On the classification and false alarm of RPKI based BGP route origin validation

Wenjie Xu, Deliang Chang and Xing Li
Tsinghua University, Beijing, China

Introduction

Border **G**ateway **P**rotocol(BGP) connects different ASes

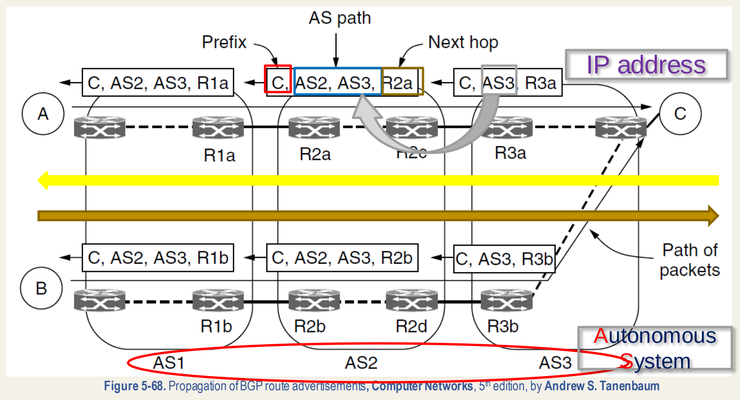
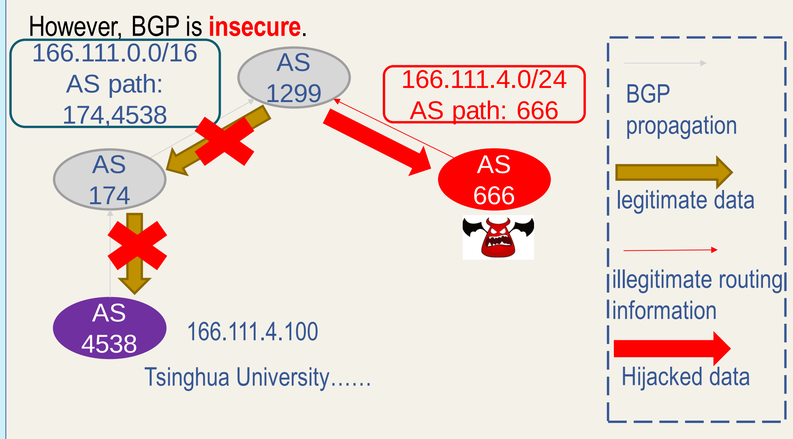


Figure 5-68. Propagation of BGP route advertisements, **Computer Networks**, 5th edition, by **Andrew S. Tanenbaum**

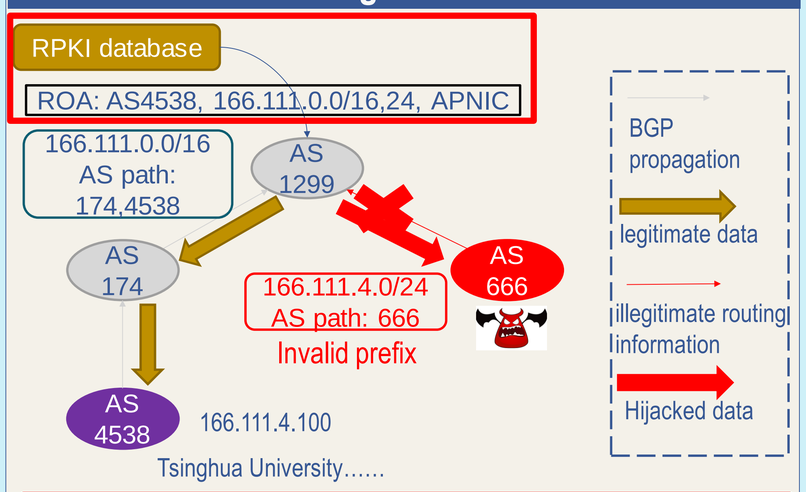
However, BGP is **insecure**.



Two lines of efforts to secure BGP

- Detection based method
  - Detect the anomaly
  - High false alarm rate
- Rule based method(RFC6480)
  - Build an RPKI (Resource Public Key Infrastructure) database
  - Verify the BGP origin and IP prefix pair by comparing with the database
  - Currently under deployment

Is RPKI enough to secure BGP?

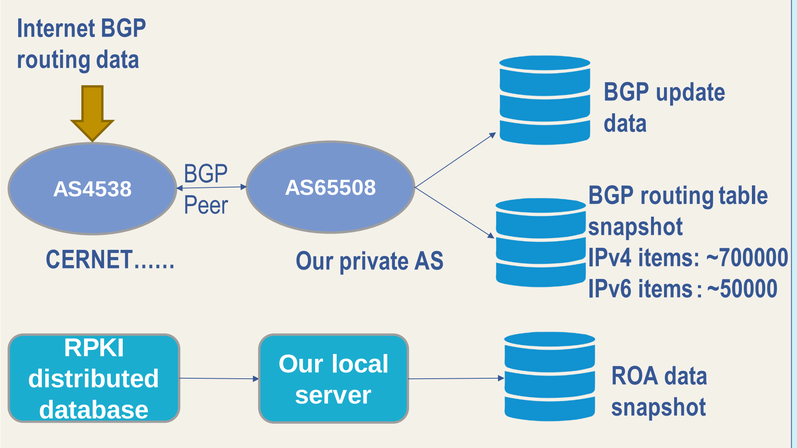


What if the ROA(route origin authorization) item in RPKI database is not reliable?

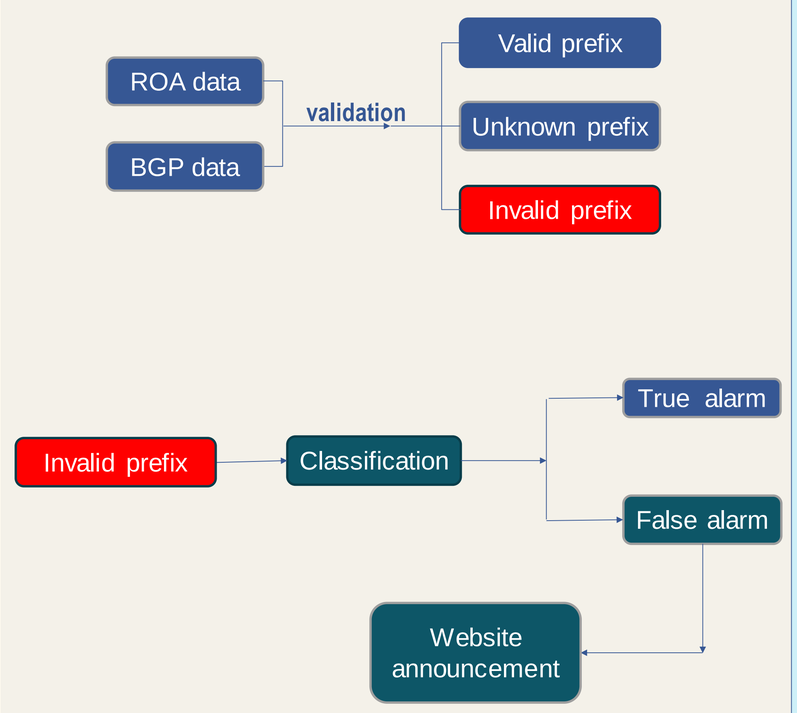
Our goal

- Systematically measure and analyze the invalid prefixes.
- Classify the invalid prefixes into different types.
- Based on the classification results, evaluate the reliability of the RPKI database.

Data collection



Analysis pipeline



Validation result

Validation Result	Number of Routing Items	Ratio
Unknown	635412	90.87%
Valid	58931	8.43%
Invalid	4949	0.71%

TABLE I
RPKI BASED ROUTE ORIGIN VALIDATION RESULT(DATA COLLECTED ON 16TH, MAY, 2018)

Types of invalid prefixes

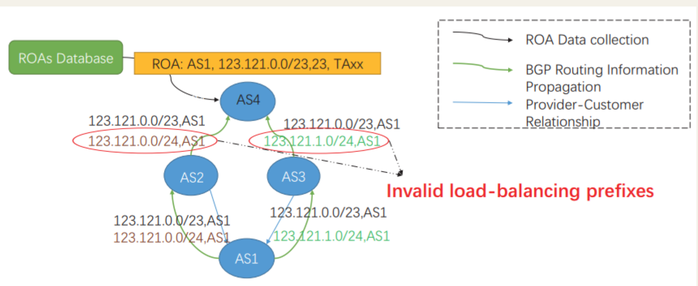


Fig. 1. An illustration of invalid load-balancing prefix

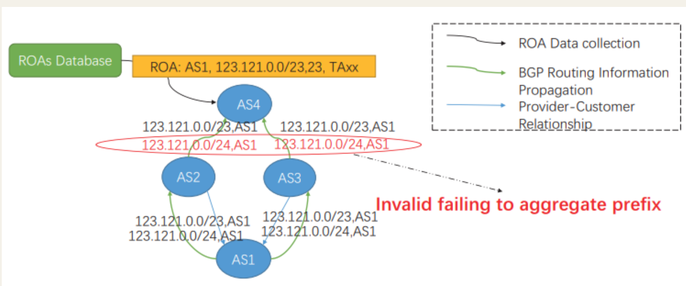


Fig. 2. An illustration of invalid failing to aggregate prefix

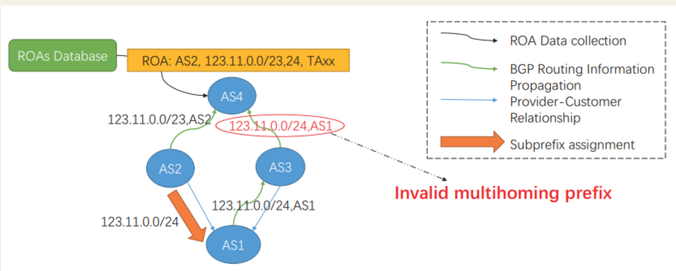


Fig. 3. An illustration of invalid multihoming prefix

Types of invalid prefixes(cont.)

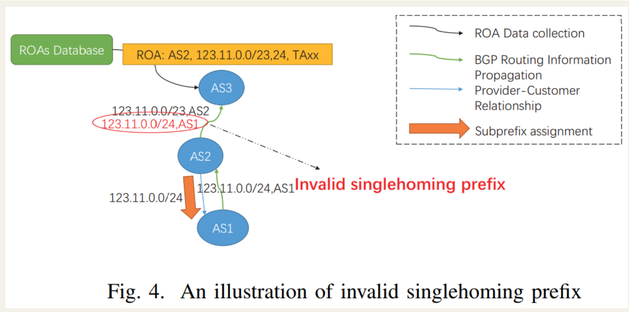


Fig. 4. An illustration of invalid singlehoming prefix

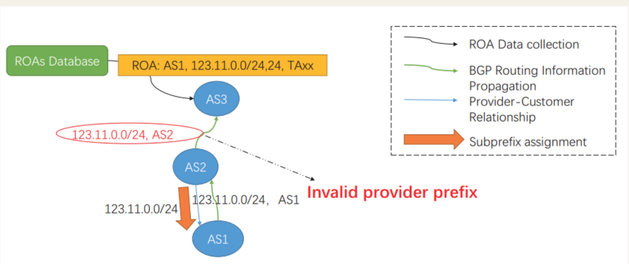


Fig. 5. An illustration of invalid provider prefix

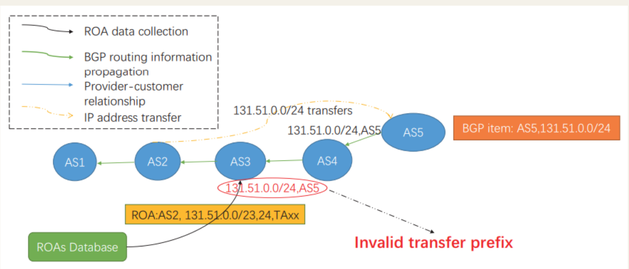


Fig. 6. An illustration of invalid transfer prefix

Classification result and its implication

Type of Invalid prefix	Number	Percentage in invalid prefix	Number of long-lived (invalid prefix, origin AS) pairs	Percentage of prefixes with long-lived (prefix, origin AS) pair in this type
Invalid load-balancing prefix	923	18.7%	770	83.4%
Invalid failing to aggregate prefix	703	14.2%	684	97.3%
Invalid mul-tihoming prefix	378	7.6%	355	93.9%
Invalid sin-glehoming prefix	204	4.1%	177	86.8%
Invalid provider prefix	186	3.8%	147	79.0%
Invalid transfer prefix	737	14.9%	658	89.3%
Other invalid prefix	1818	36.7%	1695	93.2%

TABLE III
THE CLASSIFICATION RESULT AND STABILITY OF INVALID PREFIX(DATA COLLECTED ON MAY, 16TH, 2018)

Most of the invalid prefixes very likely result from traffic engineering, IP address transfer and failing to aggregate rather than real hijackings.

Conclusion

- More than 60% of the invalid BGP prefixes belong to the six types we describe.
- They very likely result from traffic engineering, IP address transfer and failing to aggregate rather than real hijackings.

Contact and paper Information

Wenjie Xu
Email: xw018@ie.cuhk.edu.hk
Homepage: https://jackiexuw.github.io/

Where to find our paper:

https://jackiexuw.github.io/paper/IM2018_RPKI.pdf