BGP Link Reputation Evaluator

An Algorithm based tool to identify legitimate or malicious/hijack BGP link

Alfred Arouna¹  Lionel Metongnon²  Pr. Marc Lobelle³

¹²Université d’Abomey-Calavi,²³Université Catholique de Louvain
¹alfred@arouna.net,²lionel.metongnon@uclouvain.be,³marc.lobelle@uclouvain.be

AfPIF 2017 - 22,23,24 August 2017 - Abidjan, Côte D’Ivoire
Disclaimer

- Ongoing study...
- Community input to improve current result.
- Code not yet ready for production (alpha release).
- Code available at: https://bitbucket.org/alfredarouna/bgplink
1. Base Idea

2. Tools

3. Our proposal

4. Hypothesis & verification

5. Malaysia Telecom test cases results

6. Other tests cases results

7. Improvement (proposals)
Base Idea
**LINKRANK-1**

Develop your own Link-Rank algorithm

**Background:** ASPATHs can be viewed as lists of nodes in a graph: each AS is a node in the graph, whereas ASPATH adjacencies represent links between nodes. Each link can be associated with a weight that is representative of how many AS paths traverse such link. One method for calculating a link “rank” could be weighted standard deviation over a chosen time period of the previous weight, however it would be important to have a metric/weight which is independent of the number of collectors up at a given time.

**Motivation:** Route-leaks and route-hijacks are often detected utilizing ASPATH change detection. When one of these events happens, new links may appear (e.g. backup links that are now visible because of a different outcome of the BGP decision process), or the preferred routes may start using links that were rather unused before. A Link-Rank algorithm can be used to do baseline leak/hijack detection.

**Goals:** Develop your own per-AS Link-Rank algorithm. Use this algorithm on a test case to process data of a known route-leak time period. Experiment with different time periods to determine best performance.

**Tasks:**

- Define a link weight that takes into account visibility changes
- Run this algorithm on a test case (e.g. Malaysia Telekom leak)
Linkrank Challenge from CAIDA BGP Hackathon

**Linkrank-1**

Develop your own LinkRank algorithm.

**Background:** AS PATHs can be viewed as lists of nodes in a graph; each AS is a node in the graph, whereas AS PATH adjacencies represent links between nodes. Each link can be associated.

**Goals:** develop your own per-AS Link-Rank algorithm. Use this algorithm on a test-case to process data of a known route-leak time period. Experiment with different time periods to determine best performance.

**Tasks:**

- define a link weight that takes into account visibility changes
- run this algorithm on a test case (e.g. Malaysia Telekom leak)

---

1 https://github.com/CAIDA/bgp-hackathon/wiki/List-of-Challenges#linkrank-1
Tools
Tools available and missing components

Tools available:

2https://bgpstream.caida.org/
3https://bgplayjs.com/?section=bgplay
4https://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt
Tools available and missing components

Tools available:

- **BGPStream**\(^2\) (from CAIDA) framework to easily collect BGP records.

---

\(^2\)https://bgpstream.caida.org/
\(^3\)https://bgplayjs.com/?section=bgplay
\(^4\)https://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt
Tools available and missing components

Tools available:

• **BGPStream**\(^2\) (from CAIDA) framework to easily collect BGP records.
• **BGPlayJs**\(^3\) (from RIPE NCC) as user-friendly view and event animation.

\(^2\)https://bgpstream.caida.org/
\(^3\)https://bgplayjs.com/?section=bgplay
\(^4\)https://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt
Tools available and missing components

Tools available:

- **BGPStream**\(^2\) (from CAIDA) framework to easily collect BGP records.
- **BGPlayJs**\(^3\) (from RIPE NCC) as user-friendly view and event animation.
- Updated list of bogon freely available\(^4\) (Team Cymru).

\(^2\)https://bgpstream.caida.org/
\(^3\)https://bgplayjs.com/?section=bgplay
\(^4\)https://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt
Tools available and missing components

Tools available:

- **BGPStream**$^2$ (from CAIDA) framework to easily collect BGP records.
- **BGPlayJs**$^3$ (from RIPE NCC) as user-friendly view and event animation.
- Updated list of bogon freely available$^4$ (Team Cymru).

Missing components:

---

2 https://bgpstream.caida.org/
3 https://bgplayjs.com/?section=bgplay
4 https://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt
Tools available and missing components

Tools available:

- **BGPStream**\(^2\) (from CAIDA) framework to easily collect BGP records.
- **BGPlayJs**\(^3\) (from RIPE NCC) as user-friendly view and event animation.
- Updated list of bogon freely available\(^4\) (Team Cymru).

Missing components:

*An acceptable algorithm for link reputation evaluation.*

---

\(^2\)https://bgpstream.caida.org/
\(^3\)https://bgplayjs.com/?section=bgplay
\(^4\)https://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt
Tools available and missing components

Tools available:

- **BGPStream**\(^2\) (from CAIDA) framework to easily collect BGP records.
- **BGPlayJs**\(^3\) (from RIPE NCC) as user-friendly view and event animation.
- Updated list of bogon freely available\(^4\) (Team Cymru).

Missing components:

*An acceptable **algorithm** for link **reputation** evaluation.*

\(^2\)https://bgpstream.caida.org/

\(^3\)https://bgplayjs.com/?section=bgplay

\(^4\)https://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt
algorithm

noun

Word used by programmers when they do not want to explain what they did.
algorithm

noun

Word used by programmers when they do not want to explain what they did.
Our proposal
Before going further, what do we have:
Our proposal

Before going further, what do we have:

- Test case: Telekom Malaysia leak.
- Metric: link weight.
Our proposal

Before going further, what do we have:

• Test case: Telekom Malaysia leak.

• Metric: link weight.

Will be interesting to have:
Our proposal

Before going further, what do we have:

- Test case: Telekom Malaysia leak.
- Metric: link weight.

Will be interesting to have:

- New metrics: link bogon degree and link stability.
Our proposal

Before going further, what do we have:

- Test case: Telekom Malaysia leak.
- Metric: link weight.

Will be interesting to have:

- New metrics: link bogon degree and link stability.
- Rename: link weight to link rank.
Before going further, what do we have:

- Test case: Telekom Malaysia leak.
- Metric: link weight.

Will be interesting to have:

- New metrics: link bogon degree and link stability.
- Rename: link weight to link rank.
- New Objective:
Before going further, what do we have:

- Test case: Telekom Malaysia leak.
- Metric: link weight.

Will be interesting to have:

- New metrics: link bogon degree and link stability.
- Rename: link weight to link rank.
- New Objective:
  - Algorithm to easily identify link with good/bad reputation.
  - Graphical view with intuitive color code: green to red.
Hypothesis & verification
Our approach (1/2)

Hypothesis

• does not carry bogon,
• have positive stability,
• are used by many AS.
Our approach (1/2)

Hypothesis

Links with *good reputation*:
Our approach (1/2)

Hypothesis
Links with *good reputation*:

- does not carry bogon,
- have positive stability,
- are used by many AS.
Our approach (1/2)

Hypothesis
Links with *good reputation*:

- does not carry bogon,
- have positive stability,
- are used by many AS.

Verification (1/2)
Hypothesis
Links with *good reputation*:

- does not carry bogon,
- have positive stability,
- are used by many AS.

Verification (1/2)
Developed an algorithm based on the hypothesis metrics:
Our approach (1/2)

Hypothesis
Links with *good reputation*:

- does not carry bogon,
- have positive stability,
- are used by many AS.

Verification (1/2)
Developed an algorithm based on the hypothesis metrics:

- bogon degree - $bogons_t(\langle A, B \rangle)$,
- link stability - $stability_t(\langle A, B \rangle)$,
- link rank - $rank_t(\langle A, B \rangle)$. 
Our algorithm...
Our approach (2/2)

Verification (2/2)

• Draw each link instead of AS_PATH.
• Use specific color (from green to red) based on link reputation.
• Routes leak with Telekom Malaysia. ⁵
• Censorship with Youtube hijack by Pakistan Telecom. ⁶
• Malicious activities with Link Telecom incident. ⁷

⁵https://bgpmon.net/massive-route-leak-cause-internet-slowdown/
Our approach (2/2)

Verification (2/2)
Modified BGPlayJS to:

5https://bgpmon.net/massive-route-leak-cause-internet-slowdown/
Our approach (2/2)

Verification (2/2)

Modified BGPlayJS to:

- Draw each link instead of AS_PATH.
- Use specific color (from green to red) based on link reputation cost.

---

5 https://bgpmon.net/massive-route-leak-cause-internet-slowdown/
Our approach (2/2)

Verification (2/2)
Modified BGPlayJS to:

- Draw each link instead of AS_PATH.
- Use specific color (from green to red) based on link reputation cost.

Tested on three cases:

---

Our approach (2/2)

Verification (2/2)

Modified BGPlayJS to:

• Draw each link instead of AS_PATH.
• Use specific color (from green to red) based on link reputation cost.

Tested on three cases:

• Routes leak with Telekom Malaysia ⁵.
• Censorship with Youtube hijack by Pakistan Telecom ⁶.
• Malicious activities with Link Telecom incident ⁷.

---

⁵ https://bgpmon.net/massive-route-leak-cause-internet-slowdown/
Three phases (1/3)

Prefixes

Time interval

Collectors

Filters

Data Collection

BGPStream
Three phases (2/3)

Prefixes

0

Time interval

Collectors

1

Data Collection

Filters

BGP Stream

BGP Links

2

Analysis

Rep Algo
Three phases (3/3)

Prefixes

0

Time interval

Collectors

Filters

1

Data Collection

BGPStream

BGP Links

2

Analysis

Rep Algo

Json file

3

Visualization

BGPlayJs
Malaysia Telecom test cases results
Test: Leak case (Telekom Malaysia)
Test: Leak case (Telekom Malaysia)
Test: Control case (Telekom Malaysia)
Test: Control case (Telekom Malaysia)
Leak and Control cases (Telekom Malaysia)
Leak and Control cases (Telekom Malaysia)

Figure 1: Leak case reputation
Figure 1: Leak case reputation

- 08:43 to 10:45 UTC.
Figure 1: Leak case reputation

- 08:43 to 10:45 UTC.
- Most links have bad reputation.
Leak and Control cases (Telekom Malaysia)

Figure 1: Leak case reputation

- 08:43 to 10:45 UTC.
- Most links have bad reputation.

Figure 2: Control case reputation
Leak and Control cases (Telekom Malaysia)

Figure 1: Leak case reputation
- 08:43 to 10:45 UTC.
- Most links have bad reputation.

Figure 2: Control case reputation
- 12:45 to 14:45 UTC.
Leak and Control cases (Telekom Malaysia)

Figure 1: Leak case reputation
- 08:43 to 10:45 UTC.
- Most links have *bad* reputation.

Figure 2: Control case reputation
- 12:45 to 14:45 UTC.
- Mix of *good* and *bad* reputation.
Other tests cases results
Censorship test case (YouTube Hijack)
Censorship test case (YouTube Hijack)

Figure 3: Hijack case reputation
Censorship test case (YouTube Hijack)

Figure 3: Hijack case reputation

- 19:00 to 20:51 UTC.
Figure 3: Hijack case reputation

- 19:00 to 20:51 UTC.
- Youtube links have bad reputation.
Censorship test case (YouTube Hijack)

Figure 3: Hijack case reputation

- 19:00 to 20:51 UTC.
- Youtube links have *bad reputation*.

Figure 4: Control case reputation
Censorship test case (YouTube Hijack)

Figure 3: Hijack case reputation

- 19:00 to 20:51 UTC.
- Youtube links have bad reputation.

Figure 4: Control case reputation

- 21:05 to 22:56 UTC.
Censorship test case (YouTube Hijack)

Figure 3: Hijack case reputation

- 19:00 to 20:51 UTC.
- Youtube links have **bad reputation**.

Figure 4: Control case reputation

- 21:05 to 22:56 UTC.
- Mix of **good reputation** and **bad reputation**.
Malicious activities test case (Link Telecom Hijack)
Figure 5: Leak case reputation
Malicious activities test case (Link Telecom Hijack)

Figure 5: Leak case reputation

- 08:00 to 10:00 UTC (August 24, 2011).
Malicious activities test case (Link Telecom Hijack)

Figure 5: Leak case reputation

- 08:00 to 10:00 UTC (August 24, 2011).
- Most links have *bad reputation*. 
Malicious activities test case (Link Telecom Hijack)

Figure 5: Leak case reputation

- 08:00 to 10:00 UTC (August 24, 2011).
- Most links have bad reputation.

Figure 6: Control case reputation
Malicious activities test case (Link Telecom Hijack)

**Figure 5:** Leak case reputation

- 08:00 to 10:00 UTC (August 24, 2011).
- Most links have *bad* reputation.

**Figure 6:** Control case reputation

- 08:00 to 10:00 UTC (September 9, 2011).
Malicious activities test case (Link Telecom Hijack)

Figure 5: Leak case reputation

- 08:00 to 10:00 UTC (August 24, 2011).
- Most links have bad reputation.

Figure 6: Control case reputation

- 08:00 to 10:00 UTC (September 9, 2011).
- No event.
Improvement (proposals)
Improvement (proposals)
Improvement (proposals)

• Better view
Improvement (proposals)

- Better view
  - [Problem] Unclear view with BGPlayJS.
Improvement (proposals)

• Better view
  • [Problem] Unclear view with BGPlayJS.
  • [Proposal] Draw One line between links (using netJSON ?).
Improvement (proposals)

- Better view
  - [Problem] Unclear view with BGPlayJS.
  - [Proposal] Draw **One** line between links (using netJSON ?).
- Inputs flexibility
Improvement (proposals)

• Better view
  • [Problem] Unclear view with BGPlayJS.
  • [Proposal] Draw One line between links (using netJSON ?).

• Inputs flexibility
  • [Problem] Collectors and time interval are hard coded.
  •
Improvement (proposals)

• Better view
  • [Problem] Unclear view with BGPlayJS.
  • [Proposal] Draw **One** line between links (using netJSON ?).

• Inputs flexibility
  • [Problem] Collectors and time interval are hard coded.
  • [Proposal] Allow user to select collectors and time interval for analysis.
Improvement (proposals)

• Better view
  • [Problem] Unclear view with BGPlayJS.
  • [Proposal] Draw **One** line between links (using netJSON ?).

• Inputs flexibility
  • [Problem] Collectors and time interval are hard coded.
  • [Proposal] Allow user to select collectors and time interval for analysis.

• More testing
Improvement (proposals)

• Better view
  • [Problem] Unclear view with BGPlayJS.
  • [Proposal] Draw **One** line between links (using netJSON ?).

• Inputs flexibility
  • [Problem] Collectors and time interval are hard coded.
  • [Proposal] Allow user to select collectors and time interval for analysis.

• More testing
  •
  •
Improvement (proposals)

• Better view
  • [Problem] Unclear view with BGPlayJS.
  • [Proposal] Draw One line between links (using netJSON ?).

• Inputs flexibility
  • [Problem] Collectors and time interval are hard coded.
  • [Proposal] Allow user to select collectors and time interval for analysis.

• More testing
  • [Problem] Only three test cases.
Improvement (proposals)

- Better view
  - [Problem] Unclear view with BGPlayJS.
  - [Proposal] Draw One line between links (using netJSON ?).

- Inputs flexibility
  - [Problem] Collectors and time interval are hard coded.
  - [Proposal] Allow user to select collectors and time interval for analysis.

- More testing
  - [Problem] Only three test cases.
  - [Proposal] Add more (well-known) BGP incidents.
### Improvement (proposals)

- **Better view**
  - [Problem] Unclear view with BGPlayJS.
  - [Proposal] Draw **One** line between links (using netJSON ?).

- **Inputs flexibility**
  - [Problem] Collectors and time interval are hard coded.
  - [Proposal] Allow user to select collectors and time interval for analysis.

- **More testing**
  - [Problem] Only three test cases.
  - [Proposal] Add more (well-known) BGP incidents.

- **Large scale algorithm**
Improvement (proposals)

• Better view
  • [Problem] Unclear view with BGPlayJS.
  • [Proposal] Draw One line between links (using netJSON ?).

• Inputs flexibility
  • [Problem] Collectors and time interval are hard coded.
  • [Proposal] Allow user to select collectors and time interval for analysis.

• More testing
  • [Problem] Only three test cases.
  • [Proposal] Add more (well-known) BGP incidents.

• Large scale algorithm
  • 
  •
Improvement (proposals)

• Better view
  • [Problem] Unclear view with BGPlayJS.
  • [Proposal] Draw One line between links (using netJSON ?).

• Inputs flexibility
  • [Problem] Collectors and time interval are hard coded.
  • [Proposal] Allow user to select collectors and time interval for analysis.

• More testing
  • [Problem] Only three test cases.
  • [Proposal] Add more (well-known) BGP incidents.

• Large scale algorithm
  • [Problem] BGP is large scale protocol vs limited resources.
Improvement (proposals)

• Better view
  • [Problem] Unclear view with BGPlayJS.
  • [Proposal] Draw **One** line between links (using netJSON ?).

• Inputs flexibility
  • [Problem] Collectors and time interval are hard coded.
  • [Proposal] Allow user to select collectors and time interval for analysis.

• More testing
  • [Problem] Only three test cases.
  • [Proposal] Add more (well-known) BGP incidents.

• Large scale algorithm
  • [Problem] BGP is large scale protocol vs limited resources.
  • [Proposal] Use Massive Data/AI tools for link classification.
Thanks
Thanks
Corrections / updates / comments would be appreciated