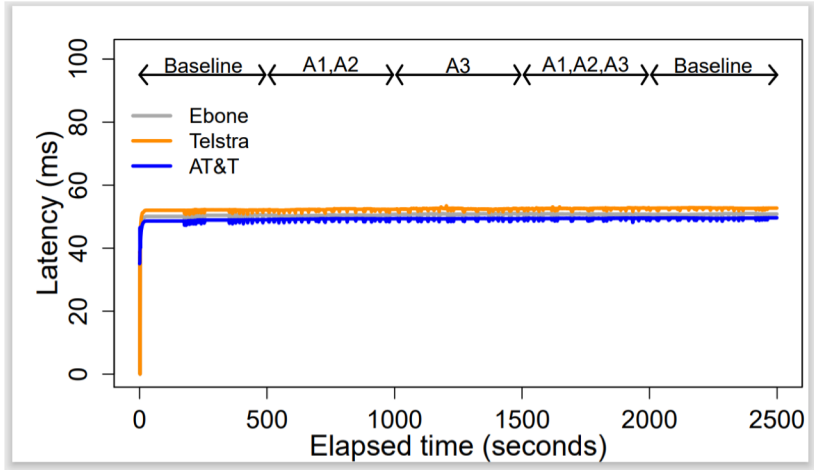


In simulation, we applied a random delay from ~N(2.56s, 0.046s) to represent puzzle solving latency (for a polynomial of degree 5000) on an Intel Core-i5, 2.5GHz, 1GB RAM machine.

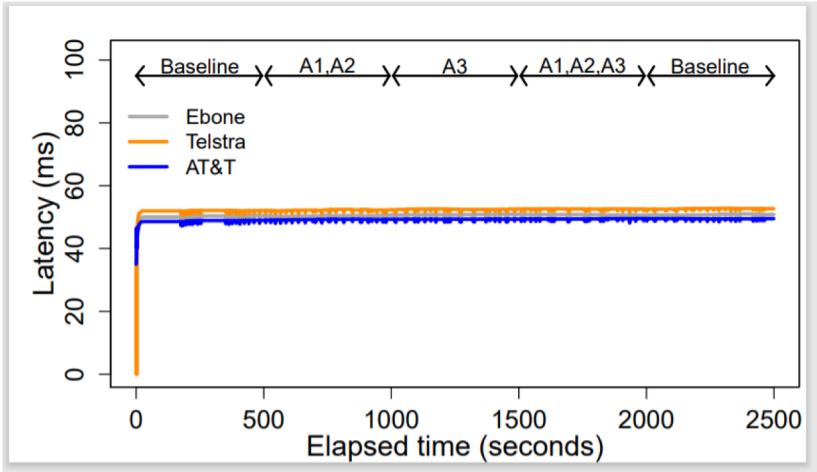
Compromised infrastructure drastically impacts users' experienced **latency** in RL but not BFA and SR+.



RL



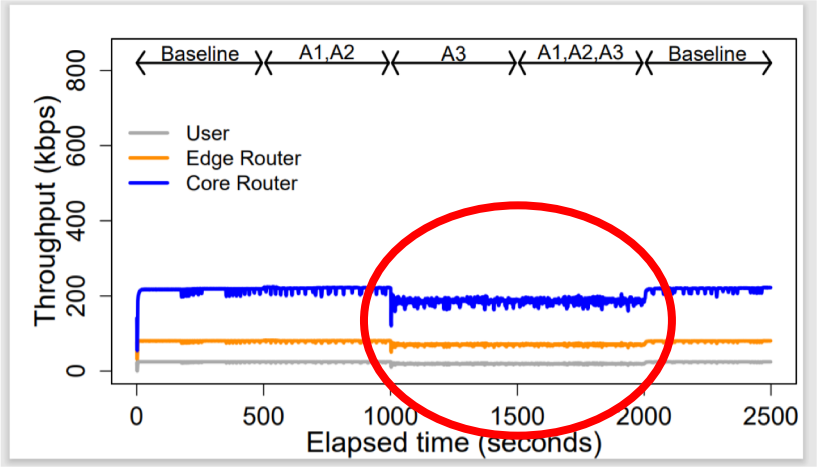
SR+



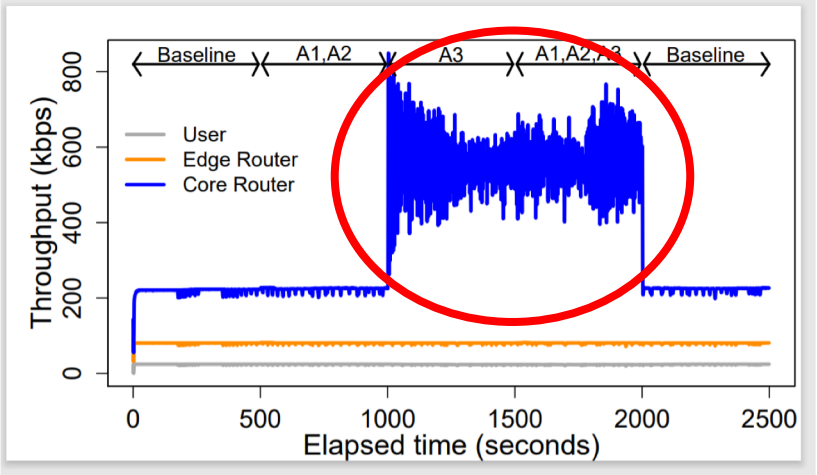
BFA

	Ebone	Telstra	AT&T
RL	85.06	75.54	80.28
SR+	99.99	99.99	99.99
BFA	99.97	99.92	99.95

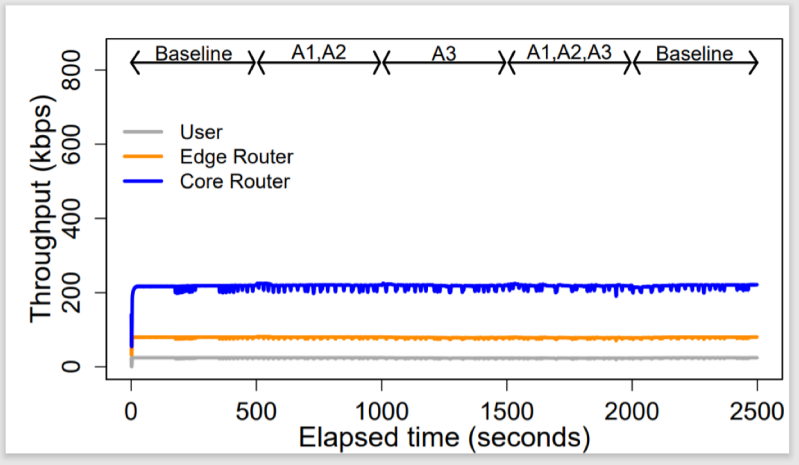
Lack of request aggregation in SR+ imposes high overhead on core routers while BFA maintains its performance.



RL

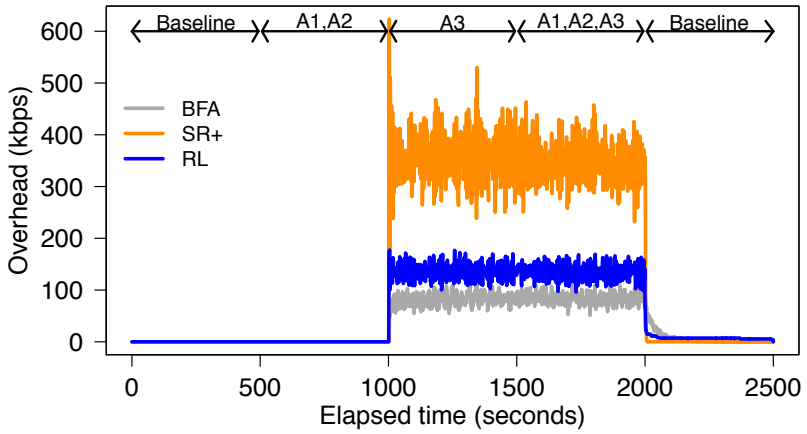


SR+

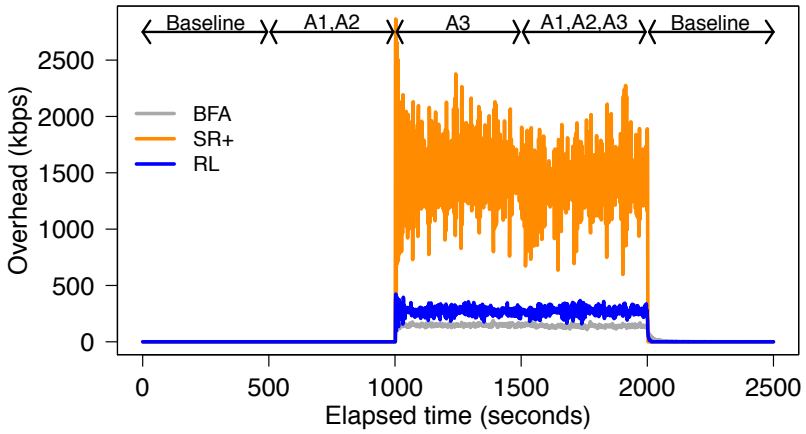


BFA

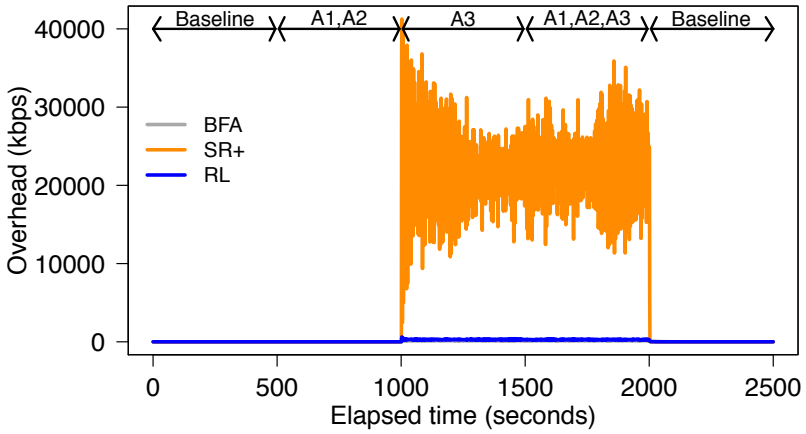
SR+ introduced the highest communication overhead followed by RL and BFA (the least overhead) across all topologies.



Ebone



Telstra



AT&T

Takeaways

PERSIA offers an edge-centric DDoS prevention mechanism and a dynamic in-network mitigation strategy that operate independently.

The main objective of PERSIA is satisfying the expected users Quality of Experience with minimal impact on network resources.

We plan to integrate PERSIA with a token-based access control mechanism towards building a secure edge-centric framework.

Questions?

Email: reza.tourani@slu.edu
Assistant Professor
Computer Science
Saint Louis University