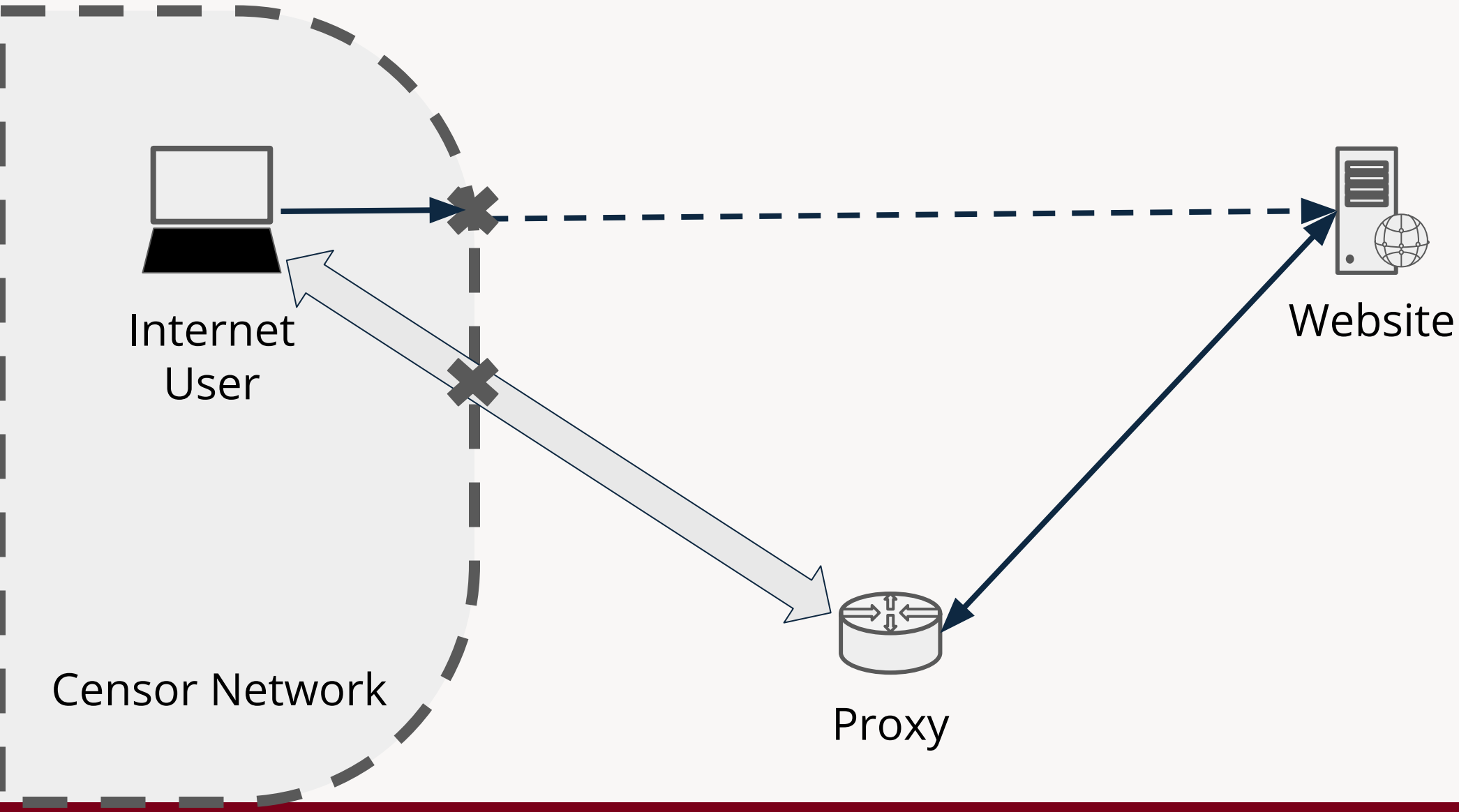
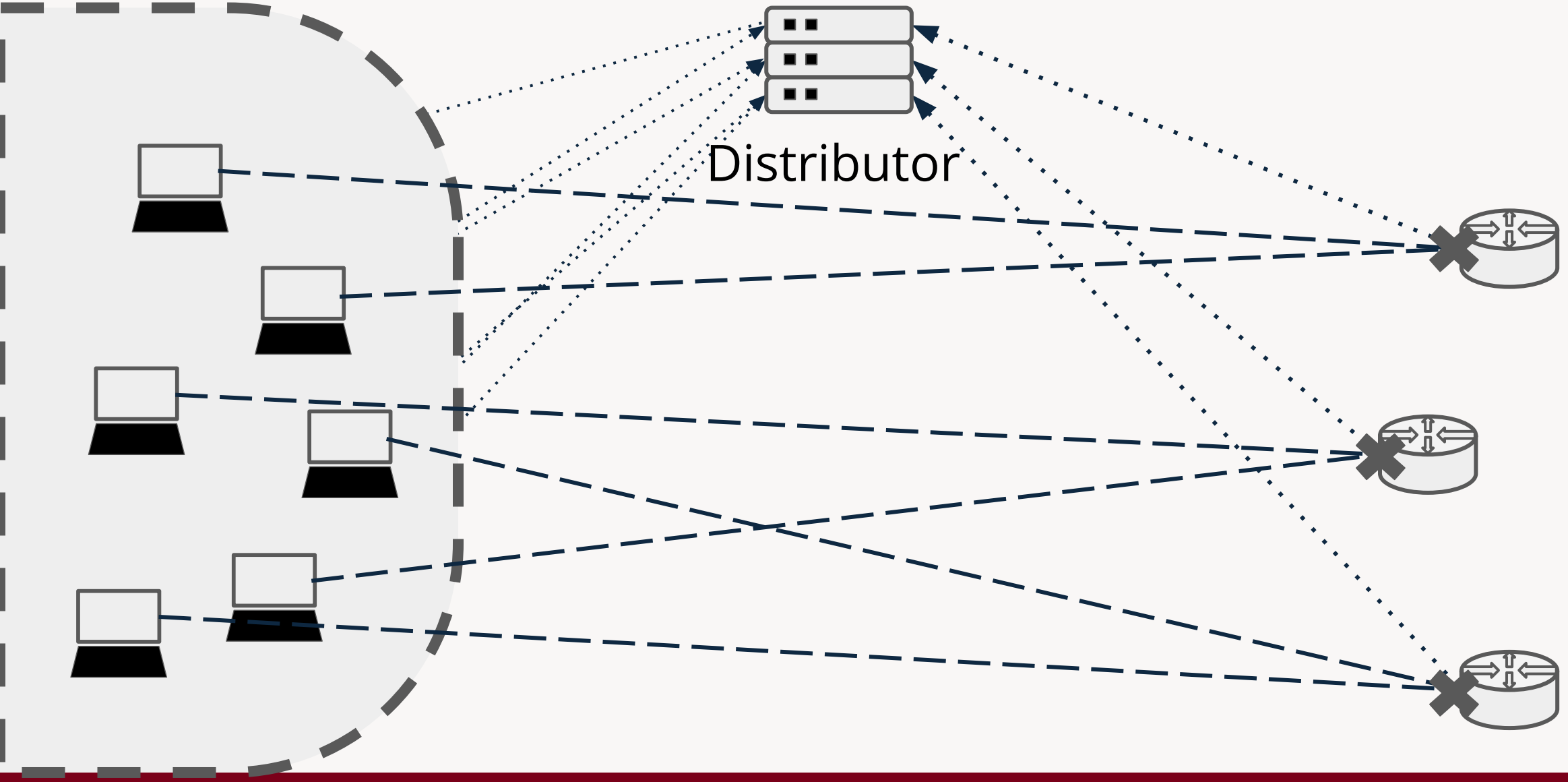
The Game Has Changed:
Revisiting proxy distribution and game theory

Hassan Fares, Omkar Fulsundar, Nick Hopper

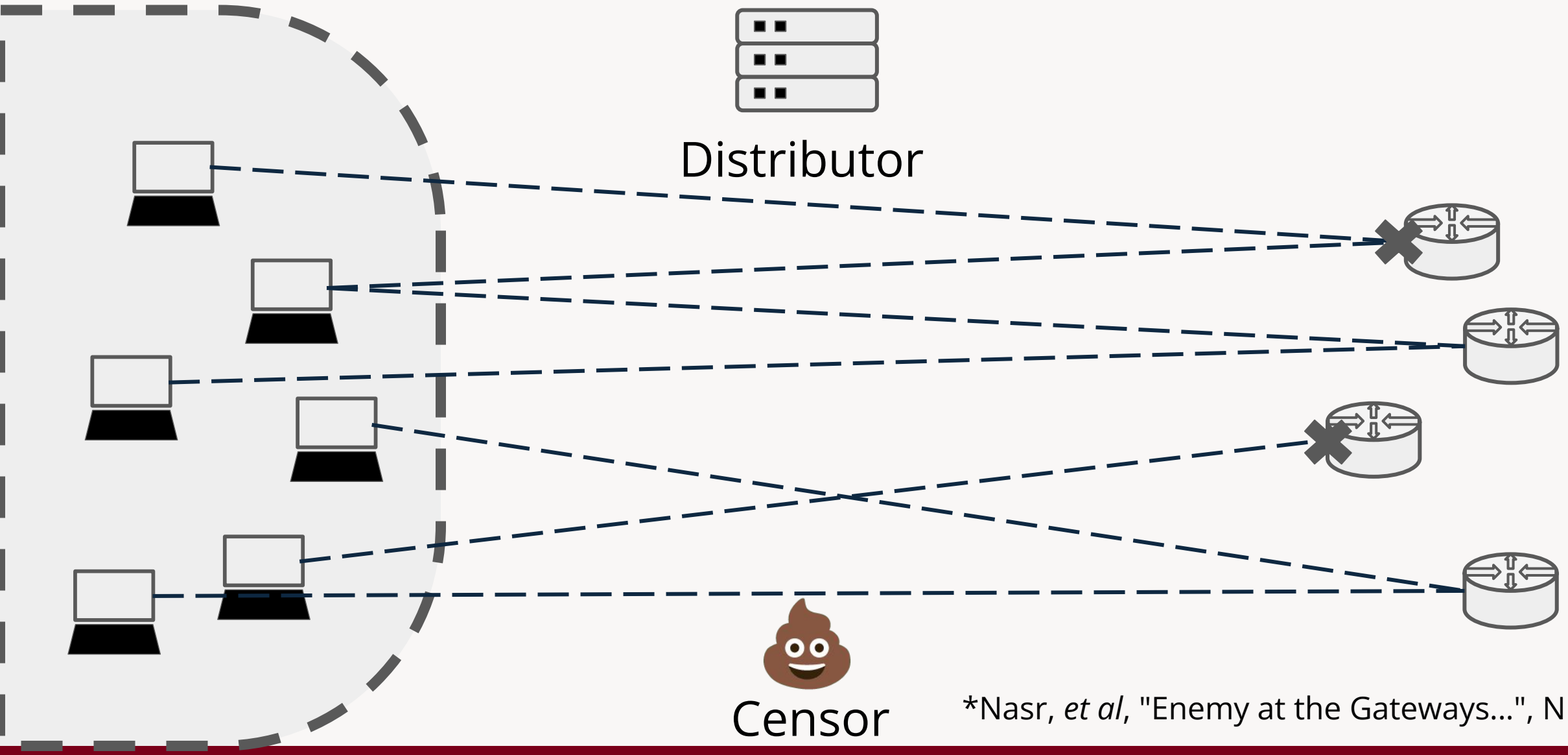
Censorship Circumvention and Proxies



Proxy Distribution



ENEM19 Framework*



*Nasr, *et al*, "Enemy at the Gateways...", NDSS19

What's new?

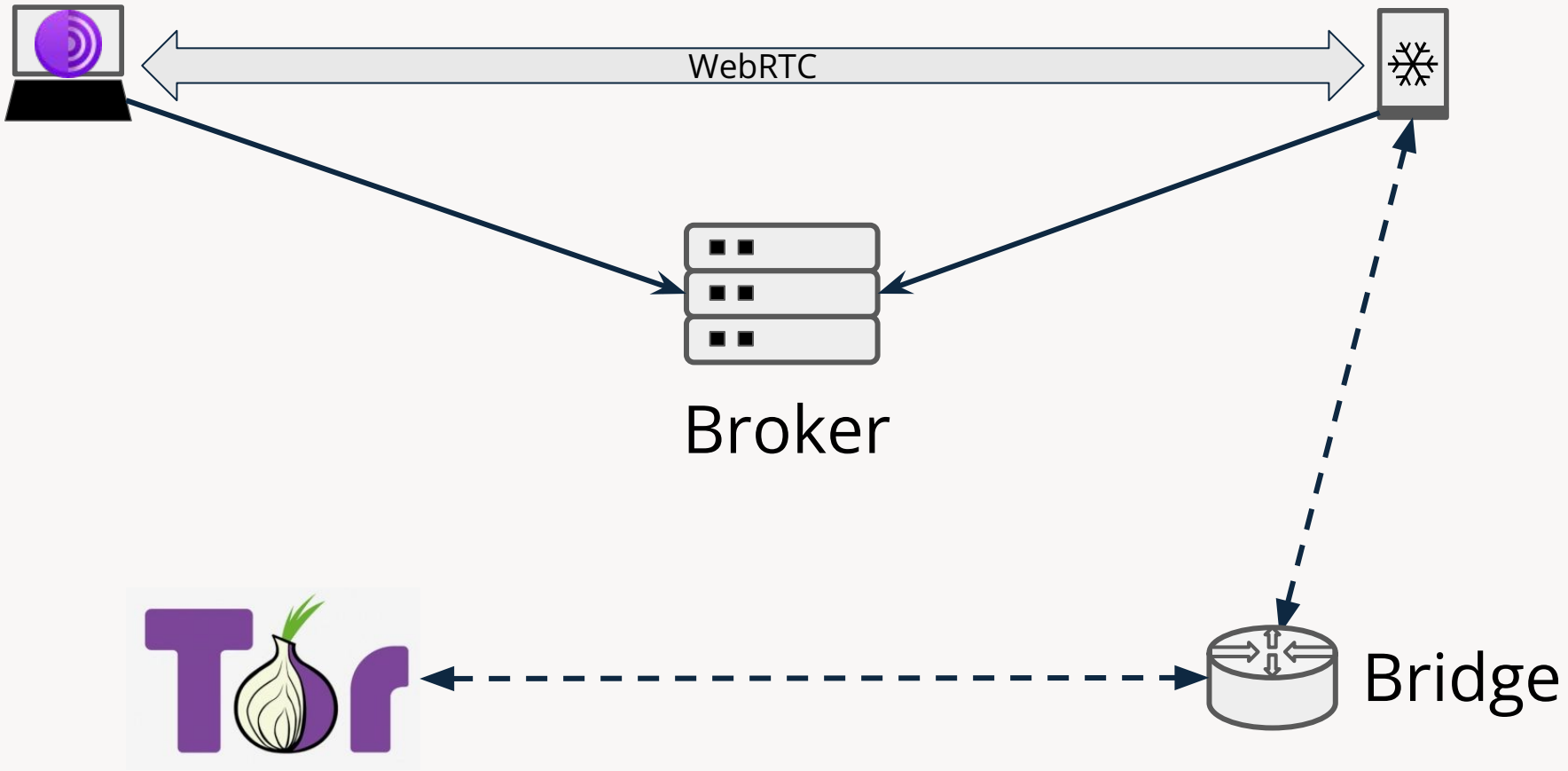
New circumvention ideas: ephemeral proxies, collateral damage, new transports...

Increased use of traffic analysis, new analysis attacks

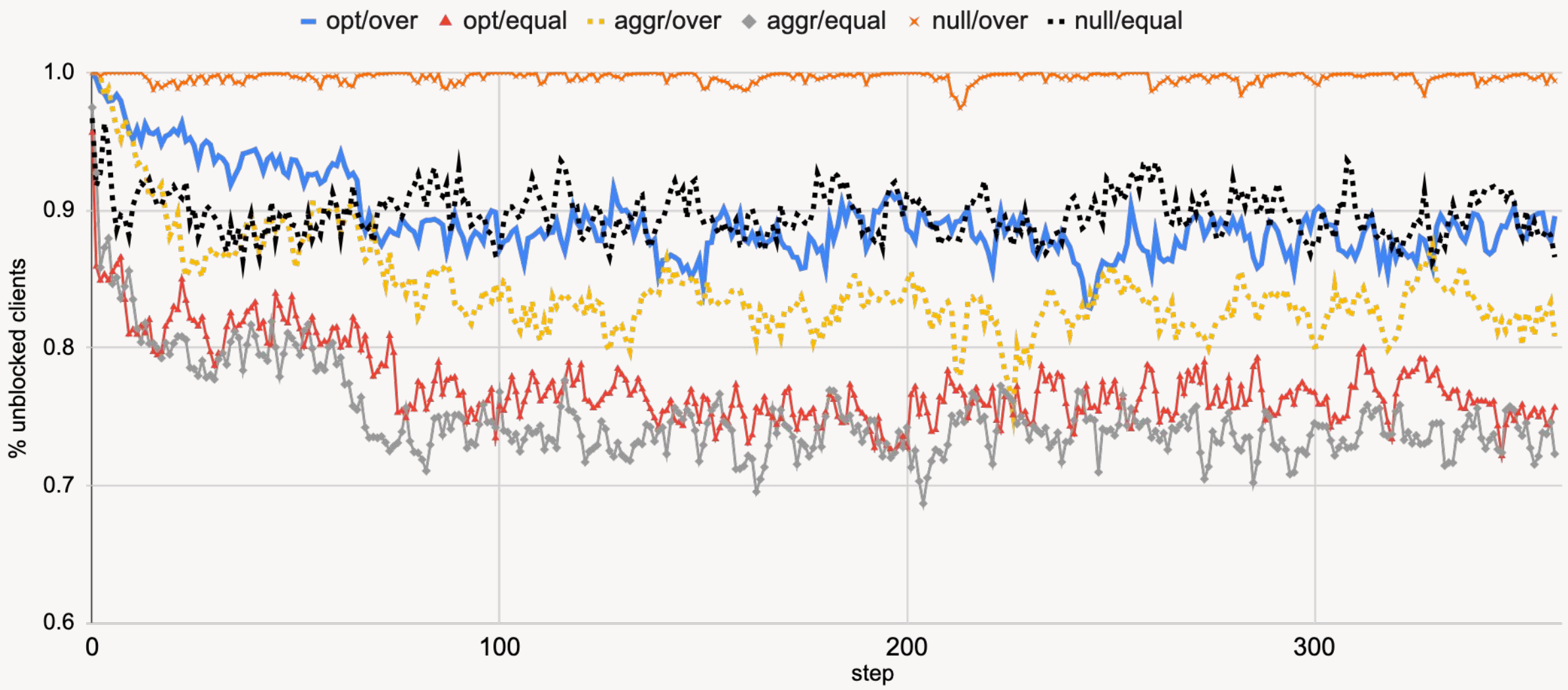
Better understanding of censor infrastructure and capabilities: censors are not monolithic, proxies are not (globally) blocked or not

RQs: How do these changes impact the game?

Ephemeral Proxies: snowflake



Snowflake availability

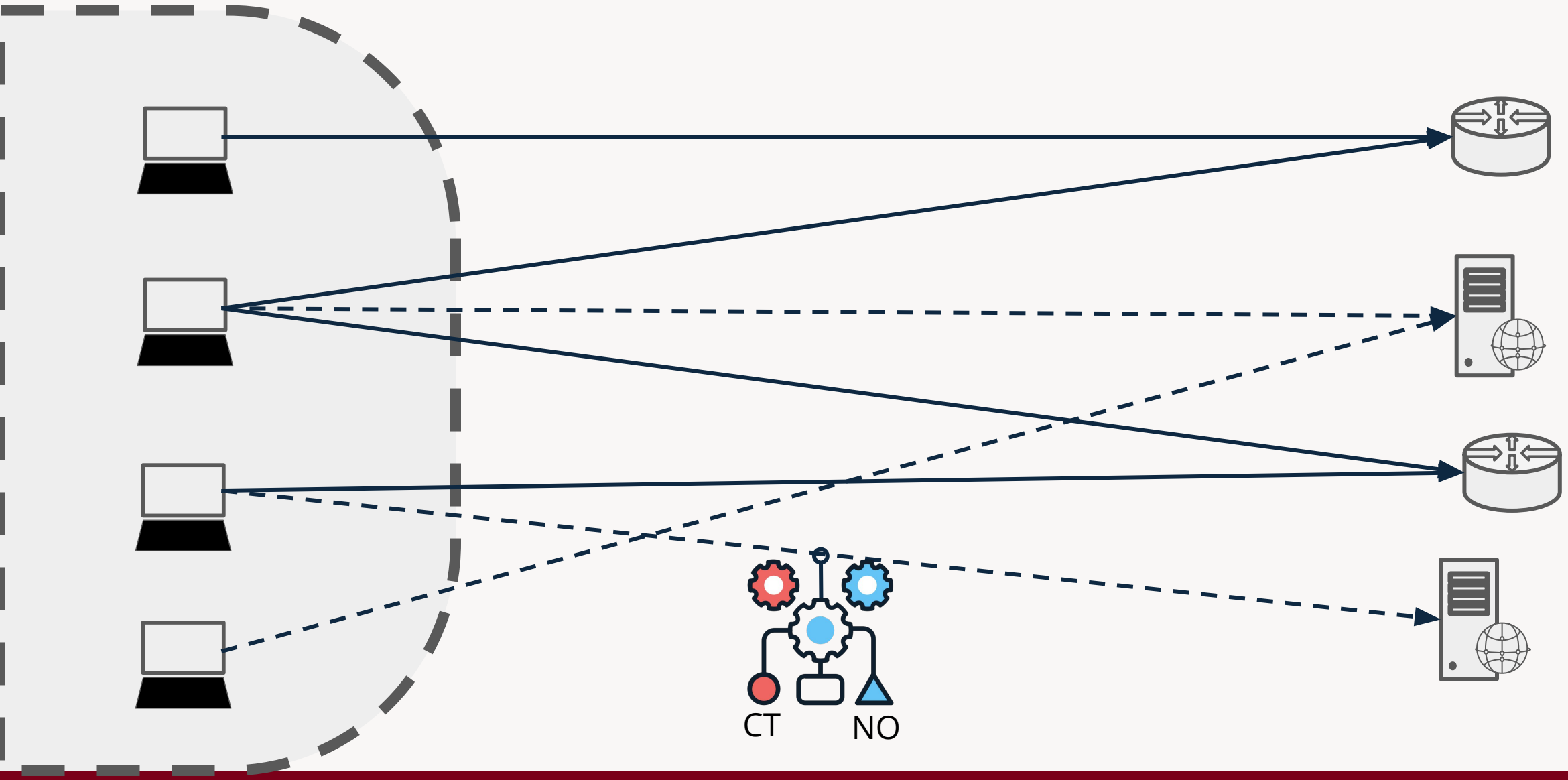


Wait times…

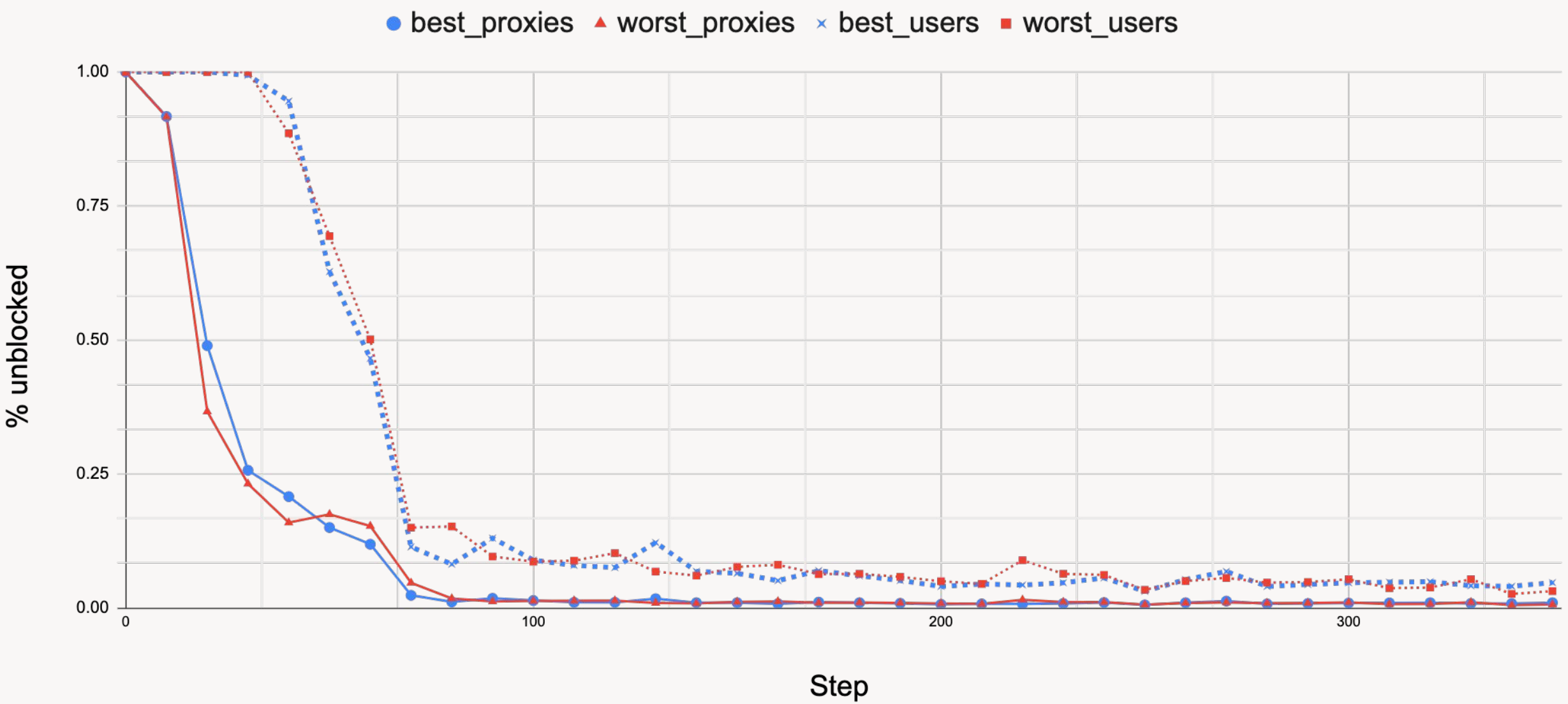
	null		optimal		aggressive	
	over	equal	over	equal	over	equal
1	99.96%	97.67%	97.02%	91.04%	95.02%	95.01%
2	0.03%	1.95%	2.53%	6.80%	4.11%	4.11%
3	0.0001%	0.31%	0.37%	1.61%	0.72%	0.72%
4	0	0.05%	0.06%	0.40%	0.13%	0.13%
≥5	0	0.01%	0.01%	0.16%	0.03%	0.03%

Conclusion: Snowflake effectively resists insider enumeration

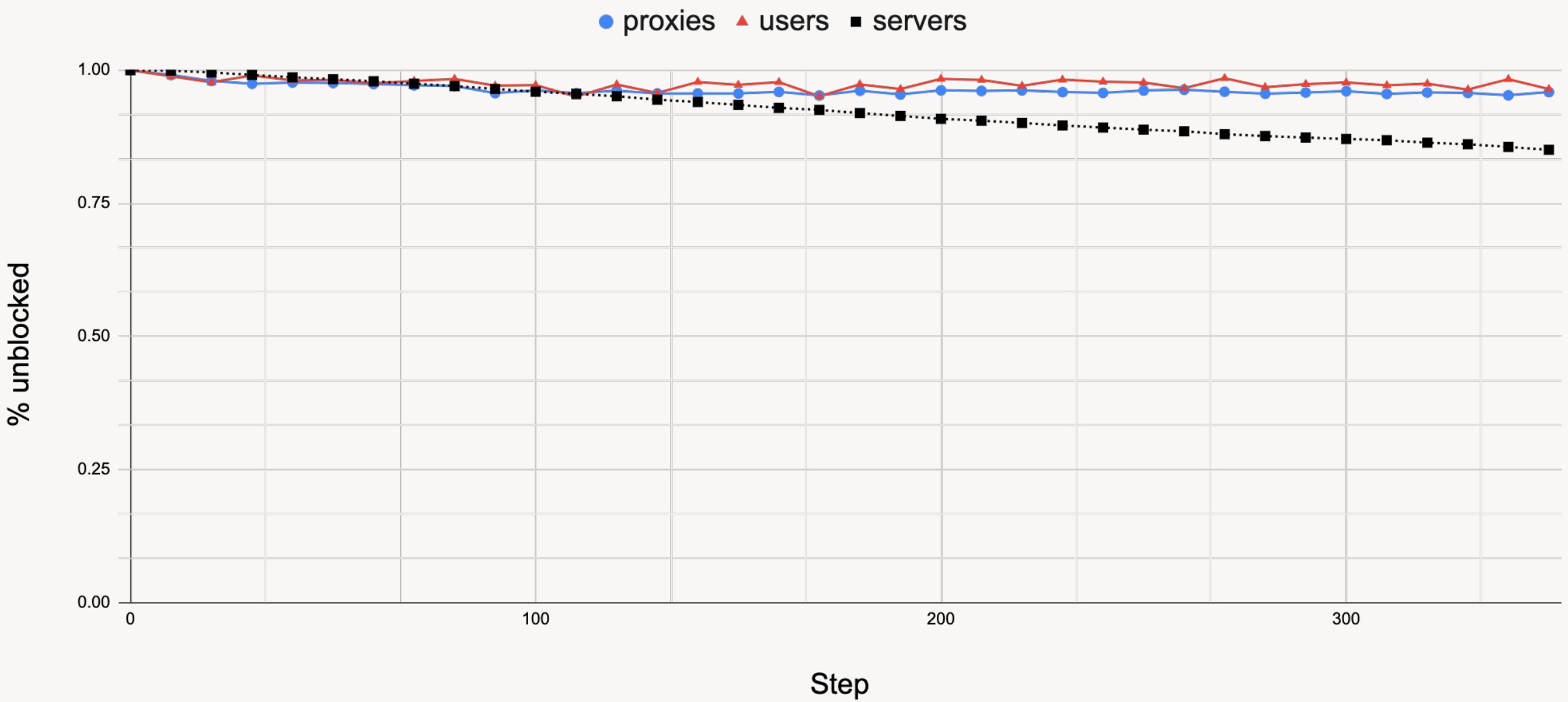
Traffic analysis: zig-zag



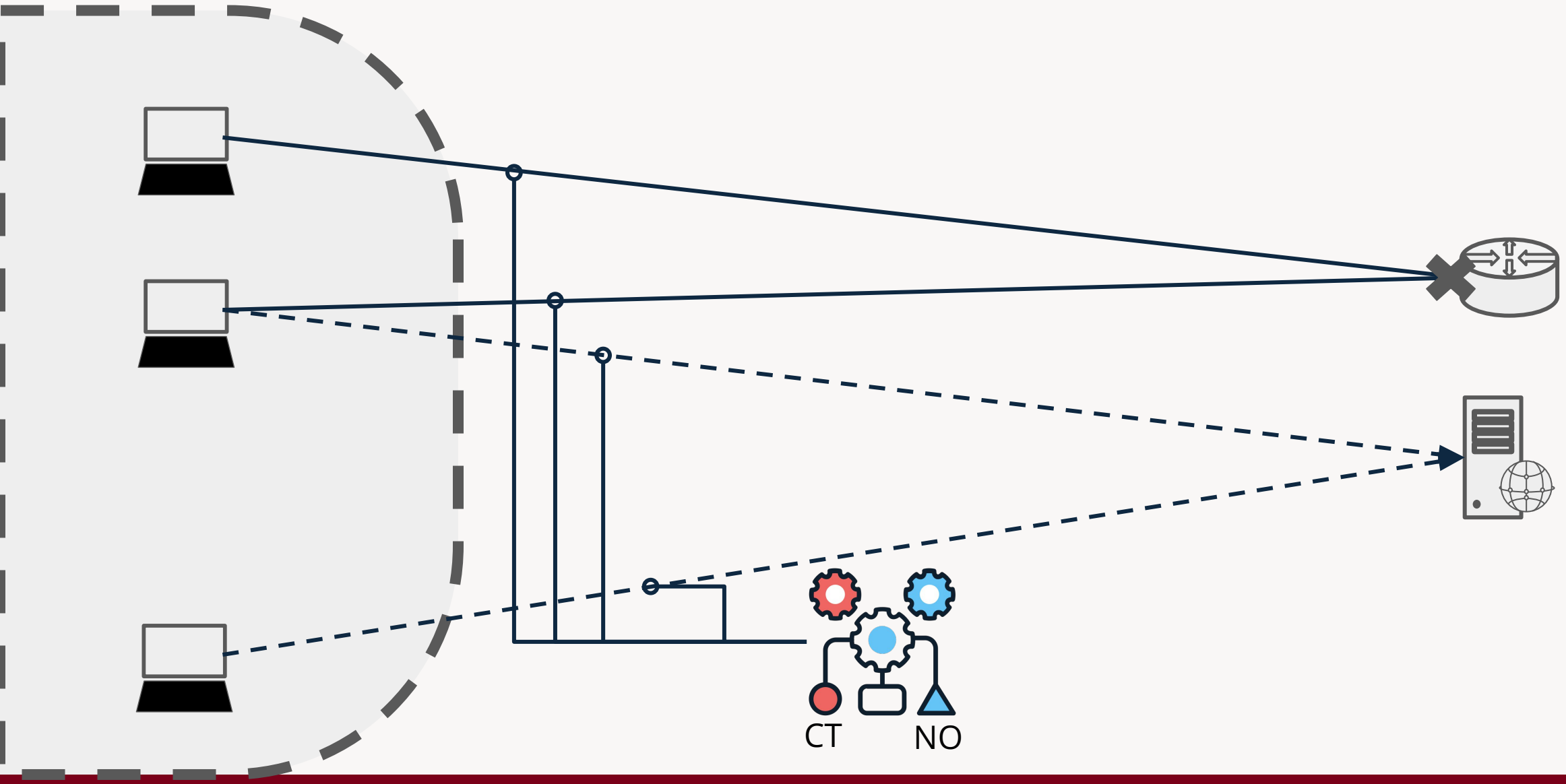
Zig-Zag Collateral Damage



Zig-Zag vs. Snowflake



Host Profiling attacks



Host Profiling & Collateral Damage

w	τ	cls	U_{70}	U_{90}	S_{70}	S_{100}	S_{final}
3	3	best	2.41%	1.05%	99.54%	99.08%	96.82%
3	3	mid	2.45%	2.13%	97.86%	95.90%	85.82%
3	3	worst	1.71%	2.95%	96.01%	92.47%	73.09%
3	9	worst	2.43%	2.10%	98.74%	98.08%	94.54%
5	5	worst	0.62%	1.07%	96.88%	94.82%	82.56%
5	15	worst	96.61%	2.09%	99.04%	98.56%	95.98%

Unblocked Users

Unblocked Servers

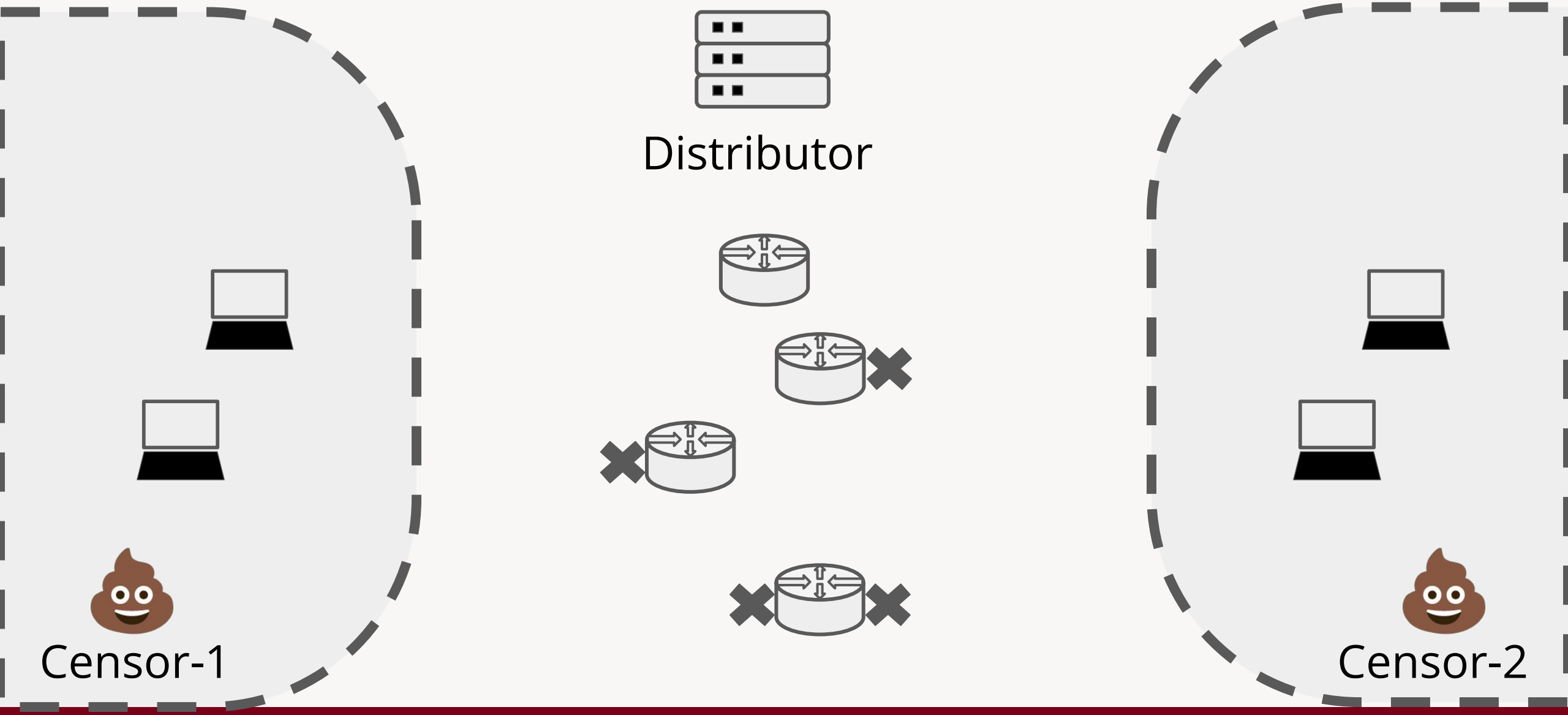
Host Profiling & Snowflake

t	1	2	3	4	5	6
$\Pr[\leq t]$,worst	84.25%	94.48%	98.01%	99.25%	99.72%	99.9%
$\Pr[\leq t]$,best	84.29%	94.50%	98.03%	99.29%	99.73%	99.9%

Host profiling reduces collateral damage and is an effective censor strategy

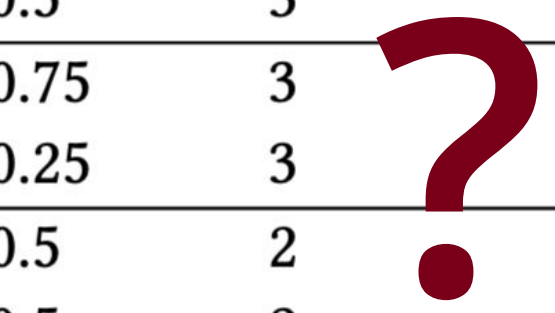
Snowflake effectively evades zig-zag and host profiling attacks

Multi-Censor Scenario



Multi-Censor Simulations

censor	weight	proxy-use	90% wait	collateral
optimal	0.75	5	25	-
optimal	0.25	6	13	-
optimal	0.5	2	27	-
optimal	0.5	3	22	-
optimal	0.75	3	38	-
aggressive	0.25	3	8	-
optimal	0.5	2	25	-
aggressive	0.5	2	7	-
optimal	0.75	6	3	-
zigzag	0.25	4	10	44.40%
optimal	0.5	11	1	-
zigzag	0.5	4	4	90.72%



Open Questions

Can we formulate optimal strategies for these scenarios?

Can we combine multiple transport or distribution strategies?

What about flow blocking?

How can we model multiple user-distributor channels?

SimProxy

https://github.com/hoppernj/ProxySimulator