Outsourcing Mitigation against BGP Prefix Hijacking

Man ZENG
zengman@bupt.edu.cn

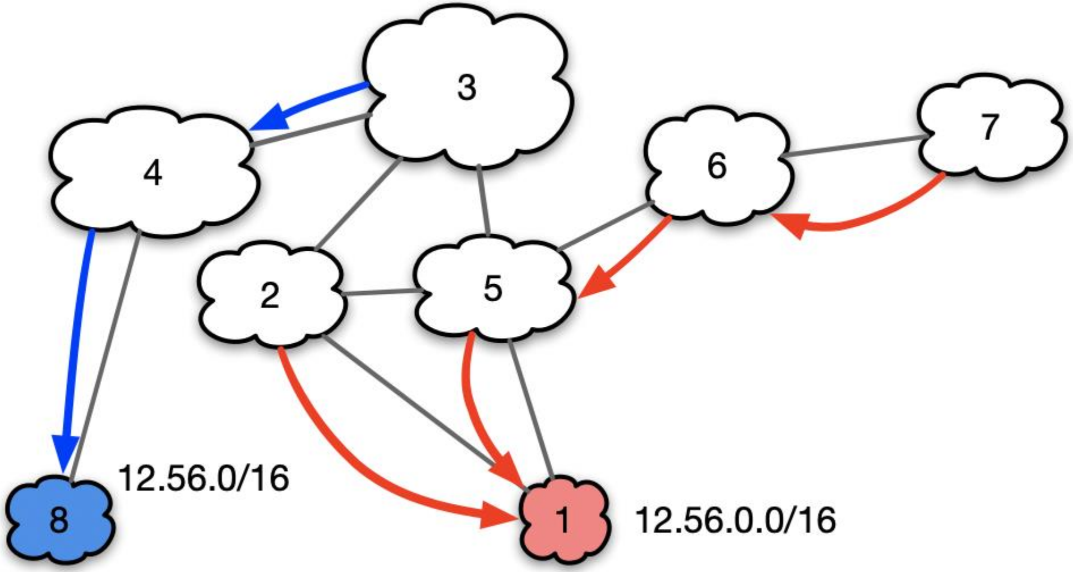
Beijing University of Posts and Telecommunications（BUPT）

Outline

- **Background**
- Method
- Experimental results
- Conclusion

Prefix Hijacking

- A prefix hijacking happens when an AS originating someone else's prefix.
  - Causing the traffic to be blackholed, or be intercepted, or be directed to wrong destination …



Solutions to Prefix Hijacking

- Preventing the hijacking before it happens
  - Proof of ownership of the address block and defensive filtering
    - — RPKI
- Fixing the hijacking when it happens
  - Monitoring to detect the prefix hijacking
    - — Route Views， RIPE RIS
    - — BGPstream
  - Mitigating the prefix hijacking
    - — Immediate action to attract the traffic back and stop malicious route

[1] http://www.cs.princeton.edu/courses/archive/fall14/cos561/

Challenges for hijacking mitigation

- Current mitigation methods have their limitations
  - Announcing a more specific prefix (prefix deaggregation)
    - Prefixes that are too long will be droped
  - Contact other networks to filter routes （email, web sites）
    - Unpredictable delay

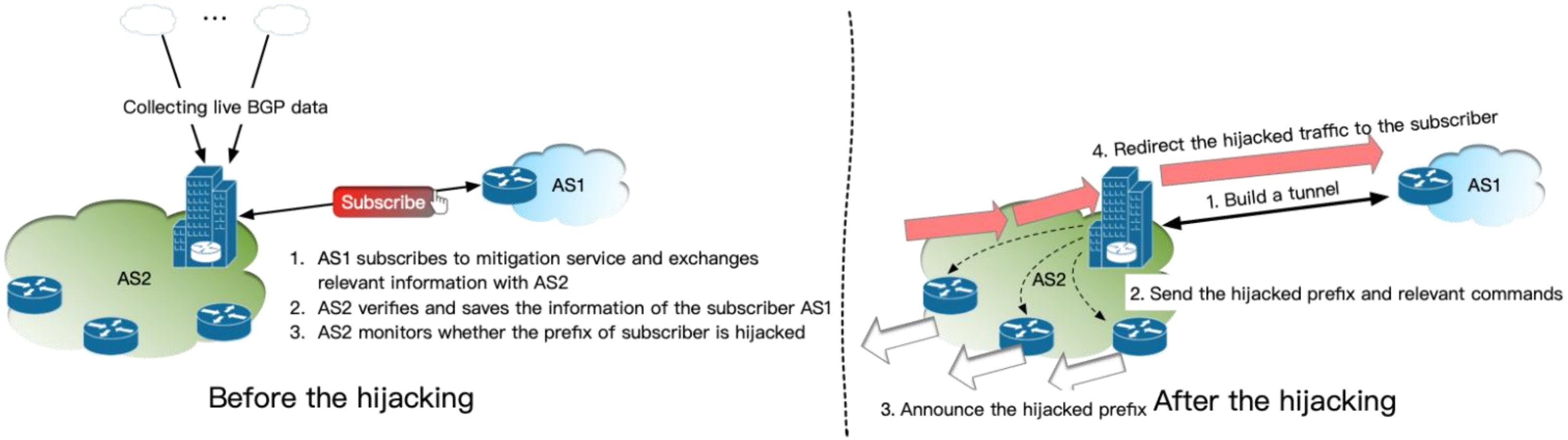
How to automatically mitigate prefix hijacking more effectively ?

Outline

- Background
- **Method**
- Experimental results
- Conclusion

Outsourcing Mitigation

- Oursourcing mitigation is an efficient mitigation method for prefix hijacking[1].
- It uses an AS (mitigator) to annouce the hijacked prefix to attract misdirected traffic, then redirecting the attracted traffic to the hijacked AS.
  - By **Tunneling** or **Direct peers**

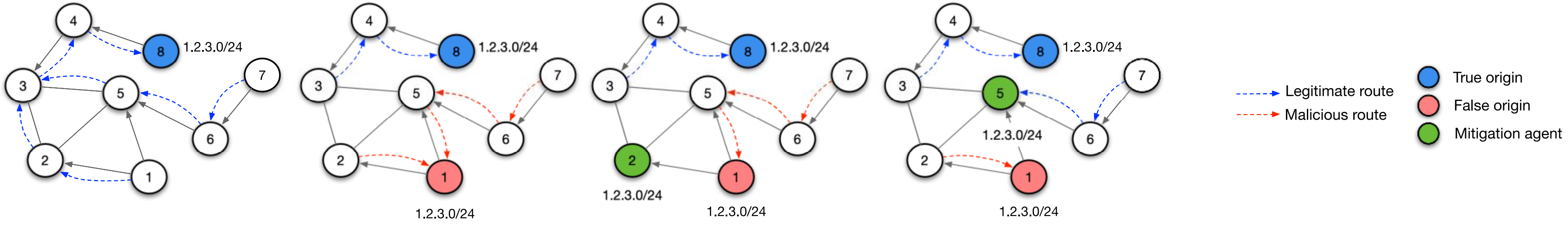


[1]. Sermpezis, Pavlos, et al. "ARTEMIS: Neutralizing BGP hijacking within a minute." *IEEE/ACM Transactions on Networking* 26.6 (2018): 2471-2486.

Outsourcing Mitigation

Mitigator Selection Problem

- Different mitigators bring different mitigation efficiency

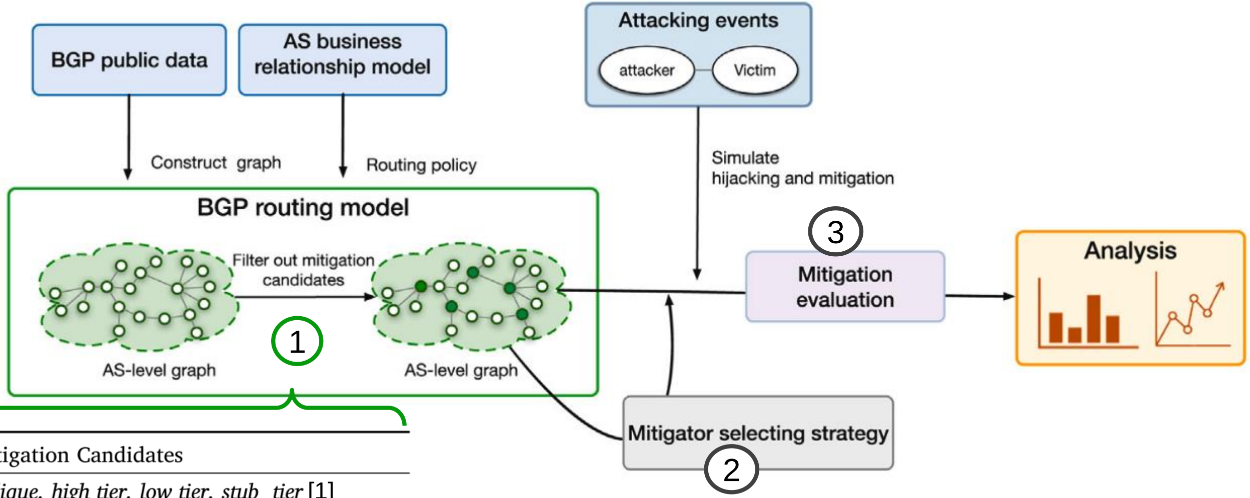


(a) Hijack scenario (b) Hijack–mitigation scenario (c) Hijack–mitigation scenario

Node 5 is a better mitigator than Node 2.

Mitigation Effectiveness Evaluating

◻ Framework overview



Algorithm 1 Computing Mitigation Candidates

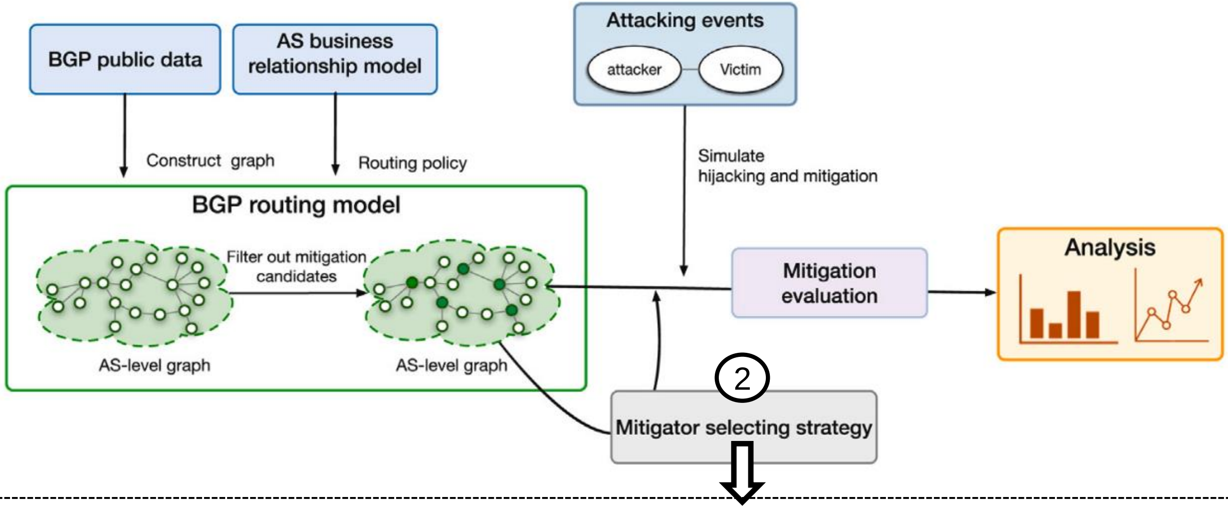
Group ASes into 4 tiers: *clique, high_tier, low_tier, stub_ tier* [1]
Mitigation candidates $M \leftarrow \varnothing$
$M \leftarrow M \cap clique \cap high\_tier$
for AS $v \in low\_tier \cap stub\_tier$ **do**
  if $v \notin M$ and v has more than one provider in $clique$ or $high\_tier$ **then**
    $M \leftarrow M \cap v$
  end if
end for

location	description
clique	clique ASes published by CAIDA
high tier	customers of clique ASes with a degree >100
low tier	ASes not in clique, high tier or stub tier
stub tier	ASes with no customers

[1].Jin, Zitong, et al. "Toposcope: Recover as relationships from fragmentary observations." *Proceedings of the ACM Internet Measurement Conference*. 2020.

Mitigation Effectiveness Evaluating

Framework overview



ASes who can reach as ***many*** as ASes with ***shorter*** paths might have high mitigation effectiveness.

ARS (AS Rechability Selection) for mitigator selction

$$ReachInf(d) = \frac{\sum_h hops(d,h) \cdot \frac{1}{h}}{|C|}$$

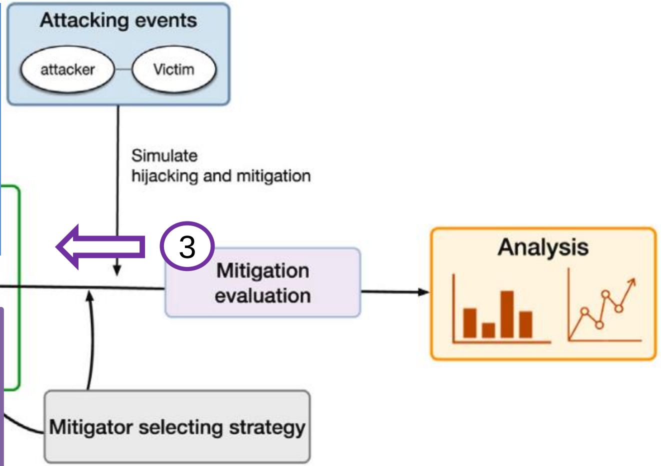
The average number of hops taken by other nodes to reach the target

$hops(d,h)$	The number of nodes reaching the origin node d with h hops.
$\|C\|$	The number of nodes who cannot reach the origin node d, $C \subset V$.

Mitigation Effectiveness Evaluating

Framework overview

When an AS chooses the route of the hijacker, it is considered that the AS is polluted. The mitigation effectiveness of ASes is measured by comparing the ***reduction of pollution rate*** before and after mitigation.



$$g'(v,x) = g(v,a,x) + g(v,t,x) + g(v,m,x) > 0$$

Pollution rate $\theta'(v,x) = \dfrac{g(v,a,x)}{g'(v,x)}$

$$\bar{\theta}_{m,a,t} = 1 - \sum_{v \in S-\{a,t,m\}} \theta'(v,x) \Big/ \sum_{v \in S-\{a,t\}} \theta(v,x)$$

Average reduced pollution rate $MP(m) = \dfrac{\sum_{(a,t)\in A} \bar{\theta}_{m,a,t}}{|A|}$

Outline

- Background
- Method
- **Experimental results**
- Conclusion

Results

- AS types

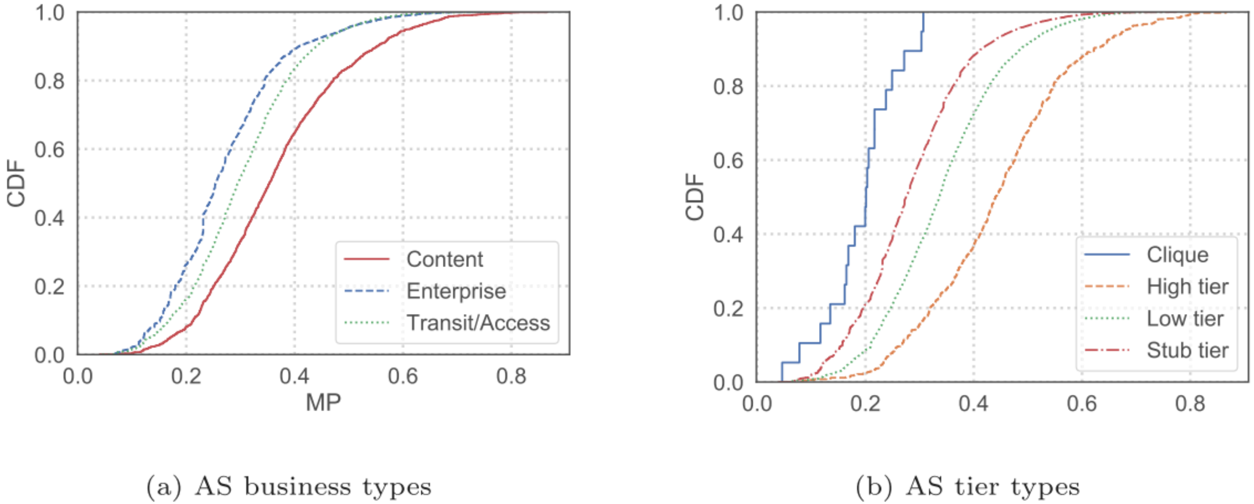
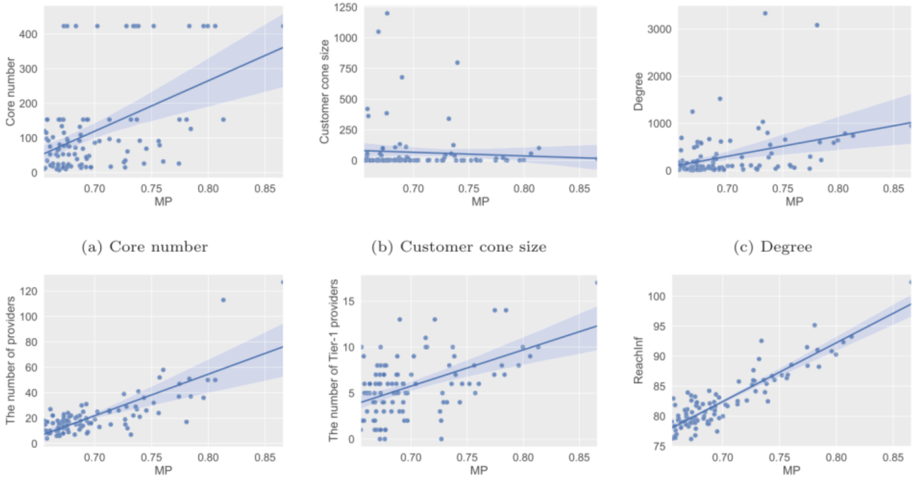


Fig. 3. Mitigation effectiveness in different AS types.

The performance of high tier (customers of Clique ASes) are better than Clique ASes

Results

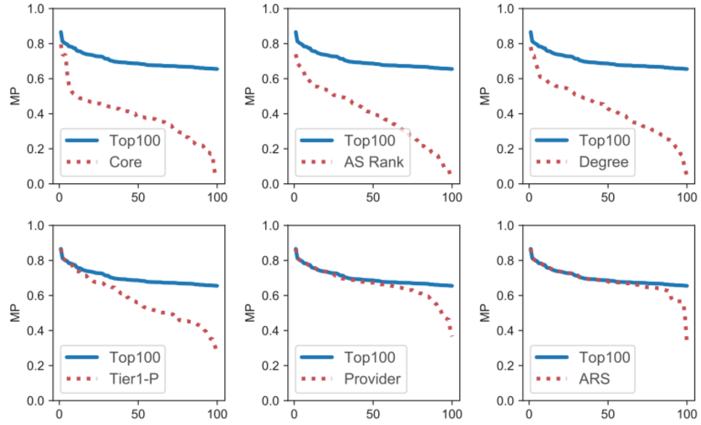
- Filter out 100 ASes with the highest MP value as Top100
- Analyze the relationship between different metrics and mitigation effectiveness of ASes



(a) Core number (b) Customer cone size (c) Degree

(d) The number of providers (e) The number of Tier-1 providers (f) ReachInf

Fig. 5. The linear regression model fit of different metrics in the Top100.



(a) The MP of 100 ASes selected by a certain strategy. The x-axis represents the 100 ASes with the highest MP under different selection strategies.

ReachInf has a higher correlation with MP than other metrics.
ARS can filter out ASes with high mitigation effectiveness.

Outline

- Background
- Method
- Experimental results
- **Conclusion**

北京郵電大學 Beijing University of Posts and Telecommunications

Conclusion

- This work contributes to a better understanding of outsourcing mitigation mechanism and mitigation efficiency of different ASes.
  - We analyzed various factors that influence the mitigation effectiveness of ASes
    - The number of providers, the number of Tier-1 providers, degree, core number, AS type, etc.
  - We also proposed a metric named ReachInf to select mitigators with high mitigation effectiveness

Thank you