Leveraging interdomain stability for squeezed and juicy BGP dynamics

Authors

Thomas GREEN
(PhD Student)

Anthony LAMBERT
(PhD Advisor)

Dario ROSSI
(PhD Director)

Cristel PELSSER
(Researcher)

Research objectives

Context

- Border Gateway Protocol : path vector protocol
- Internet (Autonomous Systems) relationships based on trust
- Robustness/integrity is questionnable : more and more incidents, attacks

Goals (long term)

- Detection of abnormal routing events
- Mitigation

Challenges

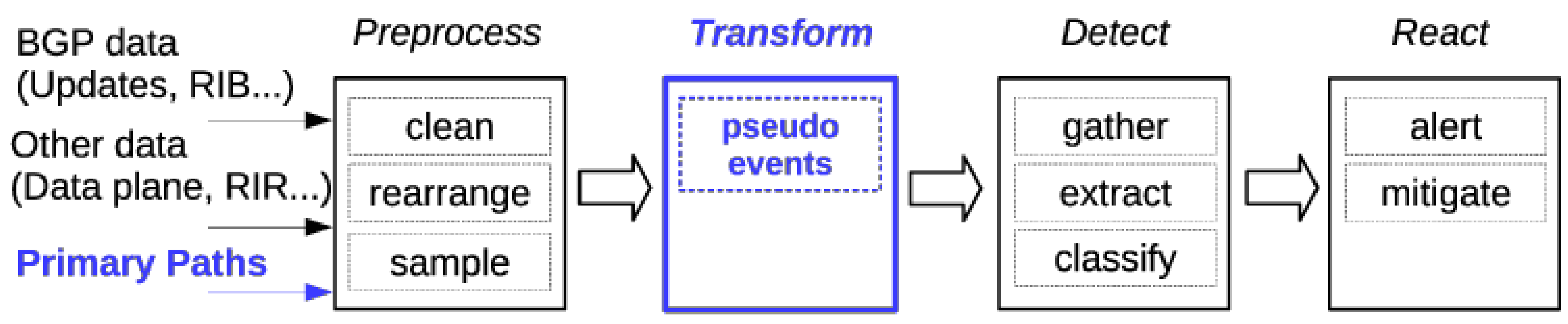
Complexity

- High verbosity and number of networks
- 'Path Selection' is made hop-by-hop
- Routing policies are not known

⇒ Opaque and complex environment

Requirements

- Online methodology
- Real-time detection and mitigation



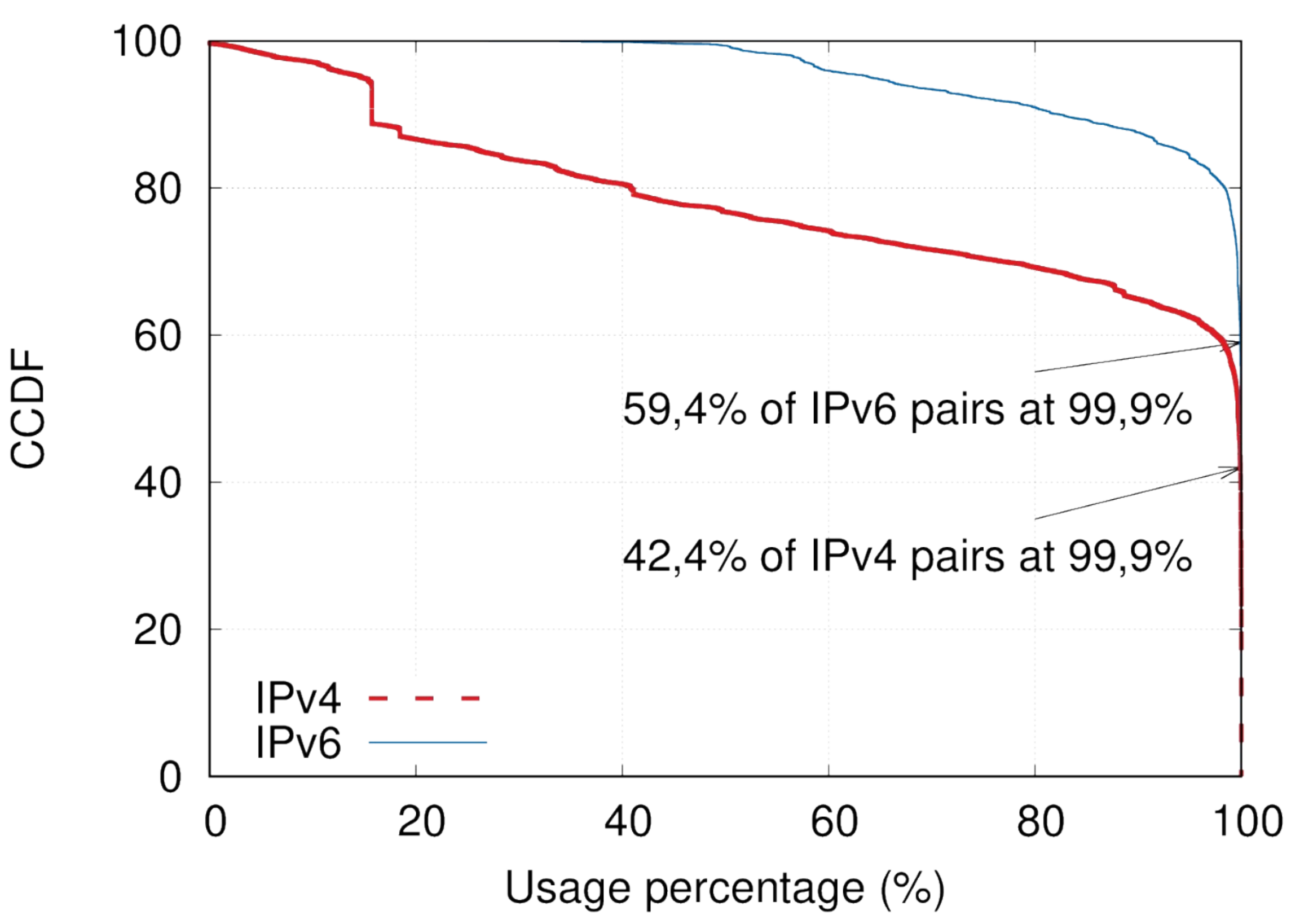
Synoptic of BGP dynamics analysis, novelty highlighted in blue

Approach

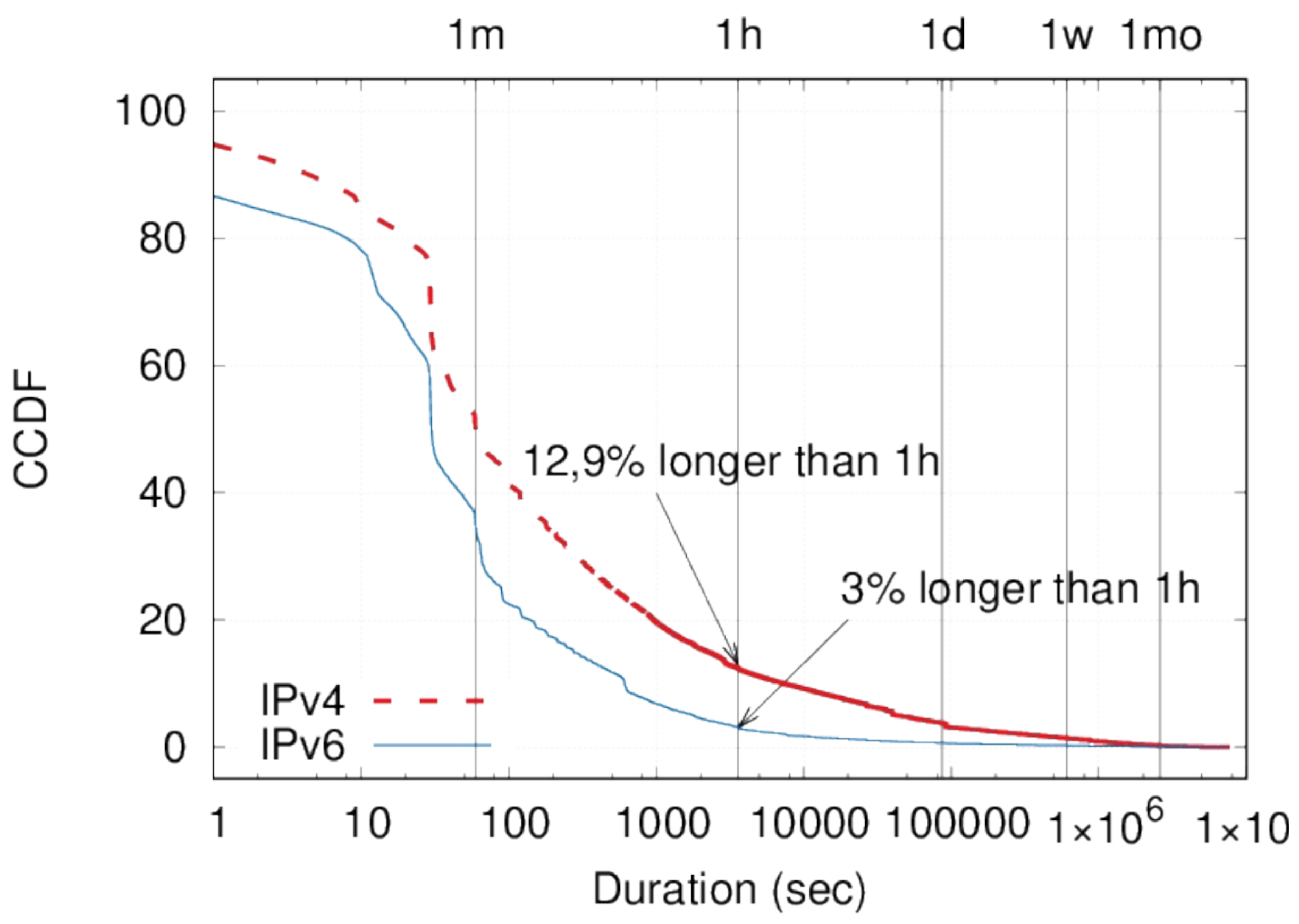
Leverage interdomain stability

- Construct a referential : « Primary Paths »
  - For each <router, prefix> pairs, one path is preferred (most used) for a given time-window
  - Updates are compared to this nominal value and interpreted as deviations (abnormal behavior) if they don't match

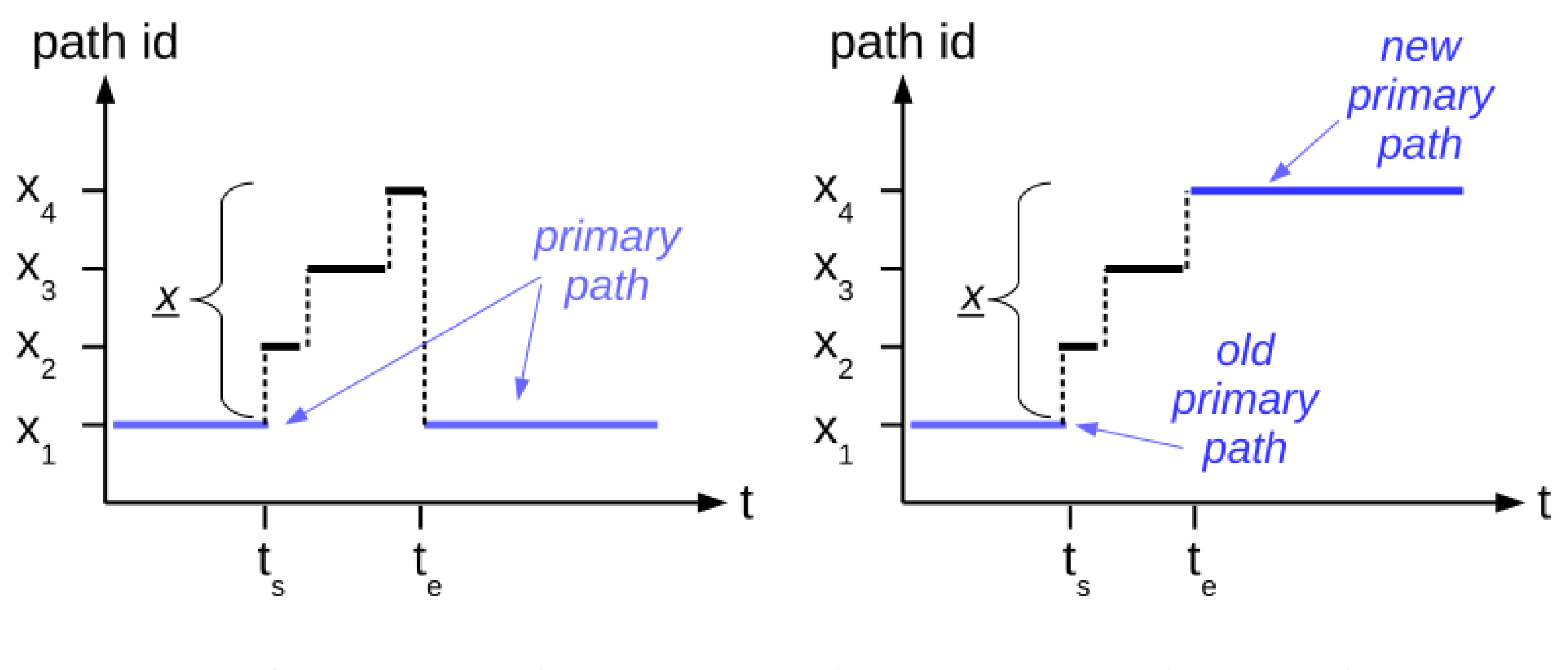
- Interpreted deviations : « Pseudo-events »
  - Primary path unavailabilities, defined by :
    - Starting time (fall of the PP) : t_s
    - End time (recovery of the PP) : t_e
    - Sequence of paths explored : $\underline{x}$
  - Two types :
    - Transient (spontaneous change)
    - Structural (planned change)



CCDF of primary path usage for all <router,prefix> pairs



CCDF of transient pseudo-events duration



(a) Transient pseudo-event (b) Structural pseudo-event

Illustration of pseudo-events

TMA 2017

- Squeezed : dimension reduction

	IPv4	IPv6
Number of events	487,104,558	157,249,182
Number of pseudo-events	57,066,053	17,687,525
Structural pseudo-events	1,406,392	78,995
Transient pseudo-events	55,659,661	17,608,530
Gain (events/pseudo-events)	8.5	8.9

Comparative table of dimension gain using pseudo-events

- Juicy : increased semantic

	Outages	
Reported	1716	
Observable	1622	
On-time detection	1355	(83.5%)
Early detection	236	(14.6%)
Undetected	31	(1.9%)

	Hijacks	
Reported	653	
Observable	306	
Confirmed	173	(56.5%)
Infirmed	133	(43.5%)
–Explicit legitimate	37	
–Implicit legitimate	96	

Comparative table of pseudo-events methodology vs BGPmon reports

June 2017

Data source: BGP raw data taken from RIPE RIS RRC01 collector from January 1st to March 31th 2017

Contact thomas.green@telecom-paristech.fr Site web