The Resilience of the Internet to Colluding Country Induced Connectivity Disruptions

Peter Mell, National Institute of Standards and Technology
Richard Harang, U.S. Army Research Laboratory
Assane Gueye, University of Maryland

Presentation for the NDSS/SENT 2015

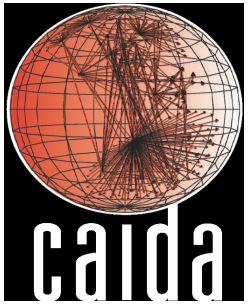
Research Focus

- In this study, we ask several questions:
  - Is the country to country Internet-based connectivity strength increasing over time?
  - To what extent can a group of collaborating countries
    - disconnect two other countries
    - isolate a set of countries from the Internet
    - break the Internet up into non-communicative clusters

Novel Contributions

- First study to construct a country to country connectivity graph of the Internet to evaluate security
- First study to evaluate the ability of countries to collude to harm other countries connectivity
- An example of how to take limited data and still produce rigorous results

Cooperative Association for Internet Data Analysis (CAIDA)



- Has a worldwide Internet monitoring network
- Provides *approximate* topological maps of the Internet
- Provides a map of autonomous system (AS) interconnectivity
  - ASs approximate the set of Internet Service Providers
- Provides a mapping of ASs to their country of registration

Our approach is to use this data to form country connectivity graphs and to explore how groups of colluding countries can disrupt the connectivity of other countries

http://www.caida.org (University of California, San Diego)

2014 CAIDA Worldwide Scanner Map ('Ark Monitors')

This set of scanners probe each IPv4 subnet every 2-3 days with random assignment

Snapshot taken 2014-08-26 from http://www.caida.org/data/monitors/monitor-map-ark.xml

Autonomous System Statistics

Year	Number of ASs	Number of Edges	Number of Scanners
2008	28,821	111,487	33
2009	32,037	127,762	42
2010	35,404	153,701	54
2011	38,732	177,891	59
2012	41,613	178,825	65
2013	44,390	213,883	89

Data Limitations

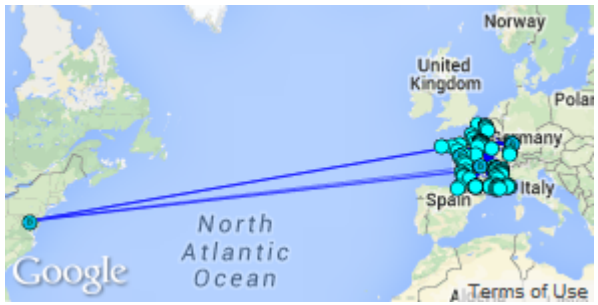
- Some routes may not be visible due to a lack of sensor coverage
- Some ASs can't be mapped to a country (.11%)
- Can't process indirect routes
- **Result**: We **do not see** all network paths
- **Consequence**: All of our results must bound the worst case (as opposed to providing strict answers)

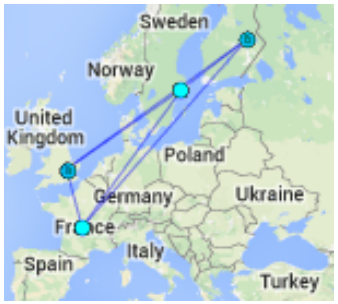
Additional Limitations

- We measure connectivity and not capacity
  - Consequence: We can't evaluate cascading failure of traffic being redirected due to failed routes
- We do not factor route policy into our calculations (removing the 'valley free' restrictions)
  - Rationale: Route policy can be quickly changed during emergency situations

Handling of Multinational Autonomous Systems

- Multinational ASs (MOAs) have points of presence in multiple countries
  - Approach: We map a MOAs to its country of registration
  - Rationale: Legal literature states that MOAs have to abide by the laws of their country of registration regardless of the physical location of the servers



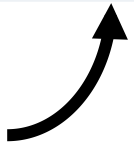


Map snapshots taken 2014-8-26, provided by CAIDA at http://as-rank.caida.org (mapping software credited to Google)

Country Connectivity Graph Statistics Using All Scanners

Year	Number of Countries	Number of Edges	Number of Scanners
2008	206	2235	33
2009	211	2343	42
2010	218	2644	54
2010	219	2925	59
2012	221	3138	65
2013	224	3452	89

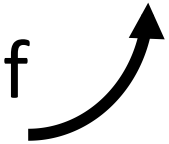
24 monitors were persistent across all years of investigation



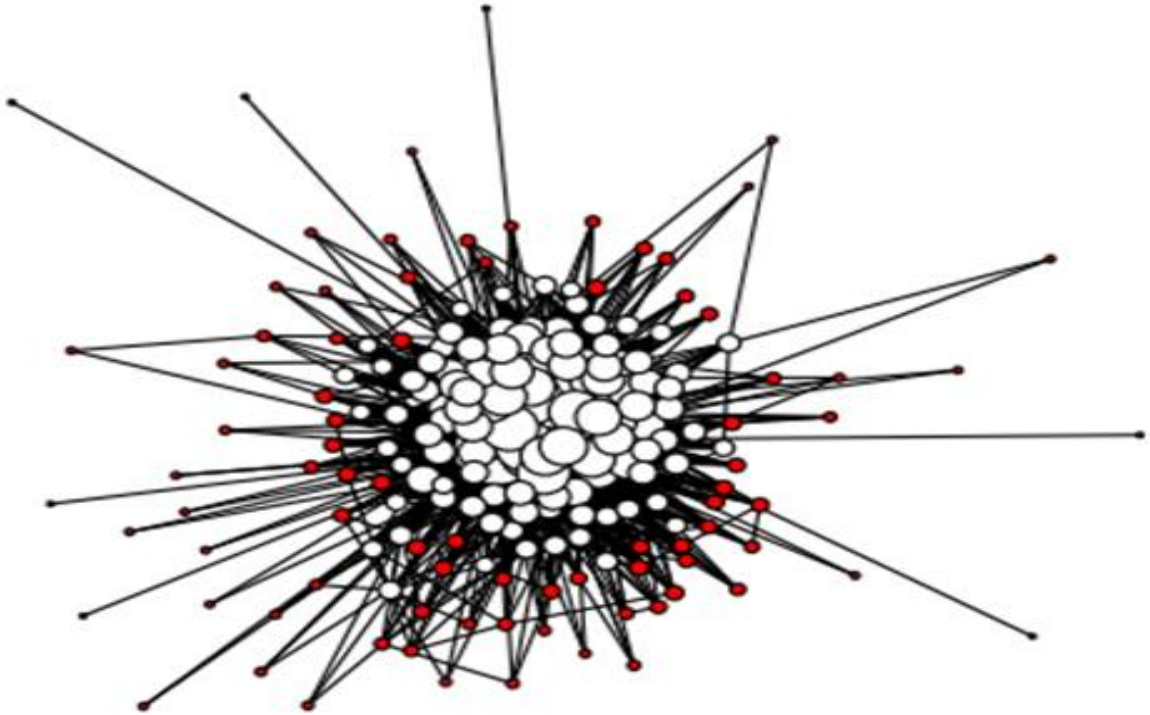
Country Connectivity Graph Statistics Using Only Persistent Scanners

Year	Number of Countries	Number of Edges	Number of Scanners	% Excluded Scanners
2008	206	2149	24	27 %
2009	210	2243	24	43 %
2010	218	2370	24	56 %
2011	219	2513	24	59 %
2012	221	2731	24	63 %
2013	223	2829	24	73 %

Exclusion of scanners represents a loss of data for discovering new network routes



Internet Map:
2013 Country Connectivity



Node sizes are proportional to their degree. The 84 red nodes have degree <= 10. Only 0.41 % of edges connect two red nodes. Graph shows negative assortativity.

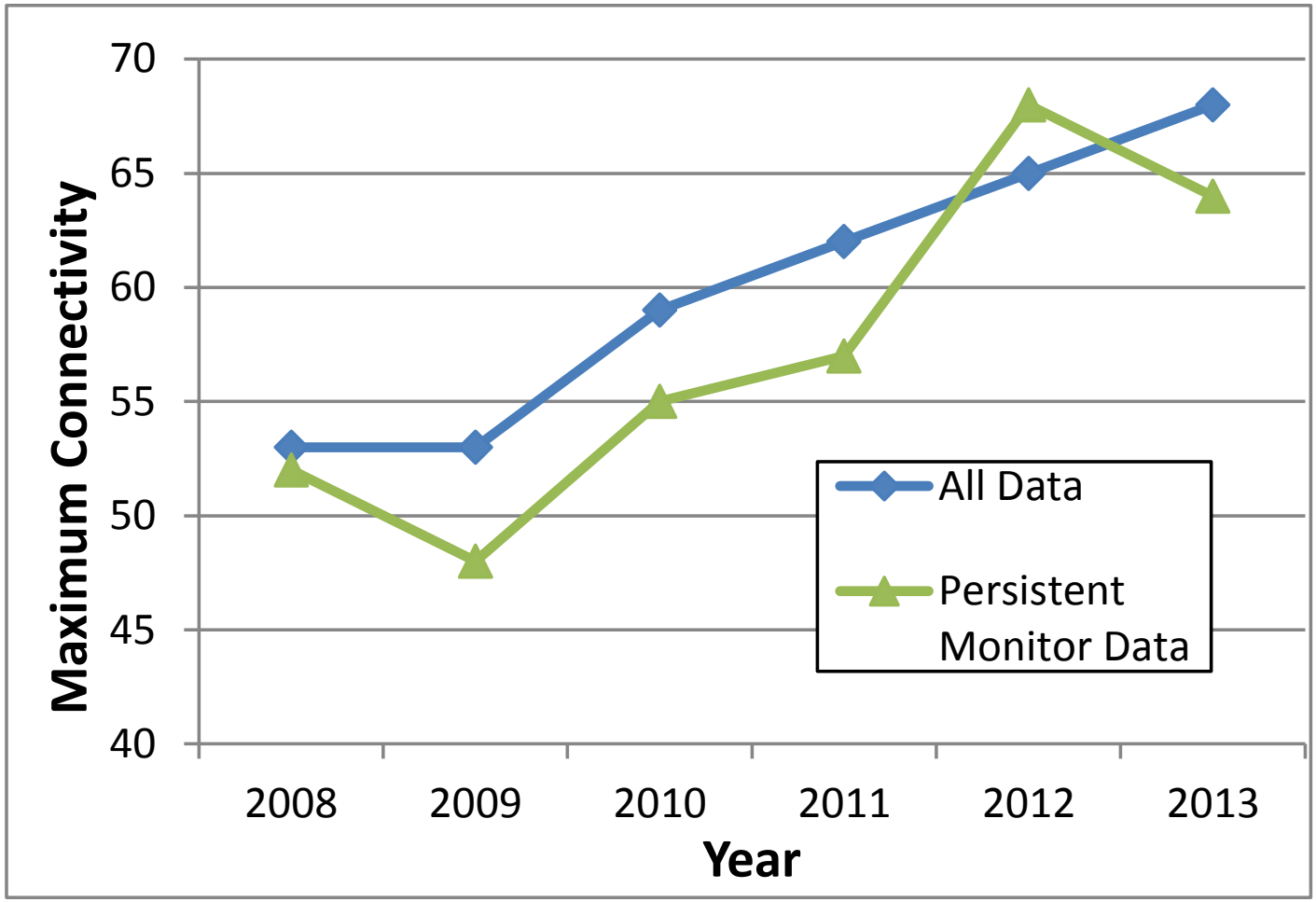
Security Questions

1. **Cutting Pairwise Communications**: What is the minimal number of colluding countries required to prevent two other countries from communicating?
2. **Country Isolation**: What is the maximal number of countries that can be cut off from the Internet by a group of colluding countries?
3. **Non-Communicative Clusters**: Into how many non-communicative clusters can a group of colluding countries divide the Internet?

Algorithm Overview

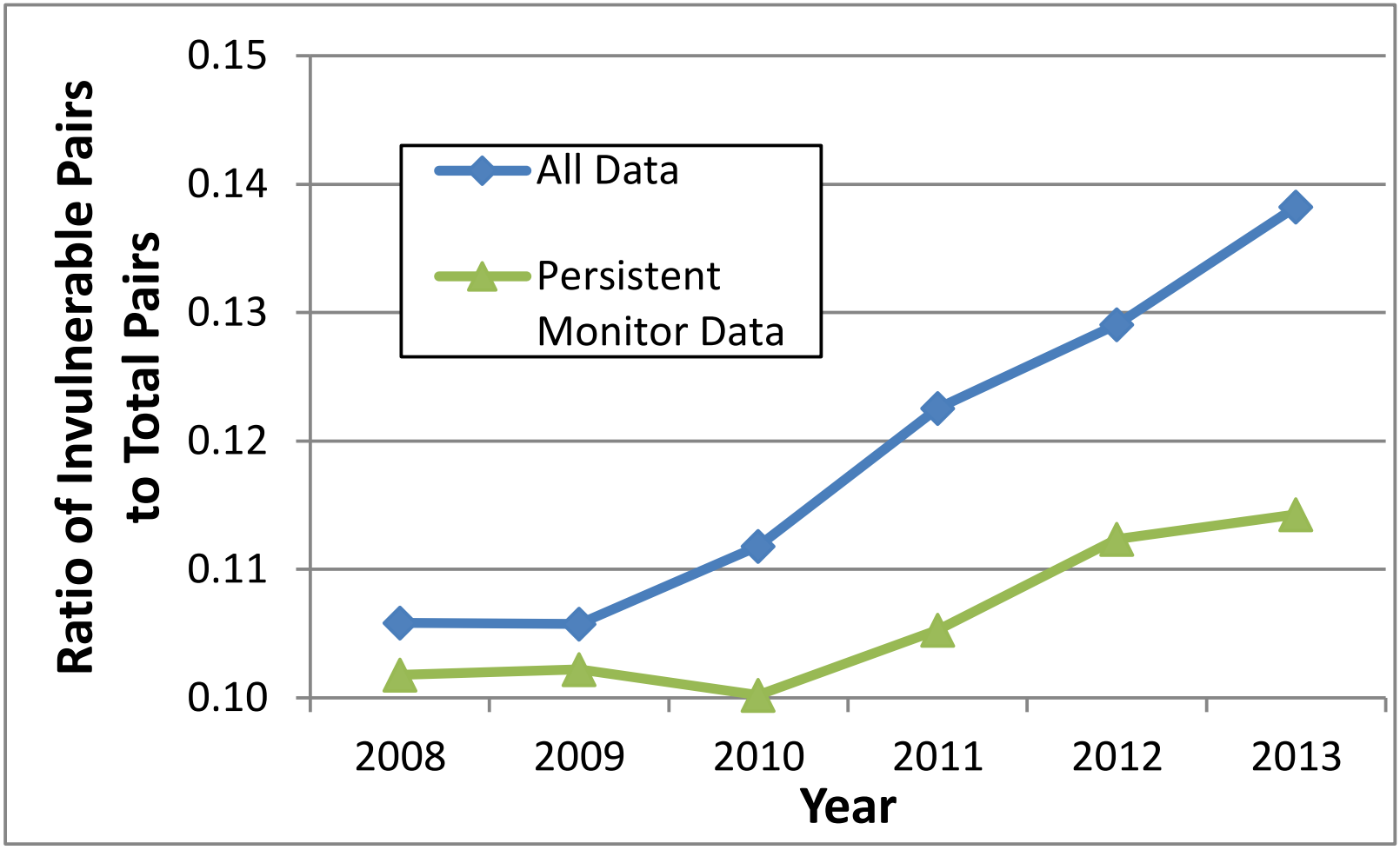
- **Security question 1**
  - Solvable through graph transformation to use flow based connectivity calculations (Ford/Fulkerson)
- **Security questions 2 and 3**
  - Solvable through vertex partitioning of the connectivity graph
  - problem is NP-Hard (i.e., exponential solutions)
  - we use a suite of 5 heuristics to obtain approximate answers (2 based on published approaches and 3 of our own design

Cutting Pairwise Communications: Maximum Connectivity



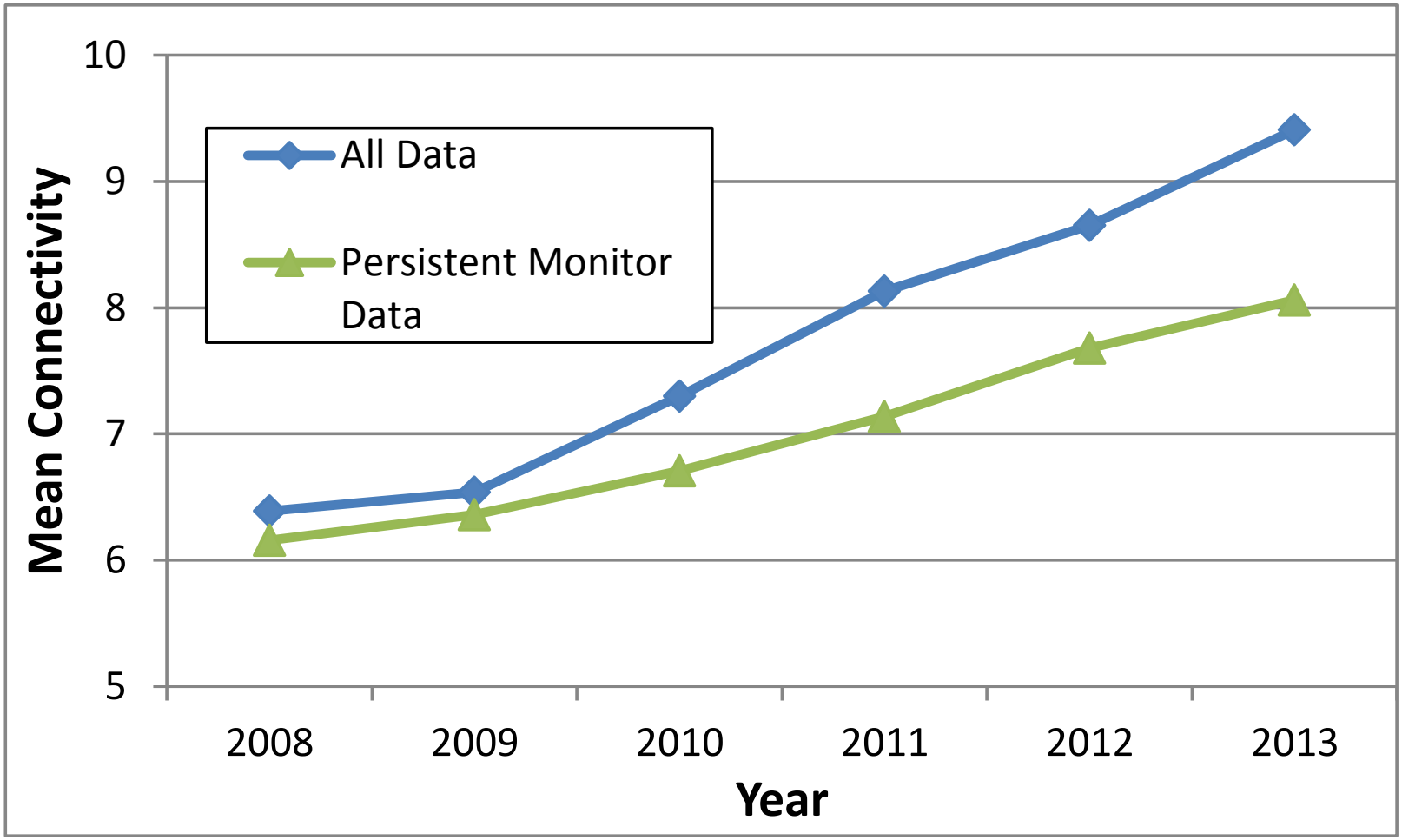
For highly connected countries, we see an increasing connectivity over time.
Note that the minimum connectivity stayed at 1 each year.

Cutting Pairwise Communications: Invulnerable Pairs



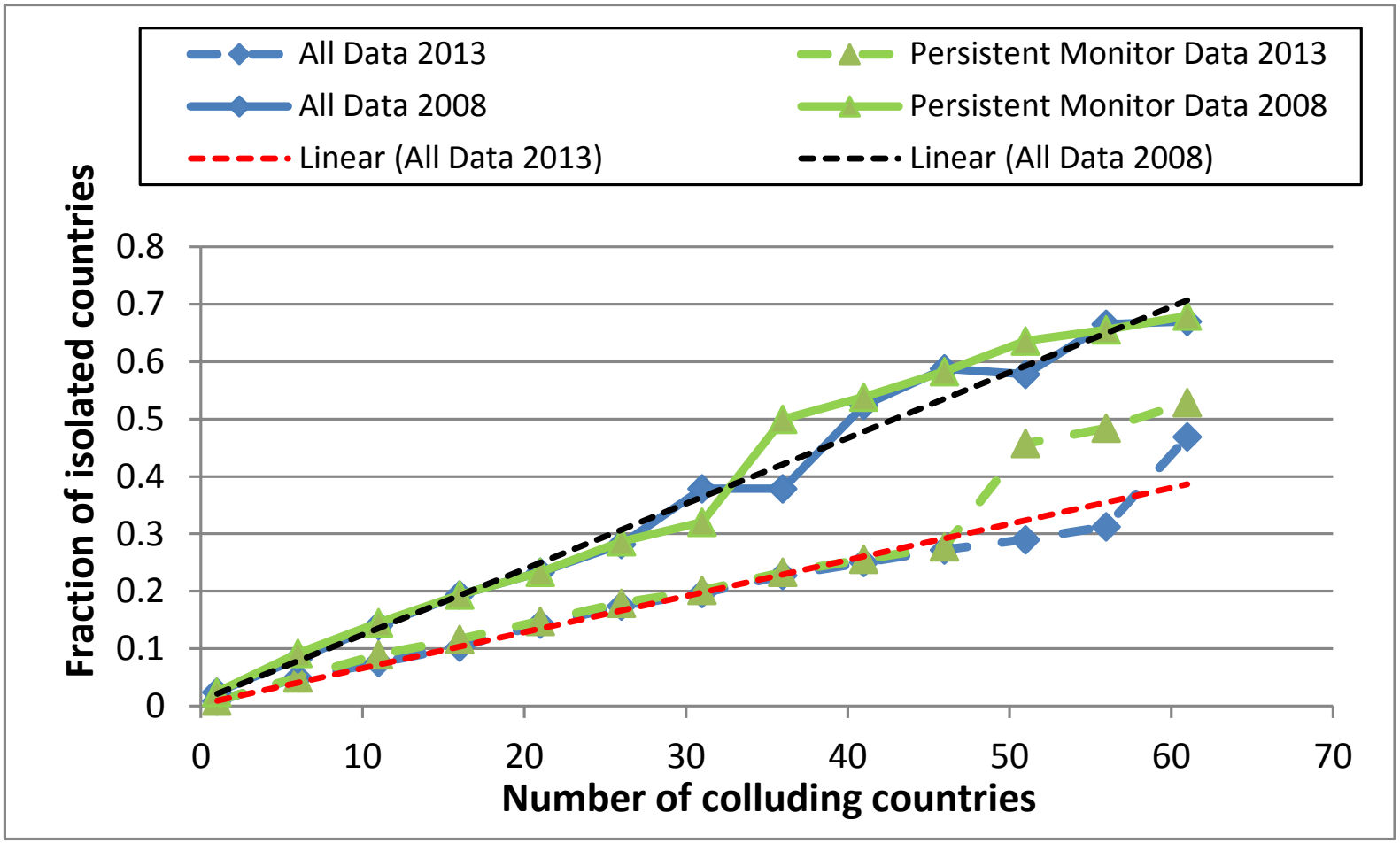
The number of adjacent countries increased over time.

Cutting Pairwise Communications: Mean Connectivity



The mean connectivity of countries increased over time.

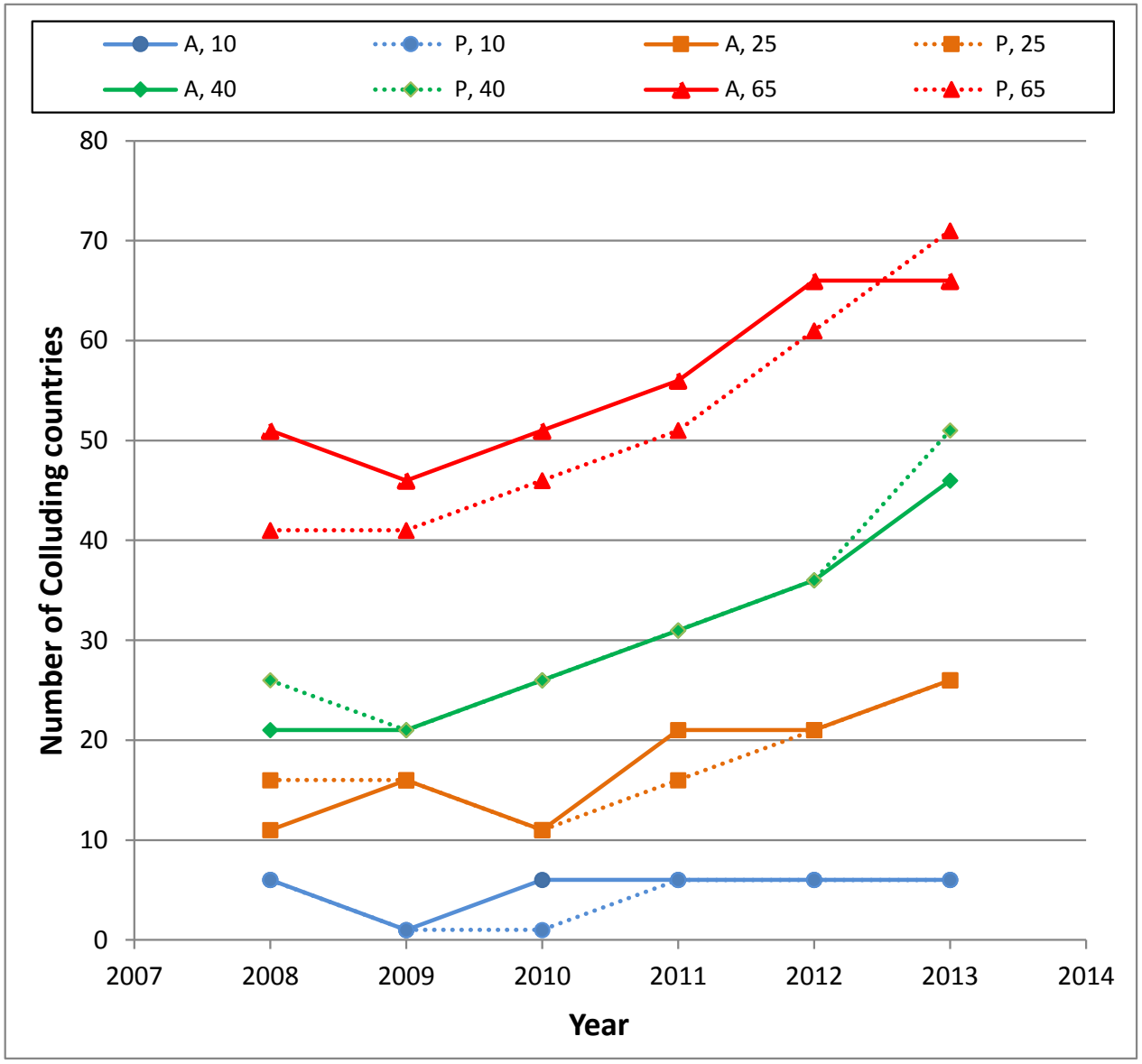
Country Isolation: Comparison of 2008 to 2013



It took more colluding countries to isolate a set fraction of countries when comparing 2008 to 2013.

Non-Communicative Clusters: Number of Colluding Countries Needed to Divide the Internet into a Certain Number of Clusters

Over time, more colluding countries were required to break the Internet up into a large number of clusters. However, this is not true for a small number of clusters.



Related Work

- Existing studies cover:
  - individual countries cutting themselves off from the Internet
  - accidental and deliberate failures of groups of autonomous systems
  - cascading router failures through shifting traffic flow
  - effects of routing policy on Internet robustness

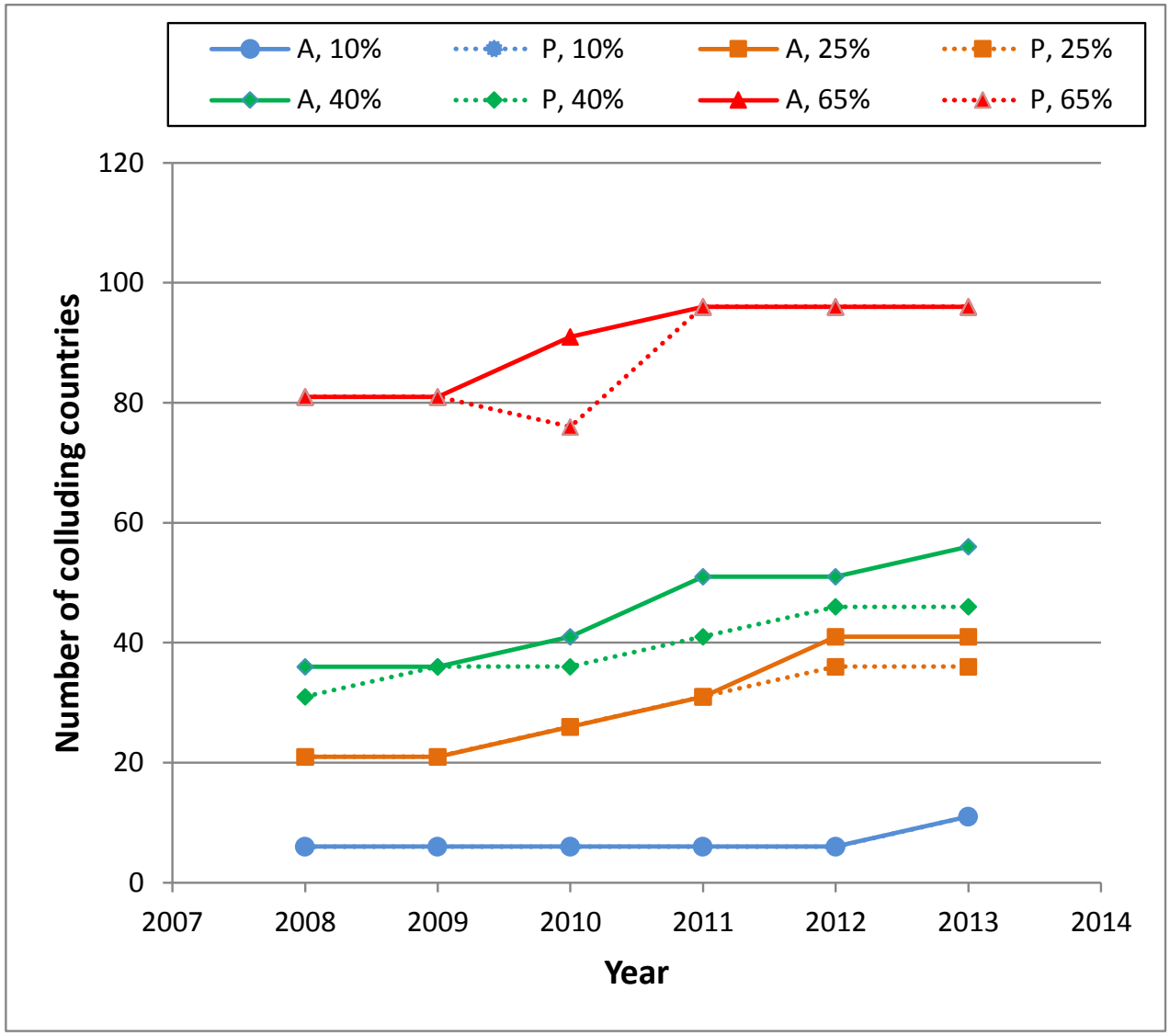
Summary and Conclusions

Overall, bounds analysis indicates that:

- the overall strength of country to country Internet connectivity is increasing
- it is feasible for a group of countries to
  - disconnect two countries
  - isolate a set of countries from the Internet
  - break the Internet up into non-communicative clusters
- the ability of countries to perform the attacks has diminished significantly from 2008 to 2013.
- countries that displayed higher initial vulnerability did not become significantly more robust over the time period of analysis.

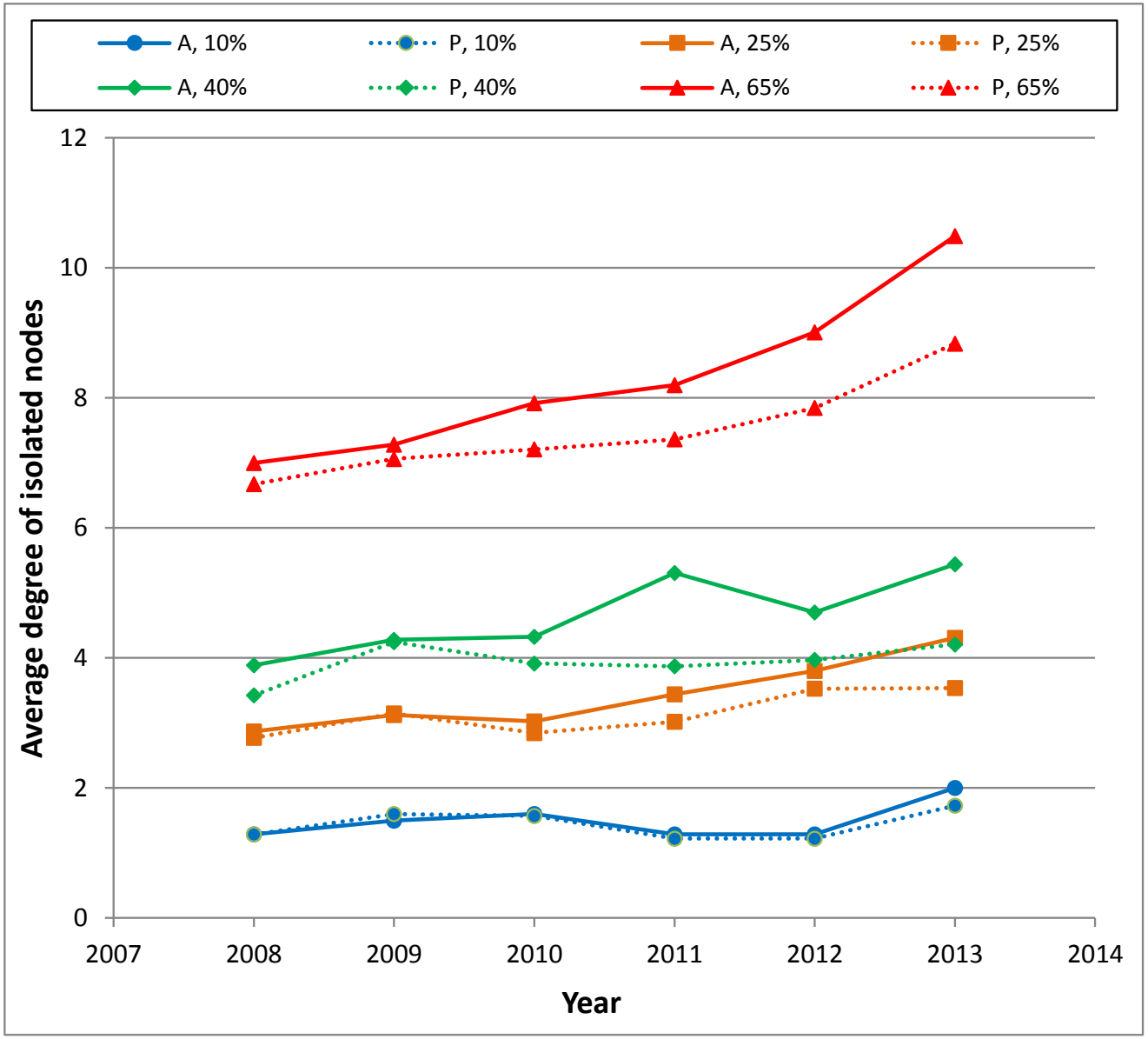
Country Isolation: Number of Colluding Countries Needed to Isolate a Fraction of Nodes

The number of colluding countries needed to isolate 10% of the countries almost did not increase from 2008-2013 (but it did for larger percentages).



Country Isolation: Average Degree of Isolated Nodes

The average degree increases over time for larger percentages of the network but not as much for the smaller percentages.



Non-Communicative Clusters: Number of Clusters vs. Number of Colluding Countries

The number of clusters into which the Internet can be broken by a fixed size set of colluding countries decreases every year.