Alias Resolution Based on ICMP Rate Limiting

Kevin Vermeulen[(1)], Burim Ljuma[(1)], Vamsi Krishna[(1)],
Reza Rejaie[(2)], Olivier Fourmaux[(1)], Timur Friedman[(1)]
[(1)]Sorbonne Université, [(2)]University of Oregon

Context

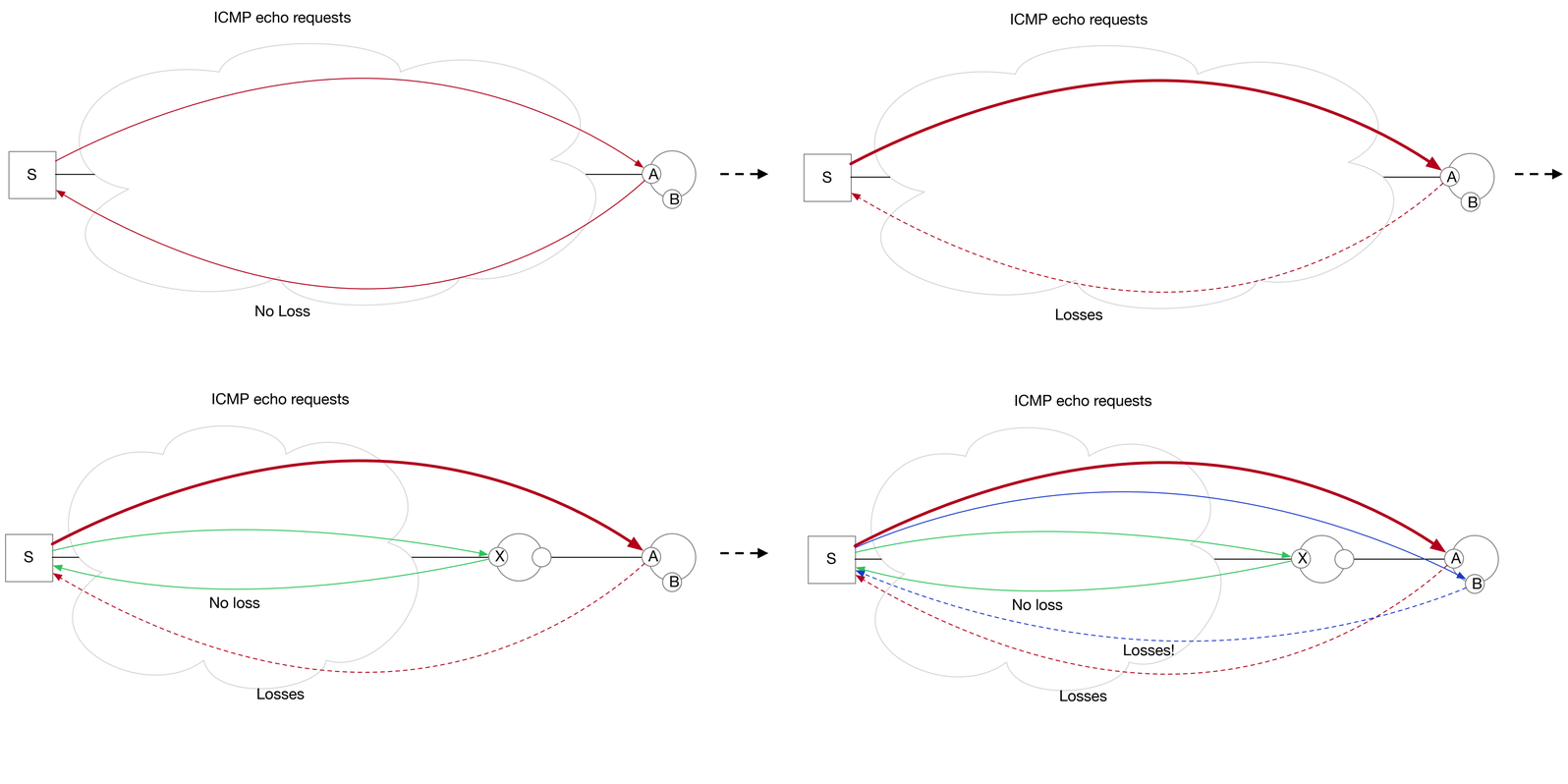
Alias resolution in Internet topology mapping:
Process of grouping IP into routers.

IPv6 alias resolution is very incomplete.
ICMP rate limiting has never been exploited.

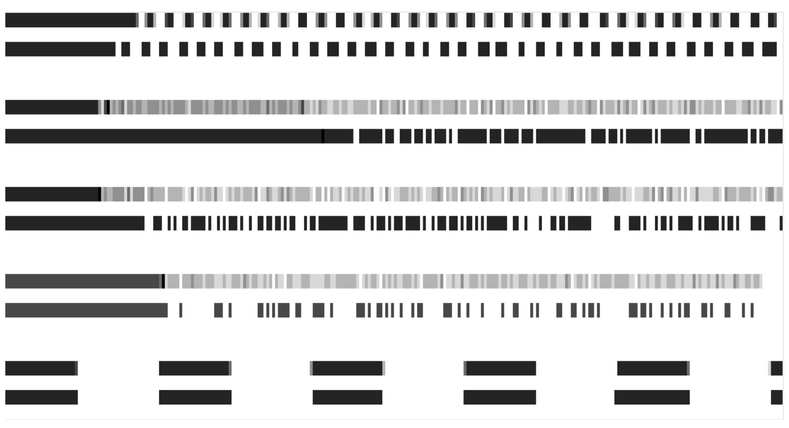
ICMP rate limiting:
Feature of routers to limit the number of ICMP packets that they send/receive within a window of time.
Implementation varies with router vendor/OS.

Pipeline

1. Trigger ICMP rate limiting on A, does it affect B?



2. Generate time series



3. Extract features

- Loss rate
- Change point
- gap -> gap transition probability
- burst -> burst transition probability
- Pearson correlation coefficient

4. Supervised classifier

- Output if two IPs are aliases
- Trained on Internet-wide alias sets

Results

Comparison with two state-of-the-art techniques, Midar (IPv4) and Speedtrap (IPv6).

Ground truth evaluation:
Precision, recall.

Internet wide data:
Portion of alias pairs found by each tool.

Ground truth networks

		Midar	Limited Ltd.	Midar ∪ Limited Ltd.
Internet2	Precision	1.000	1.000	1.000
	Recall	0.673	0.800	0.868
Switch	Precision	1.000	1.000	1.000
	Recall	0.090	0.499	0.599

		Speedtrap	Limited Ltd.	Speedtrap ∪ Limited Ltd.
Internet2	Precision	N/A	1.000	1.000
	Recall	N/A	0.684	0.684
Switch	Precision	1.000	1.000	1.000
	Recall	0.384	0.385	0.772

Internet-wide data

	Limited Ltd.	Not Limited Ltd.	
Midar	0.236	0.495	0.731
Not Midar	0.269	N/A	0.269
	0.505	0.495	1.000

	Limited Ltd.	Not Limited Ltd.	
Speedtrap	0.109	0.150	0.259
Not Speedtrap	0.741	N/A	0.741
	0.850	0.150	1.000

Acknowledgments:
This work has received funding from the French Ministry of Defense and from the LINCS laboratory.