Major Project Part II

Isolating Suspicious BGP Updates To Detect Prefix Hijacks

Author: Abhishek Aggarwal (IIT Delhi)

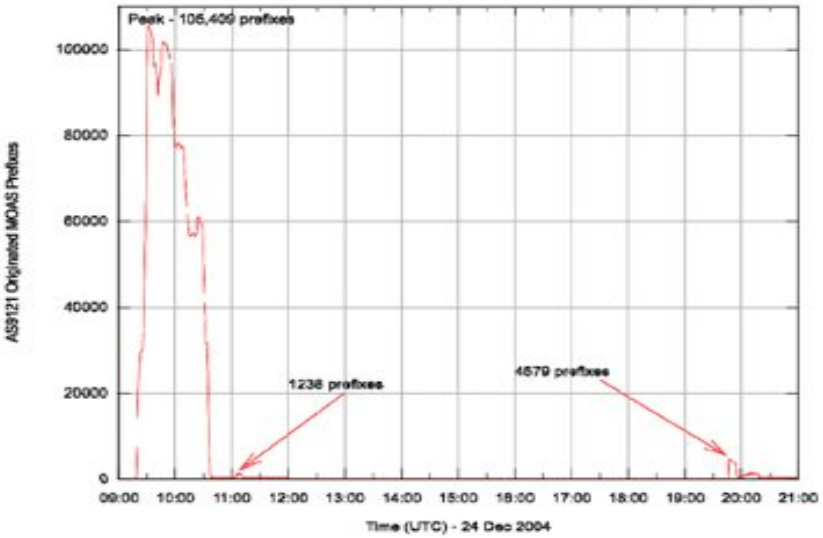
Co-authors:

Anukool Lakhina (Guavus Networks Inc.)

Prof. Huzur Saran (IIT Delhi)

Motivation

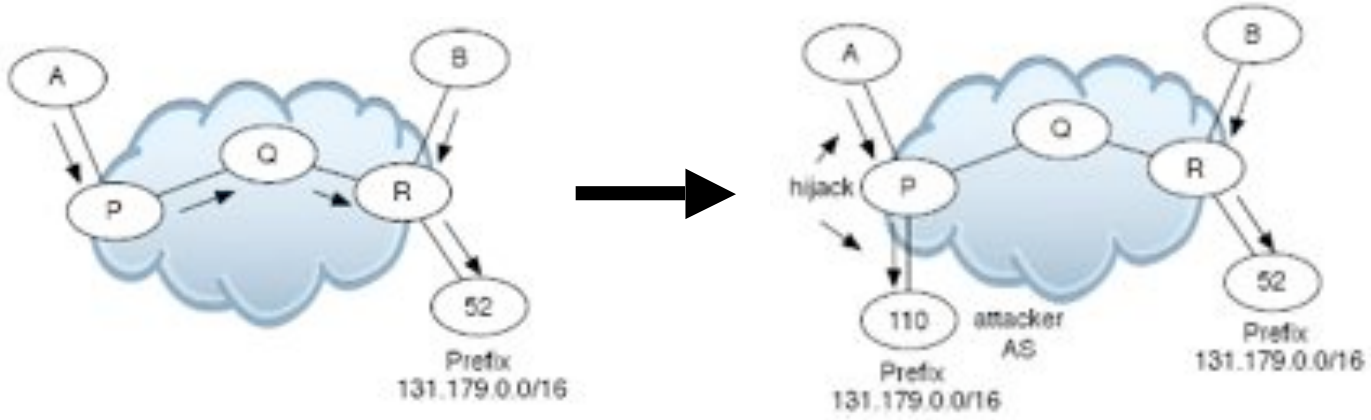
- BGP routes can be hijacked by a misbehaving or compromised router. This can have serious consequences
- Accidental hijack
  - AS 9121 incident
- Malicious hijack
  - Used to send SPAM



Objective

Isolate suspicious BGP updates for further analysis to detect prefix hijacks

Prefix Hijack: Example



a. True origin AS 52 announces prefix 131.179.0.0/16

b. False origin AS 110 announces prefix 131.179.0.0/16

Figure: AS 110 hijacks prefix of AS 52

Mohit et al., 2006, *15th USENIX Security Symposium*

Valid MOAS Case

Multihoming without BGP

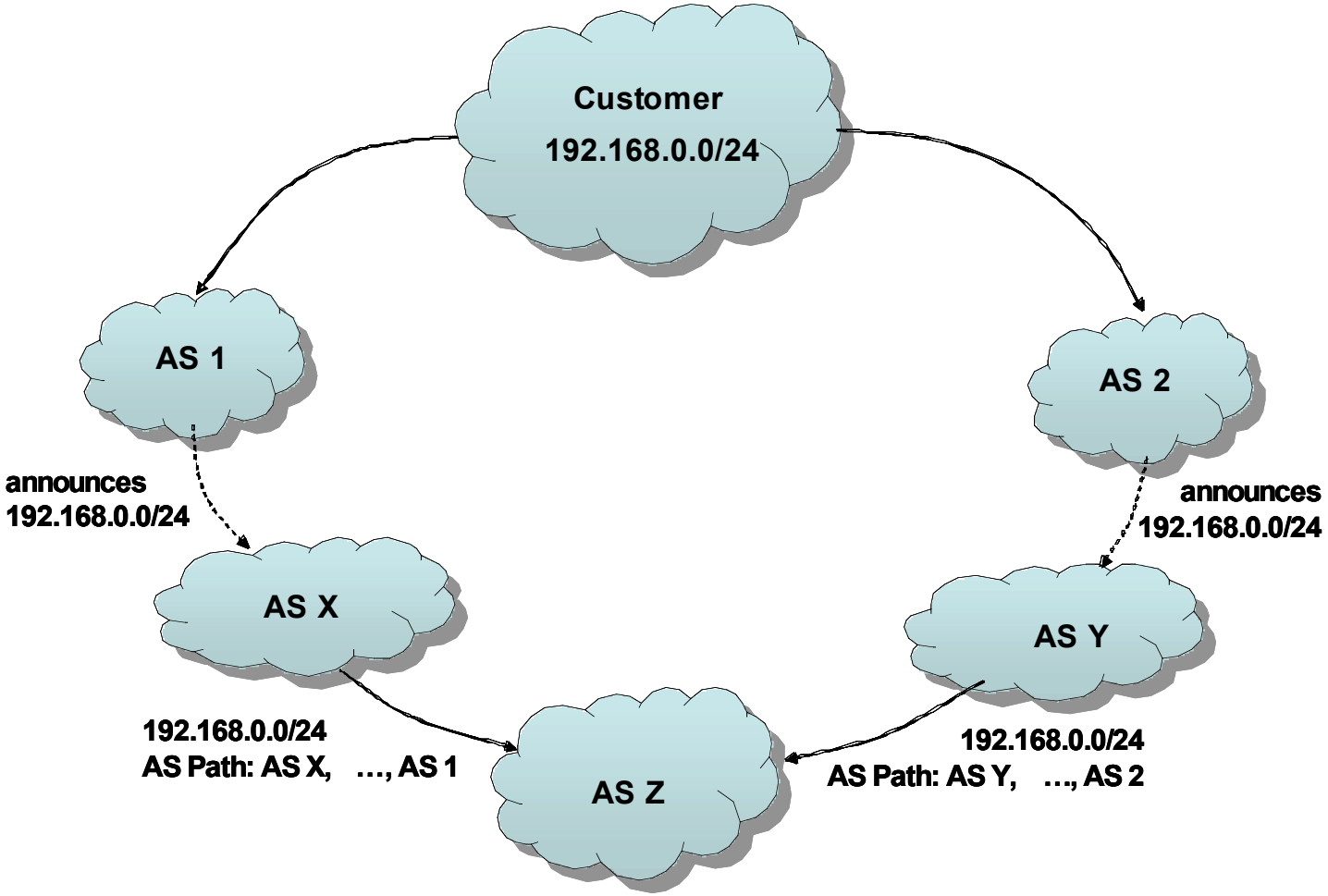


Figure: Multihoming without BGP

Valid MOAS Case

Private AS number substitution

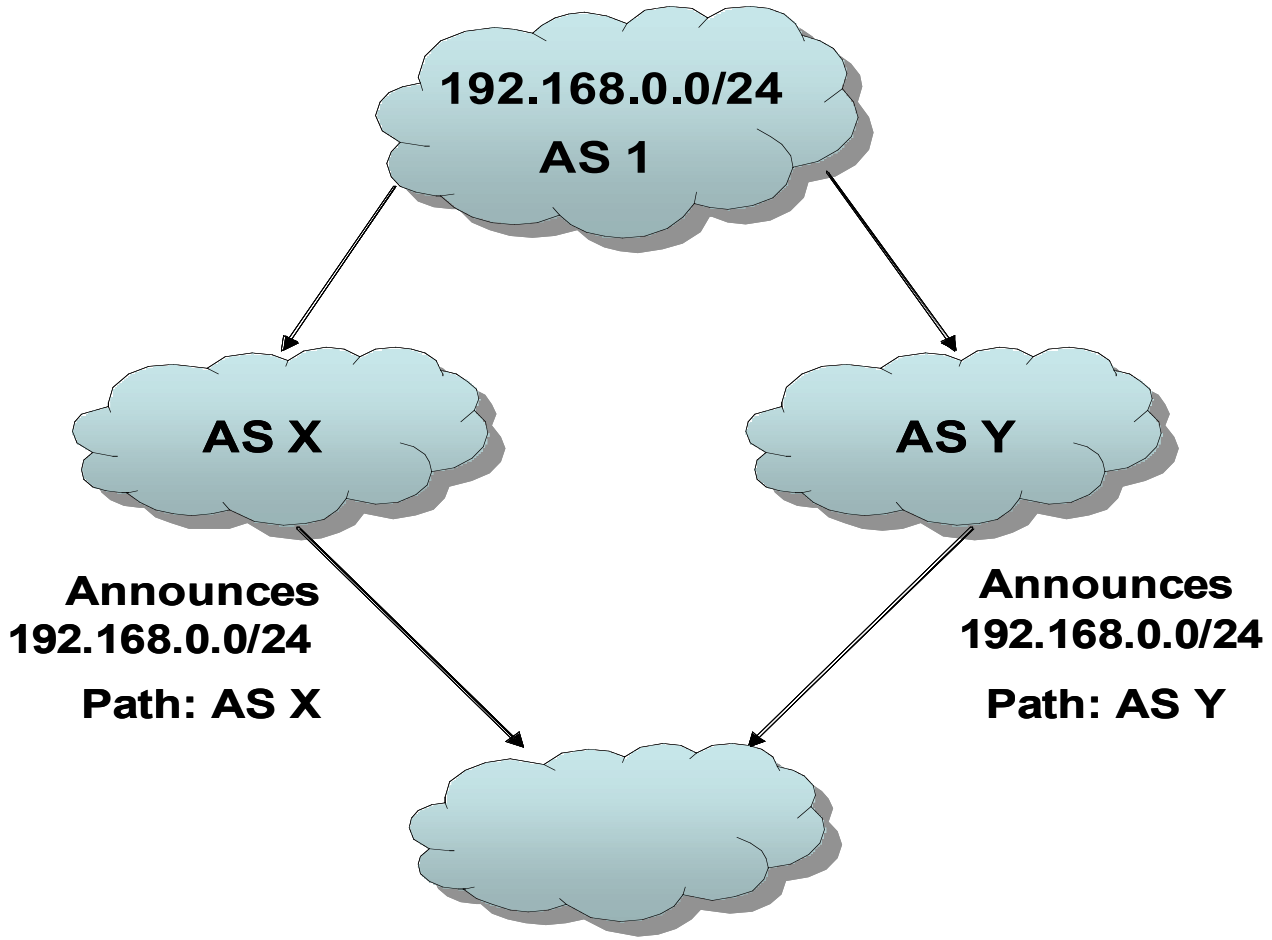


Figure: Private AS number substitution

Basic Philosophy

- Analyze past BGP data to establish normal behavior for a prefix
  - Associate a state with every prefix at a border router
  - Origin AS is state variable
  - Track changes in the state to figure out normal changes for prefix
- Analyze incoming updates and flag the ones violating the normal

Percentage hold time distribution of conflicting ASs is highly skewed

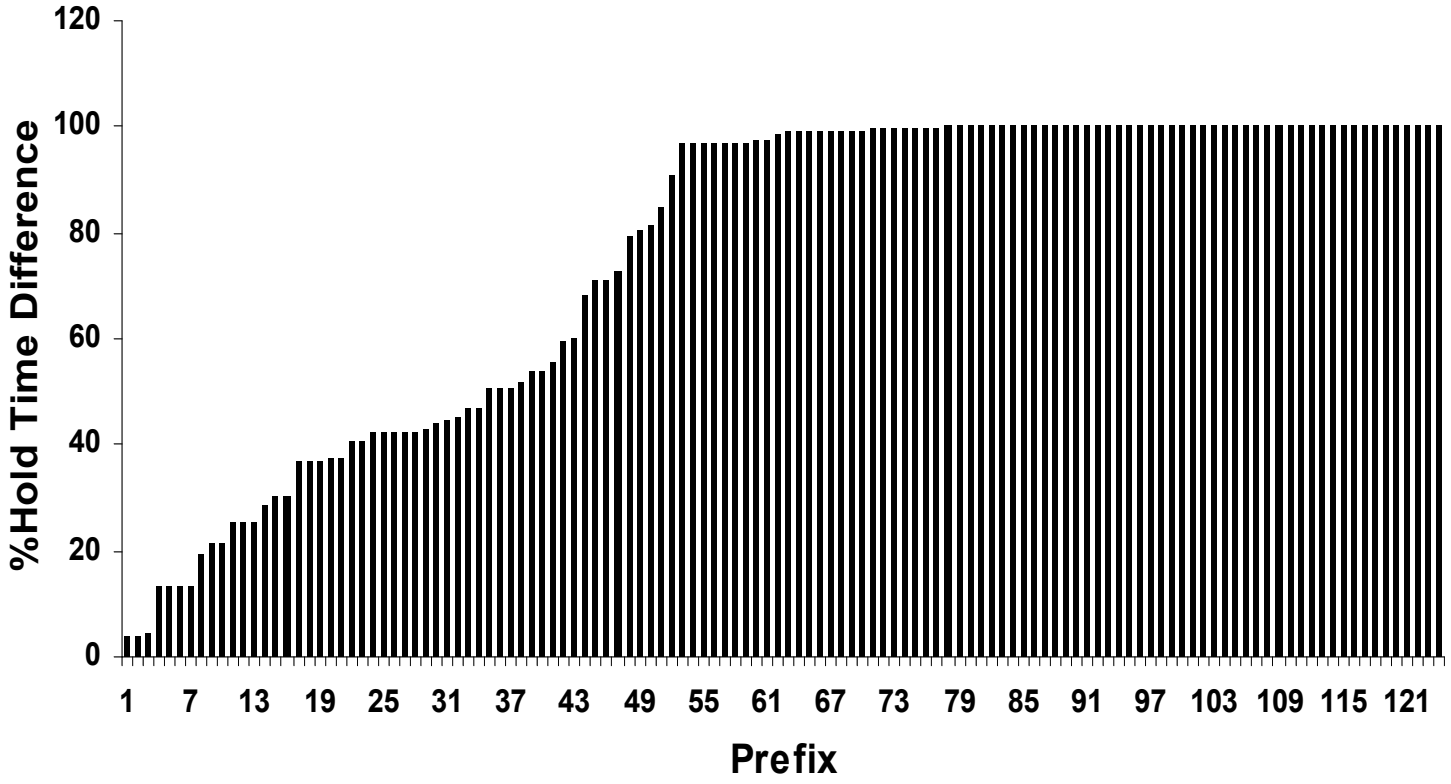


Figure: Percentage hold time difference for MOAS prefixes

Negative correlation between % Hold Time Change and AS Path Length Change

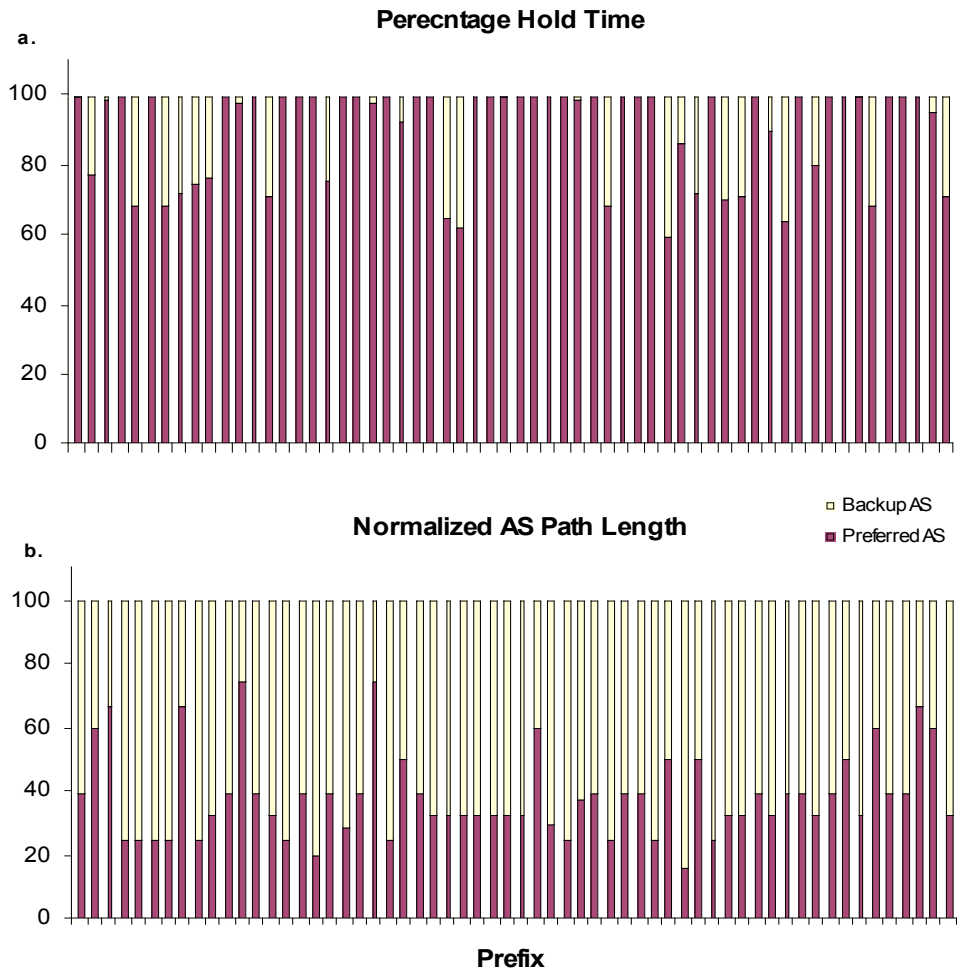


Figure: (a) Percent hold time Vs Prefix, and (b) Normalized AS path length Vs Prefix

Preferred AS Path Length

For 84 % prefixes:

AS with high percentage hold time has a shorter path length

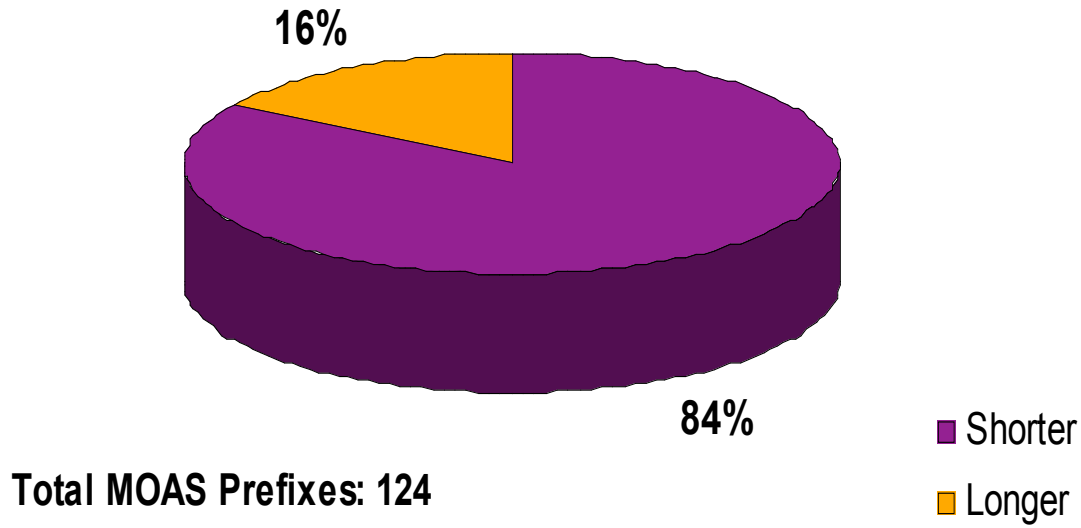


Figure: Percentage breakup of MOAS prefixes on preferred AS path length

AS Path Relationship

- Overlap
  - One path lies on the other
  - Related origin AS
- Cross
  - Intersect in unique points
- Distinct
  - Independent of each other

AS Path Relationship

For ~ 88 % multi origin prefixes:

Conflicting ASs have overlapping AS paths

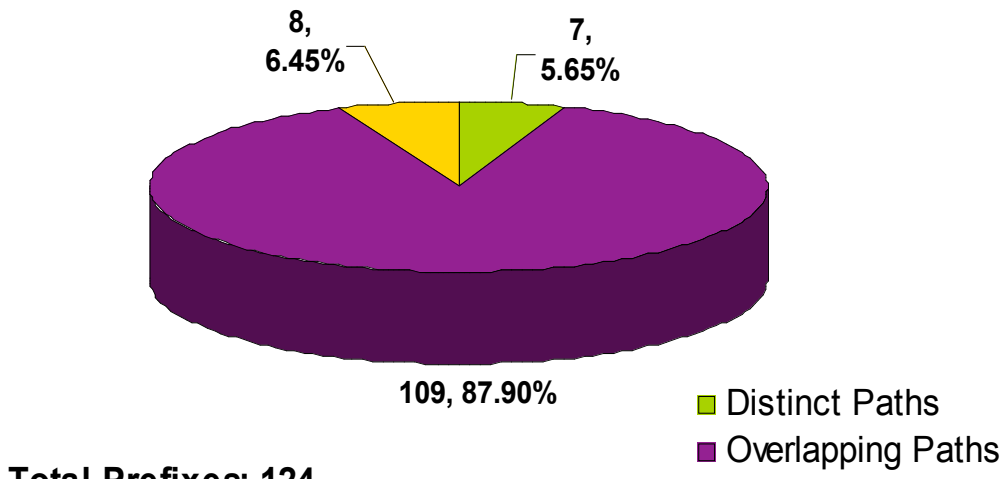


Figure: Percentage breakup of prefixes on AS path relationship of conflicting ASs

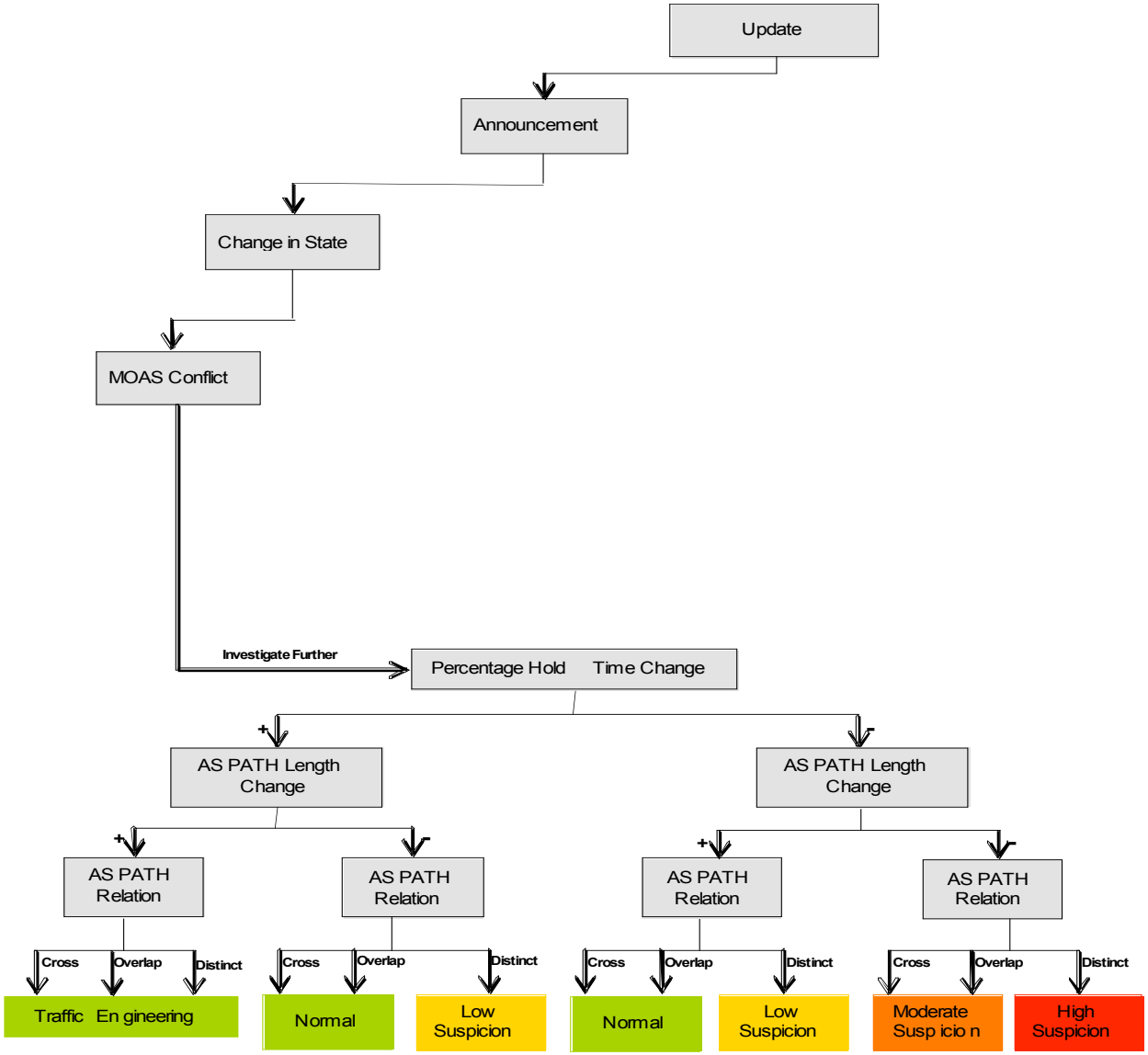
Characteristics of Possible Prefix Hijacks

- Change in state of prefix
- Multi Origin AS conflict
- False origin AS has
  - Low percentage hold time
    - → Malicious routes are short lived
  - Shorter AS path length
  - Distinct or Cross AS path relationship
- Deaggregated prefix

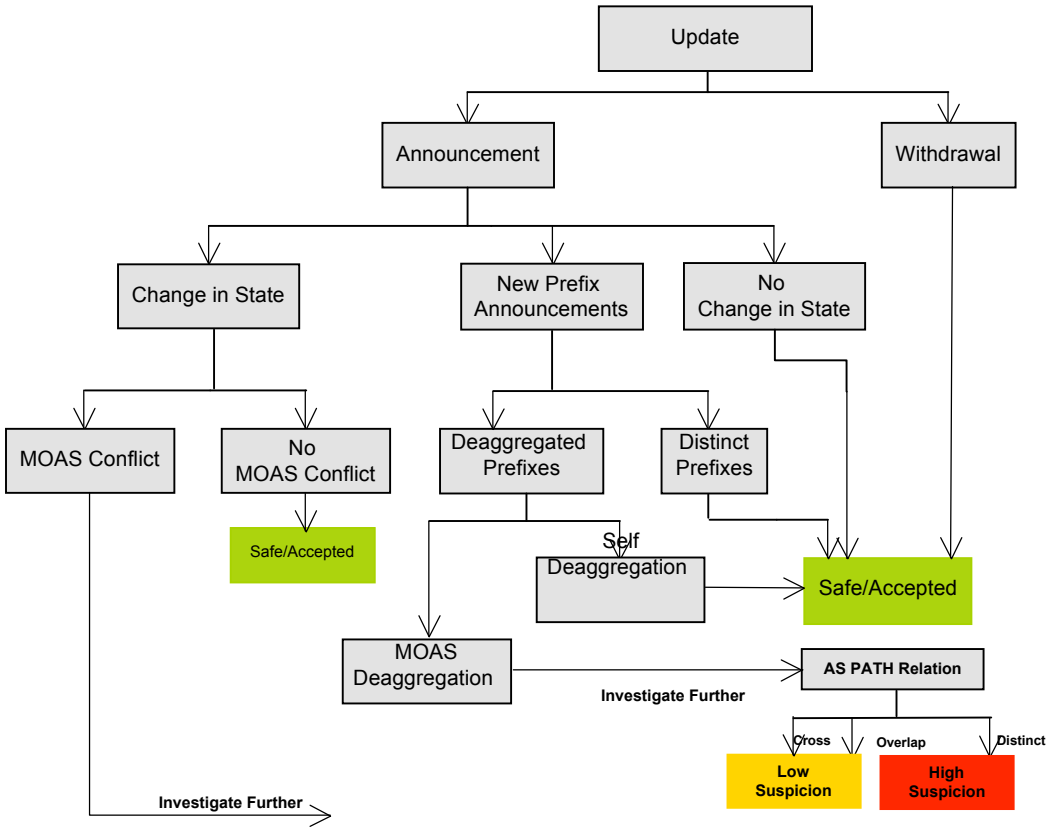
Metrics

- Change in Percentage hold time of conflicting ASs
- Change in AS path length
- AS path relationship
  - Overlapping
  - Cross
  - Distinct

Decision Tree Branch 1



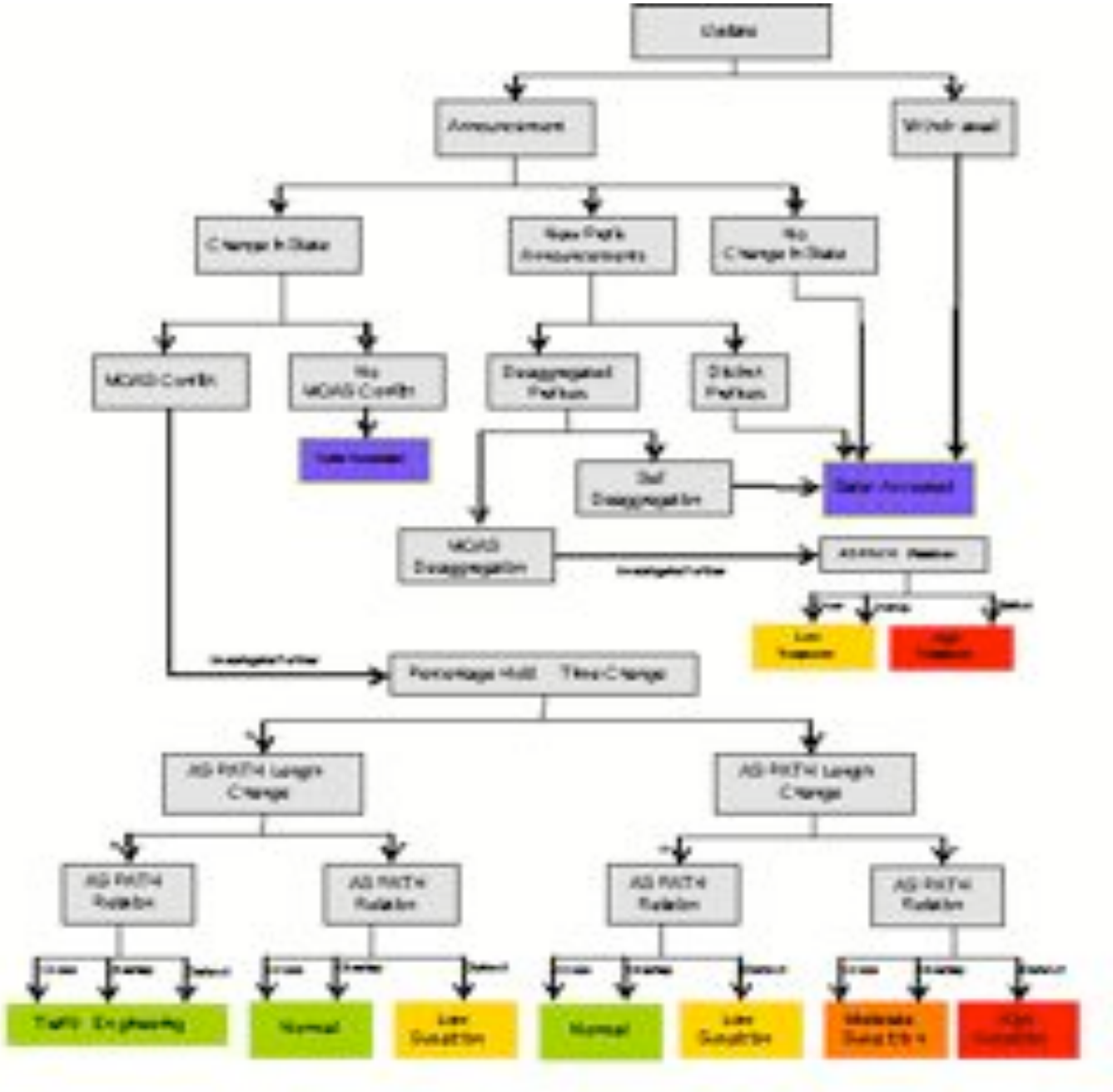
Decision Tree Branch 2



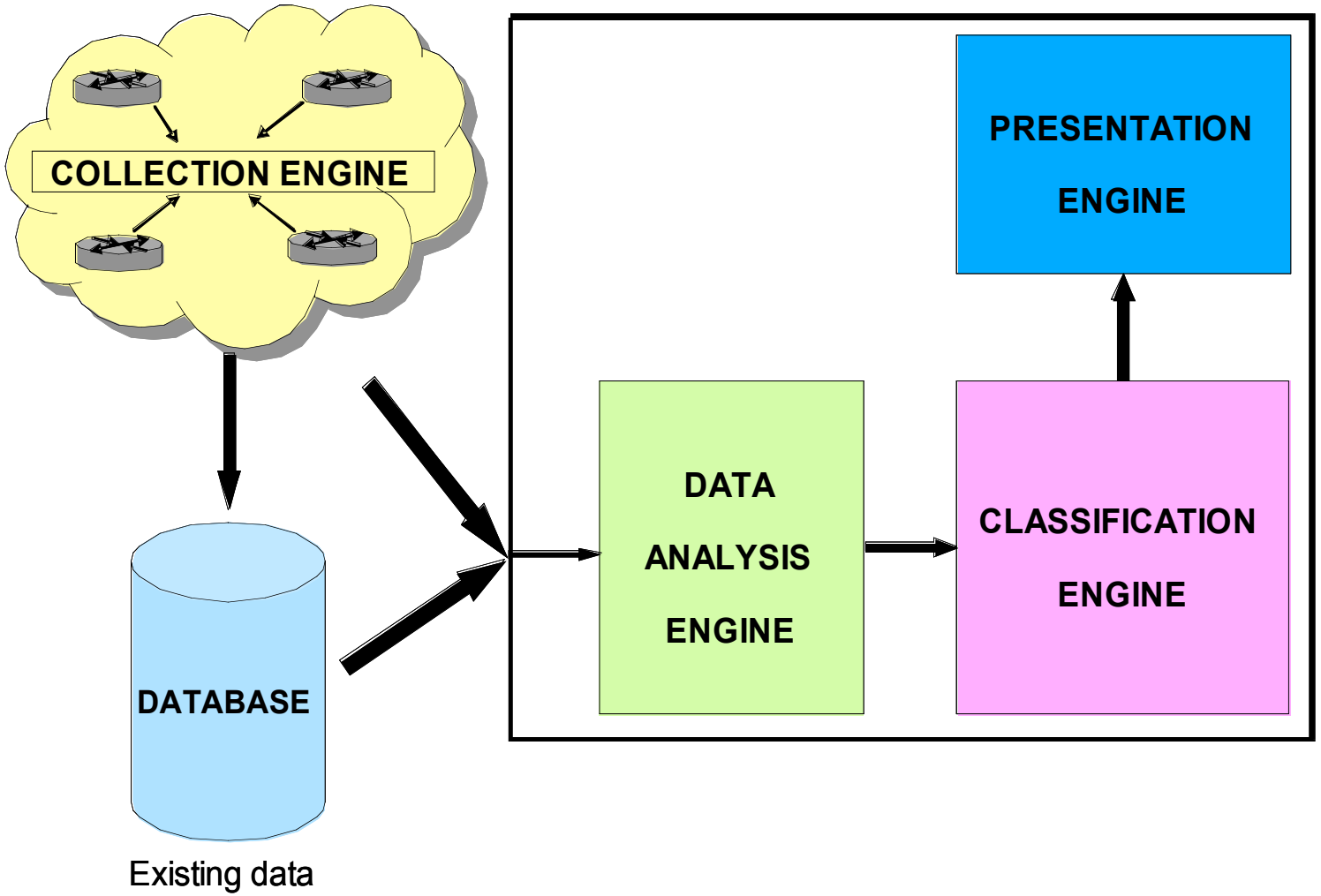
AGENDA

- Motivation
- Objective
- Background
- Data Analysis
- Characterization
- **Classification**
- Implementation
- Results
- Conclusions
- References

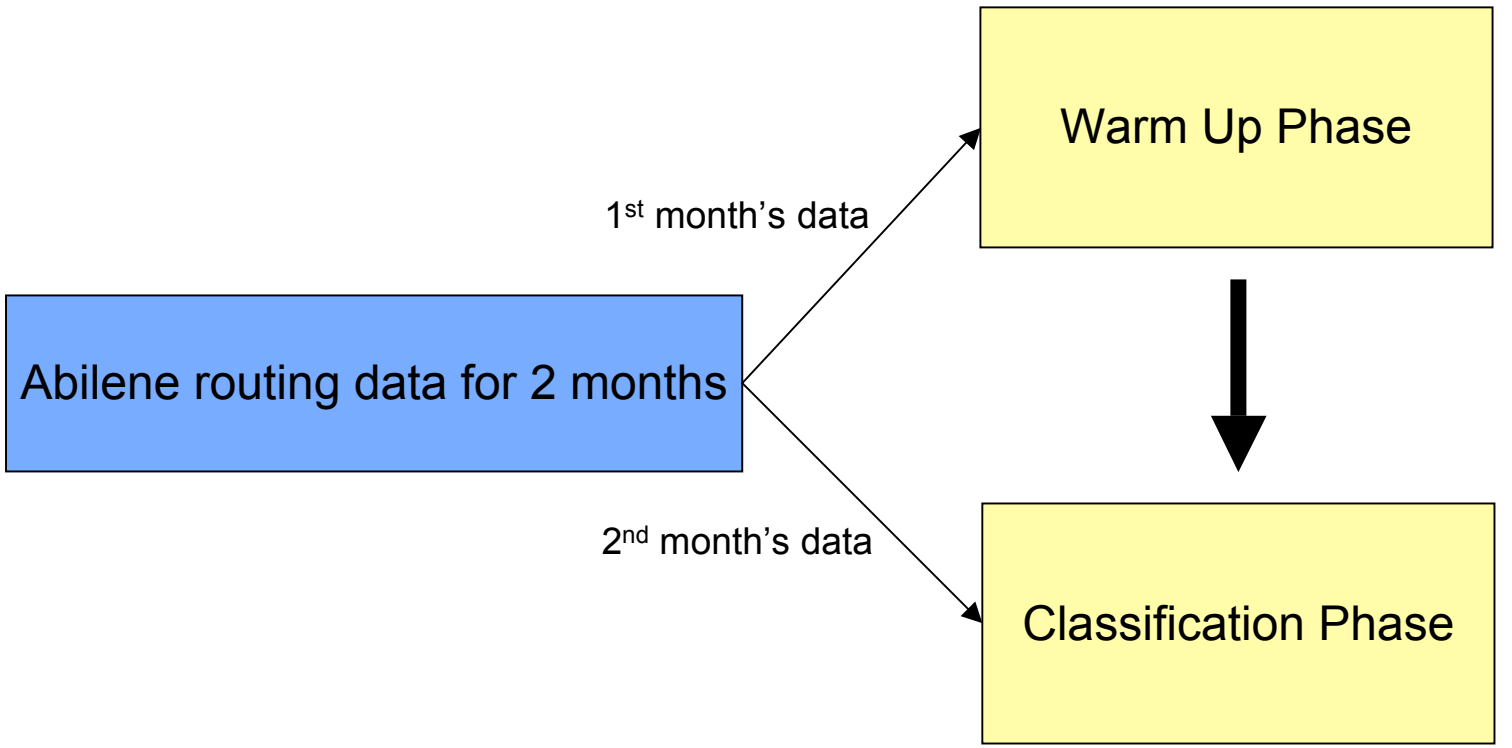
Classification Algorithm/ Decision Tree



Architecture Diagram



Implementation



Results

Total Updates processed = 671646

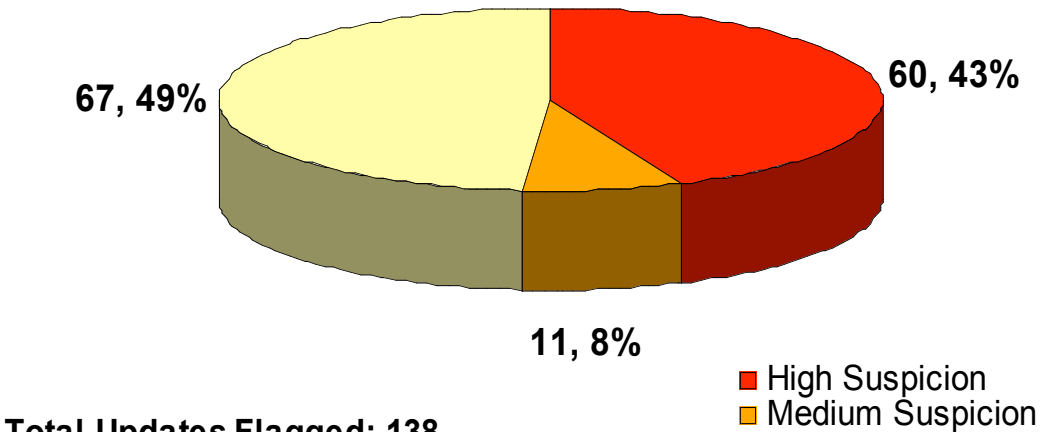


Figure: Percentage break up of flagged updates

Results

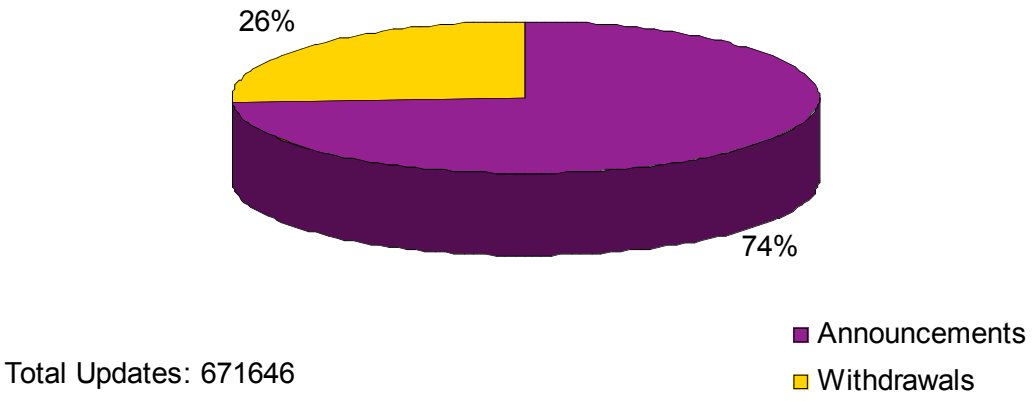


Figure: Percentage break up of updates

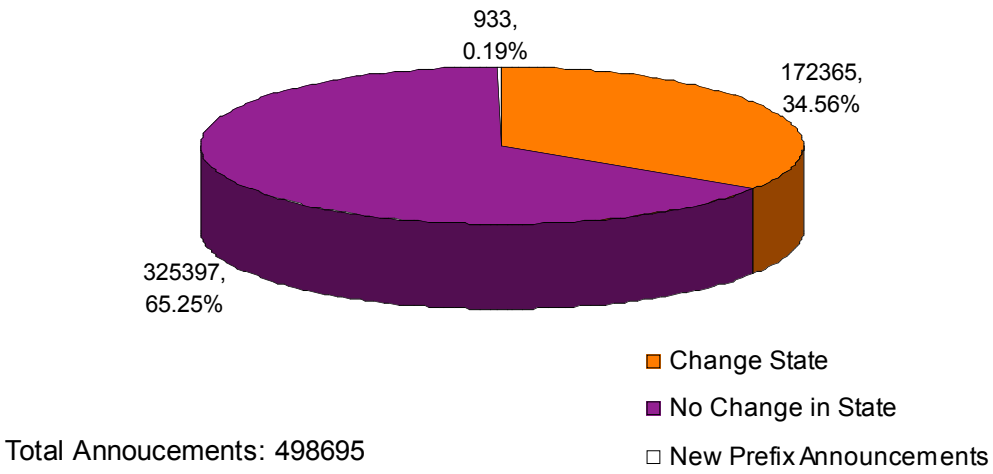


Figure: Percentage break up of announcements

Results

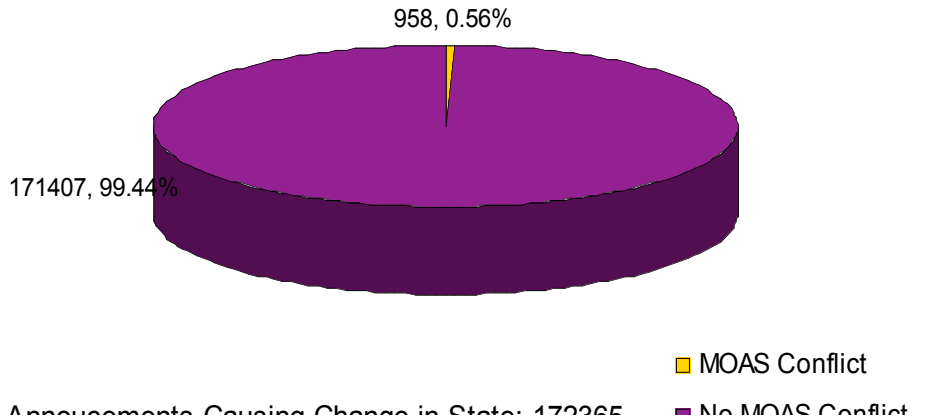


Figure: Percentage break up of announcements causing change in state

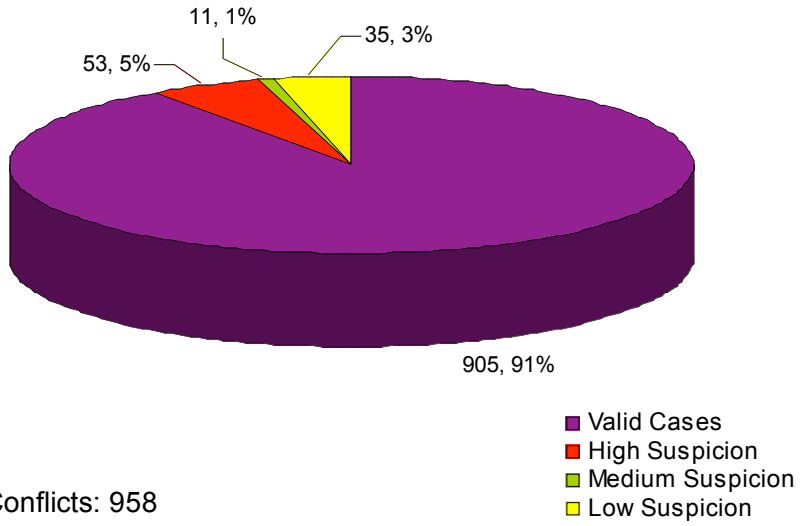
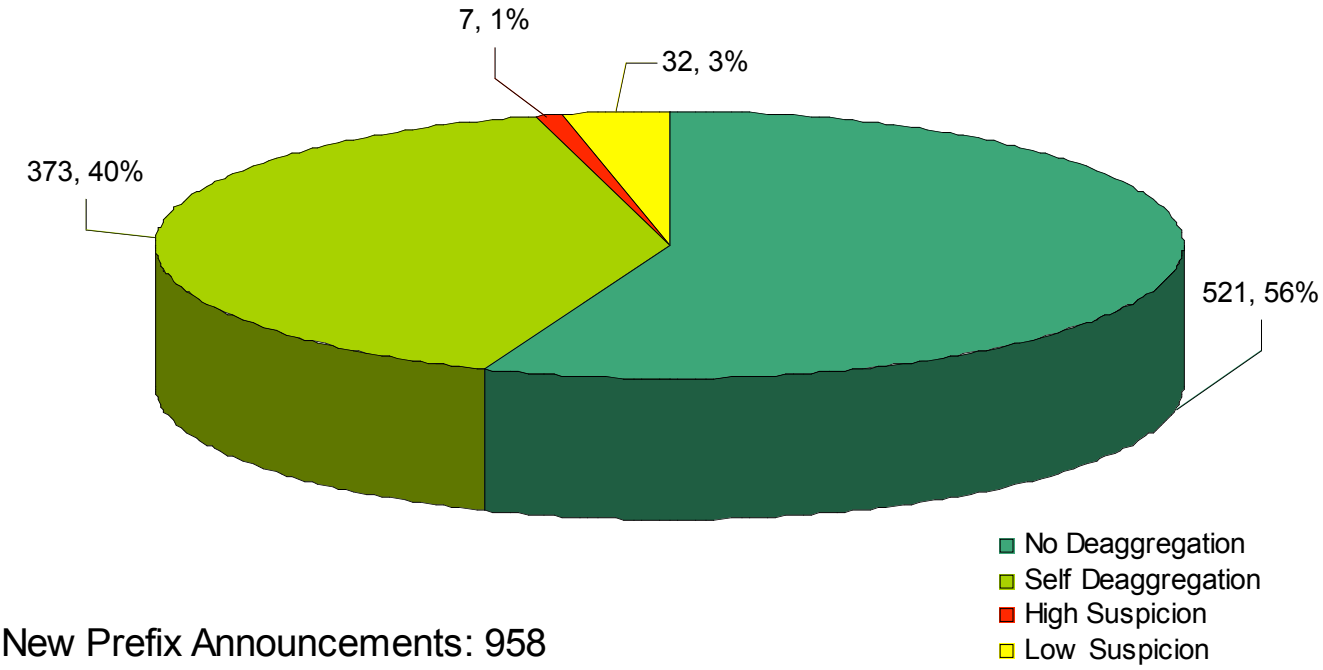


Figure: Percentage break up of MOAS conflict cases

Results



Total New Prefix Announcements: 958

Figure: Percentage break up of new prefix announcements

Some Interesting Incidents

Deaggregation

Existing	New
Covering Prefix: 138.18.0.0/16	Deaggregation Prefix: 138.18.214.0/24
Origin AS: 668	Origin AS: 14077
AS Path: 668	AS Path: 18592 2153 101 14077
AS Path Relation: *Distinct*	

Some Interesting Incidents

Replacement

Existing	New
Status: Active Origin AS: 5050 AS Path: 5050 Hold Time %: 99.99	AS Path Relationship: Distinct Origin AS: 559 AS Path: 20965 559 Hold Time %: 0.001
Prefix: 192.88.99.0/24	

Conclusions

- Past BGP data about a prefix can help to determine safe changes to the state of the prefix
- Percentage hold time change, AS path length change and AS path relationship are useful metrics to filter out valid MOAS incidents
- Normally, percentage hold time change and AS path length change have a negative correlation

Key Benefits

- Help network operators
  - Enable manual data analysis
  - Inject new detection schemes
- Readily deployable
- Incremental deployment
- Build base truth on prefix hijacks

Future Scope of Work

- Finding new relevant metrics to isolate and classify prefix hijack incidents with higher probability
- Fusing Internet wide Route Views data with local AS data
- Fusing Internet traffic data with routing data

References

- Anirudh Ramachandaran,Nick Feamster. On understanding Network Level behavior of spammers. In *Proc. ACM SIGCOMM Conference, 2006.*
- Ola Nordstrom, Constantinos Dovrolis. Beware of BGP Attacks. In *ACM SIGCOMM Communications Review, April 2004.*
- Mohit Lad, Dan Massey, Dan Pie. Prefix Hijack Alert System. In *15th USENIX Security Symposium, USENIX Security 2006.*
- Xiaoliang Zhao, Dan Pei, Lan Wang and Dan Massey. An analysis of BGP MOAS conflicts. In *ACM SIGCOMM Workshop on Internet Measurement,2002.*
- C. Lynn, S. Kent and K.Seo. Secure border Gateway protocol (S-BGP). *In IEEE JSAC Special Issue on Network Security,2002.*


AGENDA
Motivation
Objective
Background
Work Done
Data Analysis
Characterization
Classification
Results
Abilene Network
Conclusions
References

Thank You !