# Beyond Technical Solutions

## Understanding the role of governance structures in Internet routing security


*Dr Milton Mueller, School of Public Policy, Georgia Institute of Technology*
*Dr Brenden Kuerbis, School of Public Policy, Georgia Institute of Technology*


## Introduction and research design

Studies of routing security are not adequately supported by social science studies of the actual organizational arrangements and practices of network operators. To help answer these questions, this study explores whether distinct ***governance structures*** among networks are correlated with variation in the number and severity of ***routing anomalies*.**

### Independent variable: Governance structures

Governance structures are defined (Williamson, 1985; 1996) as *the institutional framework in which contracts are initiated, negotiated, monitored, adapted, enforced and terminated.* The three basic categories of governance are *markets*, *hierarchies* and *networks*. Internet routing is networked governance, involving decentralized decision making among thousands of autonomous network operators. We analyze governance structures on three levels:

***Macro-level*** - institutions affecting operators, including formal laws, the policies and contracts of the IP address registries, Internet standards and community norms.

***Meso-level*** - networked governance structures manifested in AS routing relationships and routing registries (IRRs) that develop within the constraints set by the macro-level institutions and micro-level incentives.

***Micro-level*** - network operators' firm-level decisions about routing policy and security technologies.

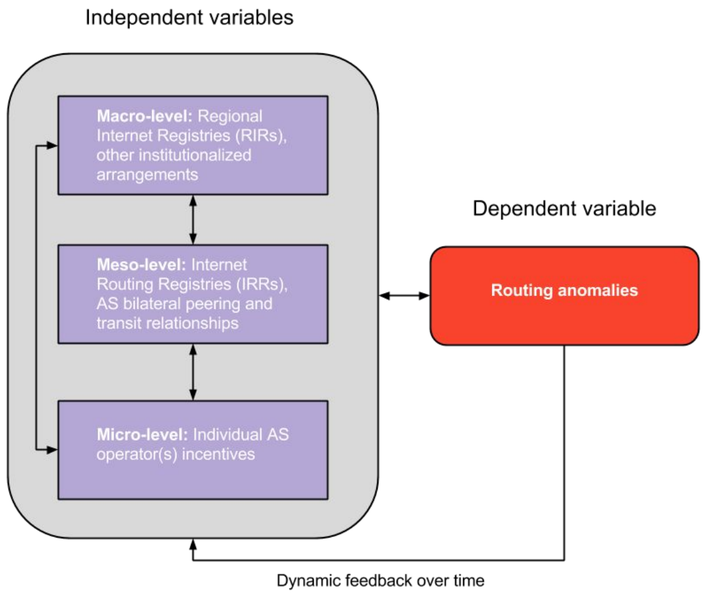
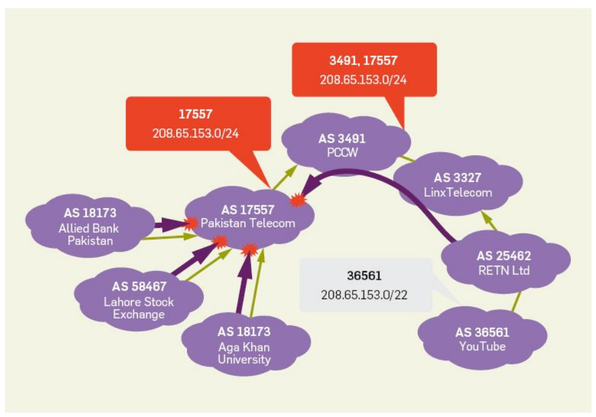



**Figure 1: Analytical model**

### Dependent variable: Routing anomalies

Measuring routing anomalies is an active area of computer science research, with numerous academic and commercial monitoring systems producing data. Anomalies fall into two general categories, use of routing resources (IP prefixes and AS numbers) and route (i.e., AS_path) manipulation, and can be identified by monitoring observed routing announcements inconsistent with 1) the BGP, 2) information contained in resource and routing repositories, and 3) expected business relationships between operators. Monitoring systems have flaws that impact our research design, including the incompleteness of the observed AS-level structure of the internet, over- and under-estimation of anomalies, and identification of perpetrators and new anomaly types.




**Source:** Goldberg, S. (2014). Why Is It Taking So Long to Secure Internet Routing? *Communications of the ACM*, *57*(10), 56–63.

An example of a routing anomaly: In 2008, ordered to block access to YouTube, Pakistan Telecom (AS17557) advertised a route for 208.65.153.0/24 (Youtube prefix) to its provider, PCCW (AS3491) which inadvertently propagated it. Because of the way the interdomain routing protocol (BGP) works, this announcement caused most routers to send traffic intended for YouTube to Pakistan Telecom, making YouTube invisible to large parts of the world for ~3 hours.

## Initial findings

Data from Argus (Tsinghua U), Routeviews (U of Oregon) and CAIDA (UCSD) yielded routing & anomaly data for 51,436 ASes over the 41 months from June 2011 to October 2014. Argus reports resource origin, AS adjacency and routing policy anomalies. Figure 2 shows how AS relationships were modeled. The directional graph reflects AS economic and organizational relations, not actual packet flows (which are bidirectional).

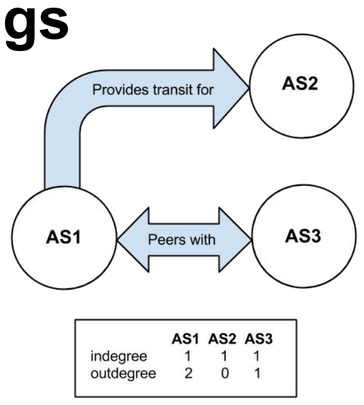
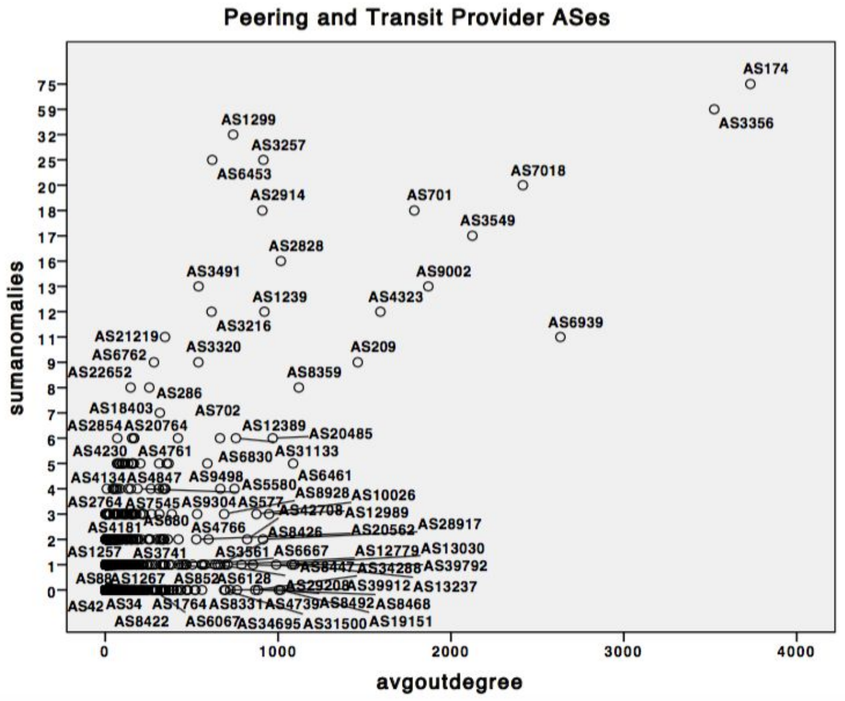



**Figure 2: AS relationship model**




The strongest factors in susceptibility to routing anomalies appear to be the number of peering and transit relationships an AS maintains with other ASes, followed by the number of prefixes it announces. Among transit and peering ASes, the data indicate a positive (. 108**) statistically significant correlation between the number of routing anomalies experienced by an AS and the number of prefixes it advertises.

If the test group is limited to AS's that have experienced one or more anomalies, the positive correlation strengthens to .286** We found the number of routing anomalies to be correlated with number of out-degrees, 0.269**. For ASes that have experienced one or more anomalies, the positive correlation strengthens to 0.469**. But Fig. 4 indicates notable variation in the number of anomalies among ASs. Can governance structures explain this variation?

### Internet Registries: Key institutions

*Internet Routing Registries (IRRs)* allow AS's to register their own routing policies and validate routing policies of other AS's based on standard formatting (RPSL). IRRs are a key meso-level networked governance structure. They exhibit important differences in the types of parties that operate them, how they are sustained economically, and policies governing data registration, replication and use. A more thorough examination of the governance and economic characteristics of IRRs can be related to observed differences in data quality (see Khan et al., 2013) and the number of routing anomalies.

*Regional Internet Registries (RIRs)* allocate and assign IP address blocks and AS numbers to organizations. Several technologies and operational practices try to leverage their status as authoritative, hierarchical sources of globally unique identifiers to improve routing security. These include RPKI, which can be affected by differing RIR and national policies, and BGPSEC which is being standardized. Recent developments suggest one RIR is seeking to link RPKI data and its own routing registry, while operators are leveraging differences in RIR's IP address registration policies to validate IRR data.

Together, IRRs and RIRs illustrate networked and hierarchically organized governance structures which impact individual operator decisions. While researchers have identified the conflicting incentives and operational tradeoffs (Kuerbis & Mueller, 2011) and technical risks (Cooper et al., 2013) of routing security technologies like RPKI, this research takes an interdisciplinary approach toward understanding the broader institutional framework that impacts routing security.


This research is supported by the U.S. National Science Foundation, Award Number SES-1422629.