

tracebox

Korian Edeline (ULg)
WP1/WP2
Oslo, July 2017



measurement and architecture for a middleboxed internet

measurement

architecture

experimentation

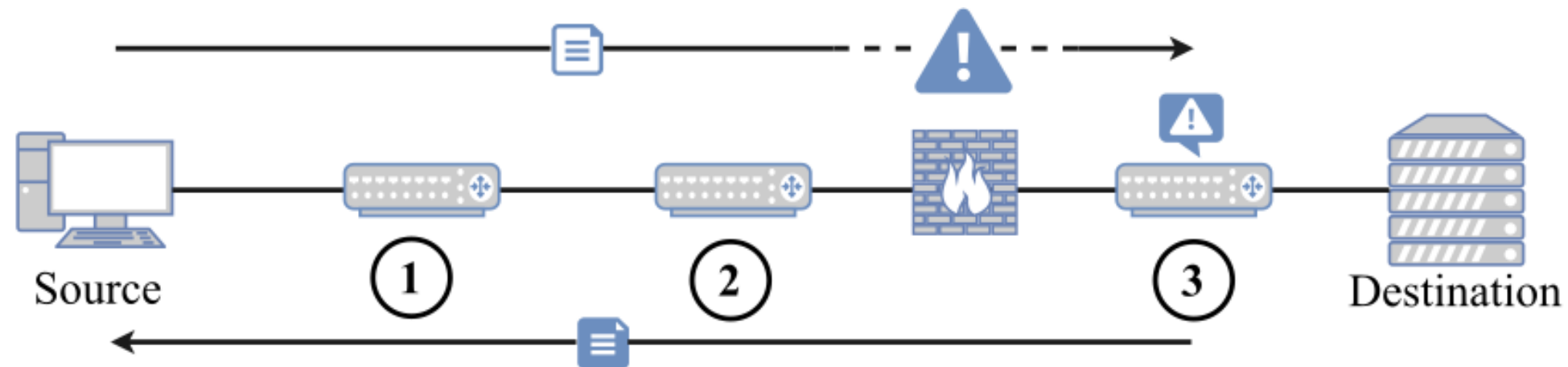
This project has received funding from the European Union's Horizon 2020 research and innovation programme

under grant agreement No 688421. The opinions expressed and arguments employed reflect only the authors'

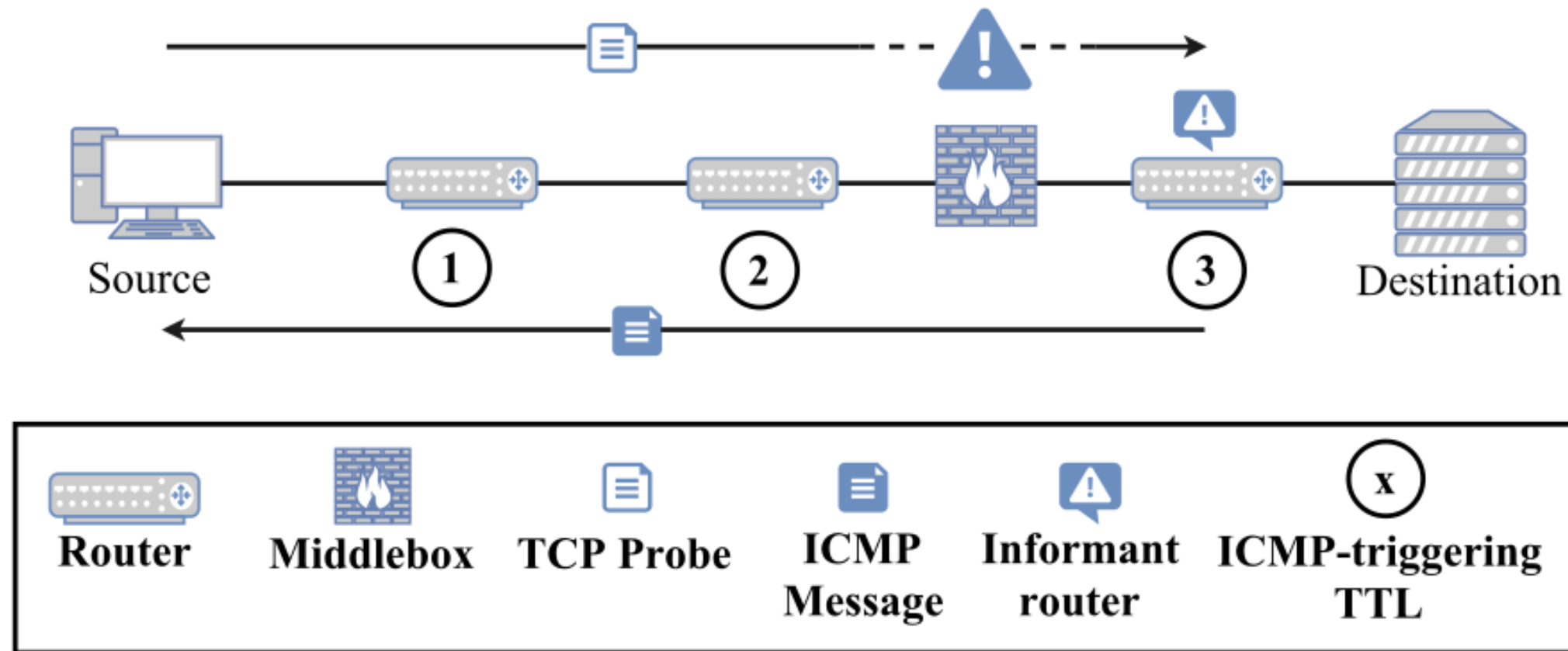
view. The European Commission is not responsible for any use that may be made of that information.



tracebox



tracebox



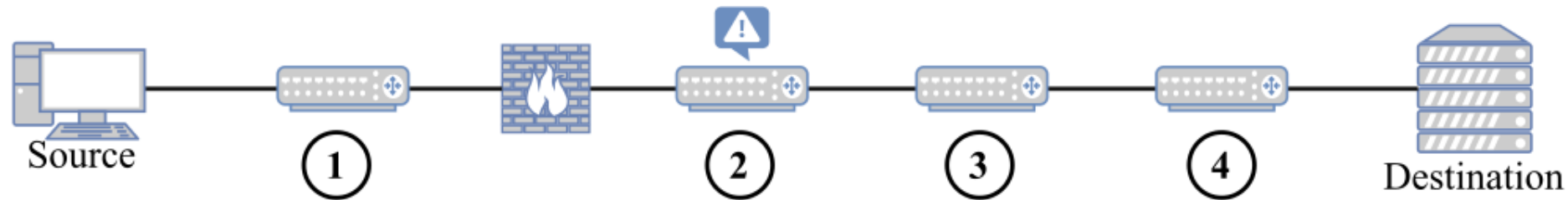
- RFC 792 : “The internet header plus the first 64 bits”
- RFC 1812 : “as much [...] as possible” (< 576 B)



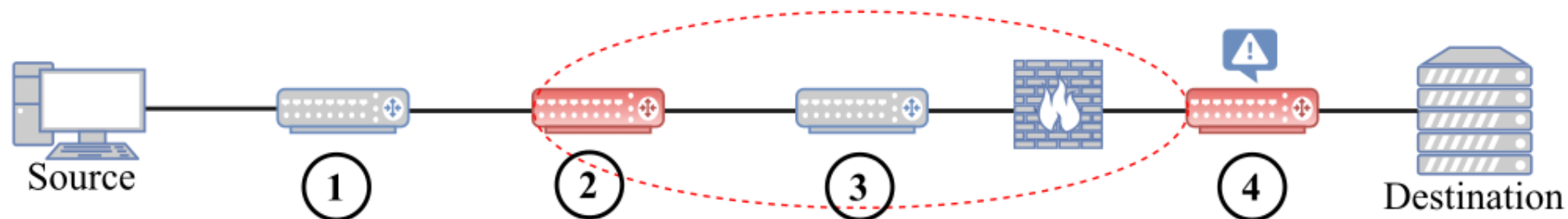
Dataset

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

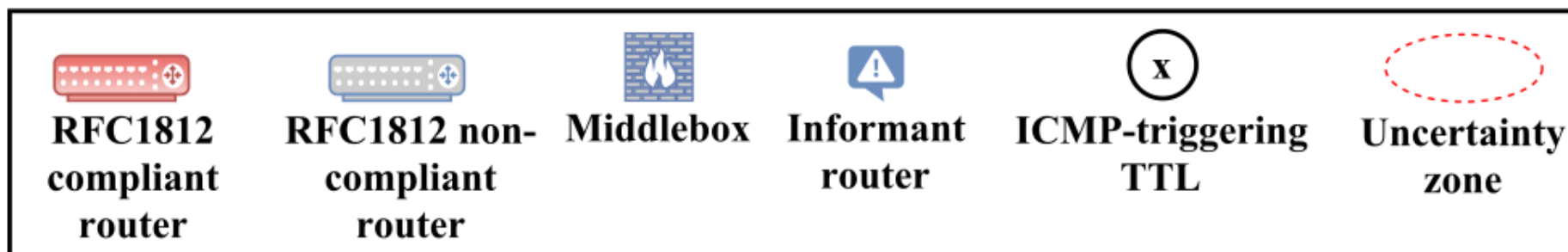
tracebox



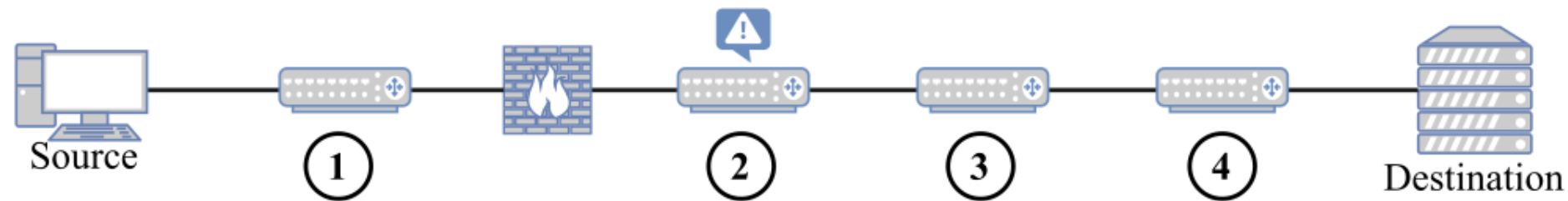
1. Modified field is within the first 48 bytes



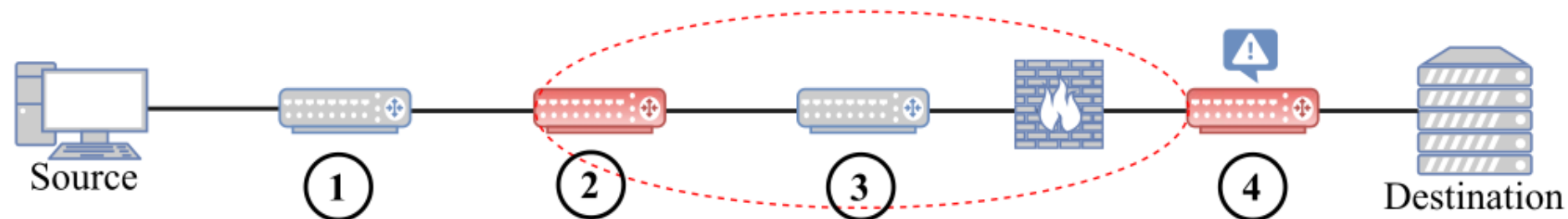
2. Modified field is outside the first 48 bytes



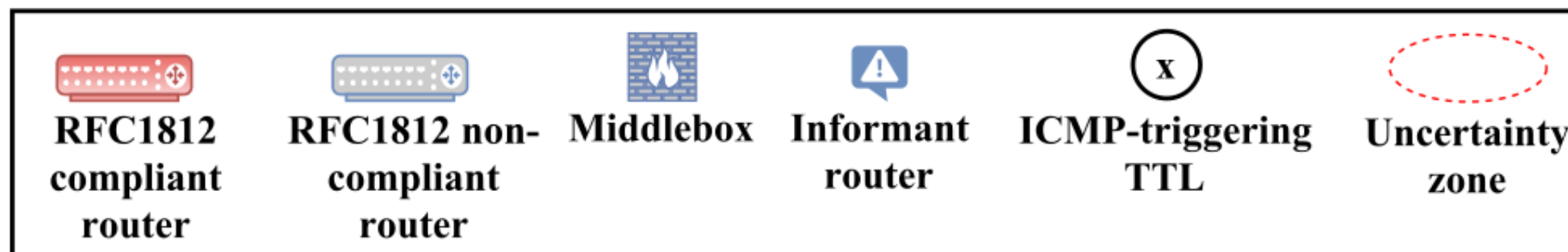
tracebox



1. Modified field is within the first 48 bytes



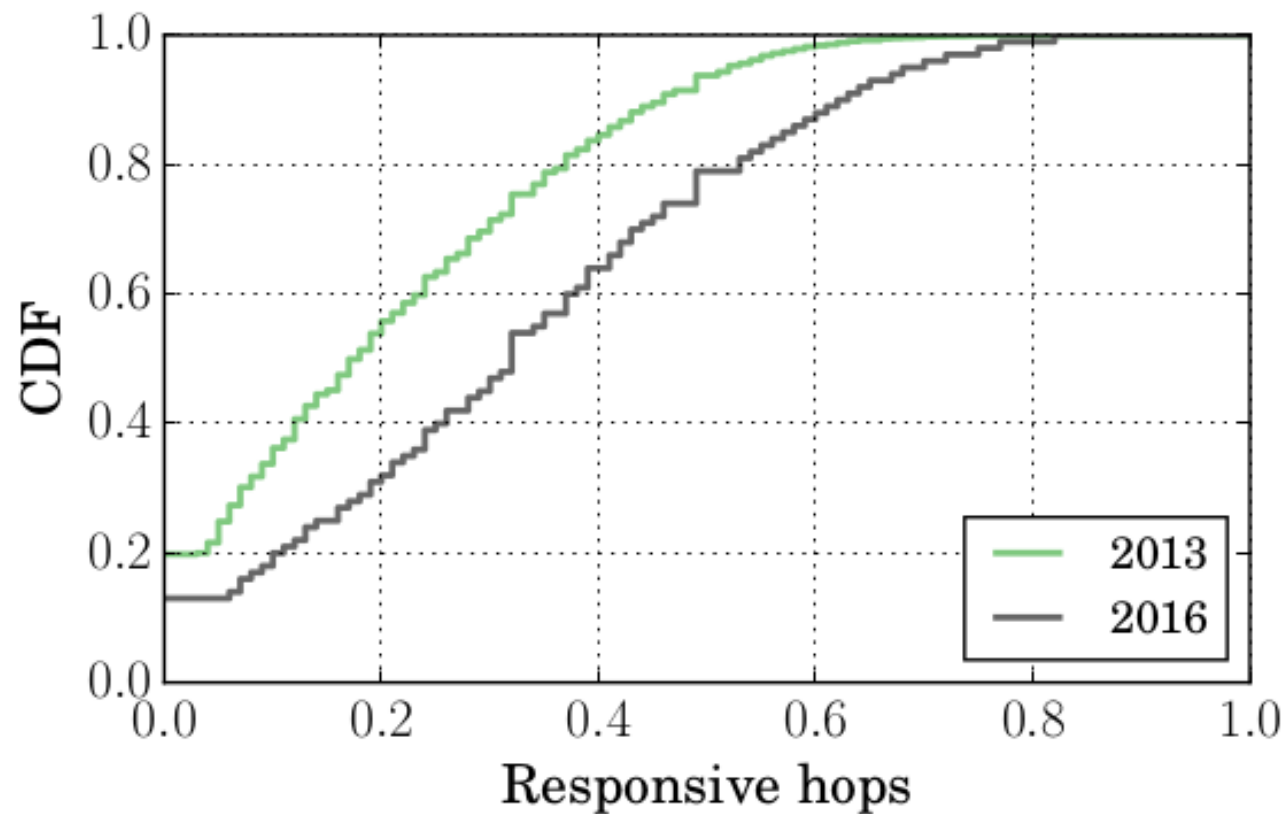
2. Modified field is outside the first 48 bytes



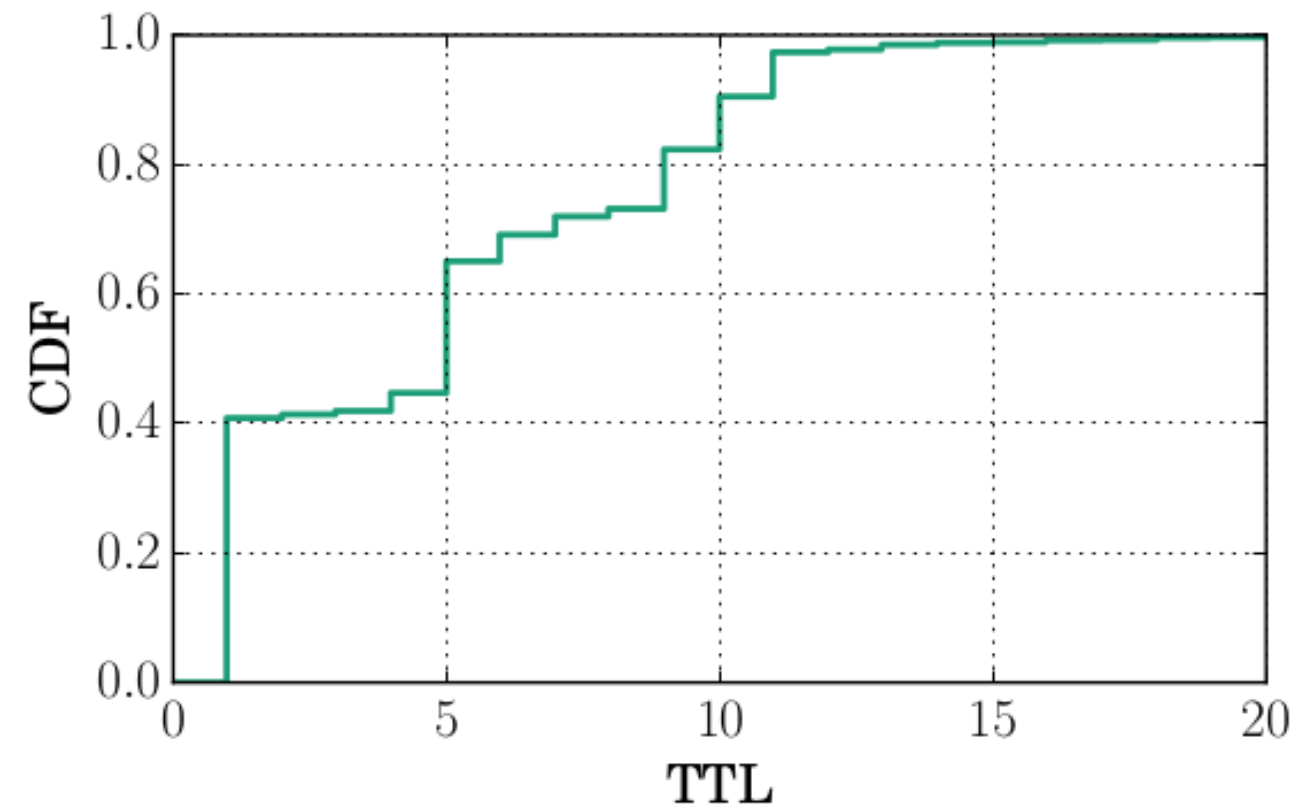
- U Zone : Observed sizes ? Workaround ?



U Zone



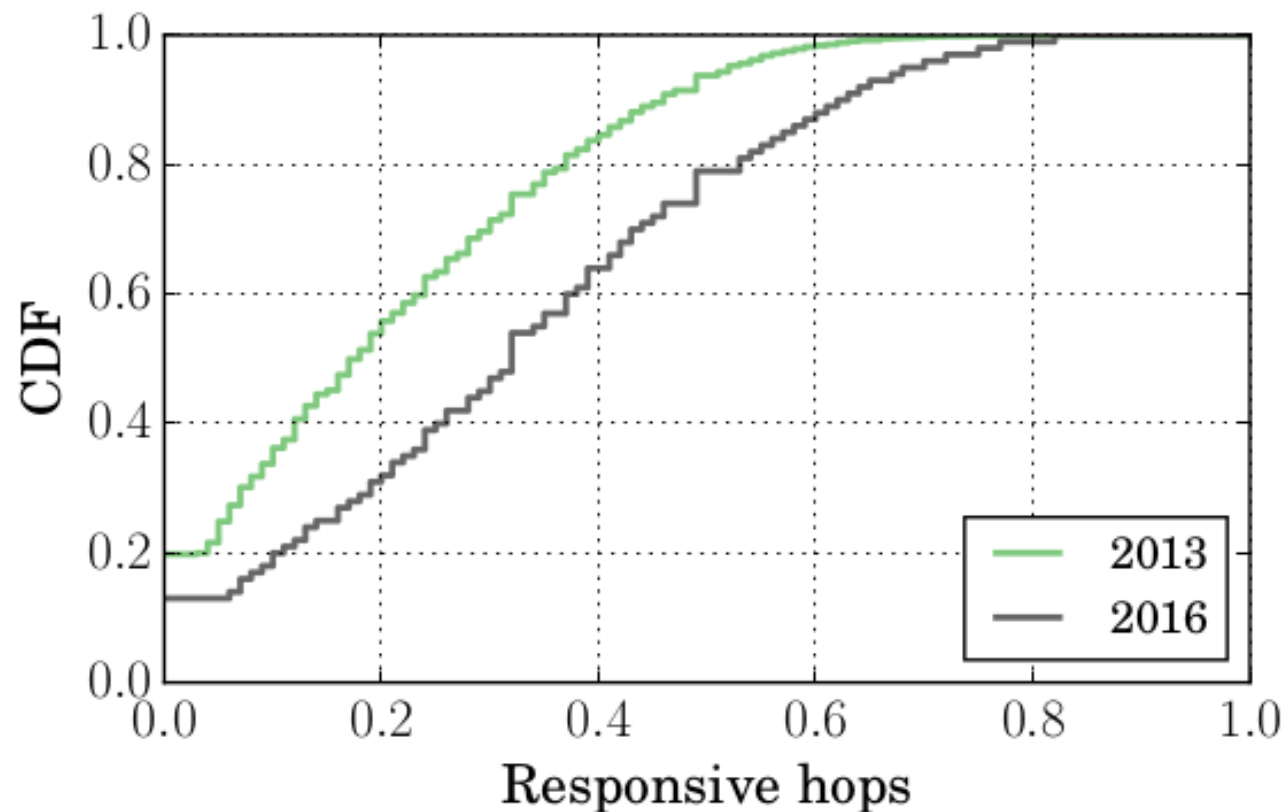
Proportion of RFC 1812
routers on observed paths



Sizes of U Zones

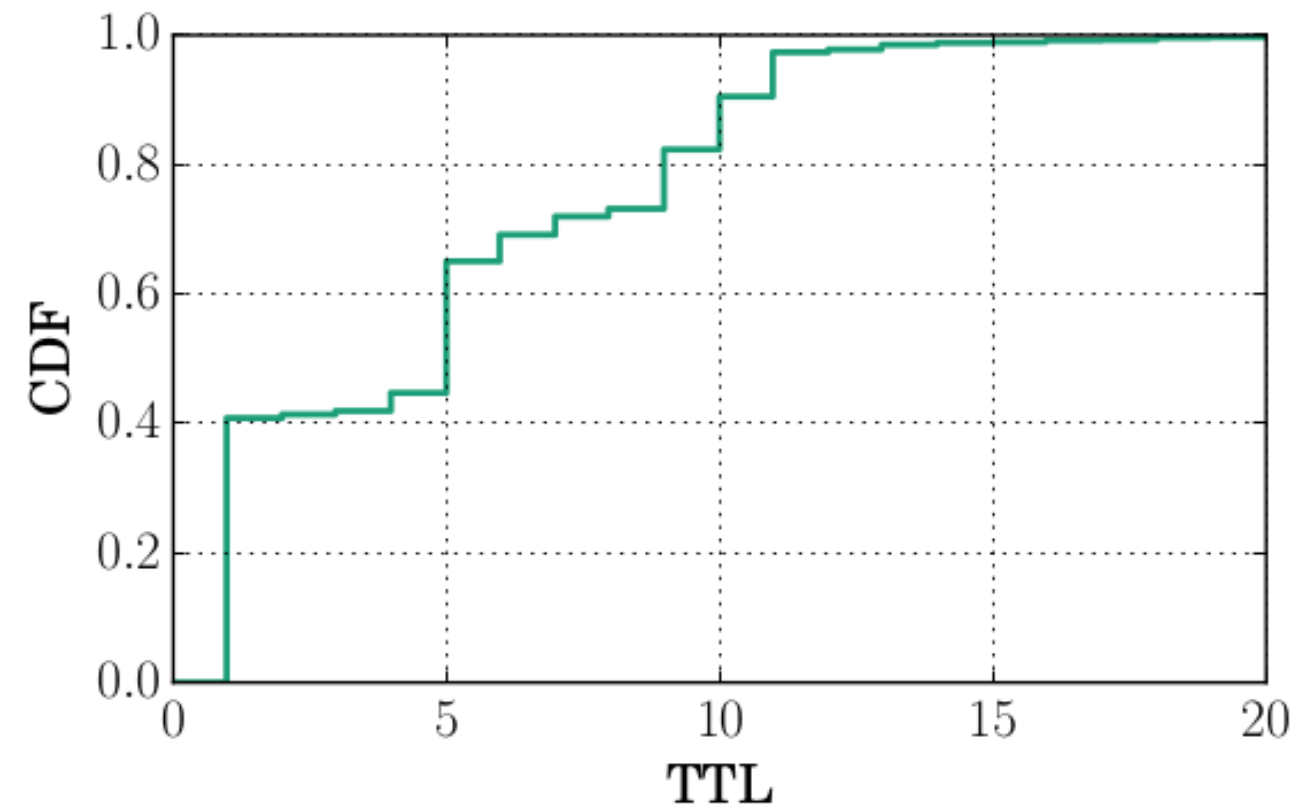


U Zone



Proportion of RFC 1812 routers on observed paths

- Increases over time



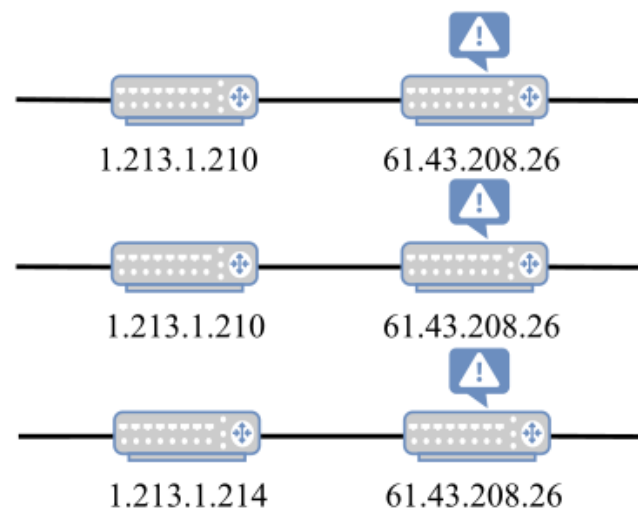
Sizes of U Zones

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

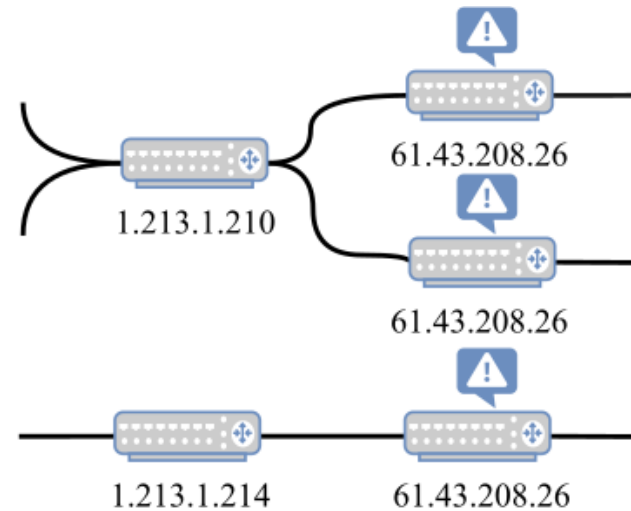


Pre-processing: summary

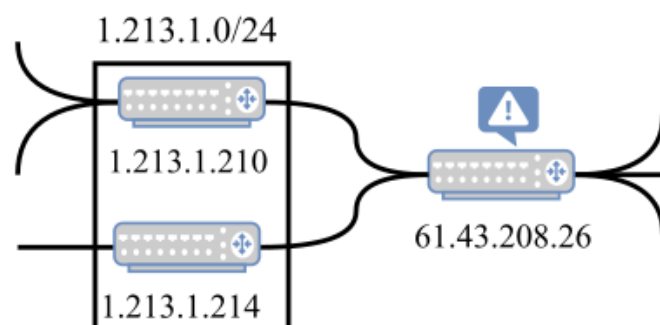
- Observation : *A single modification observed on a path during a campaign.*



a. Offenders derivation



b. Offenders grouping

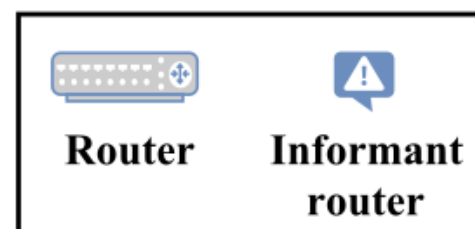


c. Offenders merging

Input: 38M obs.

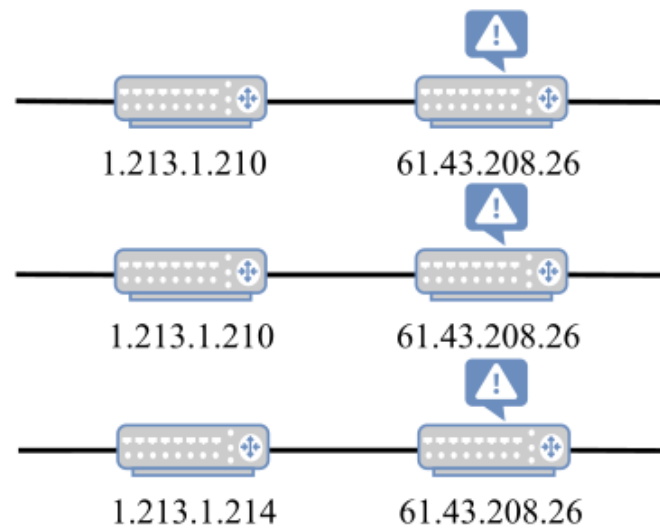
- Label observations
- Aggregate observations
- Merge offenders into middleboxes

Output: 8K MBs

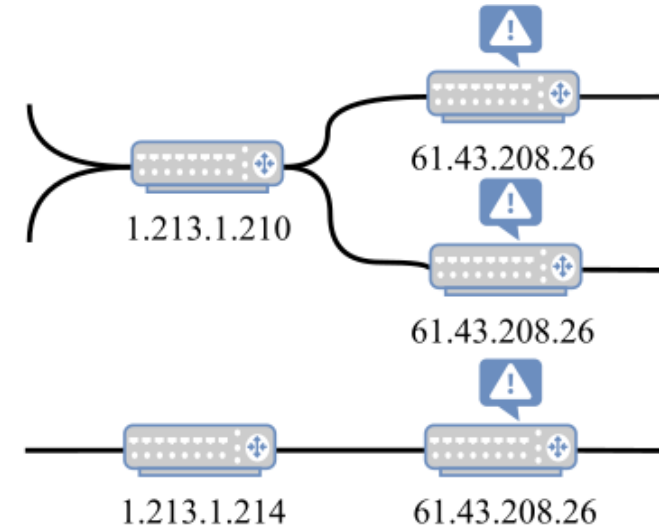




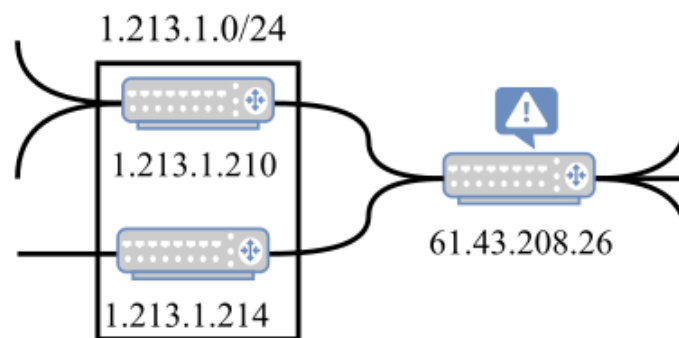
Pre-processing: derivation (Step 1)



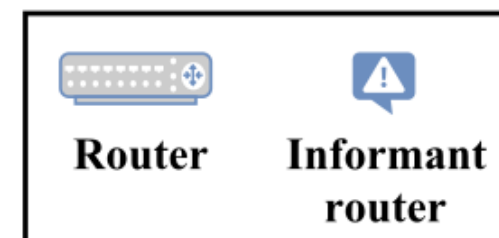
a. Offenders derivation



b. Offenders grouping



c. Offenders merging





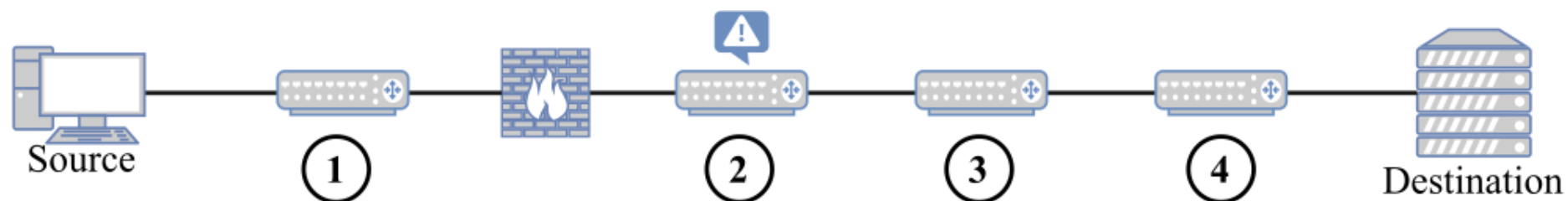
Pre-processing: derivation (Step 1)

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

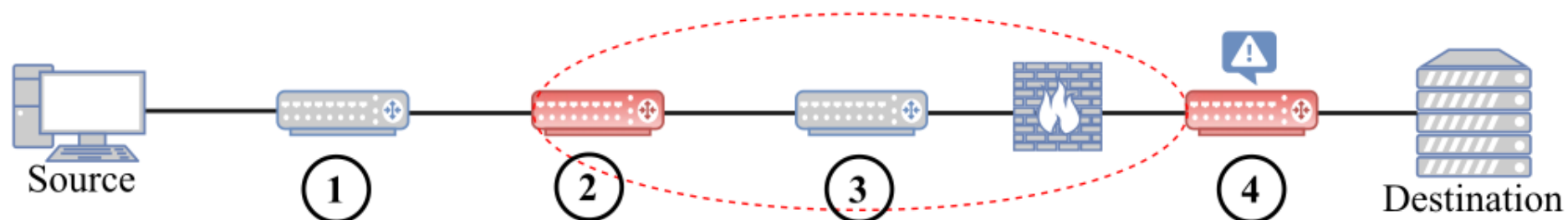


Pre-processing: derivation (Step 1)

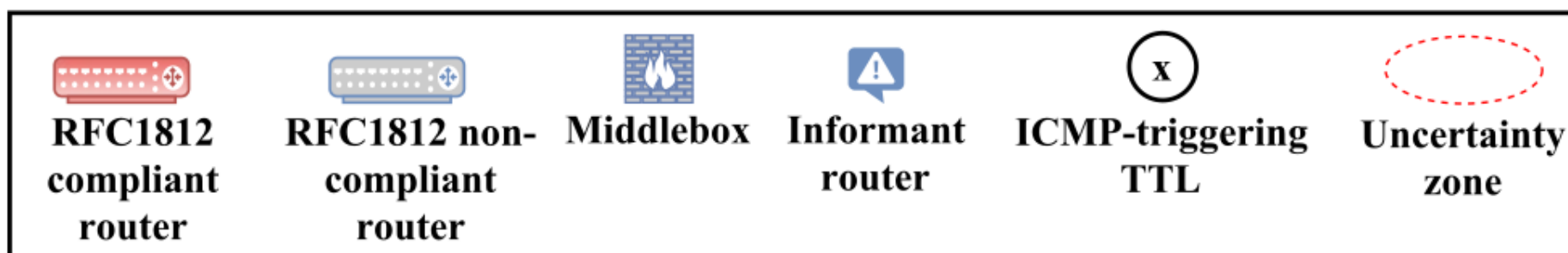
- Offender : *The router preceding the middlebox on a given path*



1. Modified field is within the first 48 bytes



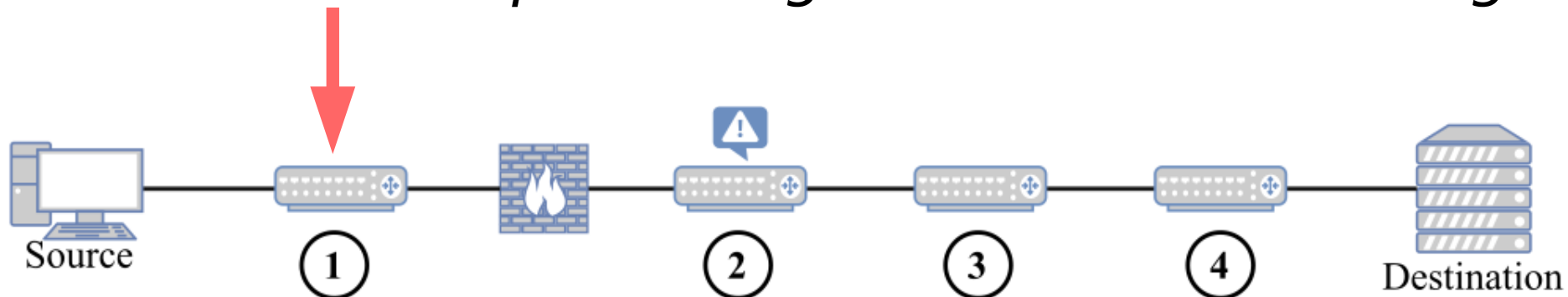
2. Modified field is outside the first 48 bytes



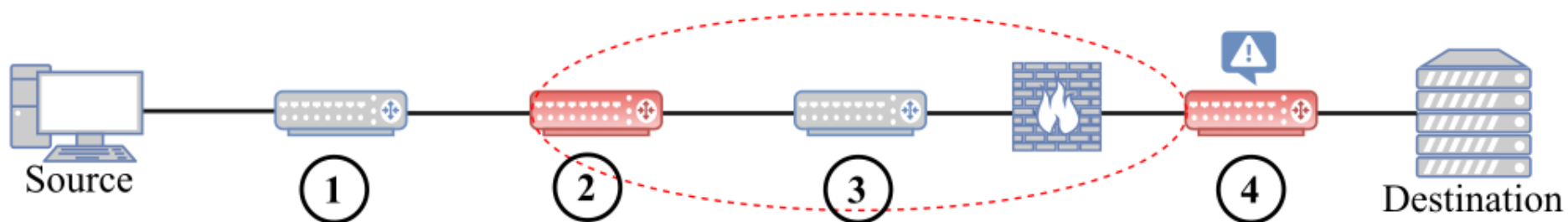


Pre-processing: derivation (Step 1)

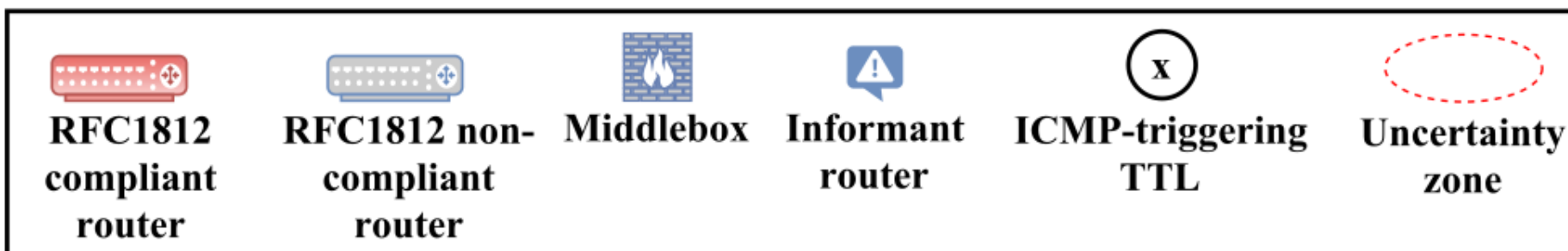
- Offender : *The router preceding the middlebox on a given path*



1. Modified field is within the first 48 bytes



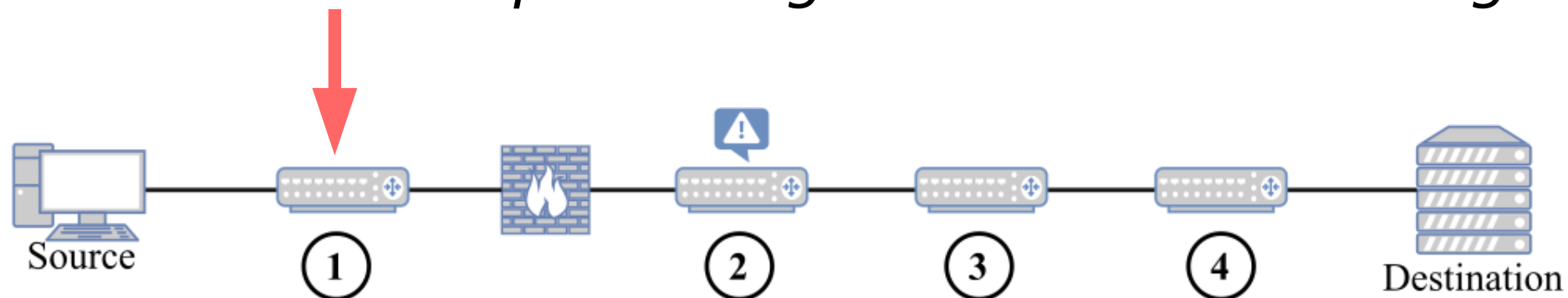
2. Modified field is outside the first 48 bytes



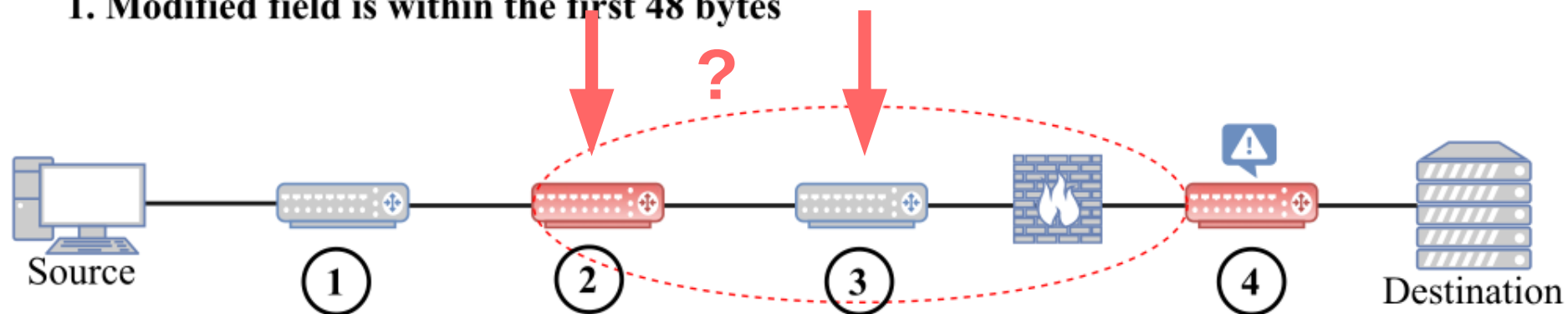


Pre-processing: derivation (Step 1)

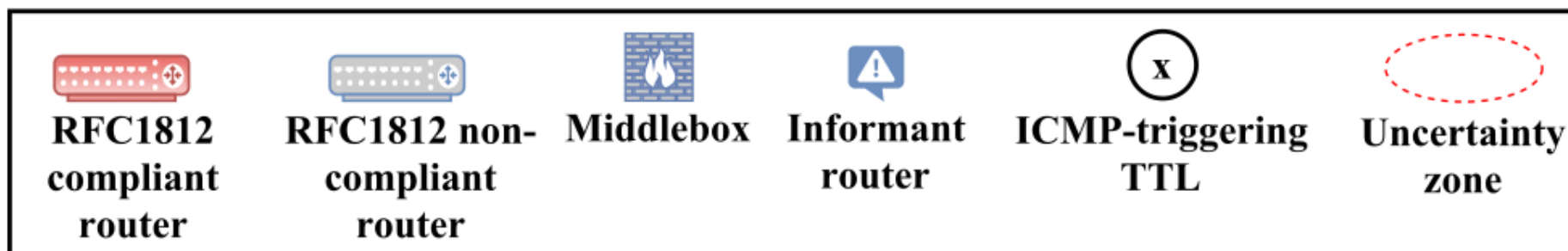
- Offender : *The router preceding the middlebox on a given path*



1. Modified field is within the first 48 bytes



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)

- 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.



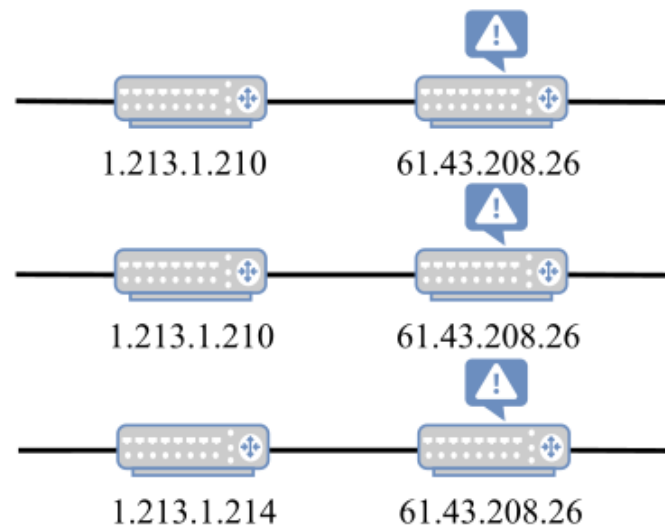
Pre-processing: derivation (Step 1)

Output:

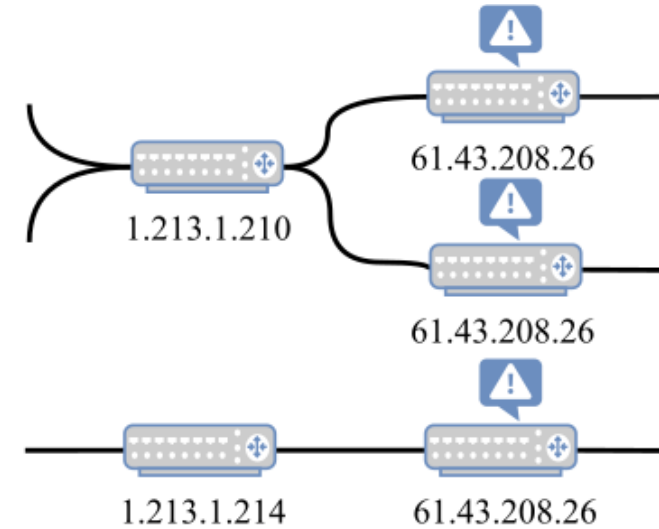
- Offender AS for 99% obs.
- Offender IP for 52% obs. (20M)



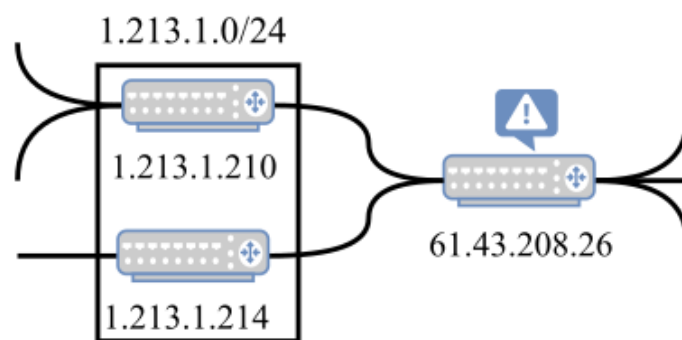
Pre-processing: grouping (Step 2)



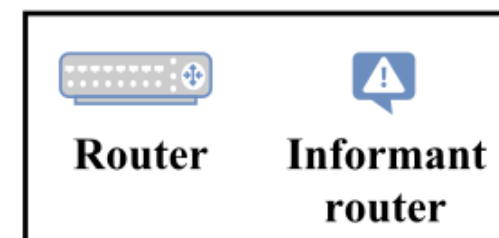
a. Offenders derivation



b. Offenders grouping



c. Offenders merging





Pre-processing: grouping (Step 2)

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



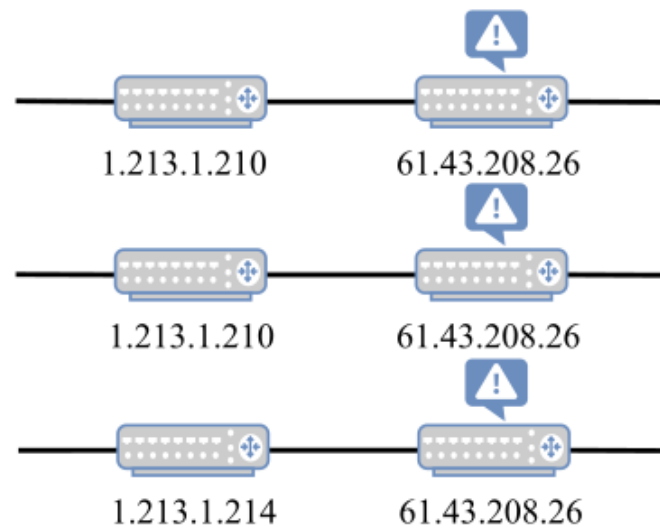
Pre-processing: grouping (Step 2)

Output:

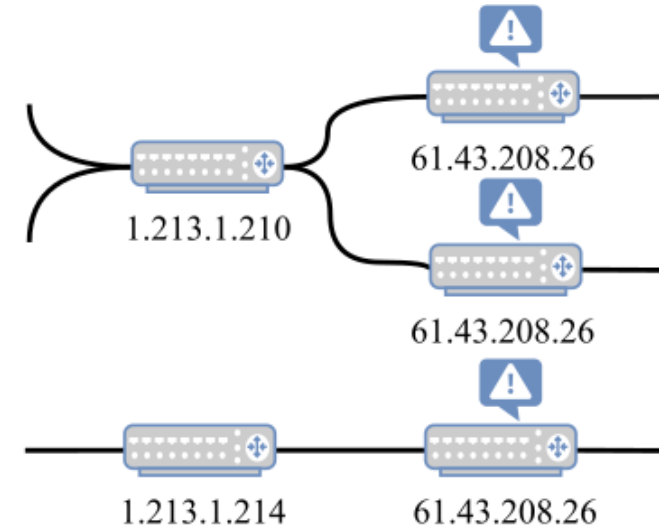
- 8,322 offenders



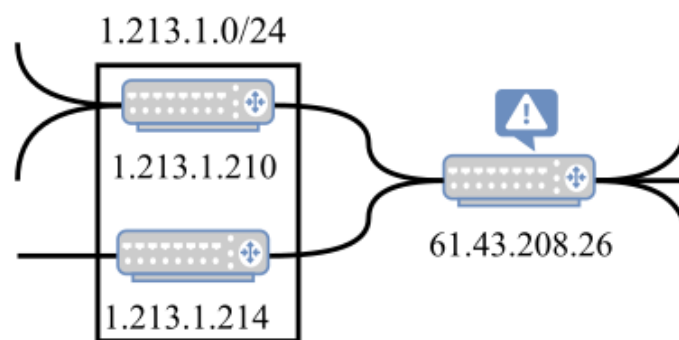
Pre-processing: merging (Step 3)



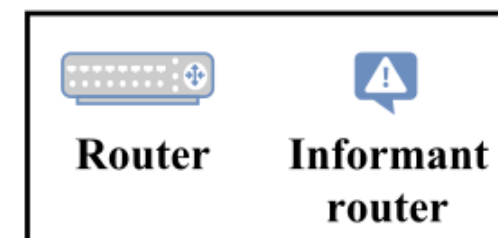
a. Offenders derivation



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

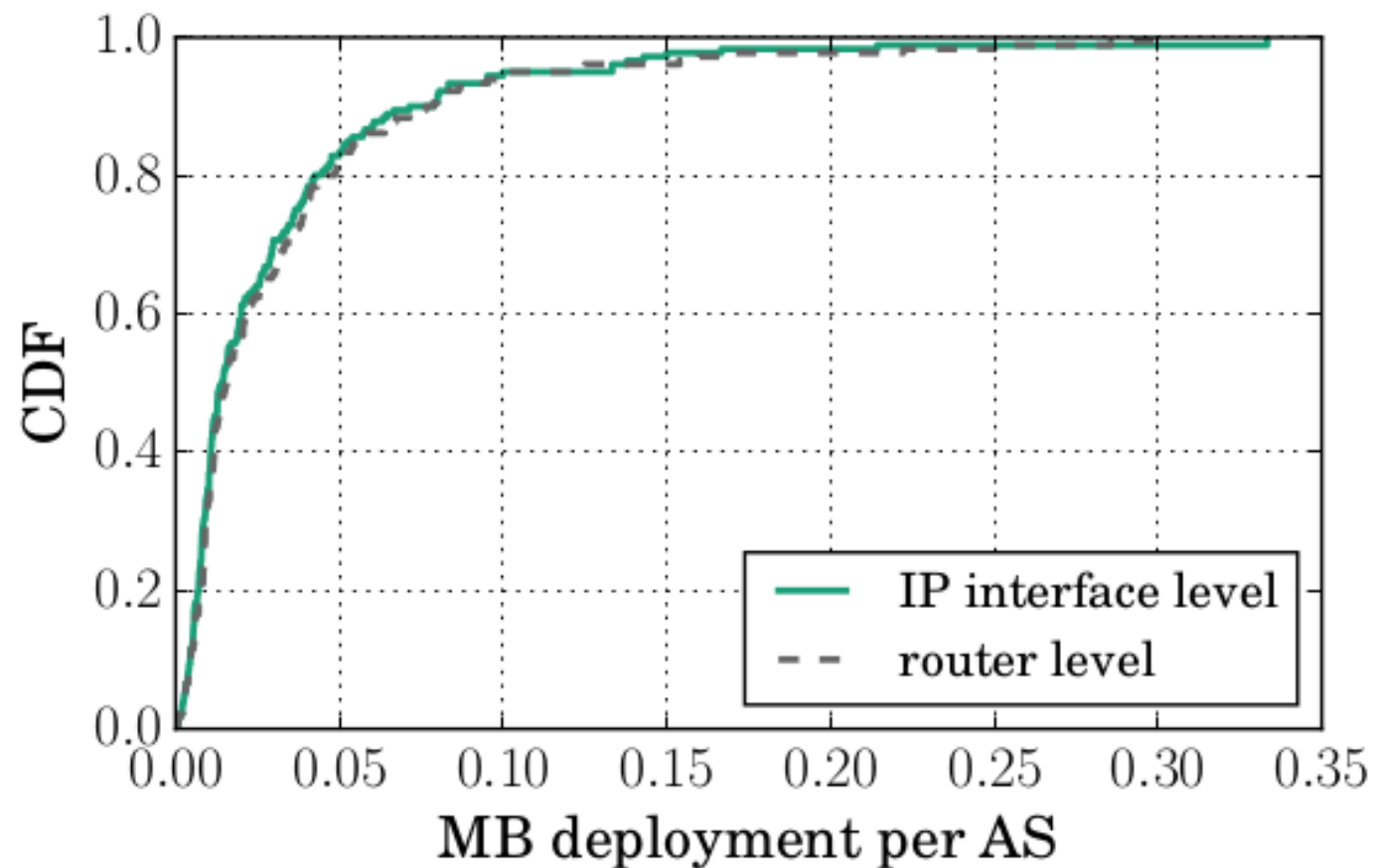


Results: prevalence

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



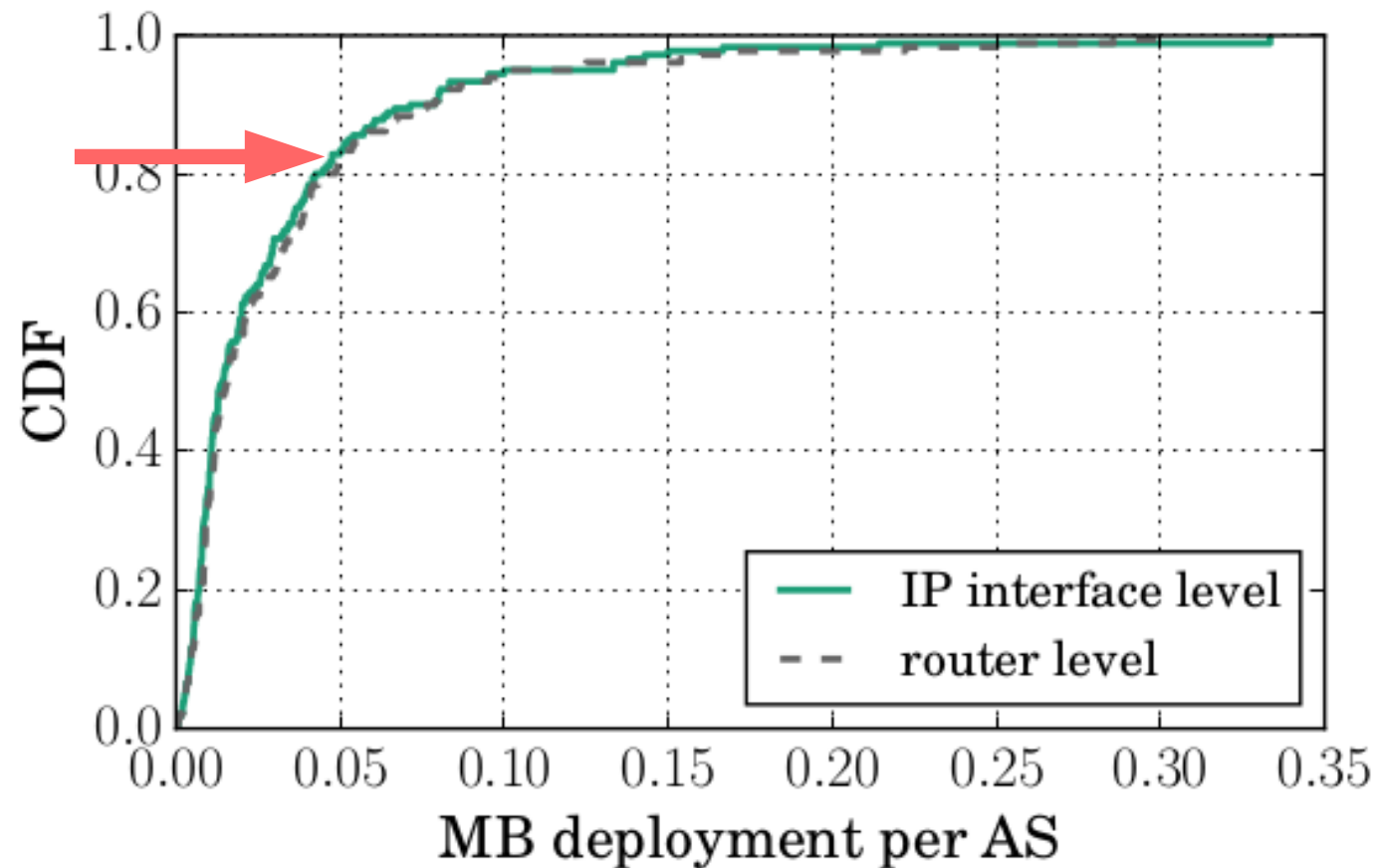
Prevalence: deployment



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



Prevalence: deployment

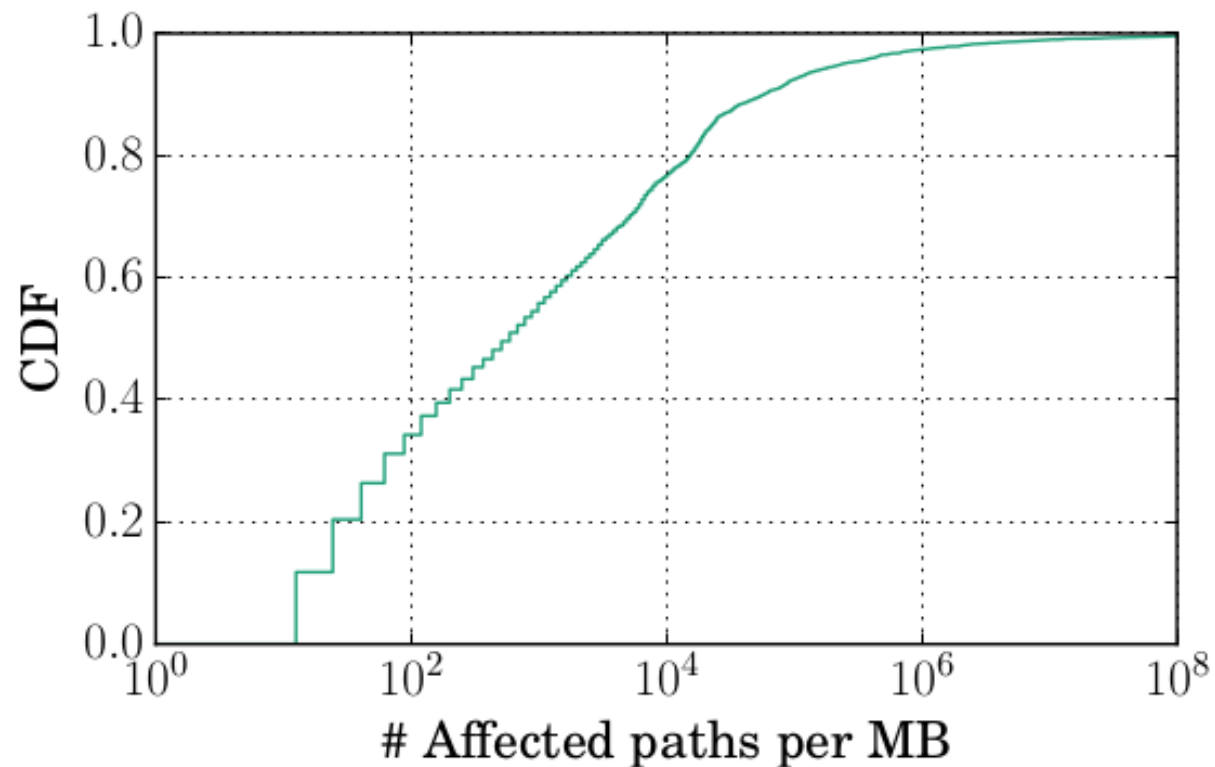


Deployed MB / IP interfaces, per AS. Alias resolution using CAIDA ITDK dataset.

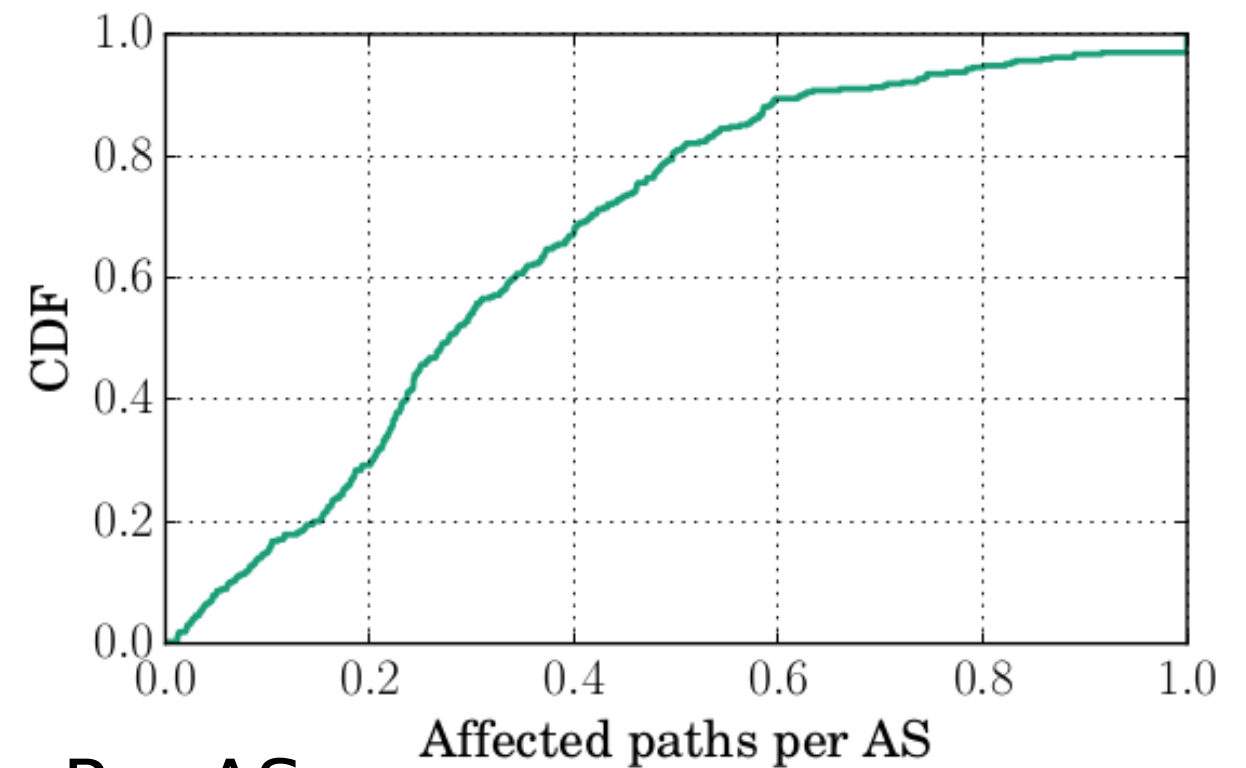
- In general, less than 5%
- Cogent: 1 - 1.5%



Prevalence: popularity



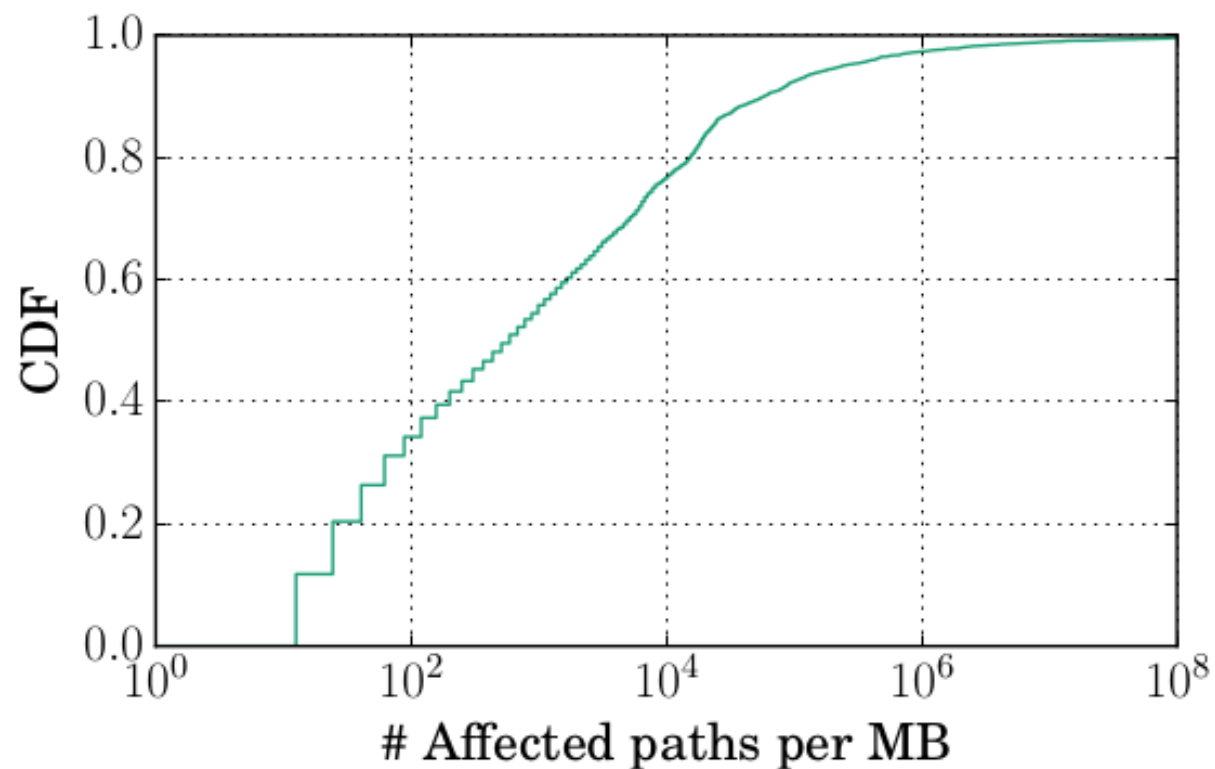
Per MB



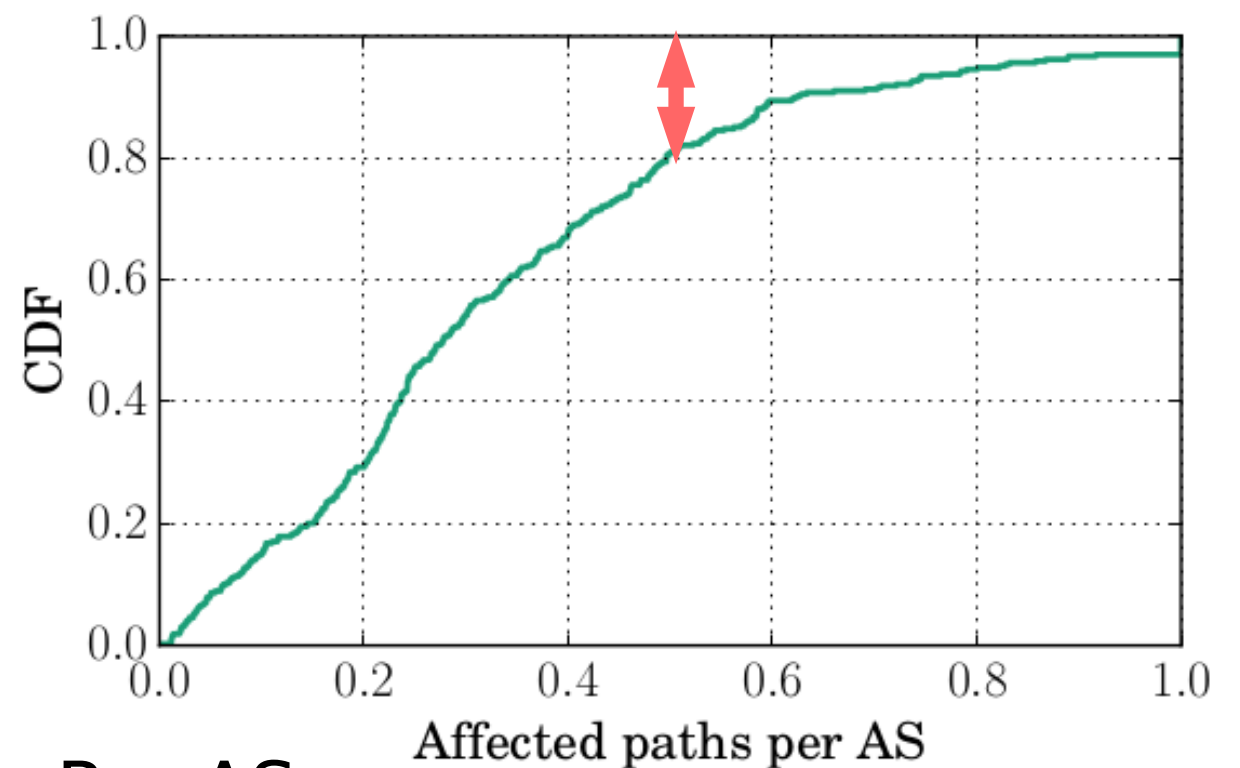
Per AS



Prevalence: popularity



Per MB

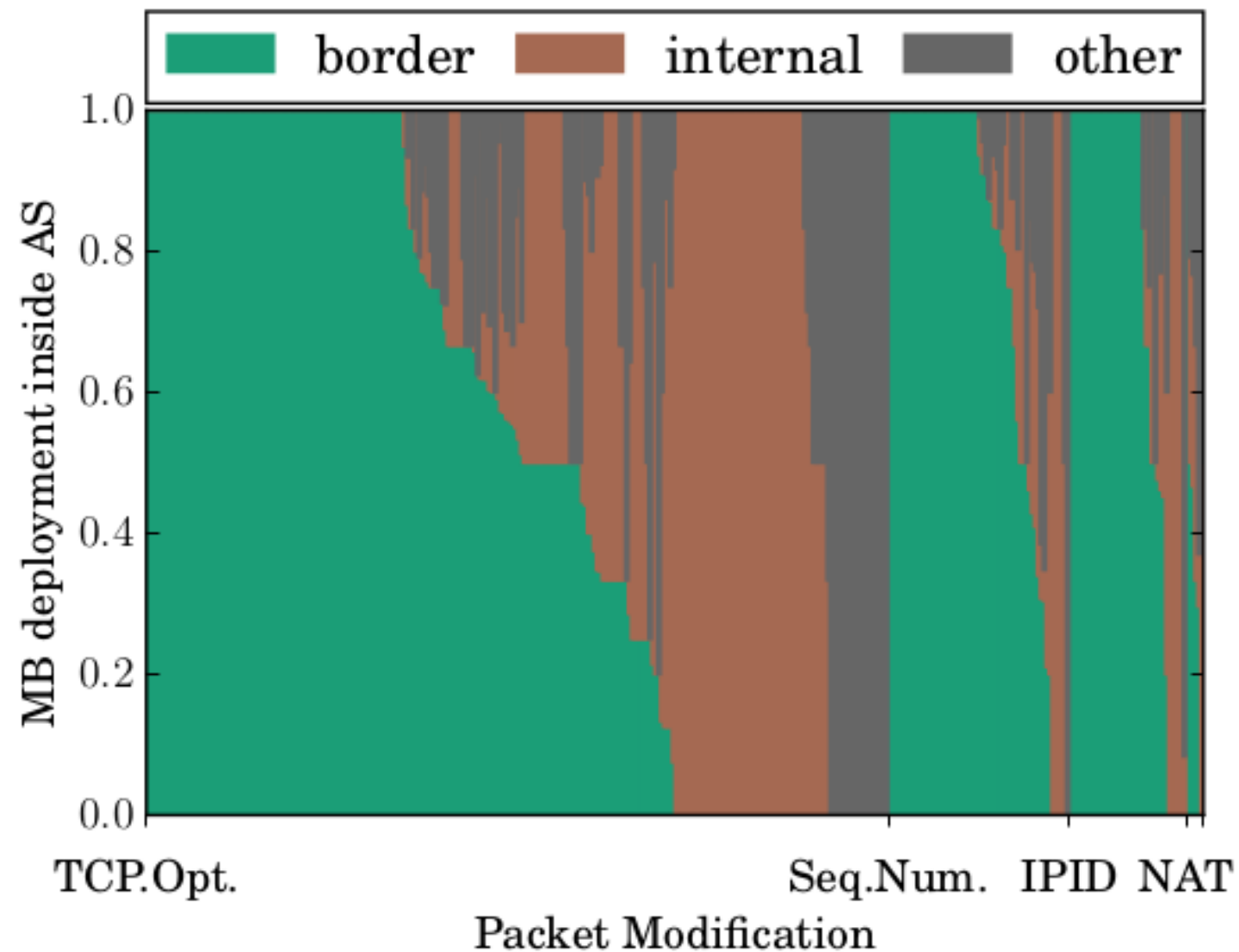


Per AS

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



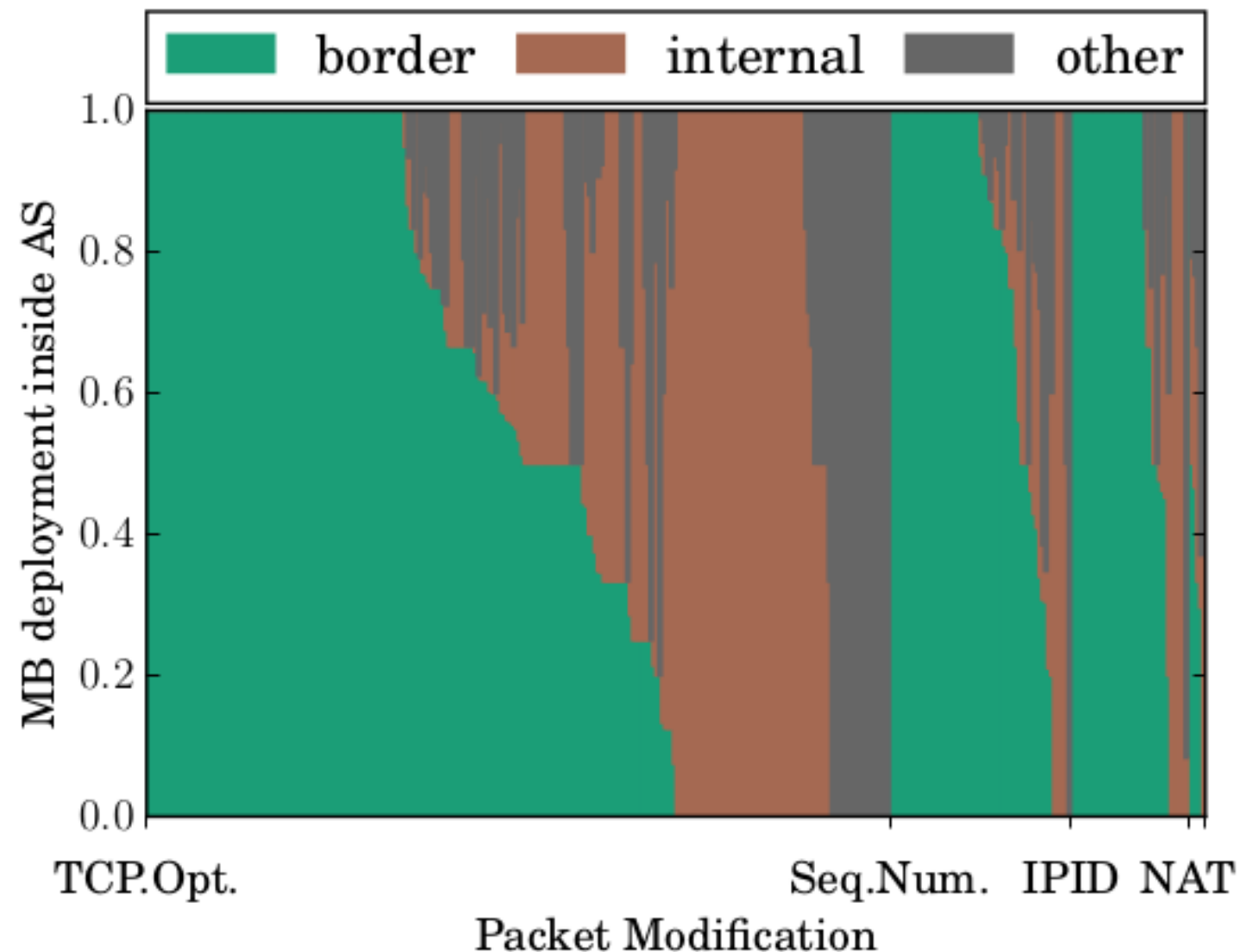
Prevalence: position



MB Positions, per categories
of modif., per AS



Prevalence: position

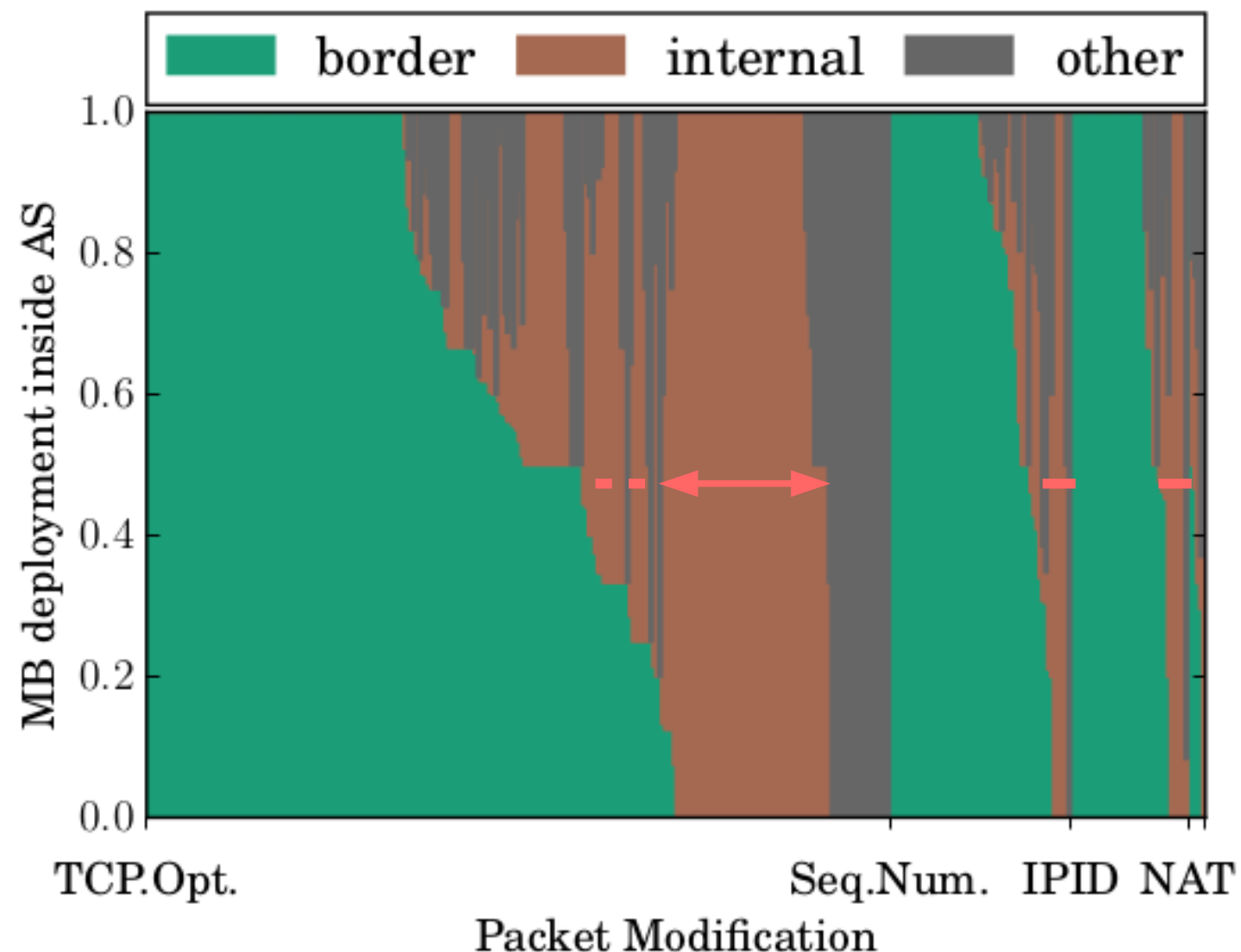


- border: 4,210 (52.6%)
- internal: 2,931 (36.6%)
- Other: conflict or unable to derive position (9.1%), or moved ? (1.7%)

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



Results: persistence

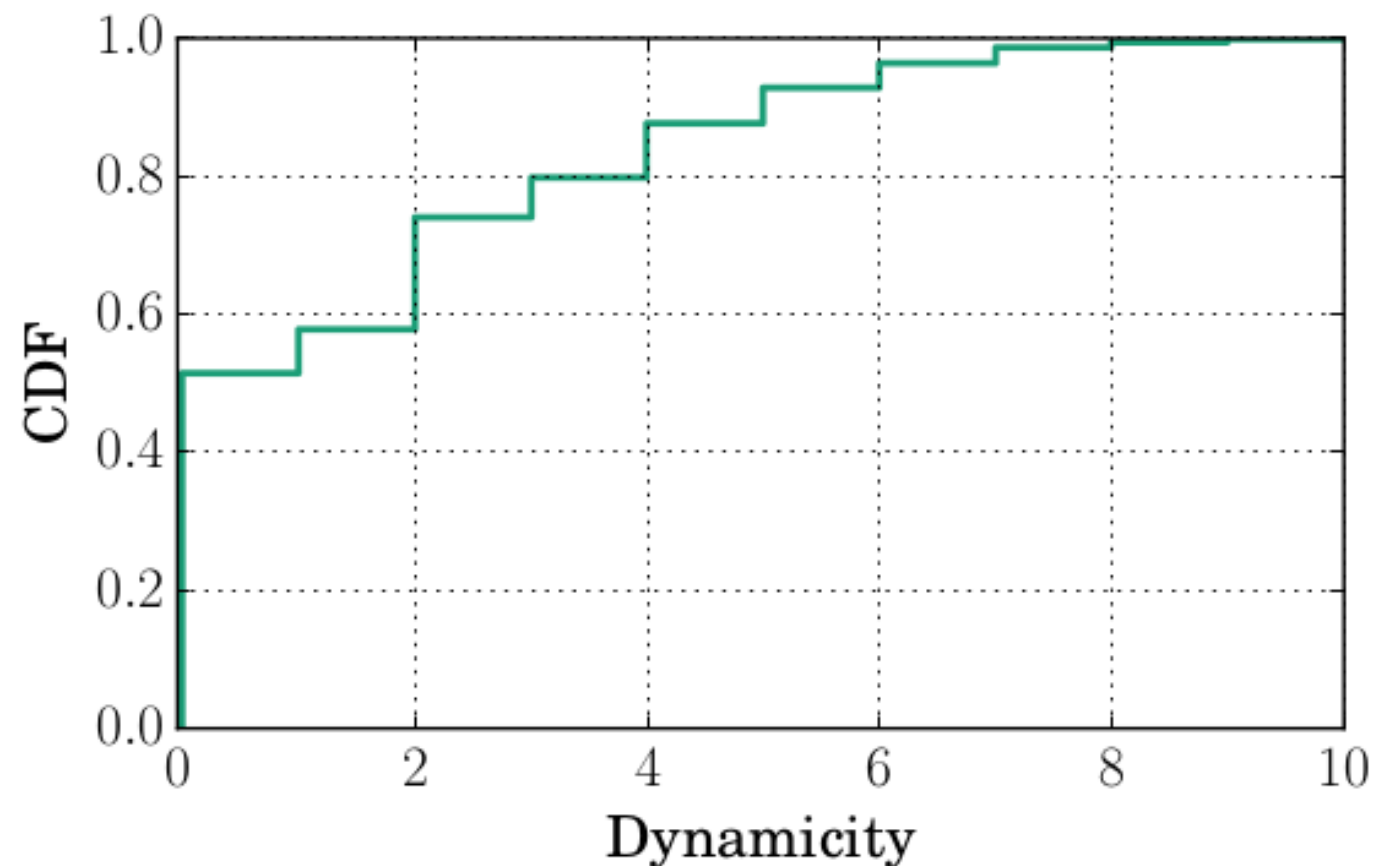


Results: persistence

- 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



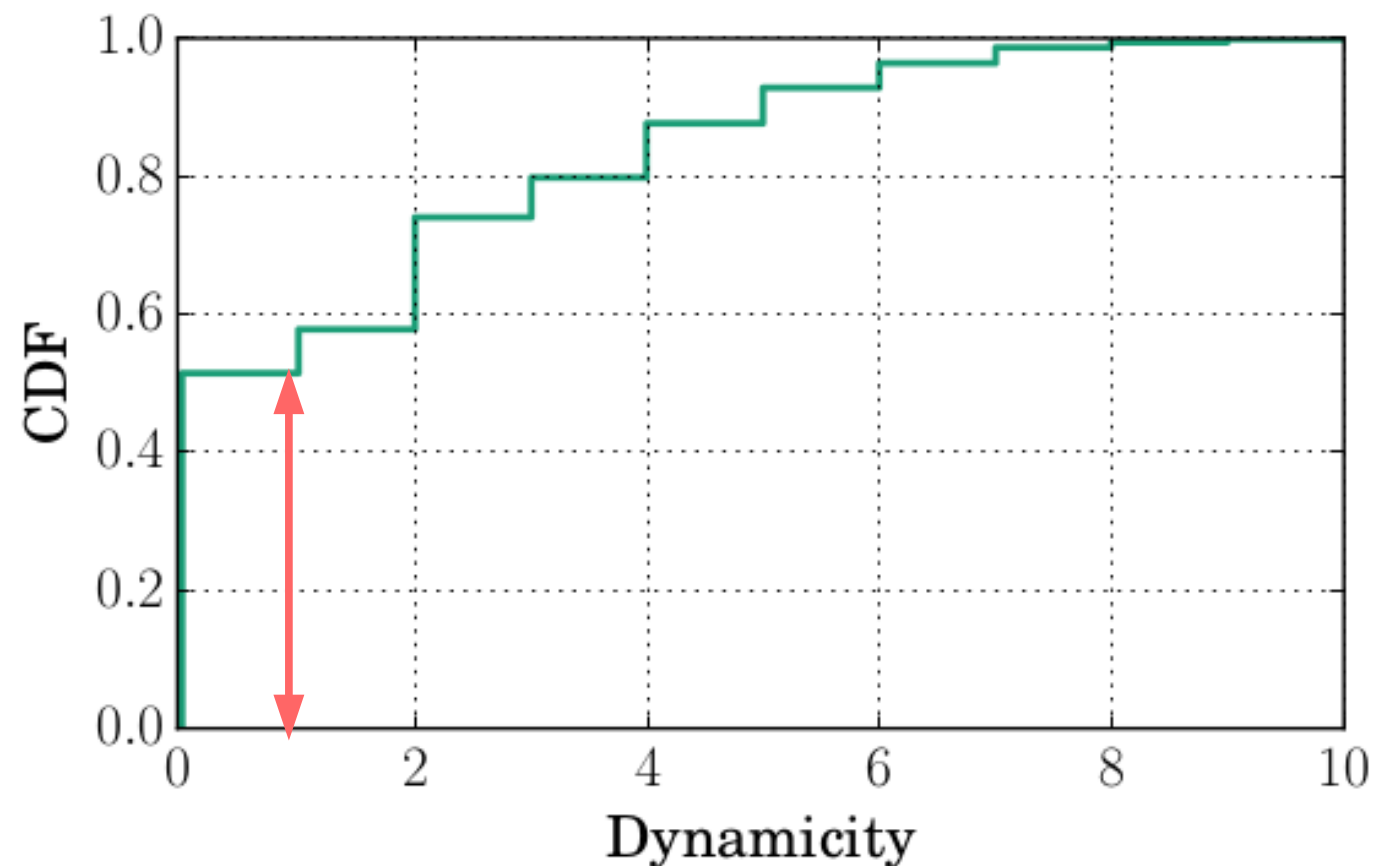
Results: persistence



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



Results: persistence

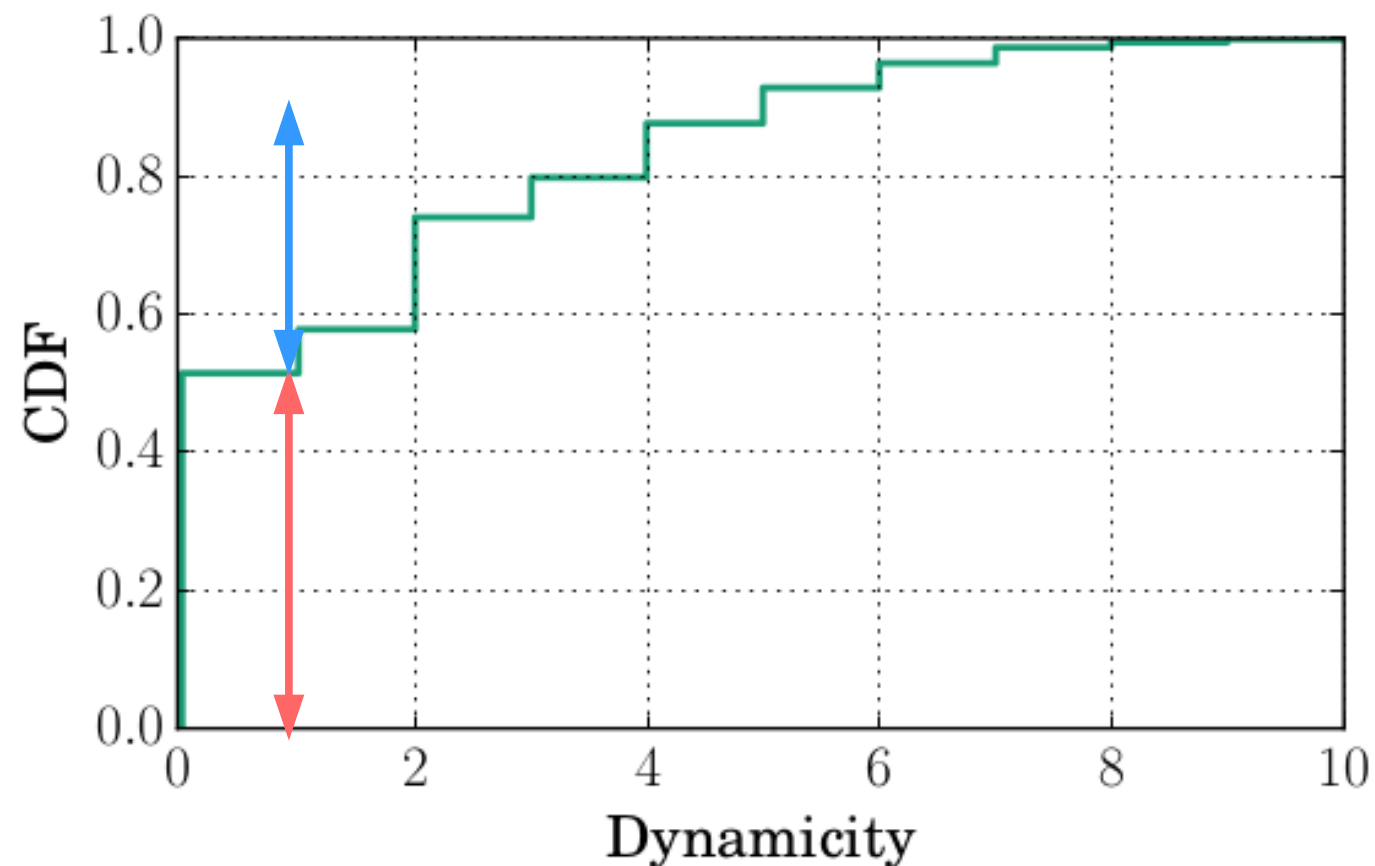


State changes per MB, Invisible == Active. 14 campaigns over 70 days.

- 51% are stable



Results: persistence

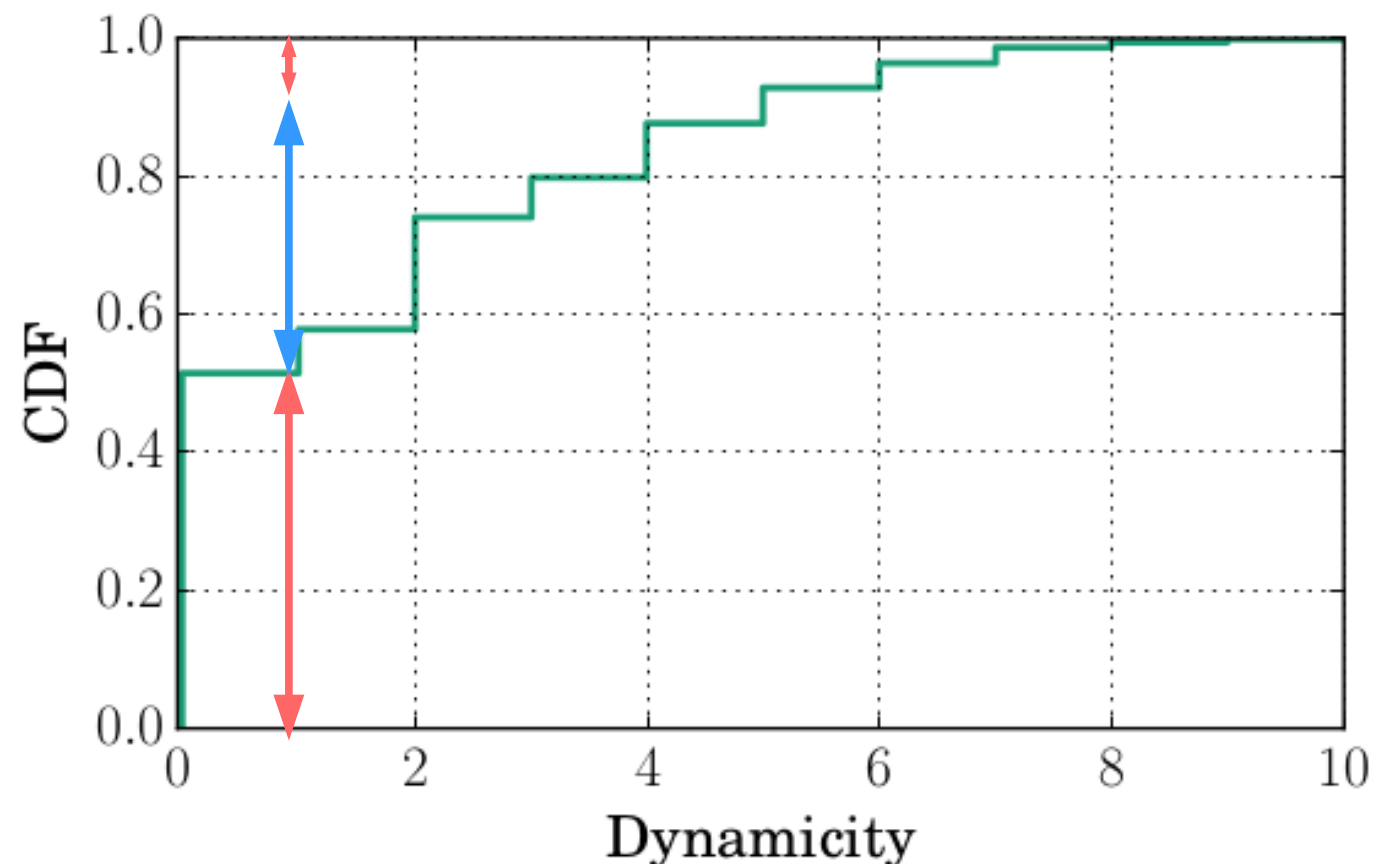


State changes per MB, Invisible == Active. 14 campaigns over 70 days.

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



Results: persistence

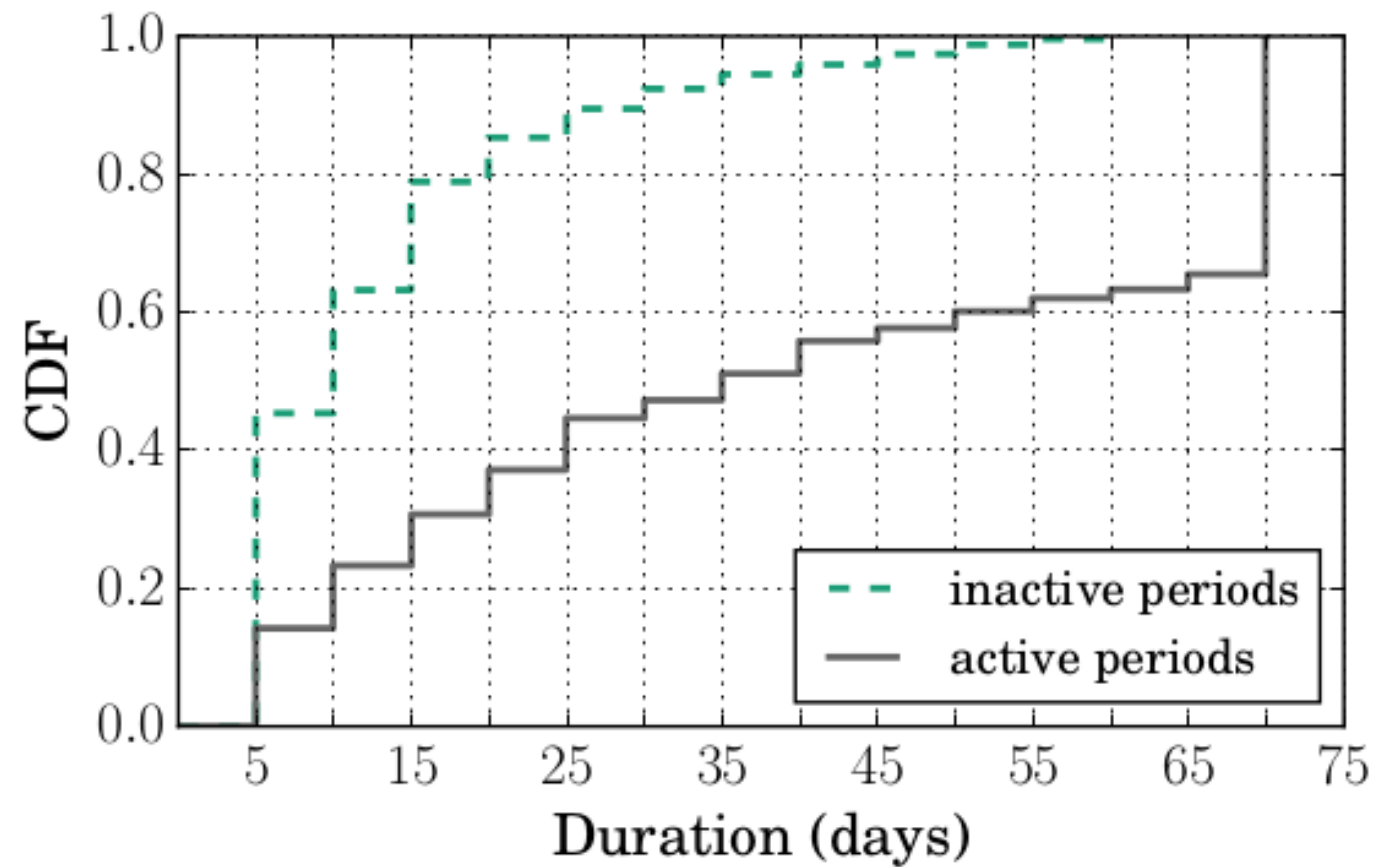


State changes per MB, Invisible == Active. 14 campaigns over 70 days.

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



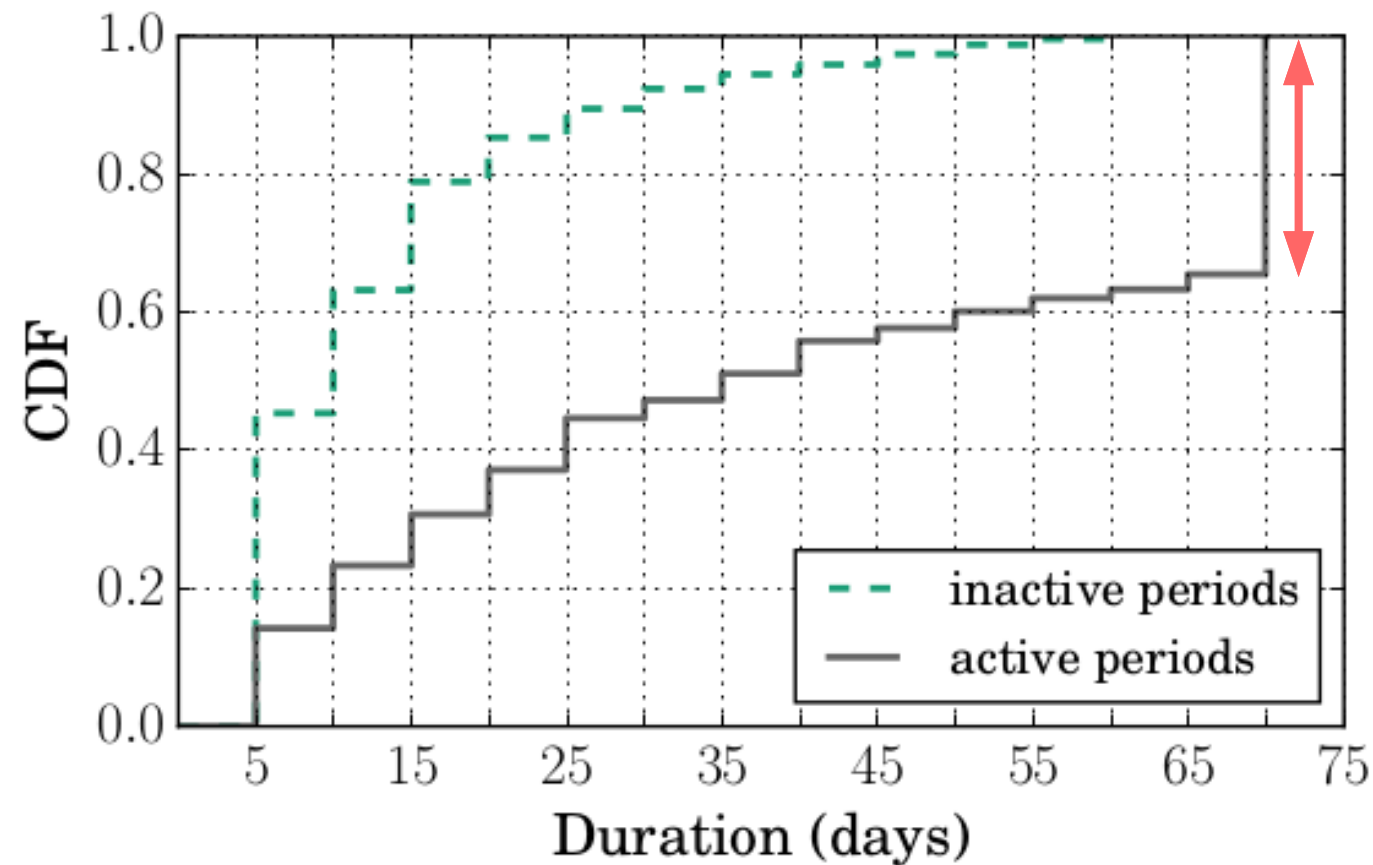
Results: persistence



state durations (max 70 days)



Results: persistence

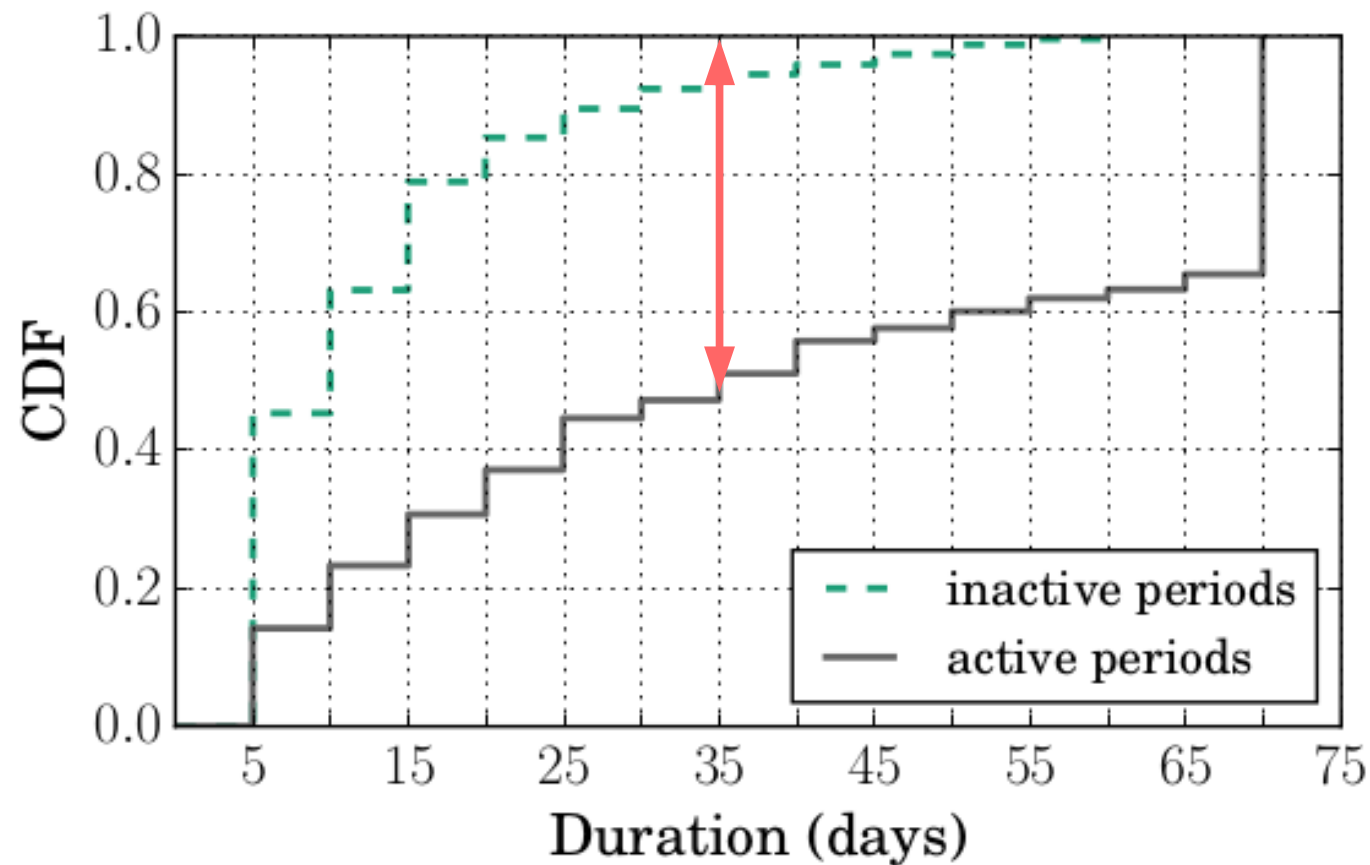


state durations (max 70 days)

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



Results: persistence

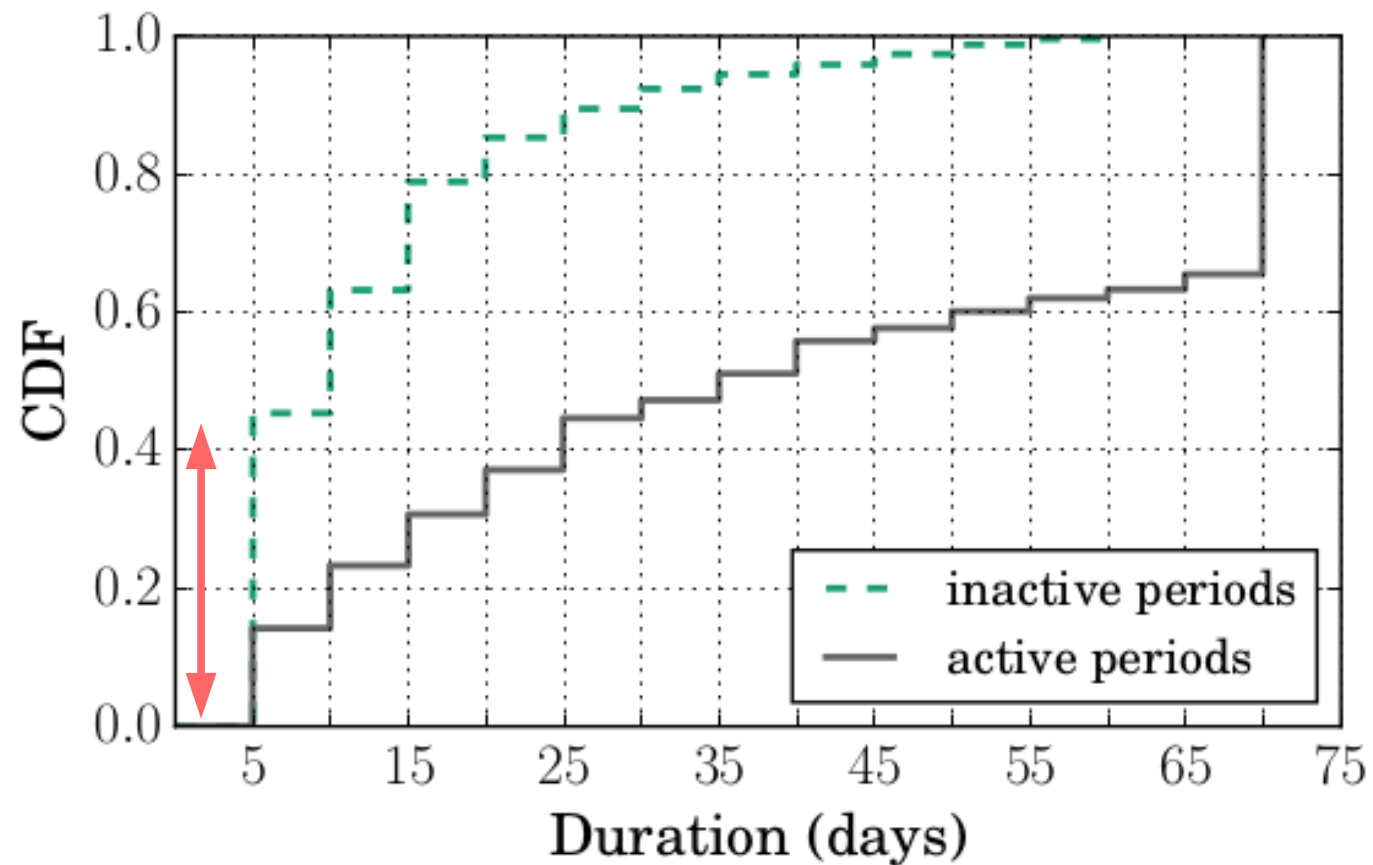


state durations (max 70 days)

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



Results: persistence

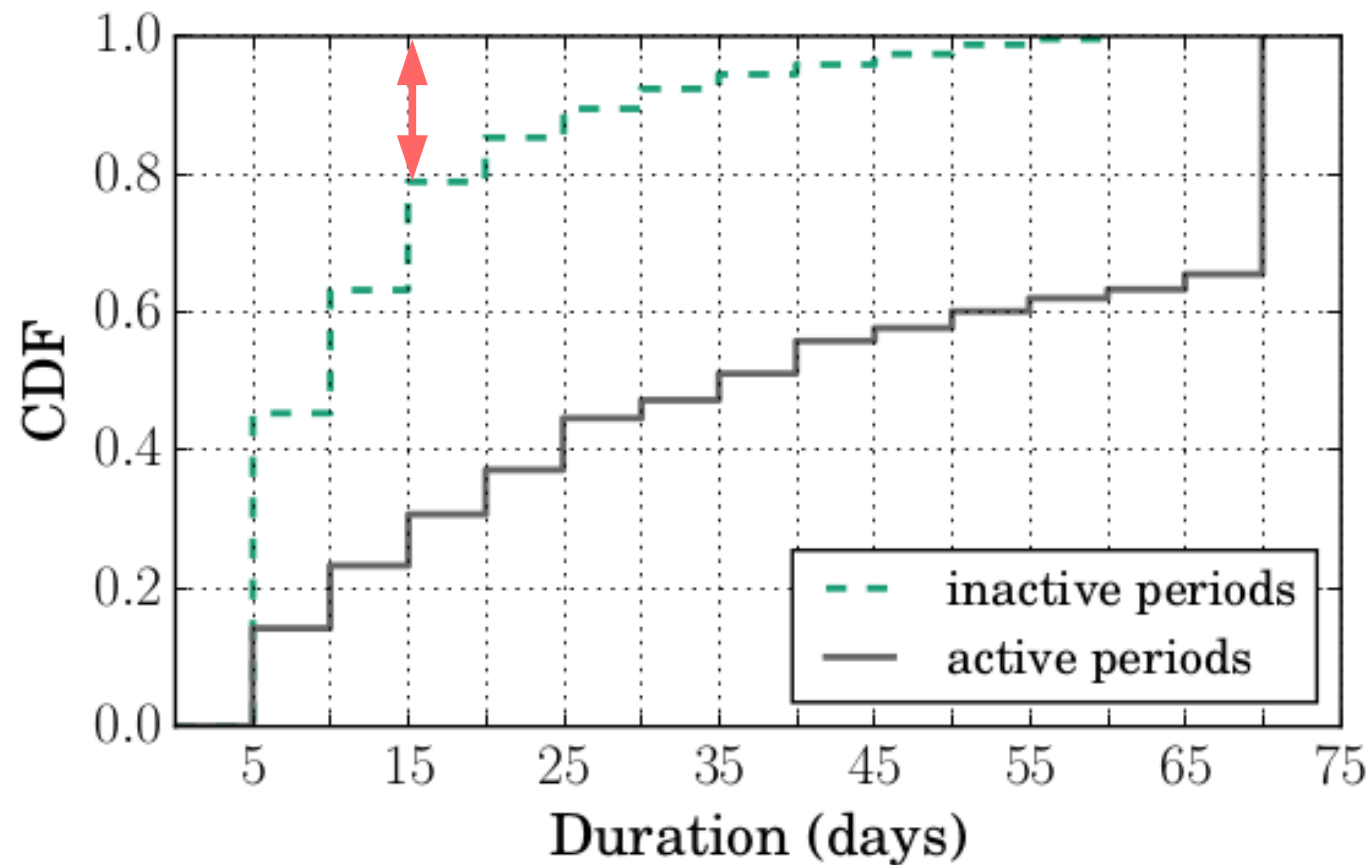


state durations (max 70 days)

- 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
- most MBs are deployed at AS borders
- MBs are relatively stable



Future works

- Investigate dynamicity
- NATs (MNM paper)
- 2-way tracebox-TCPExposure
- IPv6
- Mobile networks



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 ?



Comments ?