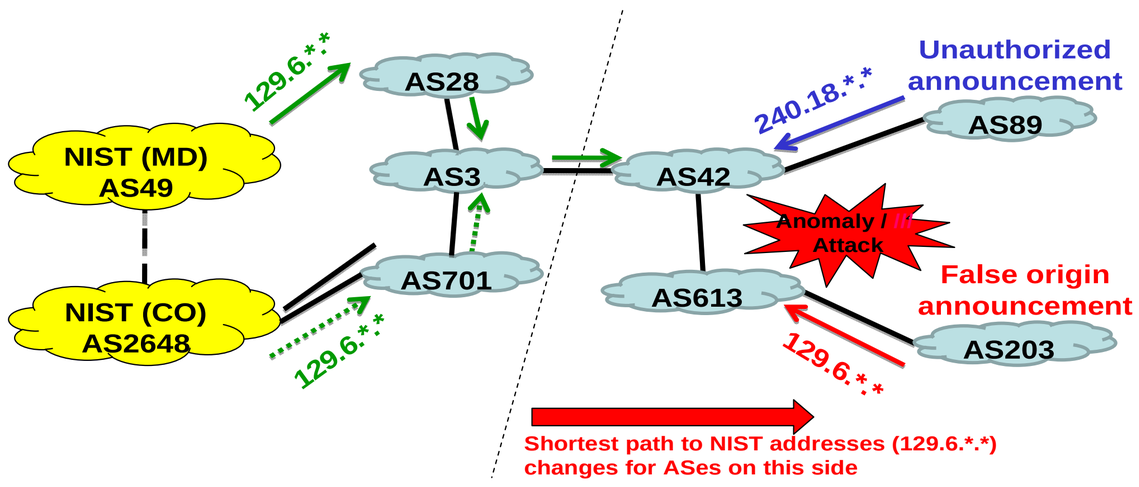
A Comparative Analysis of

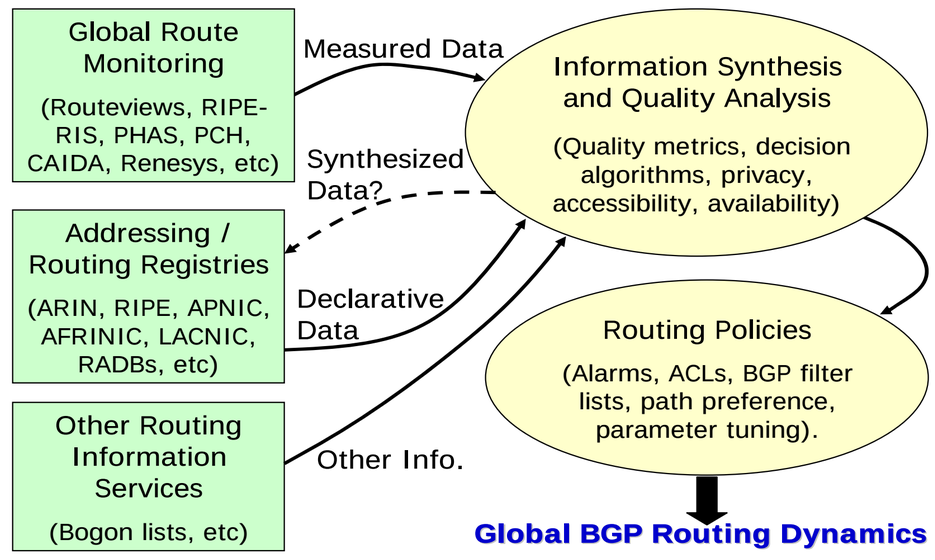
BGP Anomaly Detection and Robustness Algorithms

BGP Robustness Problem Space (Examples)

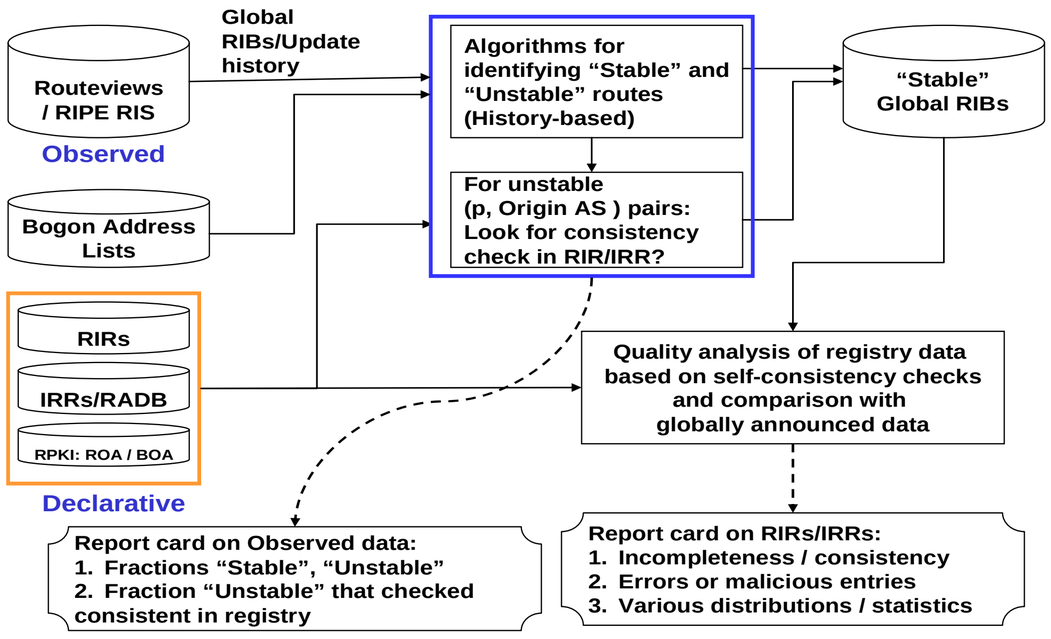


- BGP is prone to routing anomalies due to misconfigurations and malicious attacks
- The ramifications are hijacks, misroutings, DoS, spam, etc.

Solution Components / Players

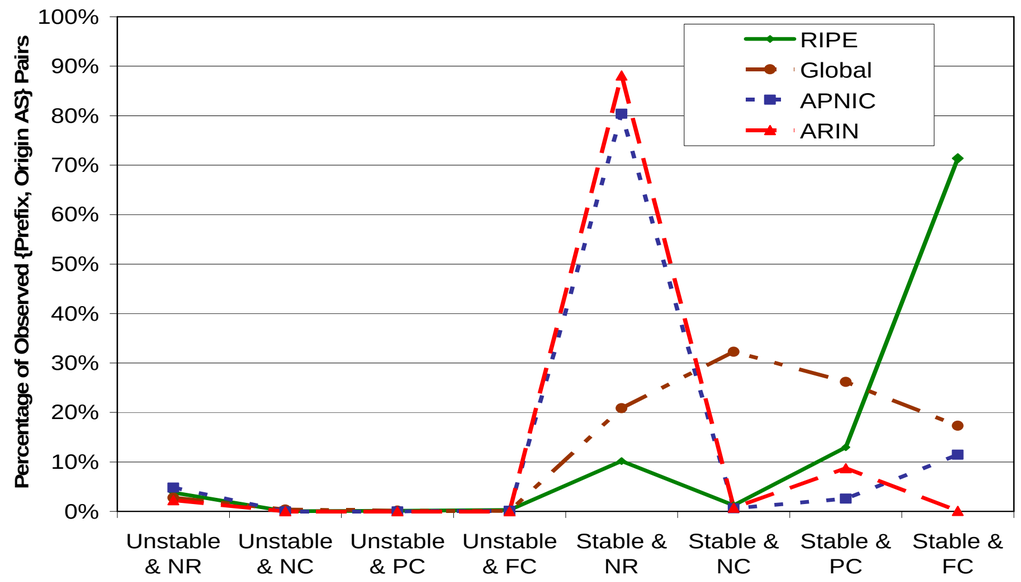


New Integrated Approach



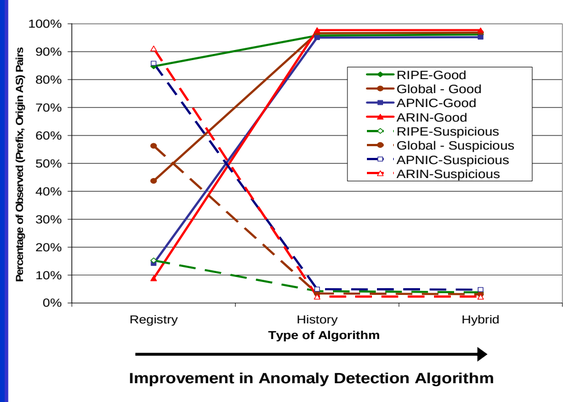
ROA: Route Origin Attestation
BOA: Bogon Origin Attestation

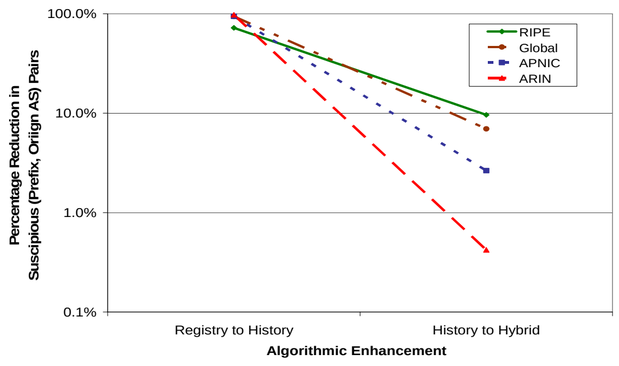
Classification of Observed (p, OAS) Pairs According to Stability / Consistency Scores



p = prefix; OAS = Origin AS; FC = Fully Consistent; PC = Partially Consistent; NC = Not Consistent; NR = Not Registered

Comparative Performance of Algorithms





Prefixes with Multiple Origin ASes

# Origin ASes	# Prefixes
1	476243
2	55673
3	10419
4	2683
5	965

For prefixes with two Origin ASes:

OAS1	OAS2	# Prefixes
FC + Stable	FC/PC + Unstable	23
PC + Stable	FC/PC + Unstable	41
NC + Stable	FC/PC + Unstable	104
NR + Stable	FC/PC + Unstable	0
Total		168

- Statistics of prefixes with two Origin ASes where the primary path is stable (with or without consistency in the registry), while the secondary (failover) path is transient (unstable) but consistent in the registry

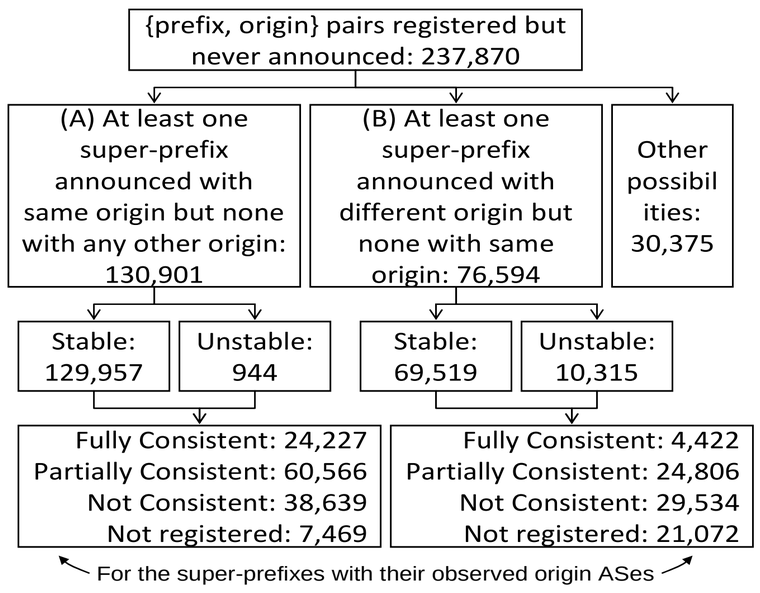
Prefixes with Multiple Origin ASes

# Origin ASes	# Prefixes
1	476243
2	55673
3	10419
4	2683
5	965

For prefixes with two Origin ASes:

OAS1	OAS2	# Prefixes
FC + Stable	FC/PC + Unstable	23
PC + Stable	FC/PC + Unstable	41
NC + Stable	FC/PC + Unstable	104
NR + Stable	FC/PC + Unstable	0
Total		168

- Statistics of prefixes with two Origin ASes where the primary path is stable (with or without consistency in the registry), while the secondary (failover) path is transient (unstable) but consistent in the registry

Analysis of Registered But Unobserved Routes

- Large number of {prefix, origin} pairs registered but never announced
- In most cases, super-prefixes are announced with the same origin AS (as in registered route) or a different origin AS
- Is it due to aggregation by customers' ISPs or by a higher tier ISP?
- Are some registry entries simply stale?
- Needs further investigation