RoutingWatch

Visual Exploration and Analysis of Routing Events

Davide Ceneda
Marco Di Bartolomeo
Valentino Di Donato

Maurizio Patrignani
Maurizio Pizzonia
Massimo Rimondini
Visual Exploration and Analysis of Routing Events
Visual Exploration and Analysis of Routing Events
Visual Exploration and Analysis of Routing Events
Davide Ceneda
Marco Di Bartolomeo
Valentino Di Donato
Maurizio Patrignani
Maurizio Pizzonia
Massimo Rimondini

RoutingWatch

Visual Exploration and Analysis of Routing Events
Visual Exploration and Analysis of Routing Events
Visual Exploration and Analysis of Routing Events
Visual Exploration and Analysis of Routing Events
State of the Art

- Management & Monitoring Tools
- Inference Algorithms
- Visualization Systems
State of the Art

Management & Monitoring Tools

Inference Algorithms

Visualization Systems

Net Inspector
event manager applet interface_Shutdown
event syslog pattern "Interface FastEthernet1/0, changed state to administratively down"
action 1.0 cli command "enable"
action 1.5 cli command "config t"
action 2.0 cli command "interface fa1/0"
action 2.5 cli command "no shutdown"
action 3.0 cli command "end"
action 3.5 cli command "who"
action 4.0 mail server "192.168.1.1" to ".engineer@cisco.com." from ".EEM@cisco.com.
subject ".ISP1_Interface_fa1/0_SHUT." body "Current users $cli_result"
State of the Art

Management & Monitoring Tools

Inference Algorithms

Visualization Systems

Nagios® Monitoring System
State of the Art

Management & Monitoring Tools

Inference Algorithms

Visualization Systems

- Raise alarms based on unexpected changes in:
  - performance levels (bandwidth)
  - health flags (interface status)
  - configurations
State of the Art

- Raise alarms based on unexpected changes in:
  - performance levels (bandwidth)
  - health flags (interface status)
  - configurations

- Require polling and/or agents

- Must support many technologies
State of the Art

  - Online BGP route analysis to find and correlate events
  - Evolution of the Routing State Distance
  - Next-hop tensor factorization
State of the Art

  - Online BGP route analysis to find and correlate events
  - Evolution of the Routing State Distance
  - Next-hop tensor factorization

Focus on BGP
- Long-term Internet evolution studies
- Limited information about each event (typically, cause AS)
State of the Art

**Management & Monitoring Tools**

**Inference Algorithms**

**Visualization Systems**

  - Online BGP route analysis to find and correlate events

  - Evolution of the Routing State Distance
  - Future work envisions combined investigation of space and time, assessment of the type of routing change, event inference

  - Next-hop tensor factorization

**Focus on BGP**

- Limited information about each event (typically, cause AS)

- Long-term Internet evolution studies
State of the Art


  - Event inference

  - Event inference

Lots of inferred events
State of the Art


  - Event inference

- Lots of inferred events
State of the Art

Management & Monitoring Tools

Inference Algorithms

Visualization Systems

Teoh et al., 2003

BGPlay

Link rank

Radian/(TPlay)

ThousandEyes
RoutingWatch

- Visual exploration tool for a large number of routing events
RoutingWatch

- Visual exploration tool for a large number of routing events
- **Target users**: high-level administrators in a NOC, interested in highly informative aggregate reports
RoutingWatch

- Visual exploration tool for a large number of routing events
- **Target users**: high-level administrators in a NOC, interested in highly informative aggregate reports
- Does not require **agents** running on devices
RoutingWatch

- Visual exploration tool for a large number of routing events
- **Target users**: high-level administrators in a NOC, interested in highly informative aggregate reports
- Does not require **agents** running on devices
- (Partial) **visibility** of events in external networks
RoutingWatch

- Visual exploration tool for a large number of routing events
- **Target users**: high-level administrators in a NOC, interested in highly informative aggregate reports
- Does not require **agents** running on devices
- (Partial) **visibility** of events in external networks
Traceroutes ➔ Events
Traceroutes ➔ Events
Traceroutes ➔ Events
Traceroutes ➔ Events
Traceroutes ➔ Events

$ traceroute 193.0.14.129
traceroute to 193.0.14.129, 30 hops max, 60 byte packets
  1 193.204.161.1 (193.204.161.1) 3.277 ms
  3.282 ms  3.397 ms
...
$ traceroute 193.0.14.129
traceroute to
193.0.14.129, 30 hops max,
60 byte packets
  1  193.204.161.1
(193.204.161.1)  3.277 ms
  3.282 ms  3.397 ms
  ...

Traceroutes ➔ Events
Traceroutes ➔ Events

$ traceroute 193.0.14.129
traceroute to 193.0.14.129, 30 hops max, 60 byte packets
1 193.204.161.1
(193.204.161.1) 3.277 ms 3.282 ms 3.397 ms ...

Event
Traceroutes → Events

```
$ traceroute 193.0.14.129
traceroute to 193.0.14.129, 30 hops max,
60 byte packets
  1 193.204.161.1
(193.204.161.1) 3.277 ms
  3.282 ms  3.397 ms
...`
```
Traceroutes $\rightarrow$ Events

```
$ traceroute 193.0.14.129
traceroute to
193.0.14.129, 30 hops max,
60 byte packets
  1 193.204.161.1
 (193.204.161.1) 3.277 ms
  3.282 ms  3.397 ms
...```

Event
Traceroutes ➔ Events

$ traceroute 193.0.14.129
traceroute to
193.0.14.129, 30 hops max,
60 byte packets
1  193.204.161.1
(193.204.161.1)  3.277 ms
  3.282 ms  3.397 ms
...
Traceroutes ➔ Events

```bash
$ traceroute 193.0.14.129
traceroute to 193.0.14.129, 30 hops max, 60 byte packets
1 193.204.161.1 (193.204.161.1) 3.277 ms 3.282 ms 3.397 ms
...```
Traceroutes $\rightarrow$ Events

```
$ traceroute 193.0.14.129
traceroute to 193.0.14.129, 30 hops max, 60 byte packets
 1  193.204.161.1
   (193.204.161.1)  3.277 ms 3.282 ms 3.397 ms
...
```
$ traceroute 193.0.14.129
traceroute to 193.0.14.129, 30 hops max, 60 byte packets
 1  193.204.161.1 (193.204.161.1)  3.277 ms  3.282 ms  3.397 ms ...

Traceroutes ➔ Events
Traceroutes ➔ Events

$ traceroute 193.0.14.129
traceroute to
193.0.14.129, 30 hops max,
60 byte packets
1  193.204.161.1
(193.204.161.1)  3.277 ms
3.282 ms  3.397 ms
...
Traceroutes ➔ Events

$ traceroute 193.0.14.129
traceroute to 193.0.14.129, 30 hops max, 60 byte packets
1 193.204.161.1 (193.204.161.1)  3.277 ms 3.282 ms 3.397 ms
...
Traceroutes ➔ Events

```bash
$ traceroute 193.0.14.129
traceroute to 193.0.14.129, 30 hops max, 60 byte packets
1 193.204.161.1 (193.204.161.1) 3.277 ms 3.282 ms 3.397 ms ...
```
User interface
User interface

space-time view
User interface

space-time view

Display events that satisfy the following conditions:

Min impact

Impacted AS is:

Target is:

Cause AS is:

filtering panel
User interface

space-time view

similarity view

Display events that satisfy the following conditions:

Min impact

5 10 15 20

AND

Impacted AS is:

<None>

Target is:

<None>

Cause AS is:

<None>
User interface

Display events that satisfy the following conditions:

- Min impact
  - 5
  - 10
  - 15
  - 20
  - AND
  - Impacted as is: <None>
  - Target is: <None>
  - Cause as is: <None>

Compute similarity between events considering:

- Sets of probes
  - 0
  - 50
  - 100
- Time
  - 0
  - 50
  - 100
- Recurrence
  - None

Edge count cap (max: 35532)

Filtering panel

Similarity view

Space-time view
User interface

Display events that satisfy the following conditions:

Min impact:

5 10 15 20

AND

Impacted A3 is:

<None>

Target is:

<None>

Cause A3 is:

<None>

Compute similarity between events considering:

Edge count cap (max: 35532)

0 2000 4000

Sets of probes:

0 50 100

Sets of causes:

0 50 100

Time:

0 50 100

Recurrence:

None
space-time view
space-time view
space-time view
space-time view
space-time view
all probes are shown
all probes are shown
all probes are shown
all probes are shown
all probes are shown
Display events that satisfy the following conditions:

Min impact [5 10 15 20] AND

Impacted AS is: <None> ▼
Target is: <None> ▼
Cause AS is: <None> ▼
filtering panel

Display events that satisfy the following conditions:

Min impact

Impacted AS is: <None>
Target is: <None>
Cause AS is: <None>
Display events that satisfy the following conditions:

Min impact [slider]

Impacted AS is: <None> [dropdown]

Target is: <None> [dropdown]

Cause AS is: <None> [dropdown]
Display events that satisfy the following conditions:

Min impact

Impacted AS is: <None>

AND

Target is: <None>

Cause AS is: <None>
all probes are shown

Display events that satisfy the following conditions:

Min impact

Impacted AS is: <None> ▼
Target is: <None> ▼
Cause AS is: <None> ▼

filtering panel
VOLUME
TREBLE
MID
BASS

similarity view
Compute similarity between events considering:

- Sets of probes
- Sets of causes
- Time:
- Recurrence:
  - None

Edge count cap (max: 35532)
Display events that satisfy the following conditions:

- Min impact: 5, 10, 15, 20
- Impacted AS is: <None>
- Target is: <None>
- Cause AS is: <None>

Compute similarity between events considering:
- Sets of probes
- Time: 0, 50, 100
- Sets of causes
- Recurrence: None
coordinated views
continuous interaction
User study

- User sample: employees of the R&D of a prominent Italian ISP (experts in IP edge innovation, cybersecurity threats, video/multimedia platforms)
User study

- User sample: employees of the R&D of a prominent Italian ISP (experts in IP edge innovation, cyber-security threats, video/multimedia platforms)

- Questionnaire results:

  1  5
User study

- User sample: employees of the R&D of a prominent Italian ISP (experts in IP edge innovation, cybersecurity threats, video/multimedia platforms)

- Questionnaire results:
  
  ![Rating Scale]

  - events are a useful aggregation of routing dynamics
User study

- User sample: employees of the R&D of a prominent Italian ISP (experts in IP edge innovation, cybersecurity threats, video/multimedia platforms)

- Questionnaire results:

1. Events are a useful aggregation of routing dynamics
2. Comparing events by probes/geography/time is useful to find related events
User study

- User sample: employees of the R&D of a prominent Italian ISP (experts in IP edge innovation, cybersecurity threats, video/multimedia platforms)

- Questionnaire results:
  - 1 to 5
  - ▢ events are a useful aggregation of routing dynamics
  - ▢ comparing events by probes/geography/time is useful to find related events
  - ▢ the tool supports it effectively
User study

- User sample: employees of the R&D of a prominent Italian ISP (experts in IP edge innovation, cybersecurity threats, video/multimedia platforms)

- Questionnaire results:
  - 5: Events are a useful aggregation of routing dynamics
  - 5: Comparing events by probes/geography/time is useful to find related events
  - 5: The tool supports it effectively
  - 5: Finding related events is useful
User study

- User sample: employees of the R&D of a prominent Italian ISP (experts in IP edge innovation, cybersecurity threats, video/multimedia platforms)

- Questionnaire results:
  1. Events are a useful aggregation of routing dynamics
  2. Comparing events by probes/geography/time is useful to find related events
  3. The tool supports it effectively
  4. Finding related events is useful
  5. The tool supports it effectively
User study

- User sample: employees of the R&D of a prominent Italian ISP (experts in IP edge innovation, cyber-security threats, video/multimedia platforms)

- Questionnaire results:
  1. Events are a useful aggregation of routing dynamics
  2. Comparing events by probes/geography/time is useful to find related events
  3. The tool supports it effectively
  4. Finding related events is useful
  5. The tool supports it effectively

Filters
User study

- User sample: employees of the R&D of a prominent Italian ISP (experts in IP edge innovation, cybersecurity threats, video/multimedia platforms)

- Questionnaire results:

1. Events are a useful aggregation of routing dynamics
2. Comparing events by probes/geography/time is useful to find related events
3. The tool supports it effectively
4. Finding related events is useful
5. The tool supports it effectively

Filters

Event patterns
User study

- User sample: employees of the R&D of a prominent Italian ISP (experts in IP edge innovation, cybersecurity threats, video/multimedia platforms)

- Questionnaire results:
  - 1 events are a useful aggregation of routing dynamics
  - 2 comparing events by probes/geography/time is useful to find related events
  - 5 the tool supports it effectively
  - 4 finding related events is useful
  - 3 the tool supports it effectively

Filters

“A tool for mining traceroutes”
Future Work
Future Work

- Scalability of the user interface (e.g., clustering leaders)
Future Work

- Scalability of the user interface (e.g., clustering leaders)
- Other notions of similarity (e.g., geography-based)
Future Work

- Scalability of the user interface (e.g., clustering leaders)
- Other notions of similarity (e.g., geography-based)
- Real-time analysis (streaming data analytics)
Future Work

- Scalability of the user interface (e.g., clustering leaders)
- Other notions of similarity (e.g., geography-based)
- Real-time analysis (streaming data analytics)
- Exploration session (to build a knowledge base)