A First Look at the Prevalence and Persistence of Middleboxes in the Wild

Korian Edeline, Benoit Donnet
Montefiore Institute, University of Liège
Belgium

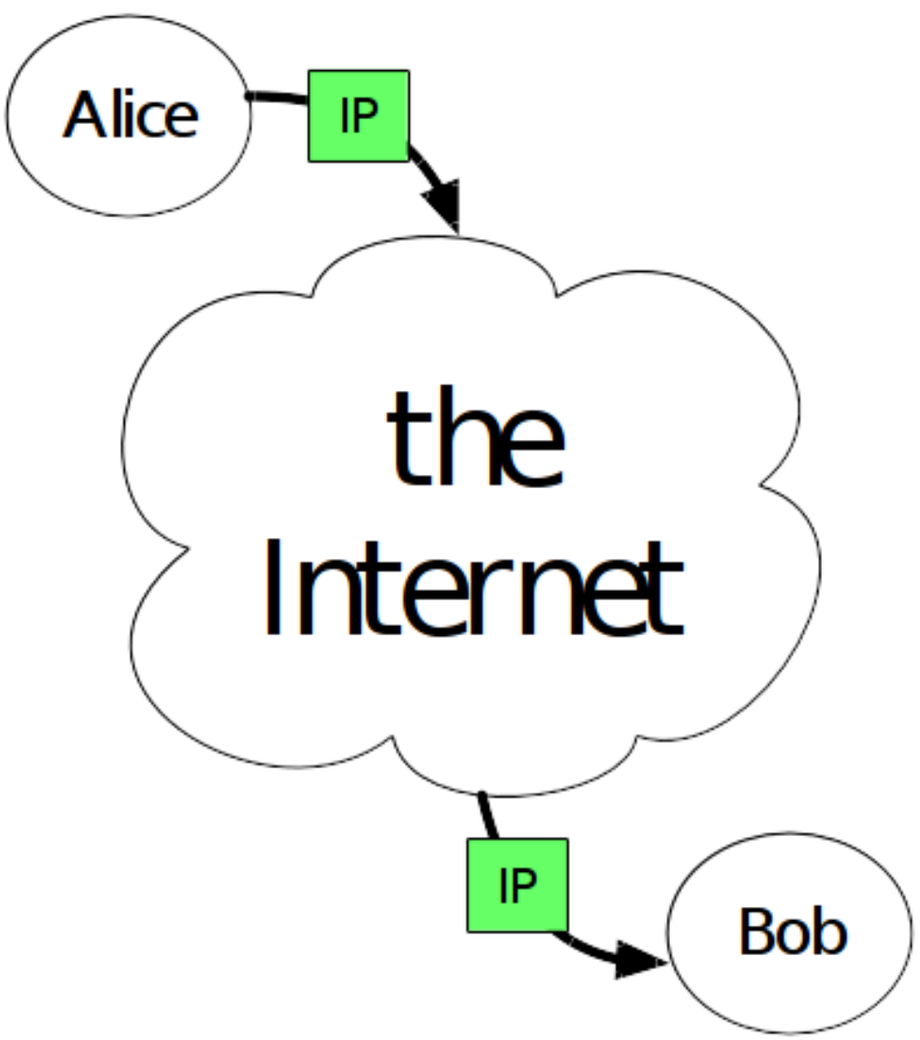
mami
measurement and architecture for a middleboxed internet

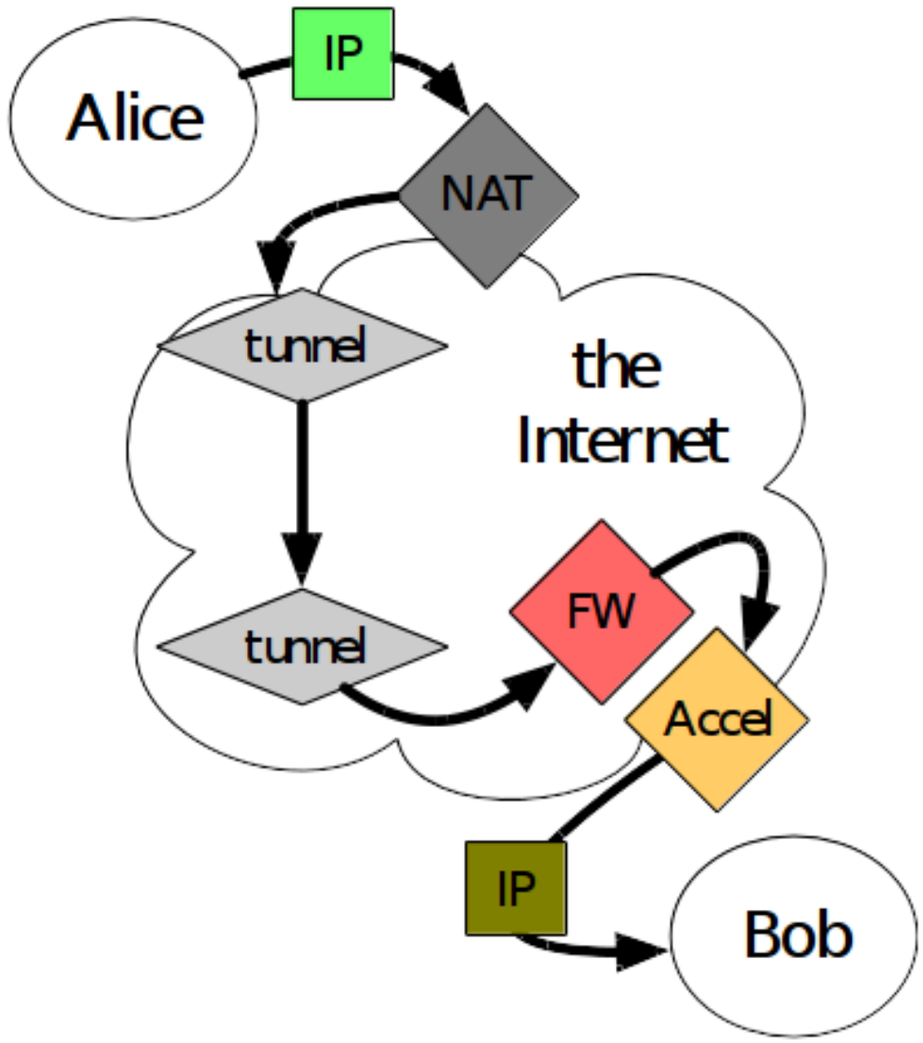
LIÈGE université

measurement | architecture | experimentation

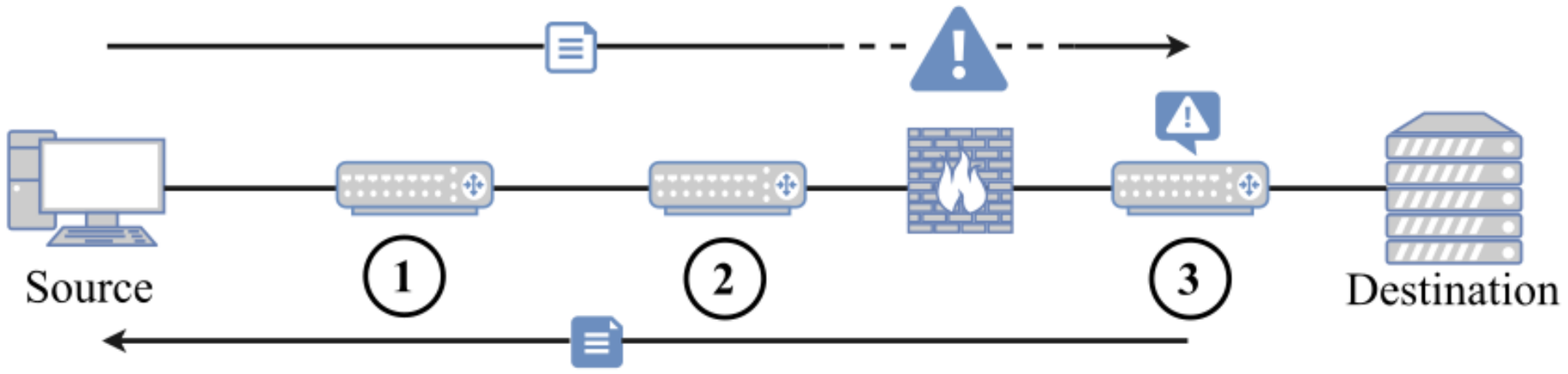
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 688421.The opinions expressed and arguments employed reflect only the authors' view. The European Commission is not responsible for any use that may be made of that information.

A middleboxed internet



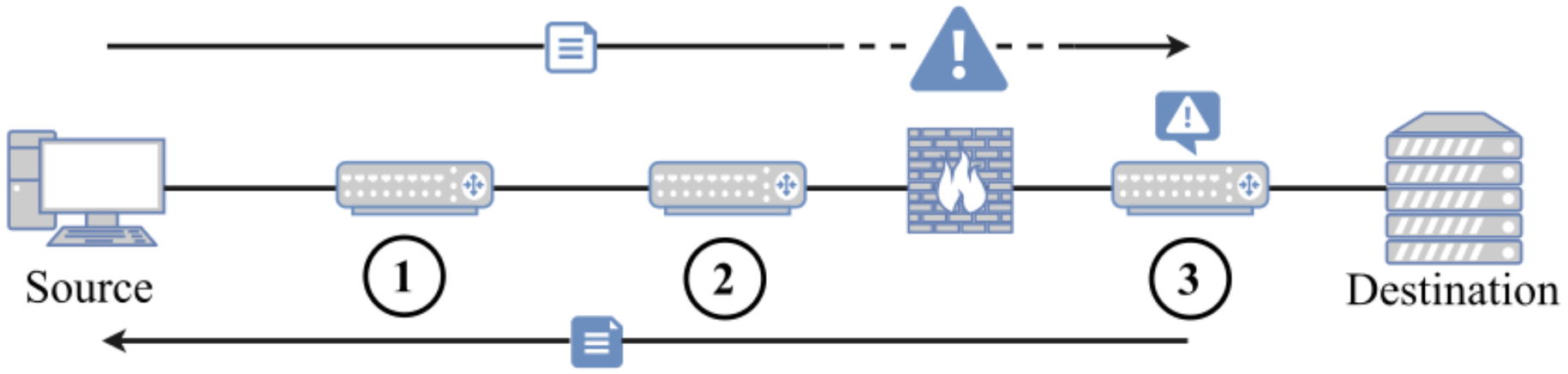


tracebox


Source
1
2
3
Destination


Router
Middlebox
TCP Probe
ICMP Message
Informant router
x
ICMP-triggering TTL

tracebox

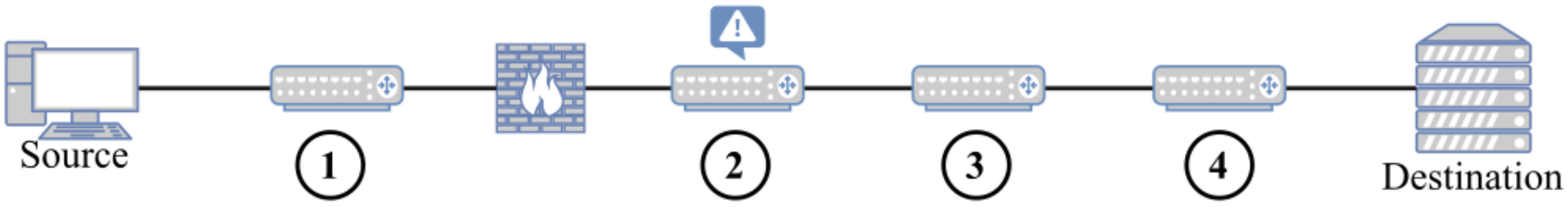


- **RFC 792** : “The internet header plus the first 64 bits”
- **RFC 1812** : “as much [...] as possible” (< 576 B)

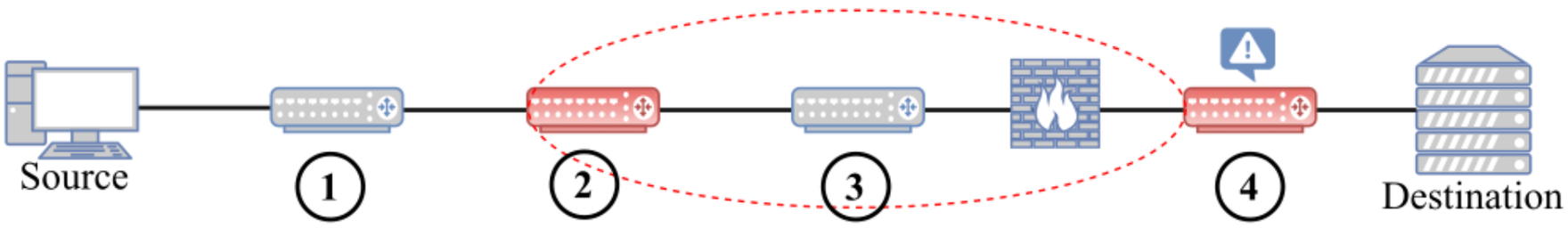
Dataset

- 14 Campaigns, one every ~5 day over 70 days.
- From 89 nodes to 594,241 destinations, 9 ports.
- 948,457 responsive intermediate hops overall (59,861 HTTP-only).
- 2,978 ASs crossed.
- **0.5B probes**

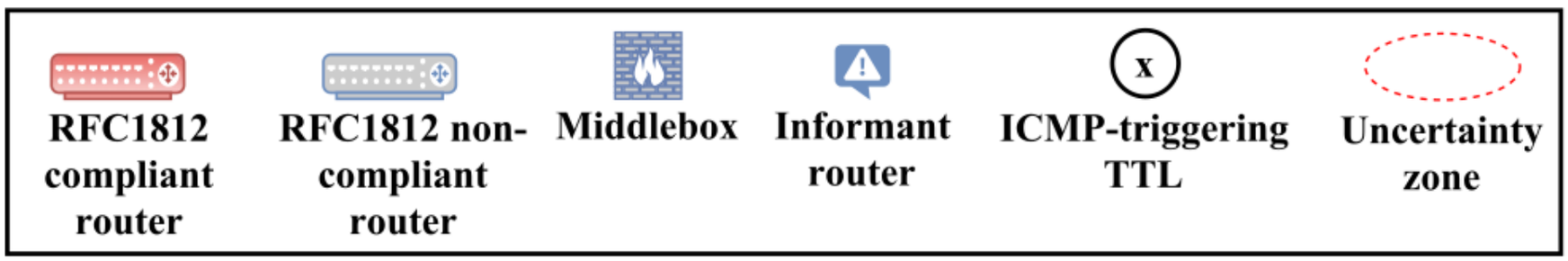
tracebox



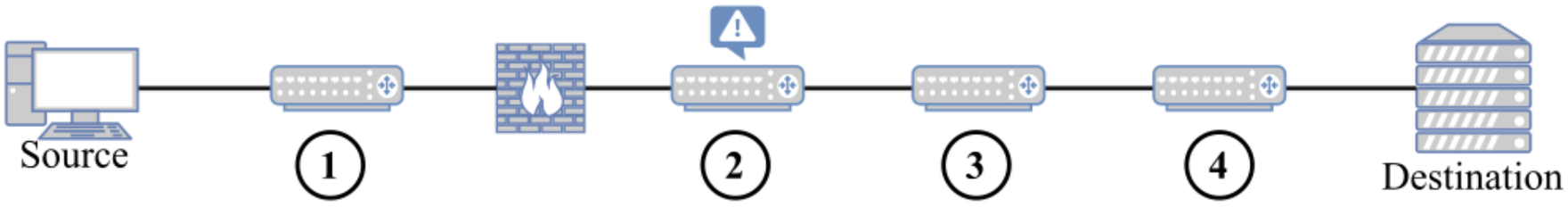
1. Modified field is within the first 48 bytes



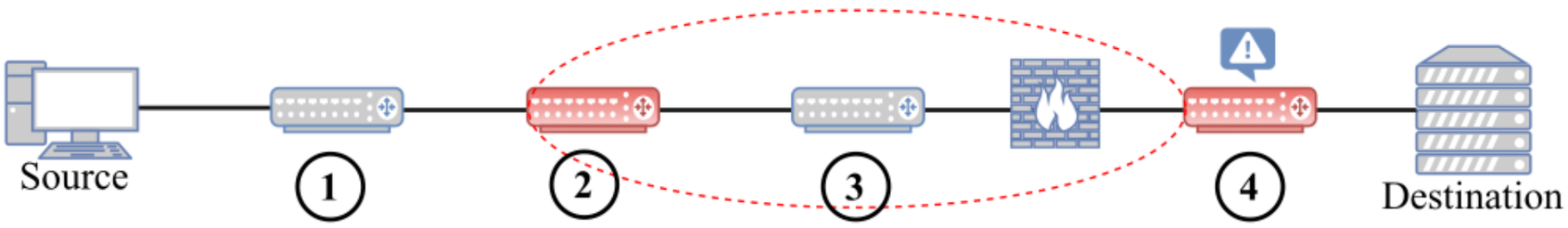
2. Modified field is outside the first 48 bytes



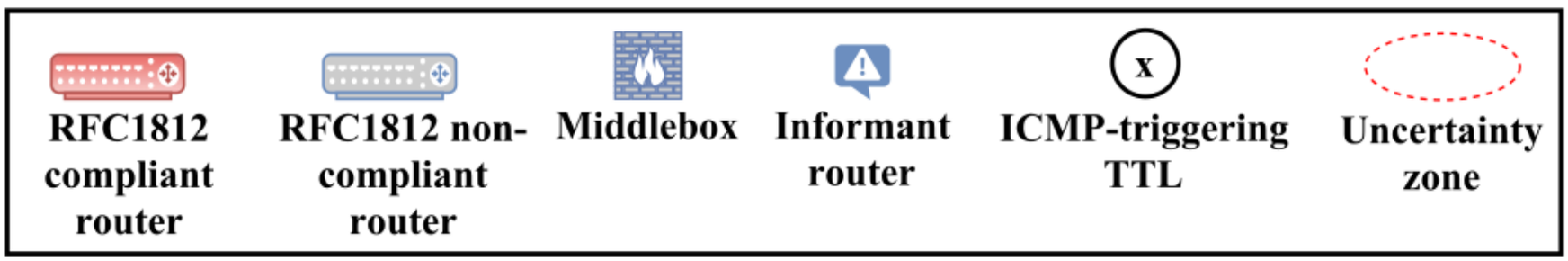
tracebox



1. Modified field is within the first 48 bytes

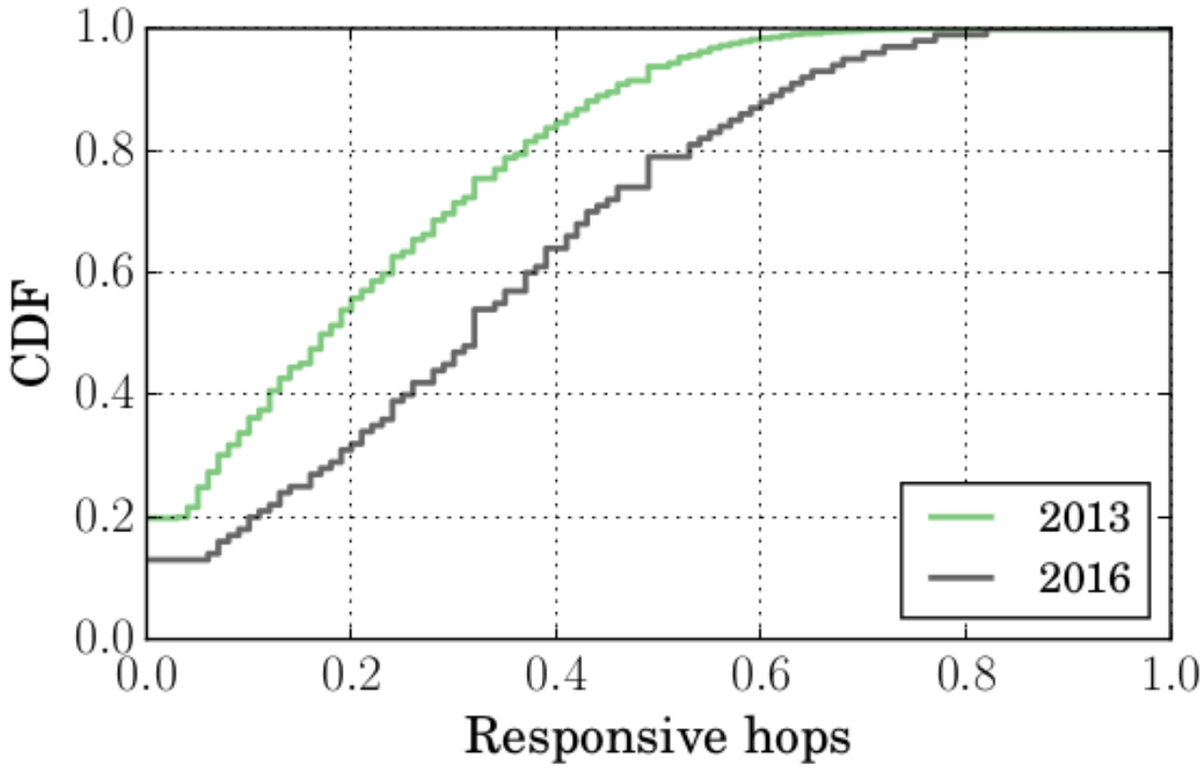


2. Modified field is outside the first 48 bytes

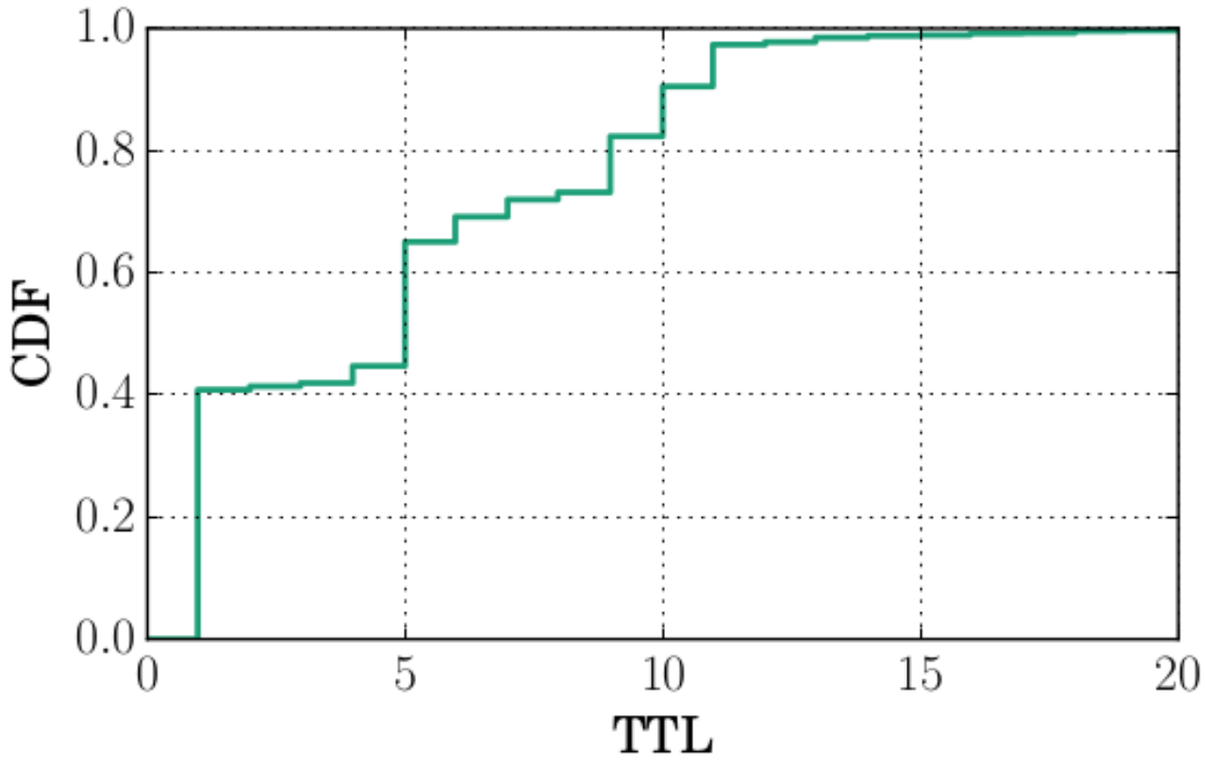


- **U Zone** : Observed sizes ? Workaround ?

Uncertainty Zone

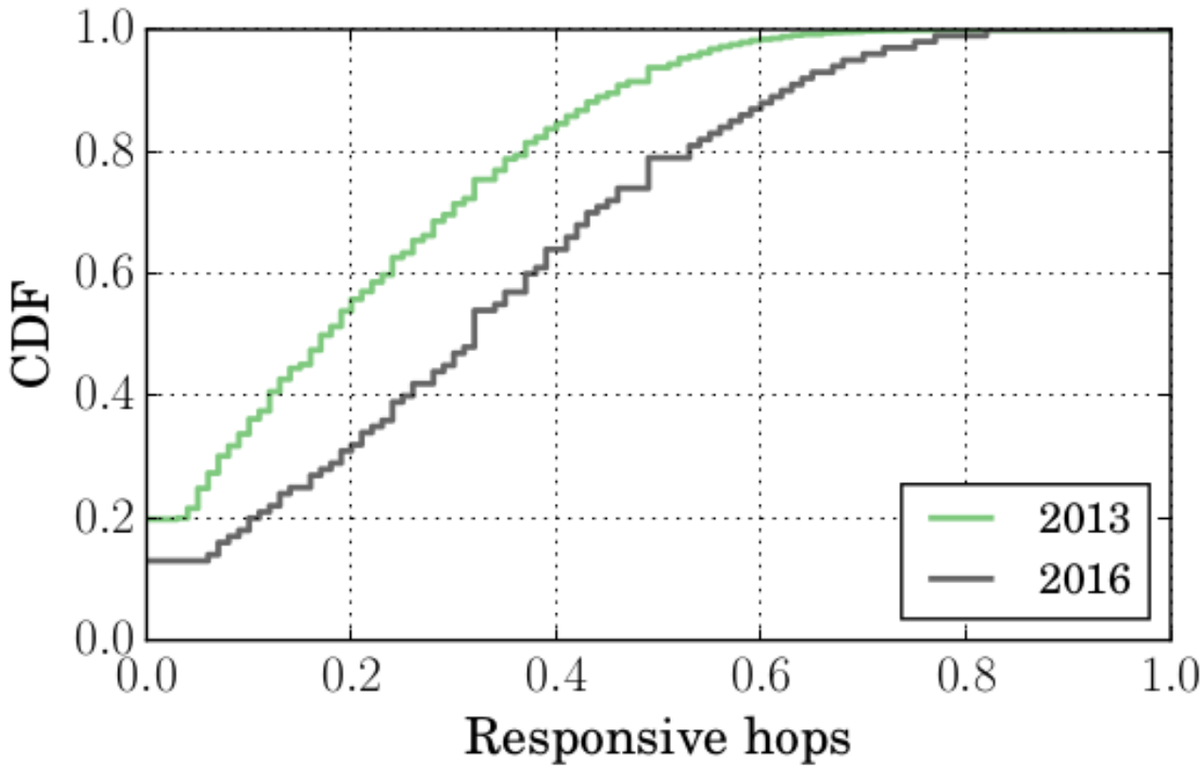


Proportion of RFC 1812 routers on observed paths



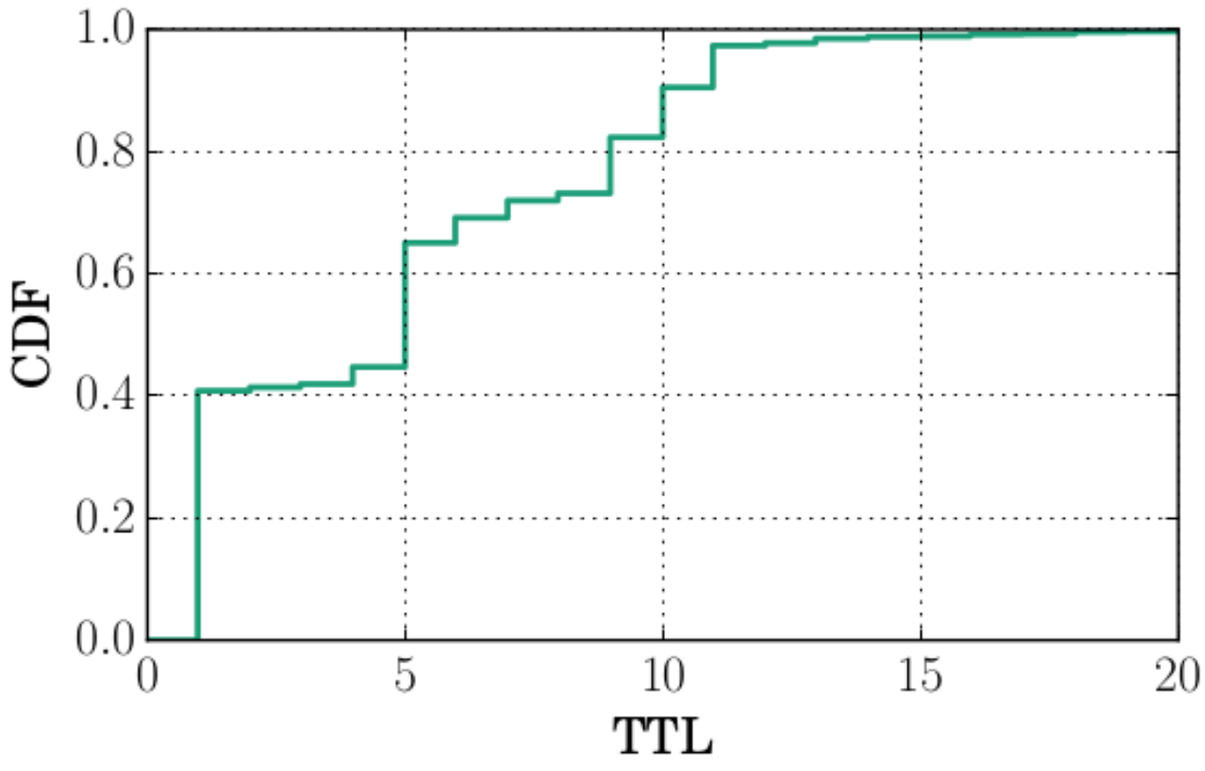
Sizes of U Zones

Uncertainty Zone



Proportion of RFC 1812 routers on observed paths

- *Increases over time*

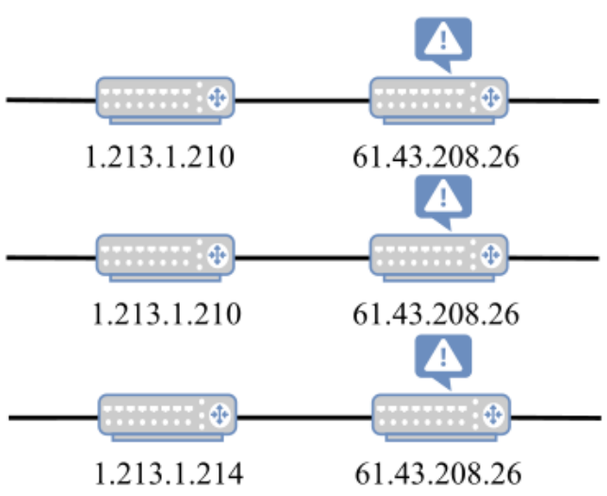


Sizes of U Zones

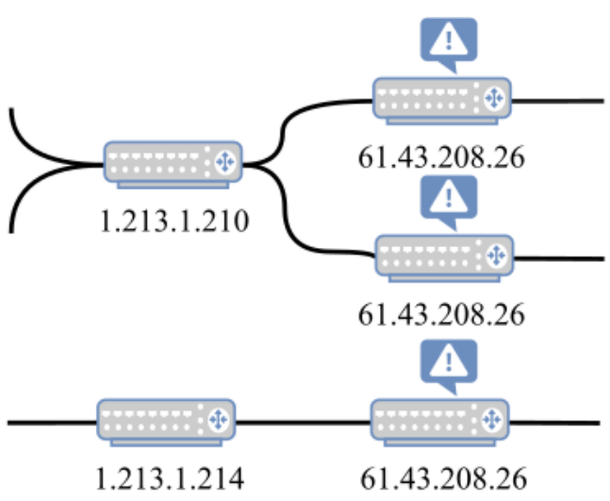
- None for 15.5M obs. (41%)
- ≤ 5 for 23M obs. (66%)

Pre-processing: Summary

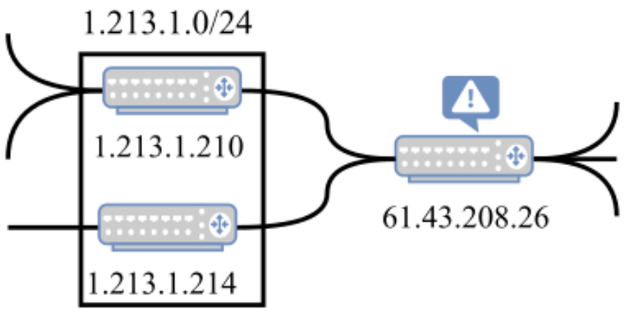
- Observation : *A single modification observed on a path during a campaign.*



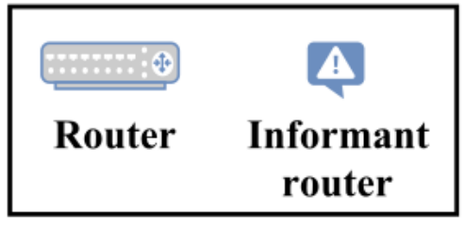
a. Offenders derivation



b. Offenders grouping



c. Offenders merging



Input: 38M obs.

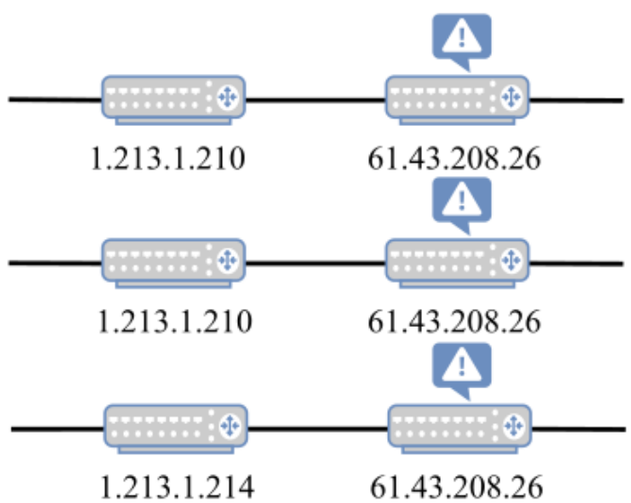
a. Label observations

b. Aggregate observations

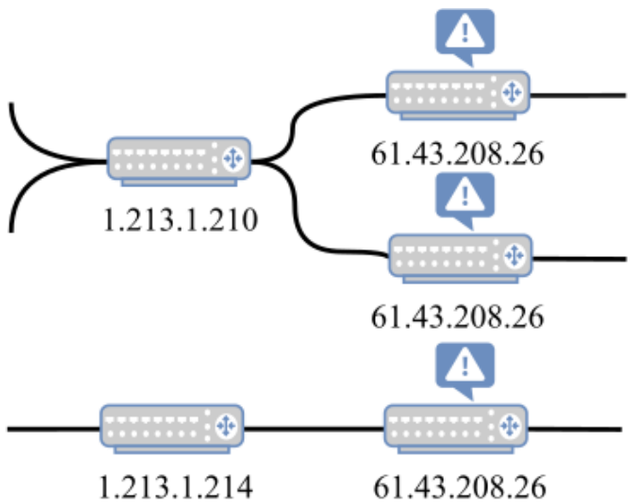
c. Merge offenders into middleboxes

Output: 8K MBs

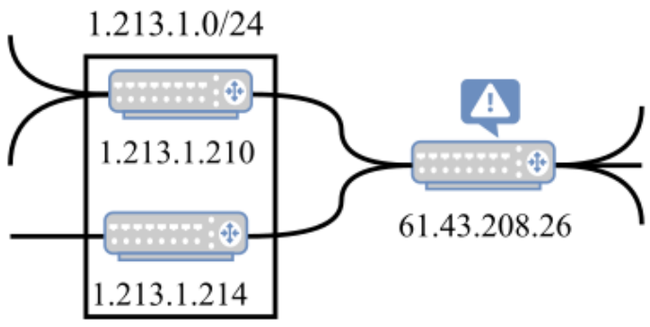
Pre-processing: derivation (Step 1)



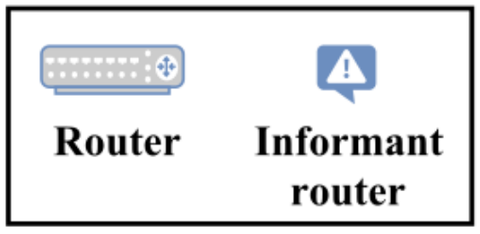
a. Offenders derivation



b. Offenders grouping



c. Offenders merging

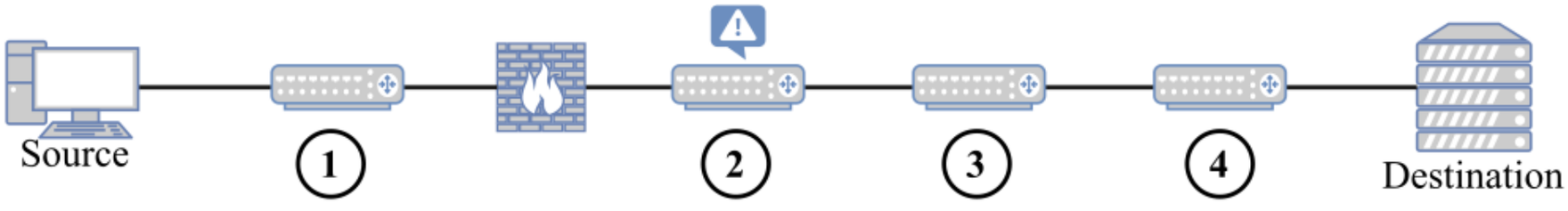


Pre-processing: derivation (Step 1)

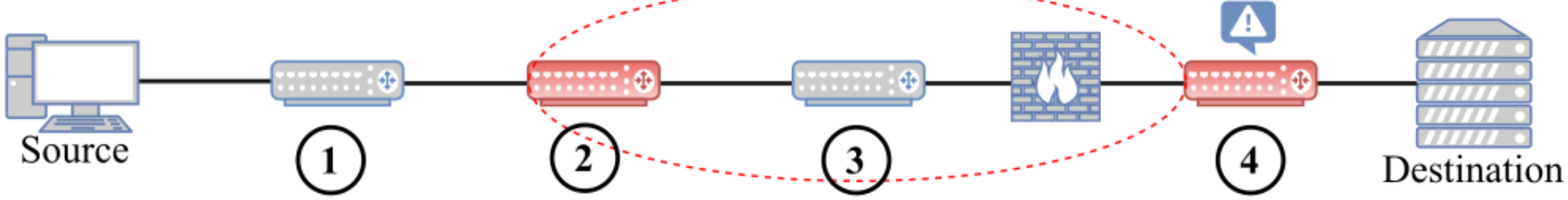
- Offender : *The router preceding the middlebox on a given path*

Pre-processing: derivation (Step 1)

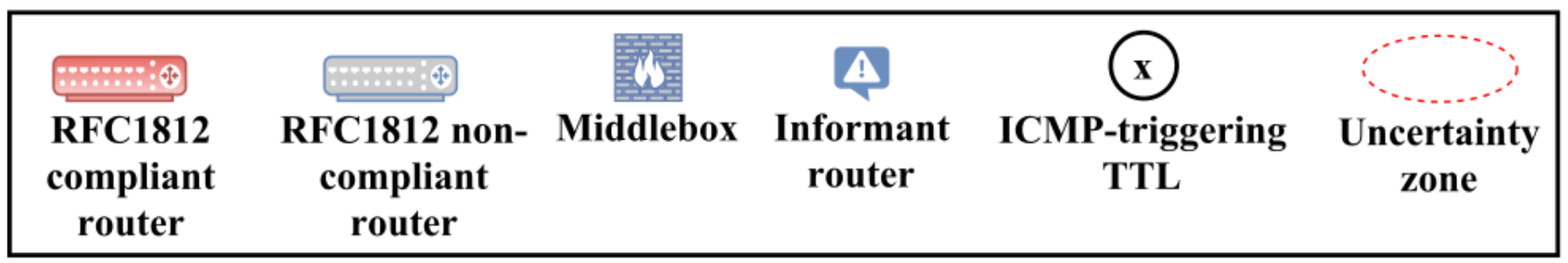
- Offender : *The router preceding the middlebox on a given path*



1. Modified field is within the first 48 bytes

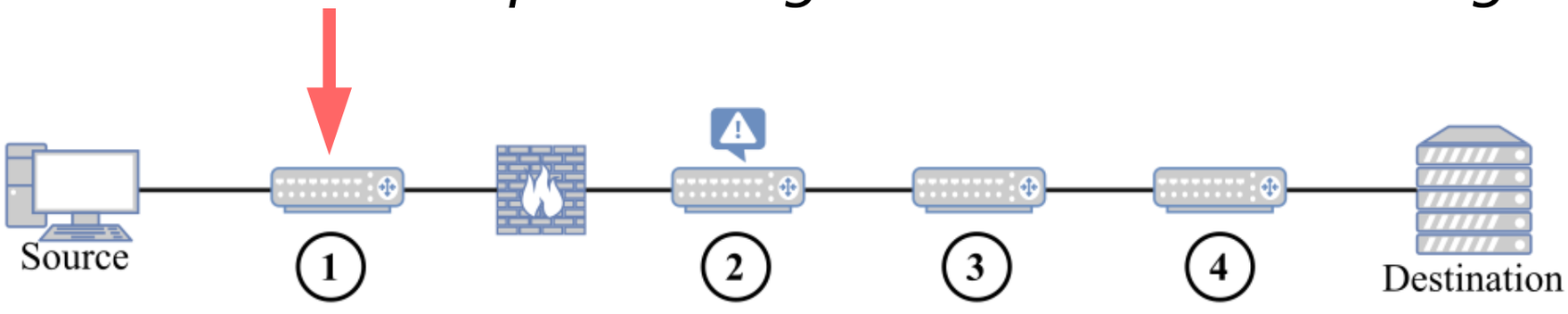


2. Modified field is outside the first 48 bytes

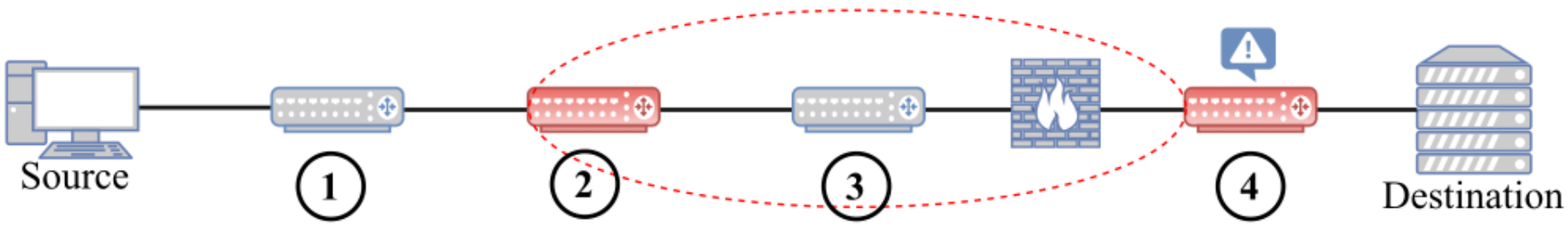


Pre-processing: derivation (Step 1)

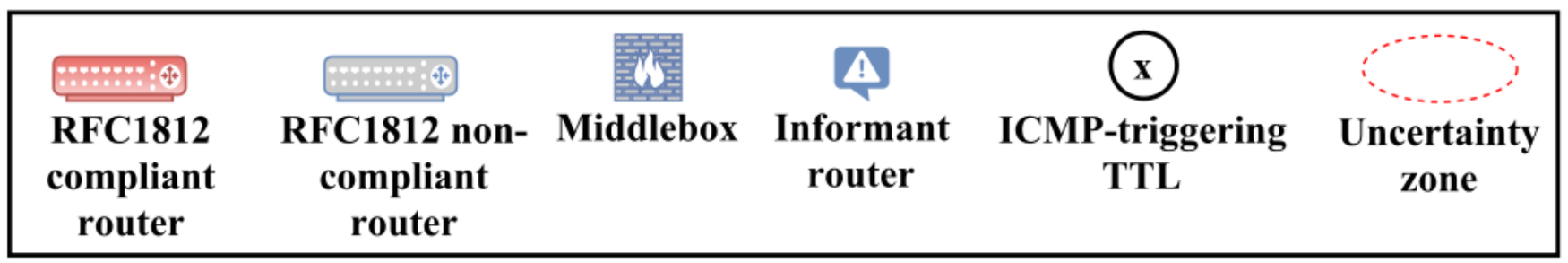
- Offender : *The router preceding the middlebox on a given path*



1. Modified field is within the first 48 bytes

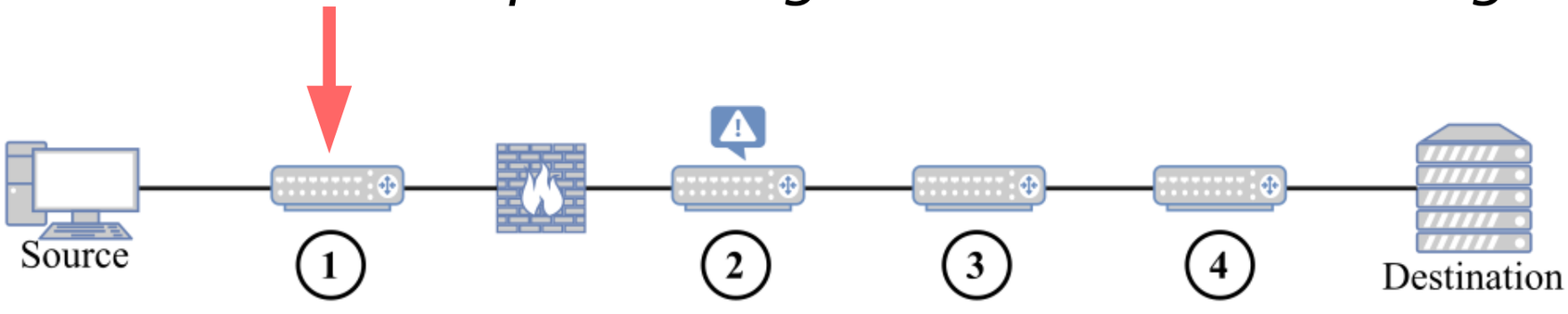


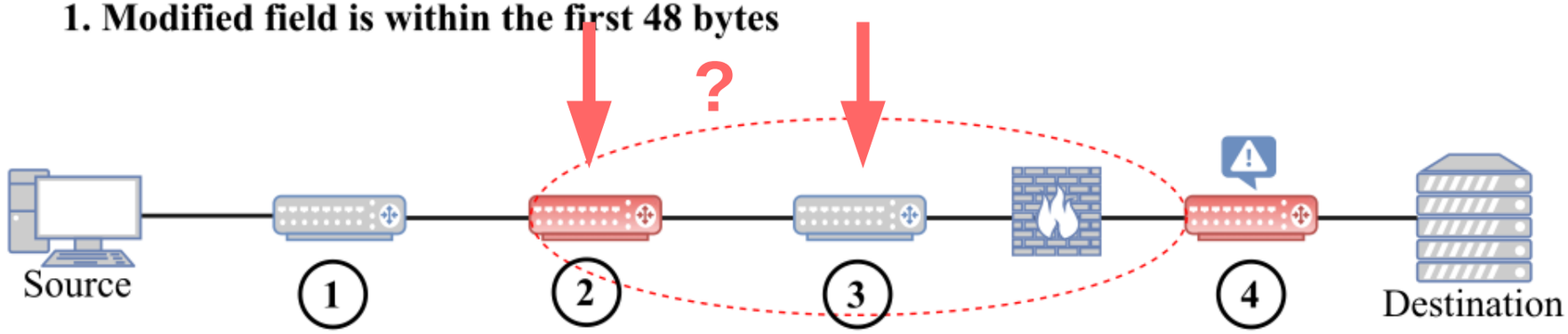
2. Modified field is outside the first 48 bytes



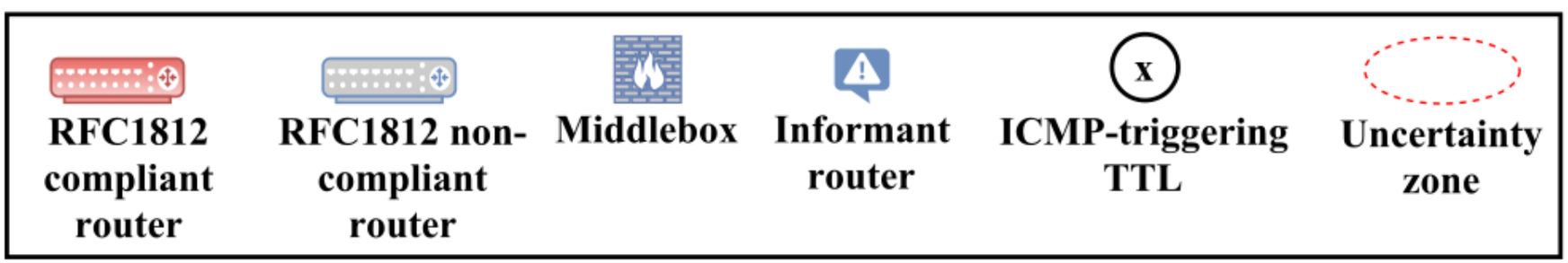
Pre-processing: derivation (Step 1)

- Offender : *The router preceding the middlebox on a given path*





2. Modified field is outside the first 48 bytes



Pre-processing: derivation (Step 1)

```
def offender(probe):
```

Pre-processing: derivation (Step 1)

def offender(probe):

- No U zone: the router that precedes the informant router
- U zone: Heuristics

Pre-processing: derivation (Step 1)

def offender(probe):

- No U zone: the router that precedes the informant router
- U zone: Heuristics

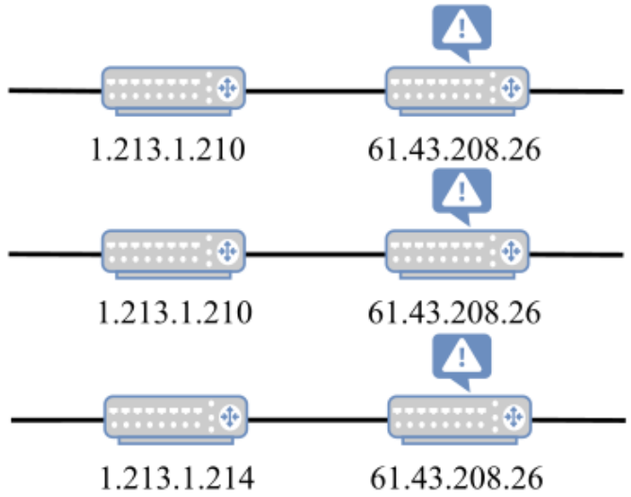
1. * at informant_TTL–1 : offender at informant_TTL-2
2. * at informant_TTL-2 : offender at informant_TTL-3
3. a)Major AS in U zone, b)If a router was used for labeling, pick it
4. First router of U zone (if used for labeling)

Pre-processing: derivation (Step 1)

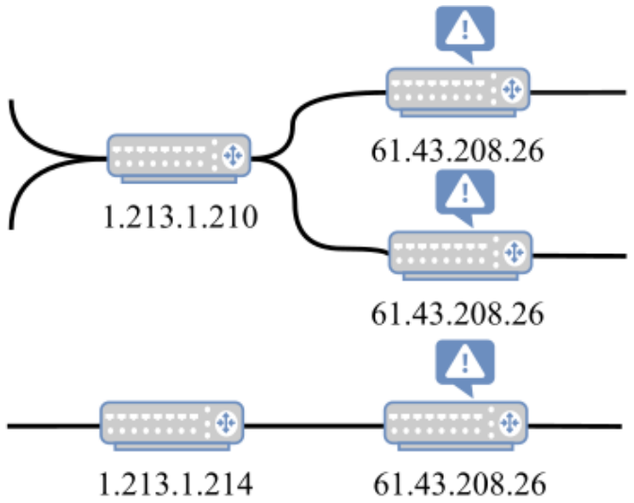
Output:

- Offender AS for 99% obs.
- Offender IP for 52% obs. (20M)

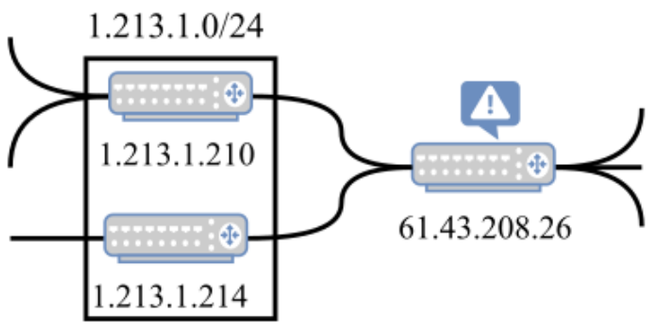
Pre-processing: grouping (Step 2)



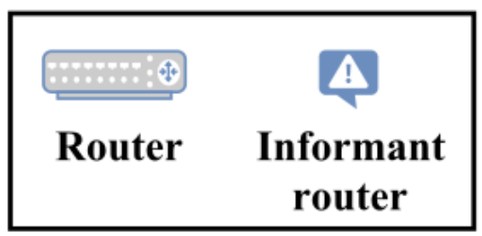
a. Offenders derivation



b. Offenders grouping



c. Offenders merging



Pre-processing: grouping (Step 2)

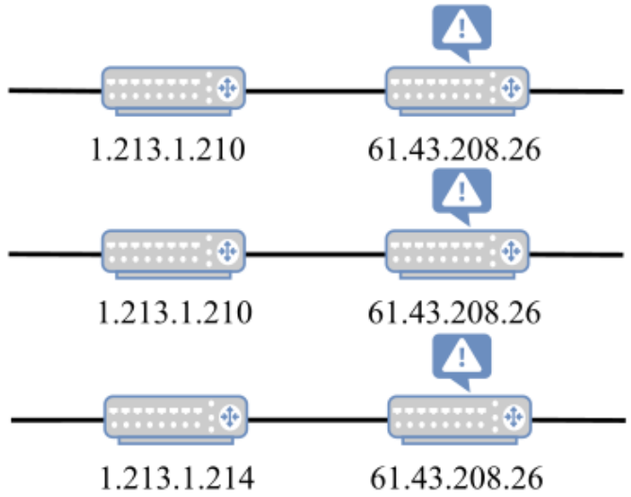
- MB profiles
- Cross-check heuristics: at least one trivial case or Heuristic#1 per offender
- 5% threshold:
  - inconsistent modifications: drop all obs.
  - inconsistent positions: mark as conflict

Pre-processing: grouping (Step 2)

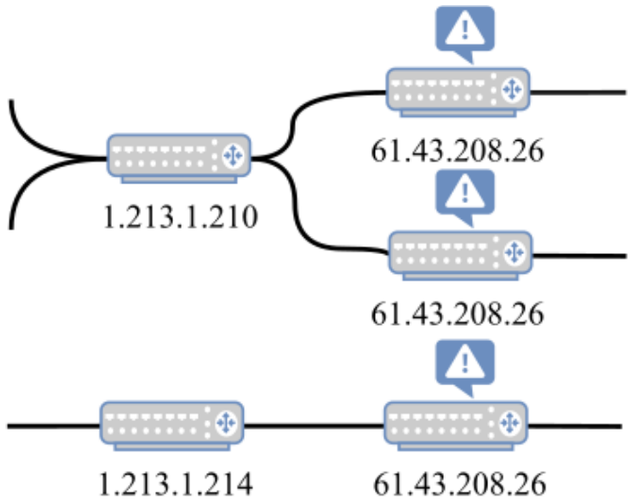
Output:

- 8,322 offenders

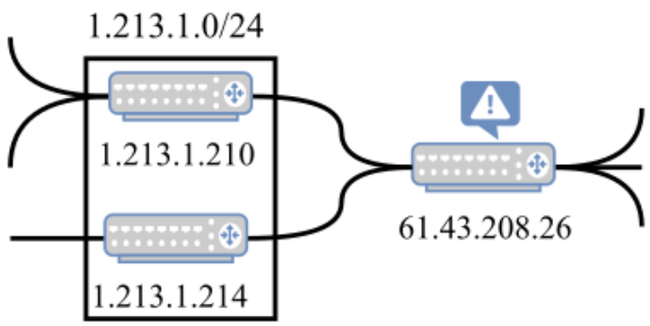
Pre-processing: merging (Step 3)



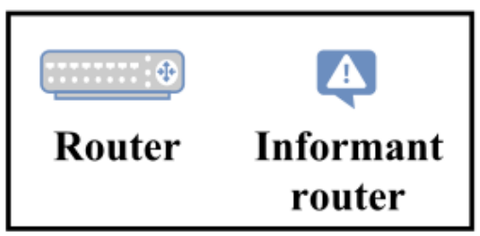
a. Offenders derivation



b. Offenders grouping



c. Offenders merging



Pre-processing: merging (Step 3)

Merge offenders if:

1. Same subnet (/24)
2. Consistent modifications
3. Same set of next hops (offender_TTL+1)

Pre-processing: merging (Step 3)

Merge offenders if:

1. Same subnet (/24)
2. Consistent modifications
3. Same set of next hops (offender_TTL+1)

- 505 merged into 198
- (7 cases of Multi-Origin AS Conflicts)

Pre-processing: merging (Step 3)

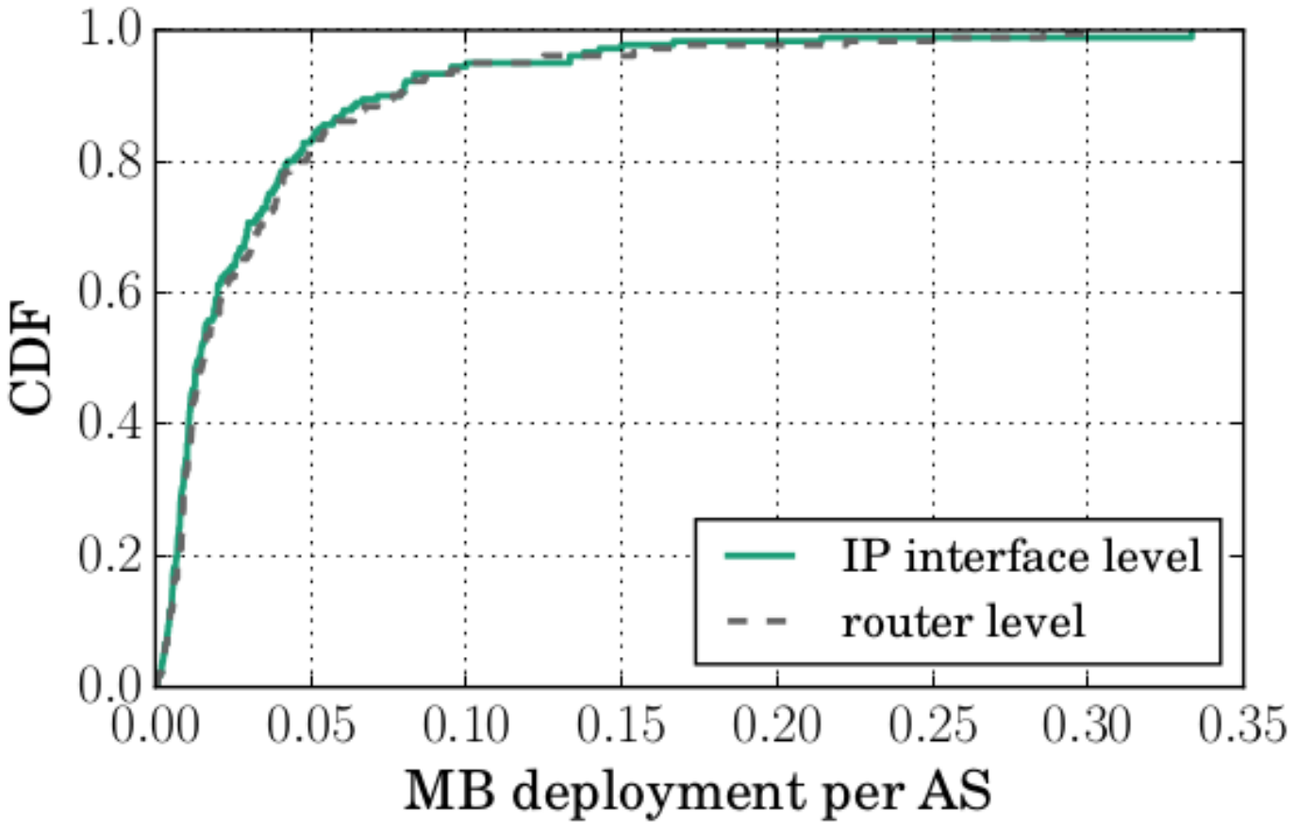
Output:

- 8,005 offenders

Results: prevalence

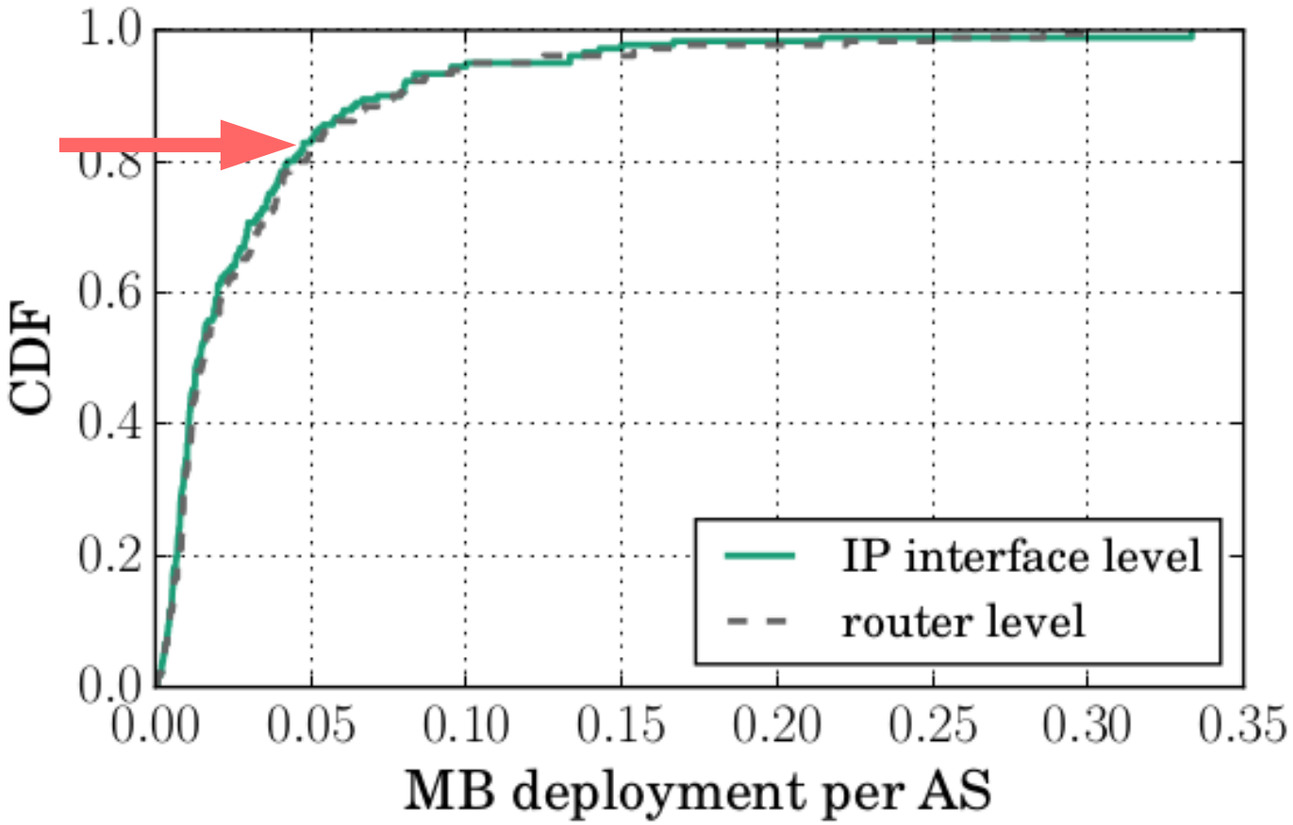
- *Deployment*: Proportion of MBs in AS
- *Popularity*: Paths affected by MB
- *Position*: Location of MB in AS topology

Prevalence: deployment



Deployed MB / IP interfaces, per AS. Alias resolution using CAIDA ITDK dataset.

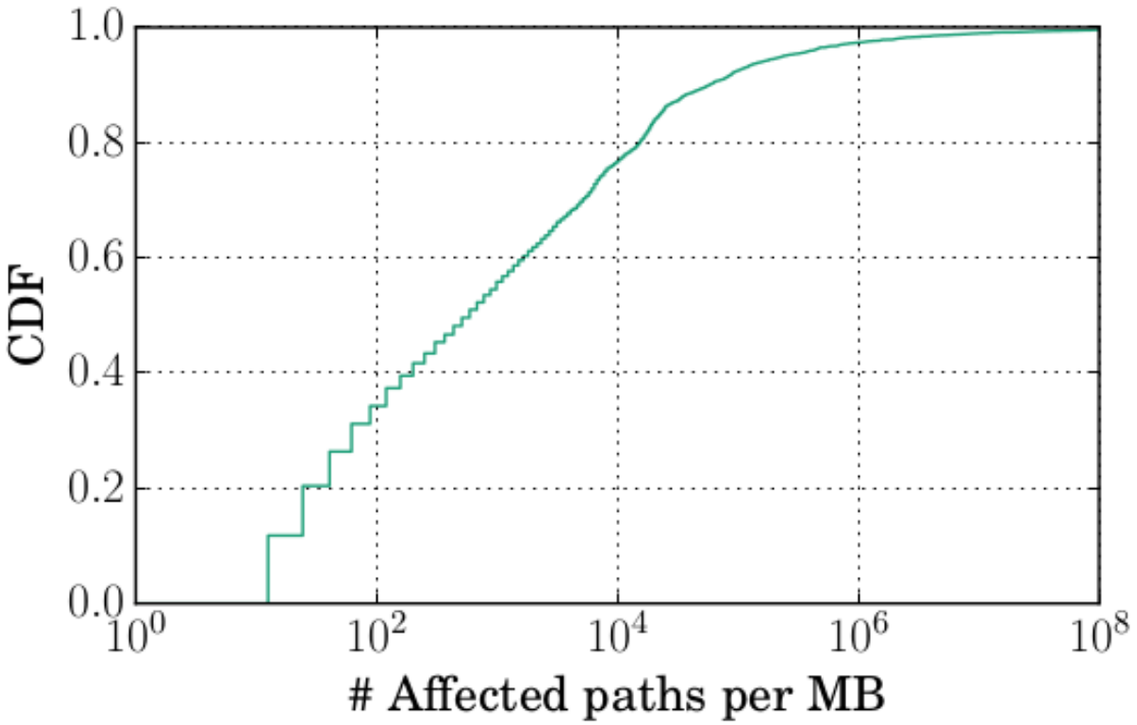
Prevalence: deployment



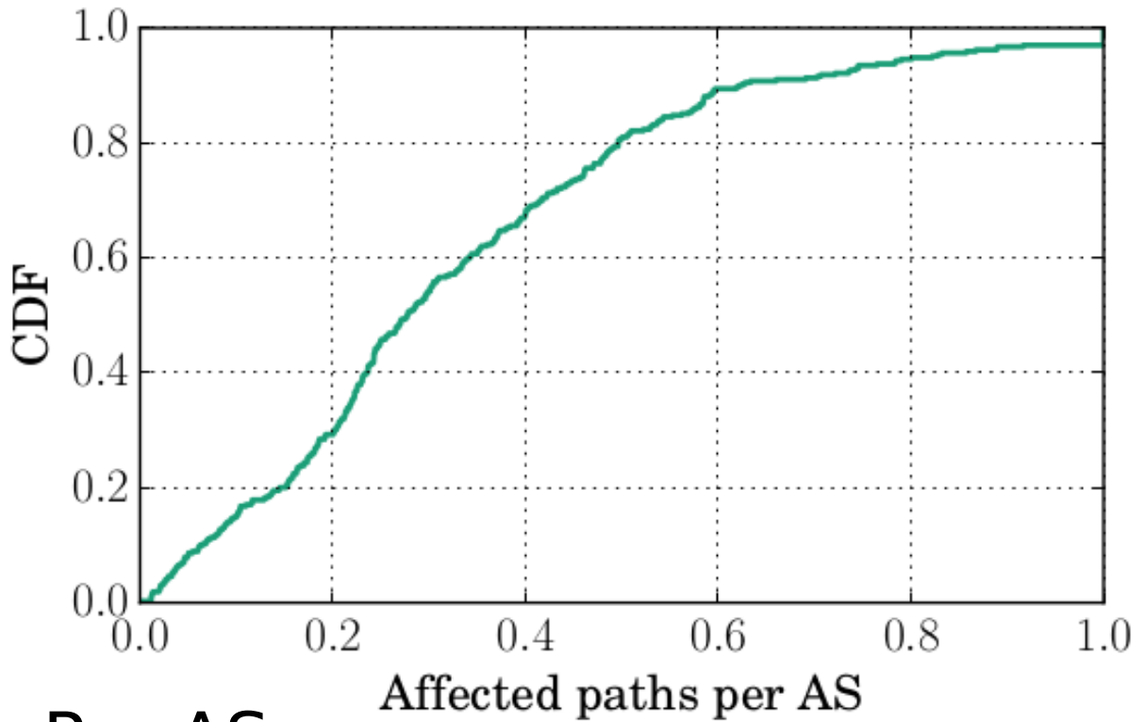
Deployed MB / IP interfaces, per AS. Alias resolution using CAIDA ITDK dataset.

- In general, less than 5%
- Cogent: 1.5%

Prevalence: popularity

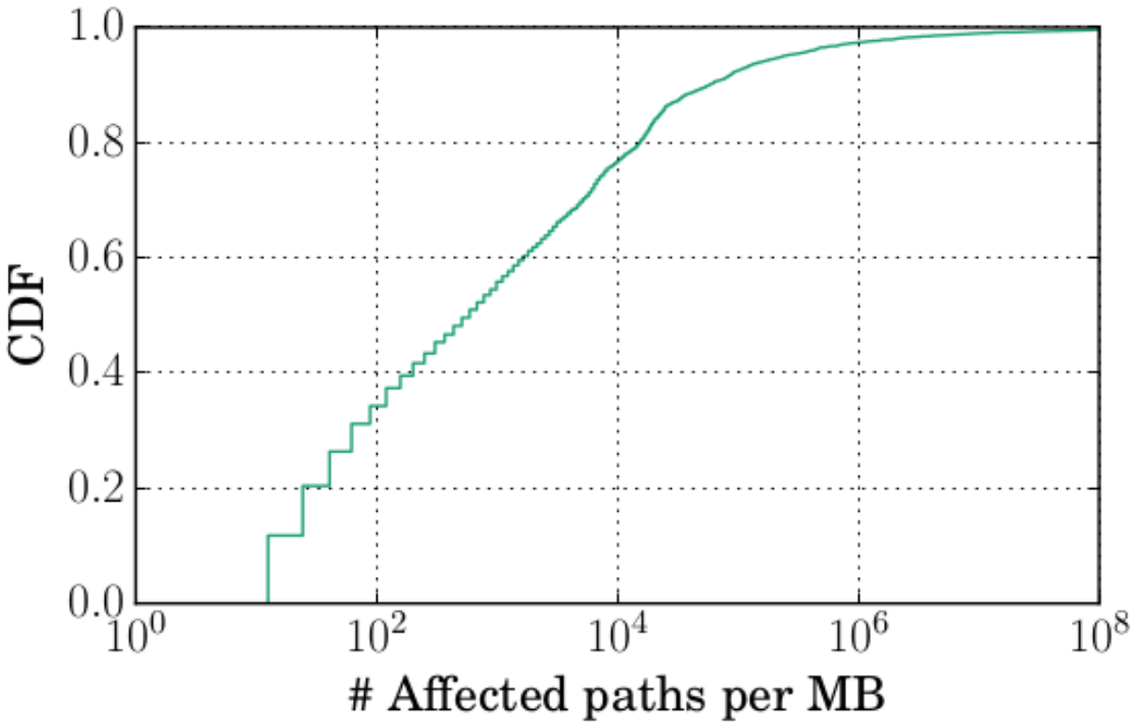


Per MB

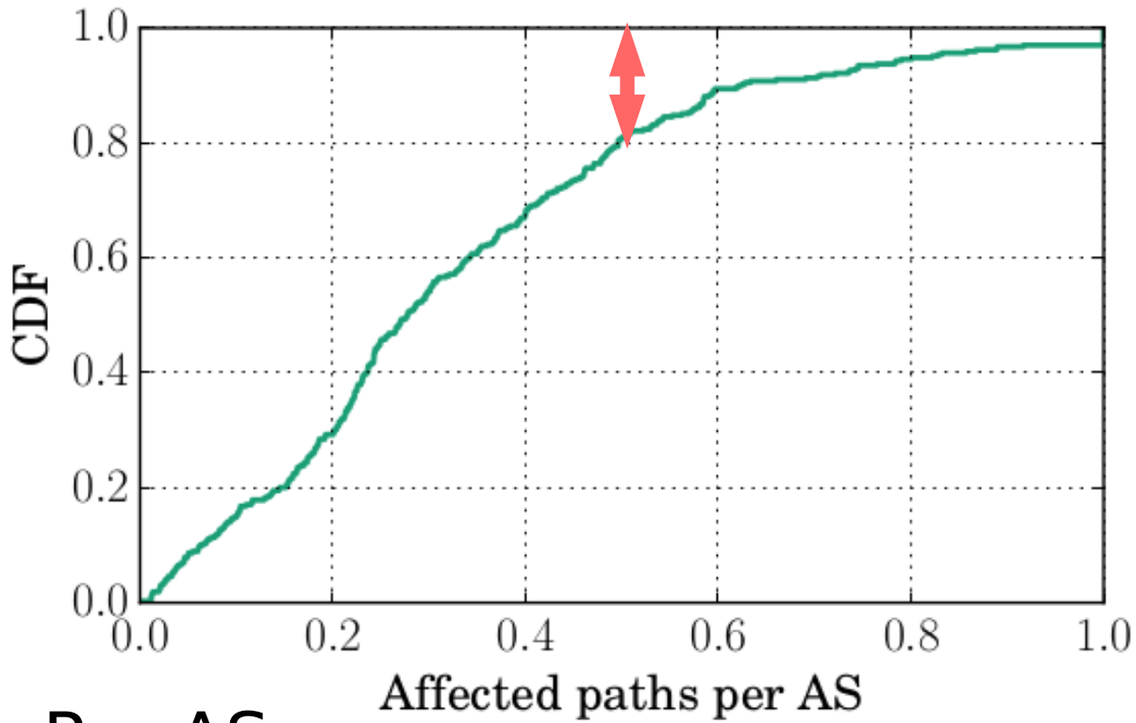


Per AS

Prevalence: popularity



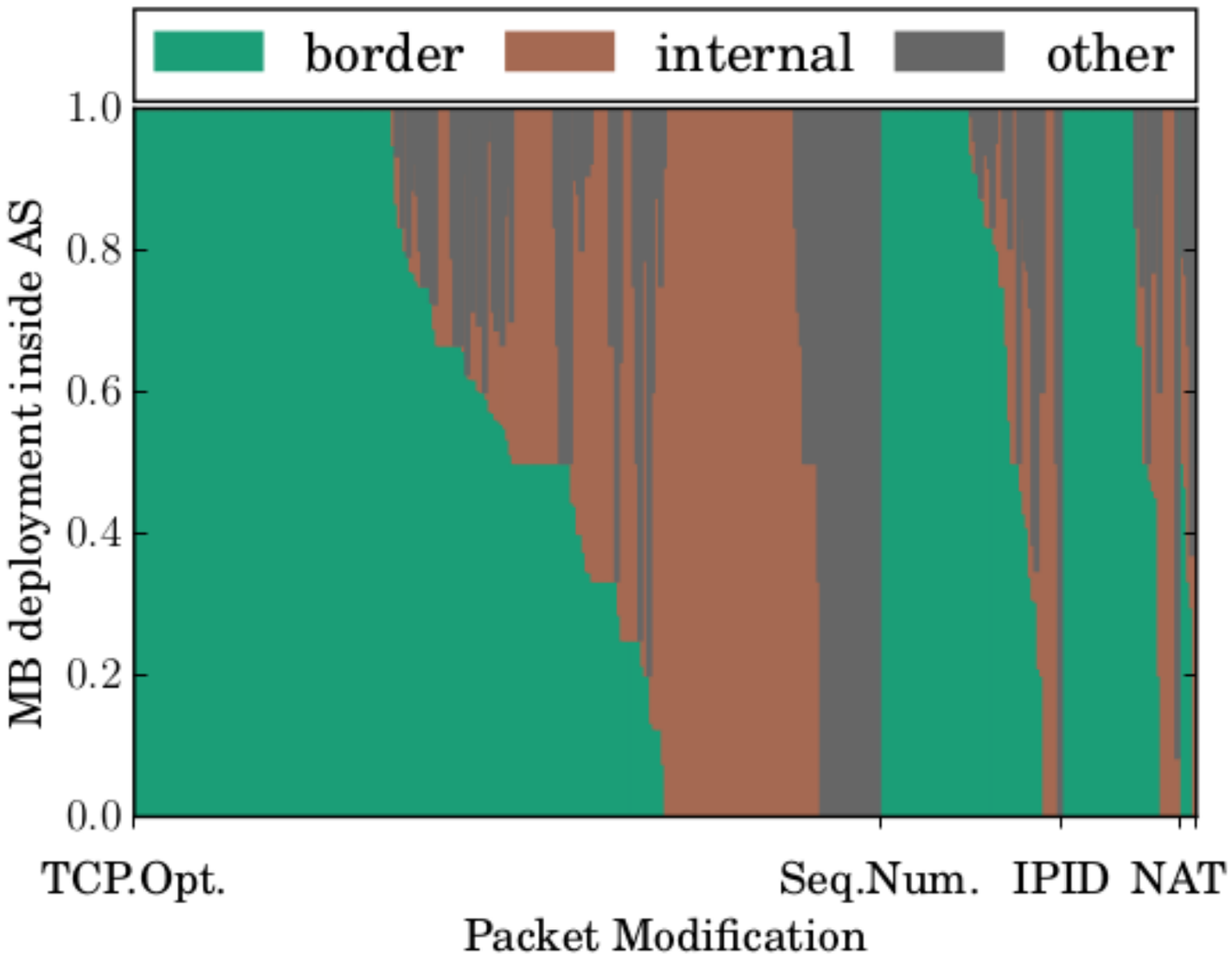
Per MB



Per AS

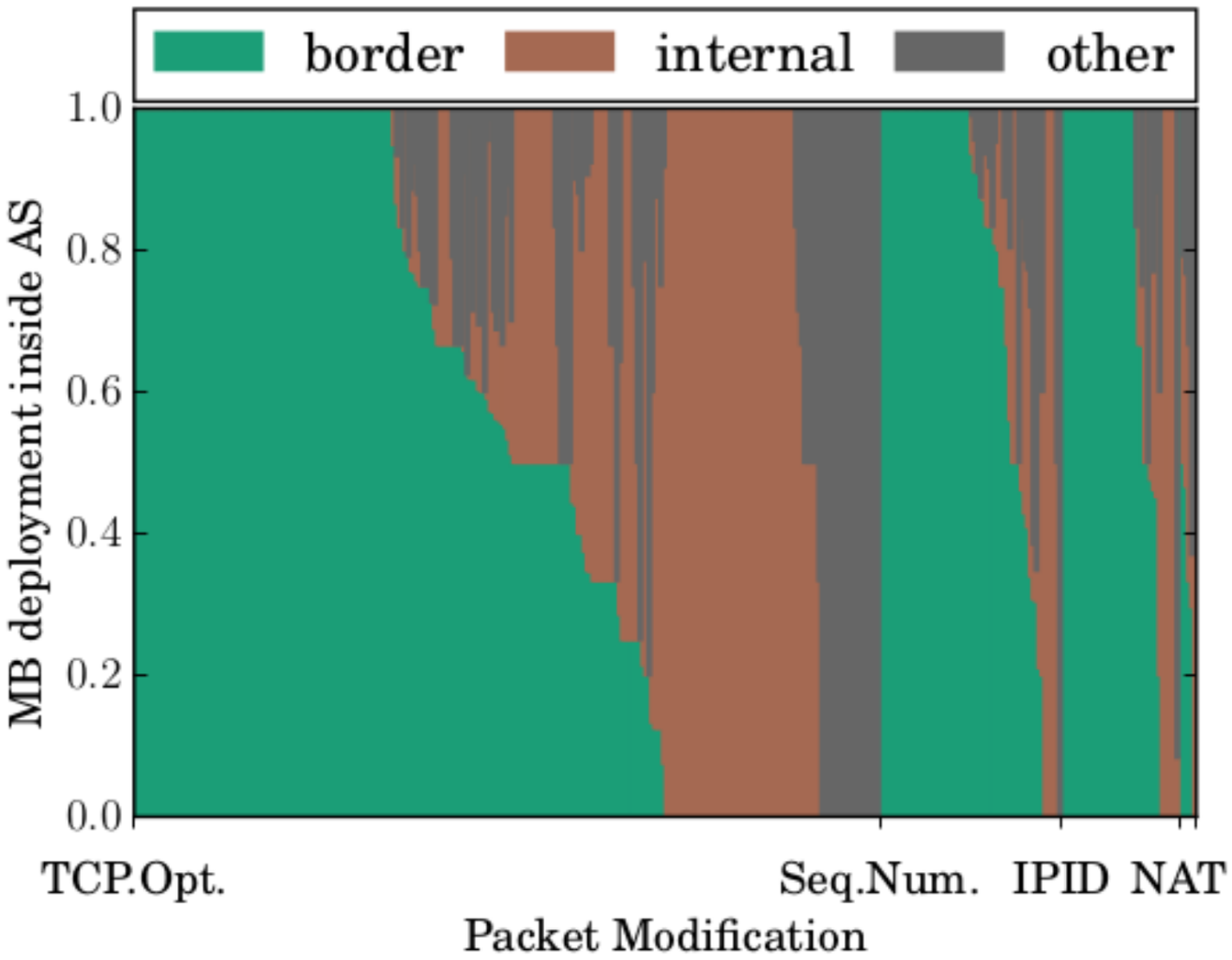
- For 20% of the ASes, more than 50% of paths crossing it are affected by 1+ MB(s)
- Cogent: 44M paths, 2.1M affected: 5%

Prevalence: position



MB Positions, per categories of modif., per AS

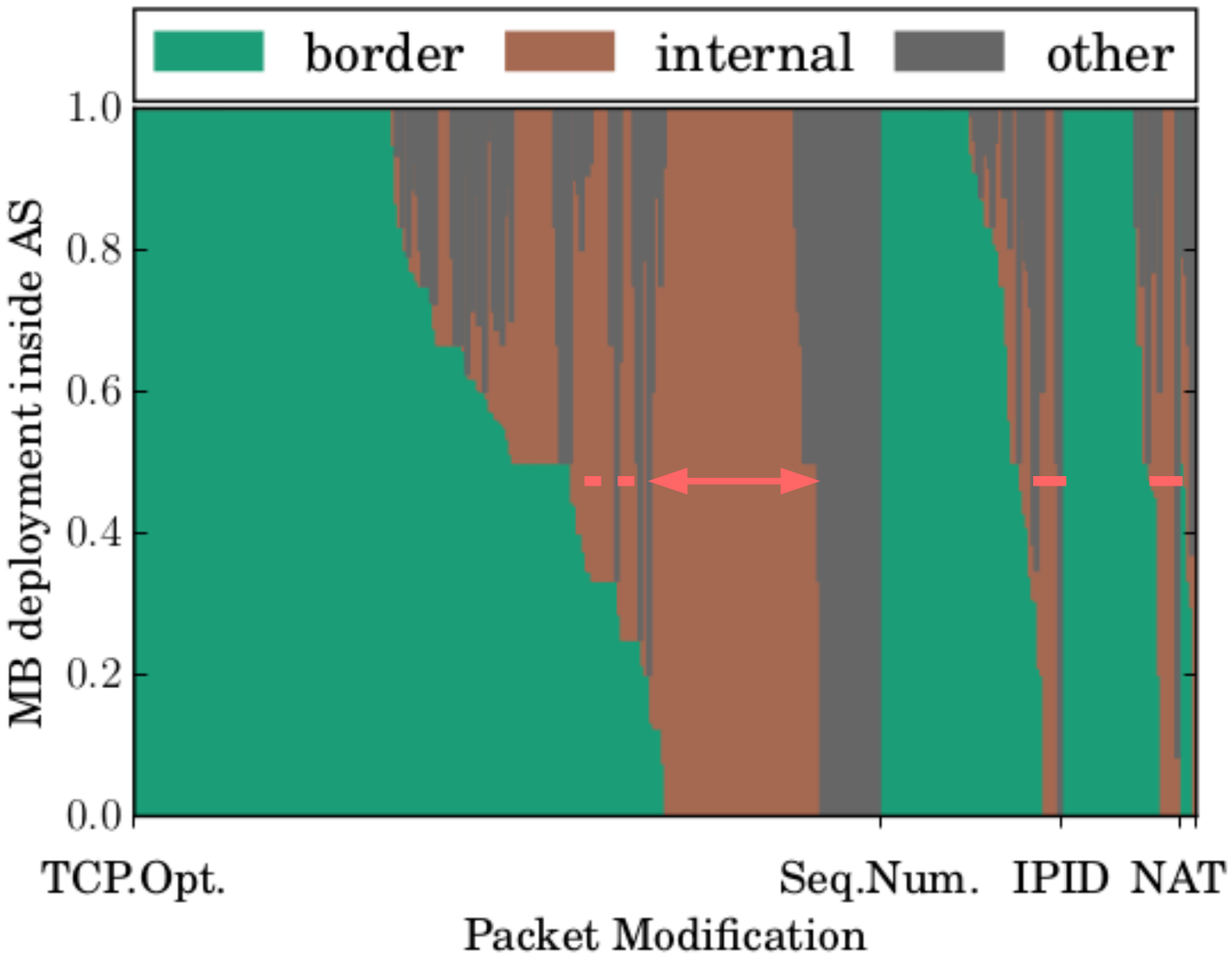
Prevalence: position



MB Positions, per categories of modif., per AS

- Border: 4,210 (52.6%)
- Internal: 2,931 (36.6%)
- Other: conflict or unable to derive position (9.1%), or moved ? (1.7%)

Prevalence: position



MB Positions, per categories of modif., per AS

- Border: 4,210 (52.6%)
- Internal: 2,931 (36.6%)
- Other: conflict or unable to derive position (9.1%), or moved ? (1.7%)

- At the exception of 65 ASes (19%) that deploys the majority of their MBs in their core, *ASes tend to deploy most of their MBs at their border*.

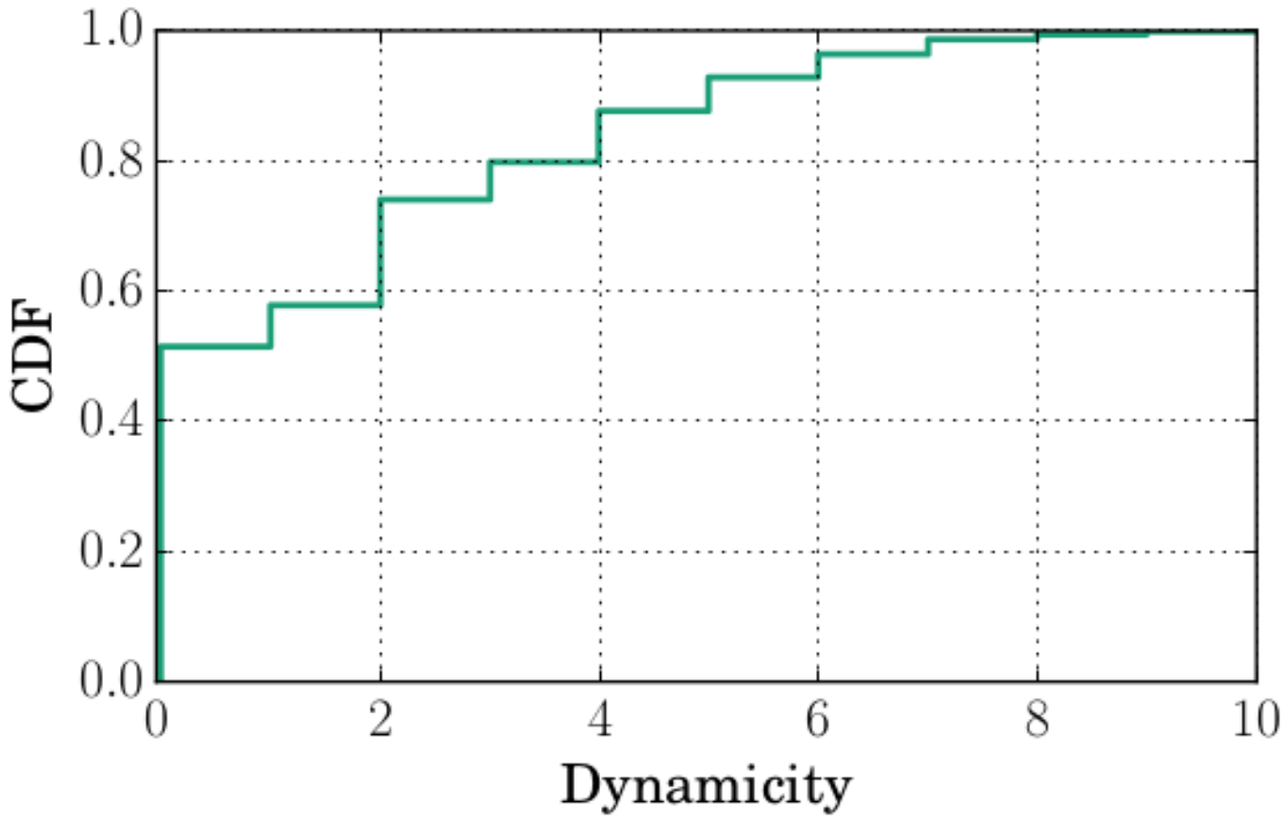
Results: persistence

Results: persistence

- Keep sub-paths visible with HTTP and non-HTTP probes
- 5,888 offenders

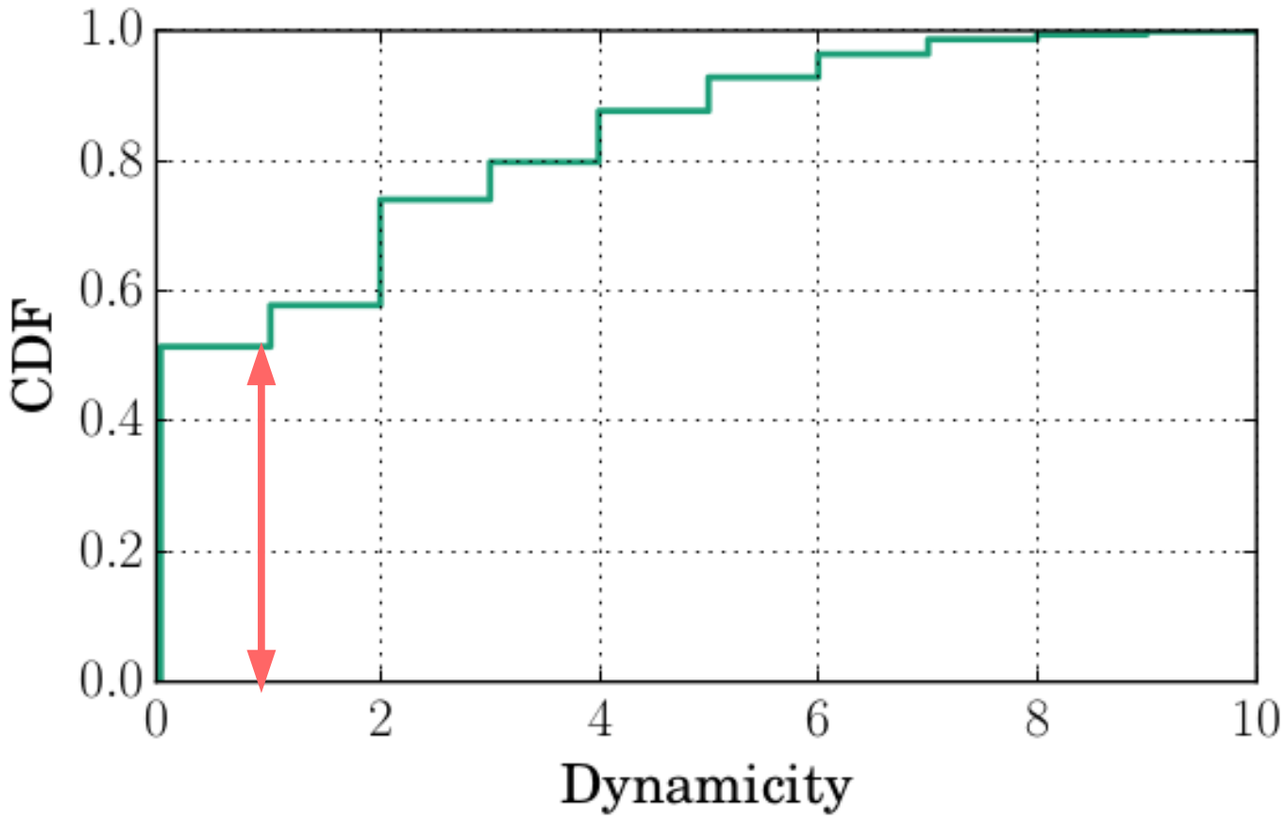
- Active: if it was used for labeling
- Inactive: if it was responsive, but not used for labeling
- Offline/invisible: it was not observed

Results: persistence



State changes per MB, Invisible == Active. 14 campaigns over 70 days.

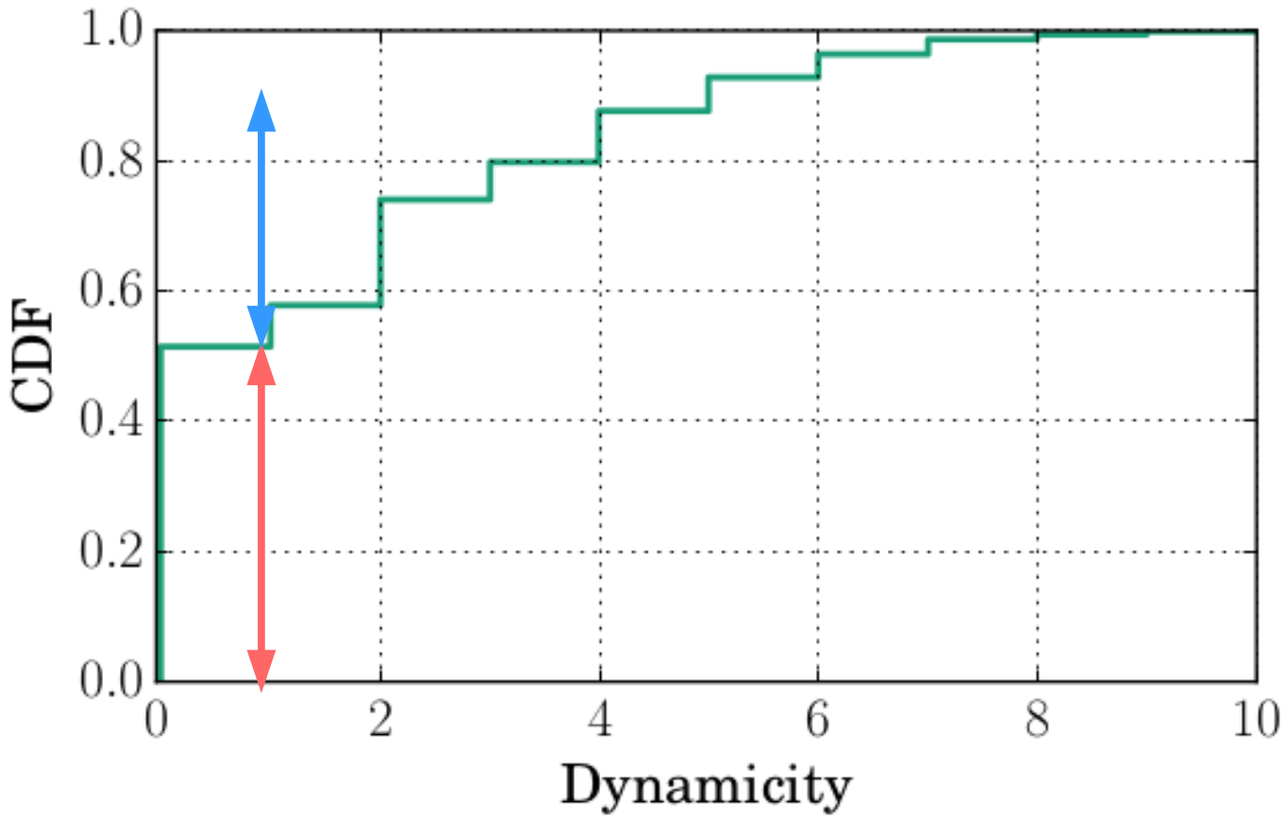
Results: persistence



State changes per MB, Invisible == Active. 14 campaigns over 70 days.

- 51% are stable

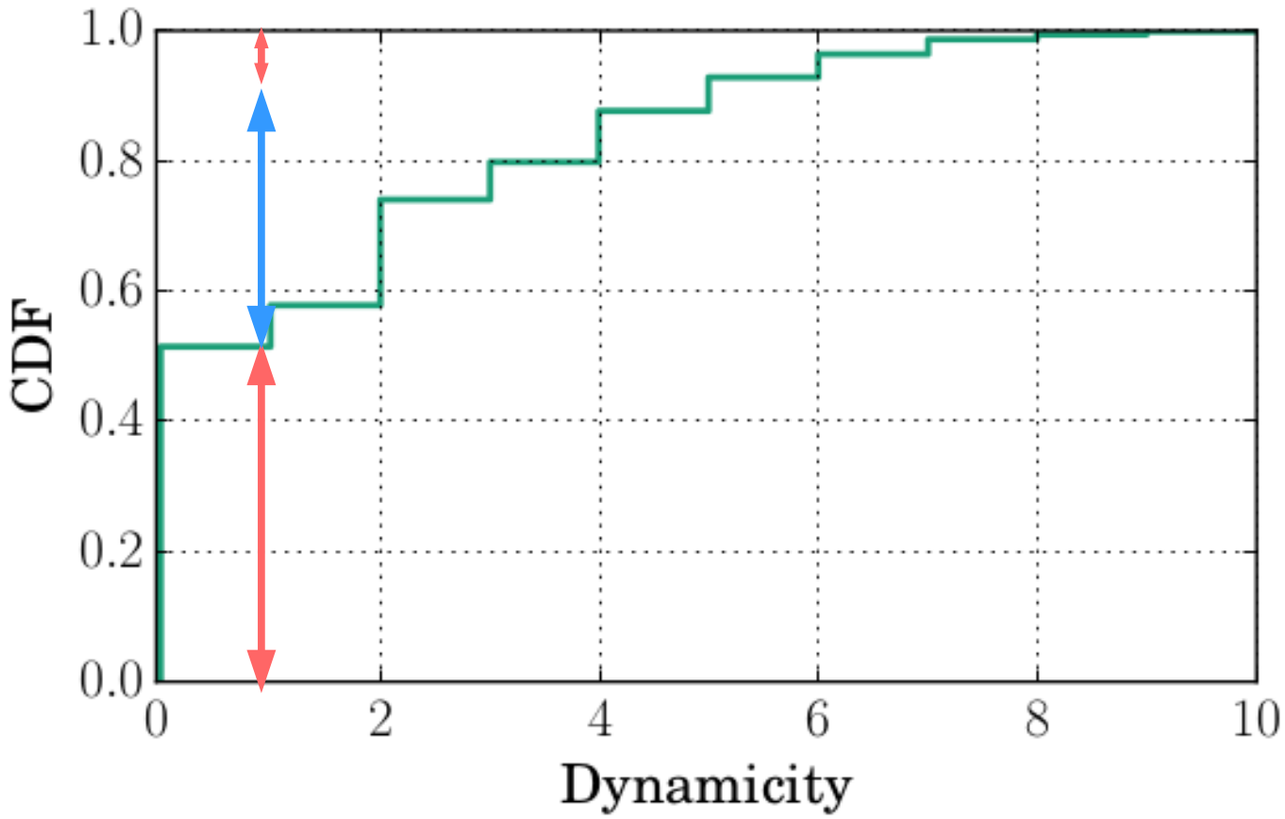
Results: persistence



State changes per MB, Invisible == Active. 14 campaigns over 70 days.

- 51% are stable
- 38% are slightly intermittent/dynamic ([1;4])

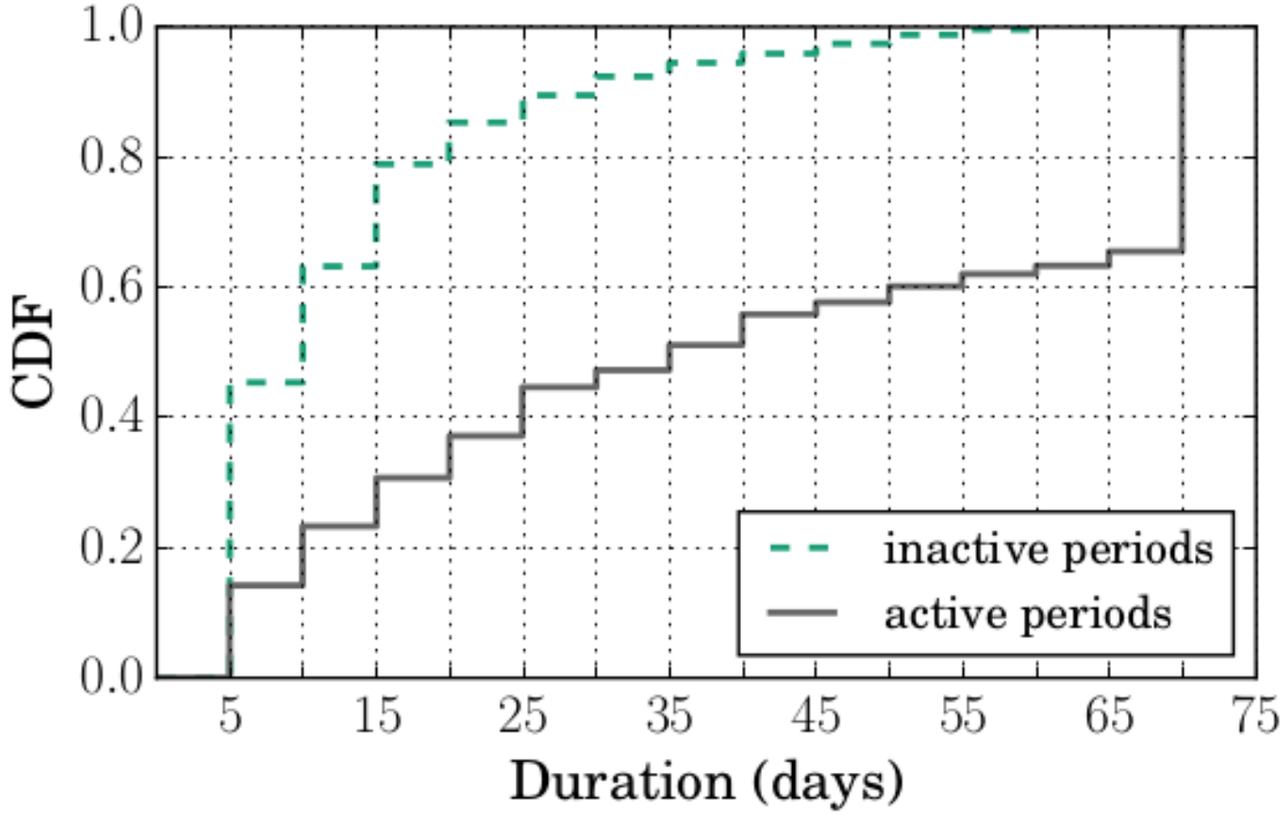
Results: persistence



State changes per MB, Invisible == Active. 14 campaigns over 70 days.

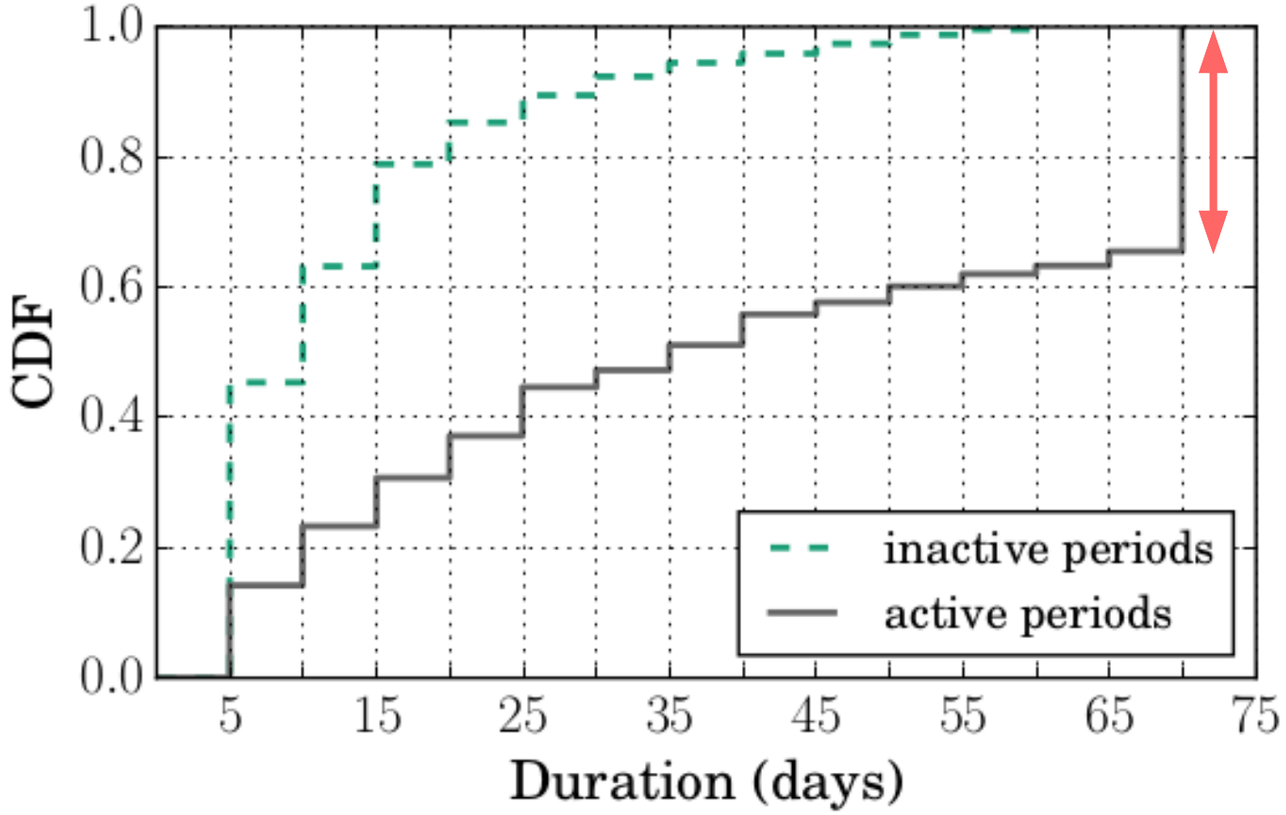
- 51% are stable
- 38% are slightly intermittent/dynamic ([1;4])
- 11% are highly intermittent ([5;10])

Results: persistence



State durations (max 70 days)

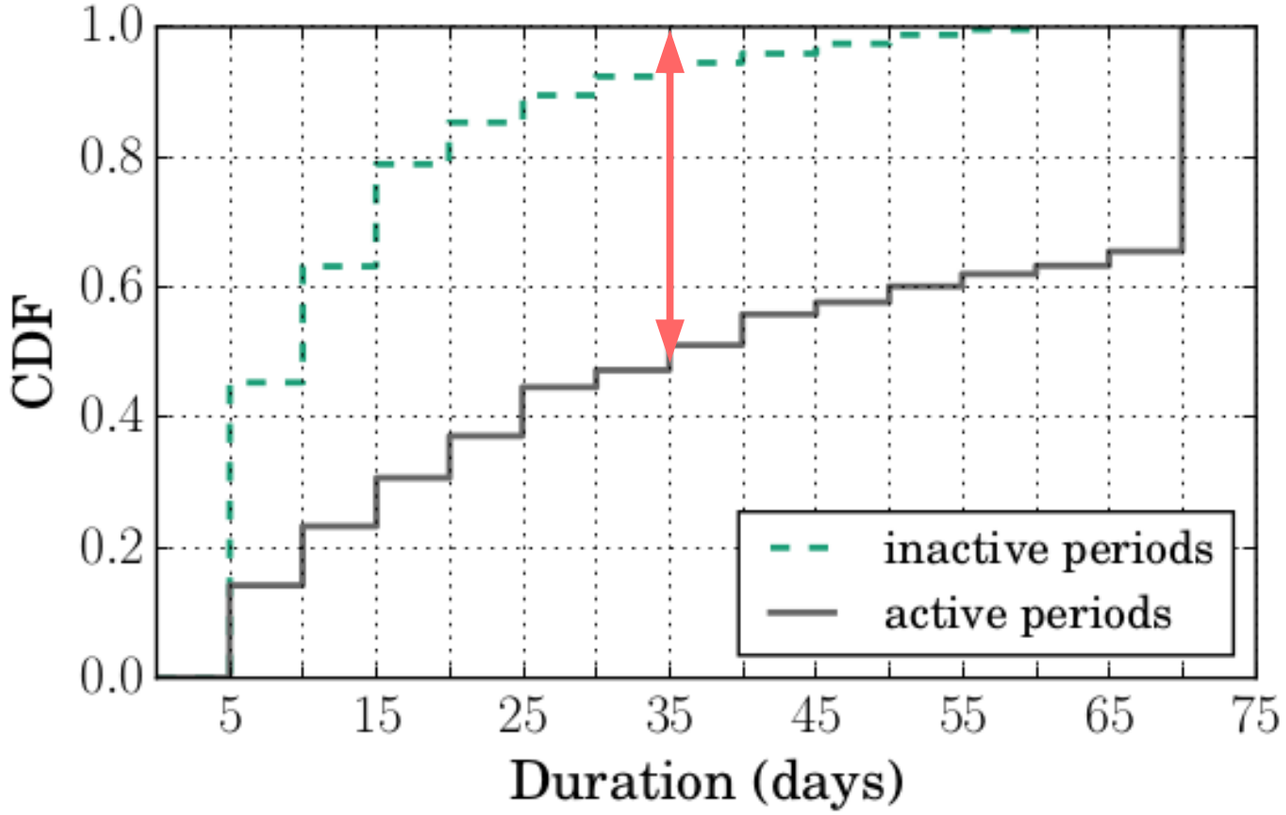
Results: persistence



State durations (max 70 days)

- 38% of periods are 70 days (the 51% stable MBs)

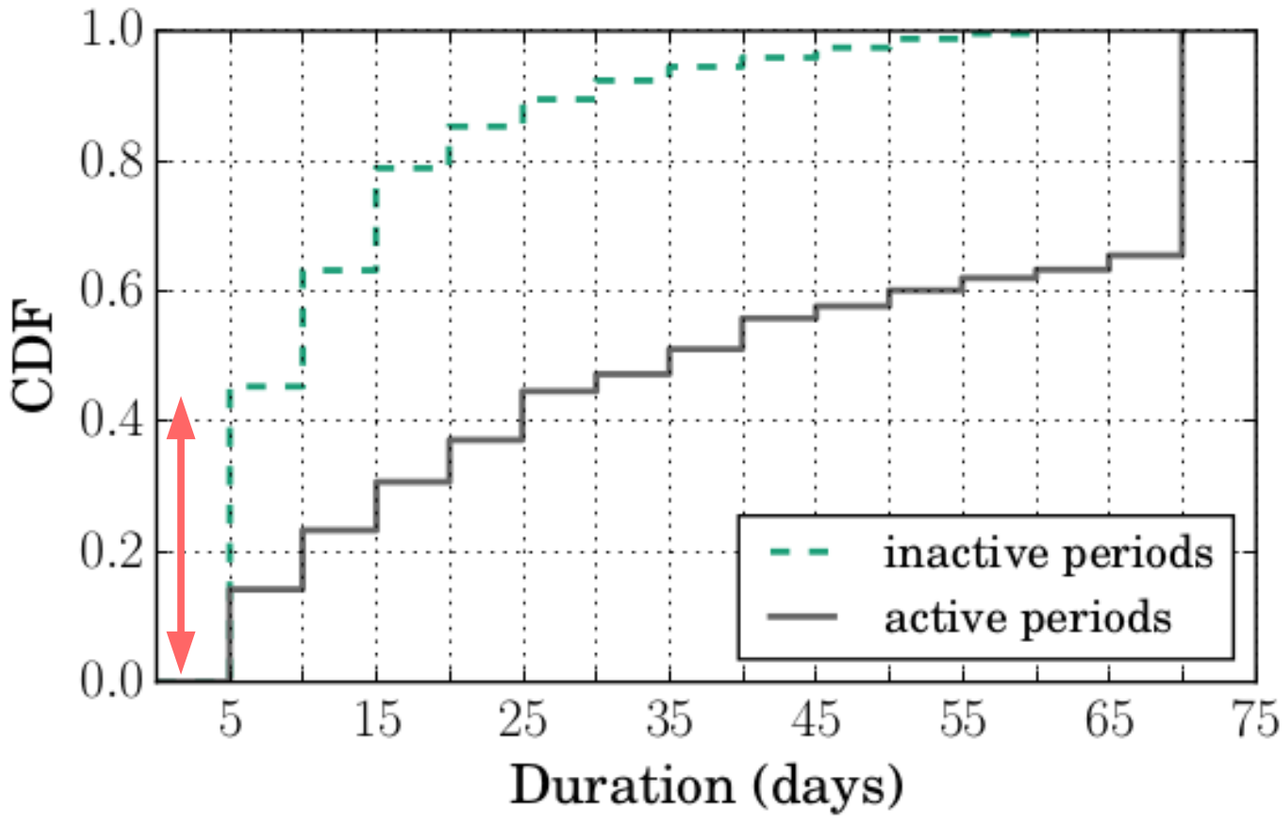
Results: persistence



State durations (max 70 days)

- 38% of periods are 70 days (the 51% stable MBs)
- 50% of active periods lasts more than 35 day

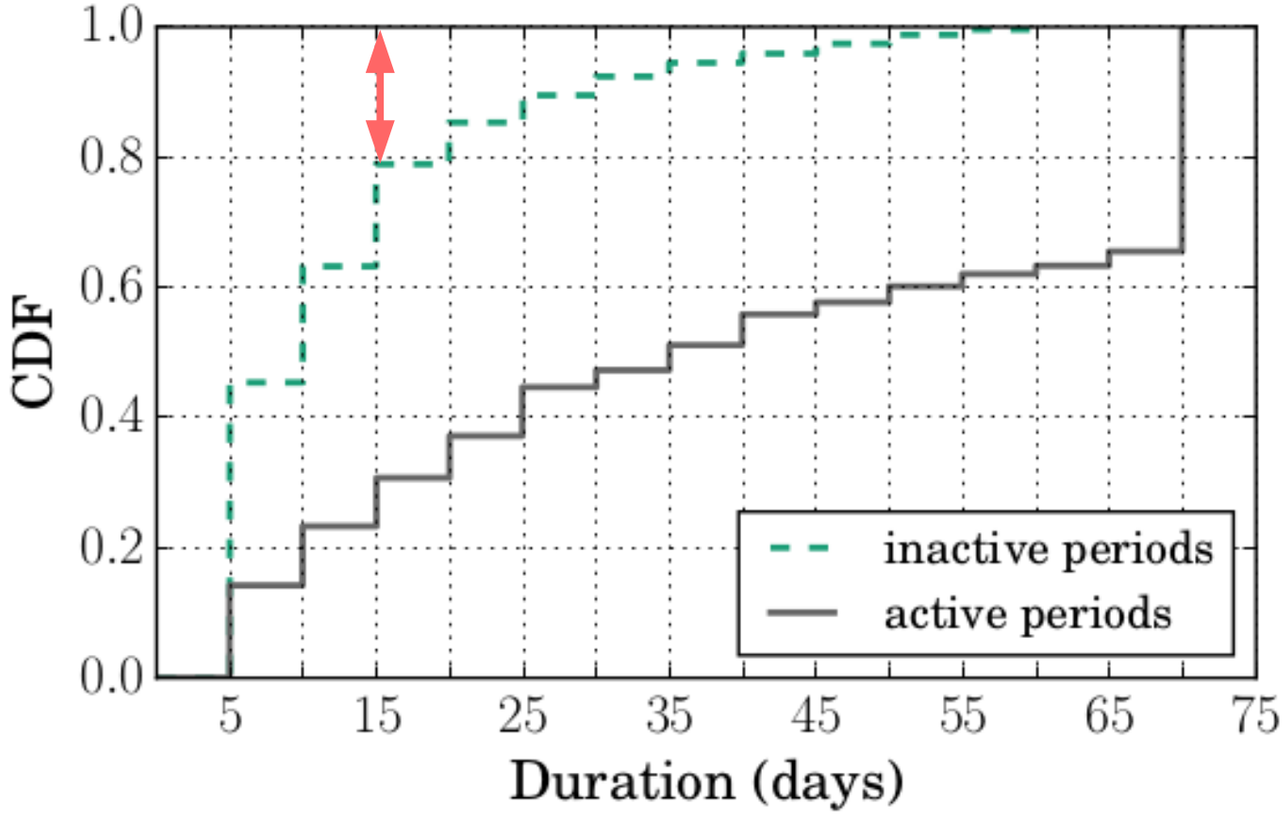
Results: persistence



State durations (max 70 days)

- 38% of periods are 70 days (the 51% stable Mbs)
- 50% of active periods lasts more than 35 days
- 44% of inactive periods are short-lived (5 days)

Results: persistence



State durations (max 70 days)

- 38% of periods are 70 days (the 51% stable Mbs)
- 50% of active periods lasts more than 35 days
- 44% of inactive periods are short-lived (5 days)
- 20% are longer than 15 days

Summary

- MB deployment is marginal
- MBs don’t affect many paths crossing its AS
- A majority of MBs are deployed at AS borders
- MBs are relatively stable

Future works

- Investigate dynamicity
- NATs (Workshop on Mobile Network Measurement (MNM’17))

- IPv6

Questions ?

Future works: NAT trick (MNM)

- **RFC 792** : “The internet header plus the first 64 bits”
- **RFC 1812** : “as much [...] as possible” (< 576 B)

- **RFC 5508** : “Revert the IP and transport headers […] to their original form”
- **RFC 5508**: “SHOULD NOT validate the transport checksum”

Future works: NAT trick (MNM)

- **RFC 792** : “The internet header plus the first 64 bits”
- **RFC 1812** : “as much [...] as possible” (< 576 B)

- **RFC 5508** : “Revert the IP and transport headers […] to their original form”
- **RFC 5508**: “SHOULD NOT validate the transport checksum”

- Correlation in transport checksums offsets == NATS ?

Example

```
ko@node1:~/$ scamper -c "tracebox -v -t -p IP/TCP/SACKP/MSS(1460)" -i 208.97.177.124
tracebox standard mode from node1 to 208.97.177.124
 result: success
  1: 78.129.127.21     (28/40) IP::TTL(01) IP::Checksum(7746)
  2: 212.68.211.181    (28/40) IP::TTL(01) IP::Checksum(7746)
  3: 149.6.135.65      (40/40) TCP::Checksum(424f) IP::TTL(01) IP::Checksum(7746)
  4: 154.54.59.57      (40/40) TCP::Checksum(424f) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
  5: 154.54.74.94      (40/40) TCP::Checksum(424f) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
  6: 130.117.14.178    (28/40) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
  7: 64.125.21.77      (40/40) TCP::Checksum(424f) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
  8: 64.125.27.0       (40/40) TCP::Checksum(424f) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
  9: 64.125.29.17      (40/40) TCP::Checksum(424f) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
 10: 64.125.29.131     (40/40) TCP::Checksum(424f) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
 11: 64.125.29.229     (40/40) TCP::Checksum(424f) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
 12: 64.125.30.249     (40/40) TCP::Checksum(424f) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
 13: 64.125.31.42      (40/40) TCP::Checksum(424f) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
 14: 208.185.23.134    (40/40) TCP::Checksum(c5d9) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
TCP::Options::MSS(0204058c)
 15: 208.113.156.4     (28/40) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
 16: 208.113.156.14    (28/40) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
 17: 208.97.177.124
```

Example

```
ko@node1:~/$ scamper -c "tracebox -v -t -p IP/TCP/SACKP/MSS(1460)" -i 208.97.177.124
tracebox standard mode from node1 to 208.97.177.124
 result: success
  1: 78.129.127.21     (28/40) IP::TTL(01) IP::Checksum(7746)
  2: 212.68.211.181    (28/40) IP::TTL(01) IP::Checksum(7746)
  3: 149.6.135.65      (40/40) TCP::Checksum(424f) IP::TTL(01) IP::Checksum(7746)
  4: 154.54.59.57      (40/40) TCP::Checksum(424f) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
  5: 154.54.74.94      (40/40) TCP::Checksum(424f) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
  6: 130.117.14.178    (28/40) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
  7: 64.125.21.77      (40/40) TCP::Checksum(424f) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
  8: 64.125.27.0       (40/40) TCP::Checksum(424f) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
  9: 64.125.29.17      (40/40) TCP::Checksum(424f) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
 10: 64.125.29.131     (40/40) TCP::Checksum(424f) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
 11: 64.125.29.229     (40/40) TCP::Checksum(424f) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
 12: 64.125.30.249     (40/40) TCP::Checksum(424f) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
 13: 64.125.31.42      (40/40) TCP::Checksum(424f) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
 14: 208.185.23.134    (40/40) TCP::Checksum(c5d9) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
TCP::Options::MSS(0204058c)
 15: 208.113.156.4     (28/40) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
 16: 208.113.156.14    (28/40) IP::DiffServicesCP(0a) IP::TTL(01) IP::Checksum(771e)
 17: 208.97.177.124
```

Example

ko@node1:~/$
1: 78.129.127.21
2: 212.68.211.181
3: 149.6.135.65
4: 154.54.59.57
5: 154.54.74.94
6: 130.117.14.178
7: 64.125.21.77
8: 64.125.27.0
9: 64.125.29.17
10: 64.125.29.131
11: 64.125.29.229
12: 64.125.30.249
13: **64.125.31.**42 (40/40)
14: **208.185.23.134** (40/40)TCP:MSS(0204058c)
15: 208.113.156.4
16: 208.113.156.14
17: 208.97.177.124

ko@node2:~$
1: 139.165.222.1
2: 193.190.228.29
3: 193.190.228.141
4: 193.190.252.97
5: 193.190.252.43
6: 193.190.200.28
7: 193.190.200.34
8: 193.191.10.19
9: *
10: 80.249.208.122
11: 64.125.21.77
12: 64.125.27.0
13: 64.125.29.17
14: 64.125.29.131
15: 64.125.29.229
16: 64.125.30.249
17: **64.125.31.**42 (40/40)
18: **208.185.23.134** (40/40) TCP:MSS(0204058c)
19: 208.113.156.4
20: 208.113.156.14
21: 208.97.177.124

ko@node3:~/$
1: 129.22.150.2
2: 10.2.0.98
3: 10.2.0.241
4: 199.18.156.65
5: 64.57.29.173
6: 206.126.236.147
7: 138.187.159.14
8: *
9: 94.102.162.99
10: 64.125.21.77
11: 64.125.27.0
12: 64.125.29.19
13: 64.125.29.131
14: 64.125.29.229
15: 64.125.30.249
16: **64.125.31.**44 (40/40)
17: **208.185.23.134** (40/40) TCP::MSS(0204058c)
18: 208.113.156.4
19: 208.113.156.14
20: 208.97.178.55

Example

ko@node1:~/$
1: 78.129.127.21
2: 212.68.211.181
3: 149.6.135.65
4: 154.54.59.57
5: 154.54.74.94
6: 130.117.14.178
7: 64.125.21.77
8: 64.125.27.0
9: 64.125.29.17
10: 64.125.29.131
11: 64.125.29.229
12: 64.125.30.249
13: **64.125.31.**42 (40/40)
14: **208.185.23.134** (40/40)TCP:MSS(0204058c)
15: 208.113.156.4
16: 208.113.156.14
17: 208.97.177.124

ko@node2:~$
1: 139.165.222.1
2: 193.190.228.29
3: 193.190.228.141
4: 193.190.252.97
5: 193.190.252.43
6: 193.190.200.28
7: 193.190.200.34
8: 193.191.10.19
9: *
10: 80.249.208.122
11: 64.125.21.77
12: 64.125.27.0
13: 64.125.29.17
14: 64.125.29.131
15: 64.125.29.229
16: 64.125.30.249
17: **64.125.31.**42 (40/40)
18: **208.185.23.134** (40/40) TCP:MSS(0204058c)
19: 208.113.156.4
20: 208.113.156.14
21: 208.97.177.124

ko@node3:~/$
1: 129.22.150.2
2: 10.2.0.98
3: 10.2.0.241
4: 199.18.156.65
5: 64.57.29.173
6: 206.126.236.147
7: 138.187.159.14
8: *
9: 94.102.162.99
10: 64.125.21.77
11: 64.125.27.0
12: 64.125.29.19
13: 64.125.29.131
14: 64.125.29.229
15: 64.125.30.249
16: **64.125.31.**44 (40/40)
17: **208.185.23.134** (40/40) TCP::MSS(0204058c)
18: 208.113.156.4
19: 208.113.156.14
20: 208.97.178.55

- 208.185.232.134 is the informant
- 64.125.31.42 and 64.125.31.44 are the offenders
- Merged into a single MB

Pre-processing: derivation (Step 1)

- *948,457 addresses observed*

Pre-processing: derivation (Step 1)

- *948,457 addresses observed*

  Unresolved addresses:

- 21,330 (2.25%) from 10.0.0.0/8, 172.16.0.0/12 or 192.168.0.0/16
- 905 (0.1%) from 100.64.0.0/10
- 20,669 (2.18%) no AS (cymru)

Pre-processing: derivation (Step 1)

- *948,457 addresses observed*

  Unresolved addresses:

- 21,330 (2.25%) from 10.0.0.0/8, 172.16.0.0/12 or 192.168.0.0/16
- 905 (0.1%) from 100.64.0.0/10
- 20,669 (2.18%) no AS (cymru)

- Keep if ends of unresolved zone are mapped to same AS.