“SASUKE” Traffic Monitoring Tool
Traffic Shift Monitoring Based on Correlation between BGP Messages and Flow Data

Atsushi Kobayashi
Yutaka Hirokawa
Hiroshi Kurakami

NTT Information Sharing Laboratories
Outline

- Introduction
  - Background
  - Motivation
  - Challenge

- System Architecture
  - BGP Collection
  - Flow Collection
  - Visualization

- Traffic Change Detection Method

- Conclusion
Background

- Announcement of unwanted or invalid BGP route suddenly leads to traffic diversions.
  - Cutting of submarine cable, route hijacking, misconfiguration, ...

- Moreover, it disrupts traffic or causes congestion on other backbone links.
Motivation

- Our goal is to reduce the load for troubleshooting.
- Our tool detects a traffic change and then identifies BGP route announcements involved.
  - Monitors traffic volume for BGP attributes that have an impact on the traffic change:
    - Origin ASN
    - Neighbor ASN (peer ASN)
    - AS Path
    - BGP Next Hop
    - Community.
  - Identifies route changes that have an impact on the traffic change.
Related Work

- **Flow records from border routers can be utilized for origin or neighbor ASN traffic analysis.**
  - However, border gateway router cannot export both origin and neighbor ASNs.
  - Difficult to collect BGP Next Hop and AS Path info.

- **Some commercial collectors with BGP sessions can sum up traffic on the basis of BGP attributes.**
  - There are few tools for analyzing the interrelation of BGP and Flow data.

- **BGP and Flow analysis system have been proposed by several groups**¹).
  - Simpler method and its visualization are required.

The challenge is to identify route changes from a huge number of BGP route announcements.
- Hundreds of thousands of route announcements per day

Handle the huge load of flow records.
- Thousands of flow records per second

Explore a simple detection method and its real-time visualization.
Data Source

- Captures BGP data from BGP sessions to border routers or route reflectors as a BGP route reflector client.
  - Border router feeds best routes to SASUKE tool.

- Sets NetFlow/sFlow observation points at the periphery of the target AS.
System Architecture

- **3 system components:**
  - BGP Collection
  - Flow Collection
  - Data Analysis: correlation between BGP and Flow data

![Diagram]

- BGP Collection
- Flow Collection
- Data Analysis: correlation between BGP and Flow data

- **BGP Collection**
- **Flow Collection**
- **Data Analysis**
  - Labeled BGP logs
  - Patricia trie (BGP routing table)
  - Traffic volume for BGP attributes

- **Web console**
- **Report visualization**
BGP Collection

- Builds BGP routing tables as Patricia trie.
  - Maintains tables for each BGP peering session.
- Creates a BGP log report $B$ to identify BGP messages that may cause a traffic change by comparing against the Patricia trie.
  - Identifies BGP message type and BGP attributes that have changed from the old ones in the Patricia trie.

**Example Log Report $B$**

- **NLRI**: 10.10.0.0/16
- **AS Path**: 4697-2914-2511
- **BGP NH**: 192.168.1.1

**Updated Log Report $B$**

- **NLRI**: 10.10.10.0/24
- **AS Path**: 4697-2914-2511
- **BGP NH**: 192.168.1.1

**Updated Patricia Trie**

- **NLRI**: 10.10.10.0/24
- **AS Path**: 4697-2914-2511
- **BGP NH**: 192.168.1.1
BGP Log Reports

- BGP log report is represented as follows.

\[ B = \{ t, c_{\text{type}}, a_{\text{type}}, a_{\text{new}}, a_{\text{old}}, \text{prefix}, \text{id} \} \]

- \( t \) is timestamp of when the BGP message arrived.
- \( c_{\text{type}} \) is change type:
  - “New”, “Withdraw”, “Change”, or “Duplicate”.
- \( a_{\text{type}} \) indicates the changed BGP attribute type:
  - “Origin ASN”, “Neighbor ASN”, “AS Path”, “BGP NH”, or “Community”
    - BGP community often gives route categories: region, peering type.
- \( a_{\text{new}}/a_{\text{old}} \) are new/old BGP attribute values.
  - When \( c_{\text{type}} \) is “New” or “Withdraw”, \( a_{\text{old}} \) or \( a_{\text{new}} \) is a “null” value.
- \( \text{Prefix} \) is network address in NLRI.
- \( \text{Id} \) is an identifier to correlate with traffic data.
  - At this stage, the value is “null”.

- BGP community often gives route categories: region, peering type.
BGP Log Reports

- Creates multiple BGP log reports when multiple BGP attributes are changed.

**Labeled BGP log report B**

- $B_1 = \{t, \text{PeerAS}(P), 4697, 7321, "10.0.0.0/8"\}$
- $B_2 = \{t, \text{BGP-NH}(B), 192.168.1.1, 192.168.1.100, "10.0.0.0/8"\}$

**Patricia trie (BGP routing table)**

- NLRI = 10.0.0/8,
  - AS Path = 4697-2914-2511
  - BGP NH = 192.168.1.1

- NLRI = 10.0.0/8,
  - AS Path = 7321-2914-2511
  - BGP NH = 192.168.1.100
Visualization for BGP Log Reports

- Labeled BGP logs are presented in time-series.
  - Top-N origin/neighbor ASNs involved in the most BGP messages are represented when the spike happens.
Flow Collection

- Selects an appropriate Patricia trie.
  - Compares the Flow Record and peering data.
    - Are Exporter and BGP router the same device or not?
    - Are Exporter and BGP router located in the same region or not?

- Sums up traffic on the basis of BGP attributes:
  - Origin ASN, Neighbor ASN, AS Path, BGP NH, Community, and Prefix
  - These BGP attributes are retrieved from the Patricia trie by a longest match based on source/destination IP addresses.
Drill down into the detailed traffic data step by step from stacked area chart.
Traffic Change Detection Method

- Focuses on a Top-$N$ ranked by traffic volume on BGP attributes:
  - Origin ASN, Neighbor ASN, AS Path, BGP NH, and Community.
- Evaluates similarities of Top-$N$ ranks between time slot $t$ and $t-1$.
  - Traffic volume weights the evaluation results.

![Traffic Volume Graph](image-url)
Traffic Change Detection Method

- Calculates the correlation coefficient $r(t,t-1)$ between the ranks of time slots $t$ and $t-1$.

$$r(t,t-1) = \frac{\sum_{i=1}^{N} (c(f(i,t), t) - c_{avg}(t))(c(f(i,t), t-1) - c_{avg}(t-1))}{\sqrt{\sum_{i=1}^{N} (c(f(i,t), t) - c_{avg}(t))^2} \sqrt{\sum_{i=1}^{N} (c(f(i,t), t-1) - c_{avg}(t-1))^2}}$$

- $f(i,t)$ is defined as a BGP attribute value ranked $i$ by traffic volume of time slot $t$.
- $c(f(i,t), t)$ is traffic volume of $f(i,t)$.
- Top-$N$ statistics data set $C(t)_i$ is presented as an array:
  - $C(t)_i = \{c(f(1,t), t), c(f(2,t), t), \ldots, c(f(N,t), t) \}$ ($i=1, 2, 3, \ldots, N$)
- $C_{avg}(t)$ gives the average of $C(t)_i$.

- Evaluates whether $r(t,t-1)$ exceeds a threshold.
Identify Most Affected Traffic

- Investigates which $f(i,k)$ has the greatest impact on traffic change, as follows.
  - Top-$N$ rank $C(k)(t)_i$ indicates $C(t)_i$ except for $c(f(k,t),t)$ ranked $k$.
  $$C(k)(t)_i = \{ c(f(1,t),t), \ldots, c(f(k-1,t),t), c(f(k+1,t),t), \ldots, c(f(N,t),t) \}$$
  - Calculates the correlation coefficient $r(k)(t,t-1)$.
  - Selects the greatest values $r(k)(t,t-1)$ from
    $$\{ r(1)(t,t-1), r(2)(t,t-1), \ldots, r(N)(t,t-1) \}.$$  

- Then, we recognize that $f(k,t)$ is the most affected BGP attribute.
Finally, it creates a traffic change report $R$.

$R=\{t, \text{type}, f(i,k), r(t,t-1), \delta, id\}$

- **type** gives traffic volume type:
  - “Origin ASN”, “Neighbor ASN”, “AS Path”, “BGP NH”, or “Community”

- **$\delta$** gives the traffic volume difference between $t$ and $t-1$.

- **$id$** is an identifier to correlate with BGP log reports.
  - At this stage, the value is set to a unique value.
Correlation between BGP and Flow

- Correlates between BGP log report $B$ and traffic change report $R$.
  - Looks for the BGP log report $B$ involved with traffic change report $R$.
  - Then, $R$ and $B$ are given the same $id$ value to link them.

$$R = \{ t, \text{type}, f(i,k), r(t,t-1), \delta, id \}$$
$$B = \{ t, c_{type}, a_{type}, a_{new}, a_{old}, \text{prefix}, id \}$$

for all BGP log reports $B$ where $t-Tw < B.t < t+Tw$ do

- if $R.\delta > 0$ and $B.a_{type} = R.type$ and $B.a_{new} = R.f(i,k)$ then
  - $B.id = R.id$;
- else if $R.\delta < 0$ and $B.a_{type} = R.type$ and $B.a_{old} = R.f(i,k)$ then
  - $B.id = R.id$;
- end if

end for
Visualization for BGP and Flow

- Creates traffic-change-related alert for operators.
  - Alert links the graphs of traffic volume area chart and of BGP log reports involved.

Alert information

- Number of prefixes
- BGP log reports involved

Incoming traffic

Outgoing traffic
Overall Traffic View

**Incoming Traffic**

- Traffic (bps)
- Time (JST)
- Prefixes (stack=OriginAS)

**Outgoing Traffic**

- Traffic (bps)
- Time (JST)
- Prefixes (stack=OriginAS)

**Number of Prefix**

- Prefixes
- Time (JST)

**BGP log reports**

- Messages
- Time (JST)
- Prefixes (stack=Messages)
“SASUKE” has been introduced in some commercial networks as an experimental phase.

Much more performance evaluation is needed.
Conclusion

- I demonstrated the traffic change detection method implemented in the “SASUKE” tool.
  - Focuses on the similarities between time consecutive Top-N ranks in time-series.
  - Correlates between BGP log reports B and traffic change reports R.
  - Alleviates the troubleshooting load for network operators.
    - Visualizes BGP log and traffic data.
    - Links multidimensional traffic data related to BGP attributes.

- More evaluation is needed for performance and accuracy.
Thank you very much.

This study was supported by the Ministry of Internal Affairs and Communications of Japan.