Modeling BGP Attacks

And Their Impacts on Routing Performance

Problem Statement & Summary of the Study

- **Border Gateway Protocol (BGP) is used to exchange routing and reachability information between networks**
- **Several BGP vulnerabilities are known and often result in attacks (both inadvertent and malicious)**
- **This study examines the impact on network performance if such vulnerabilities are exploited**
  - **Large scale simulation of BGP peering session attacks**
  - **Attack impact amplification attributable to BGP protocol features and routing policies**
  - **Topology-aware attacks**
  - **New insights lead to making better recommendations for BGP security**

This research was supported by the Department of Homeland Security under the Secure Protocols for the Routing Infrastructure (SPRI) program and the NIST Information Technology Laboratory Cyber and Network Security Program.

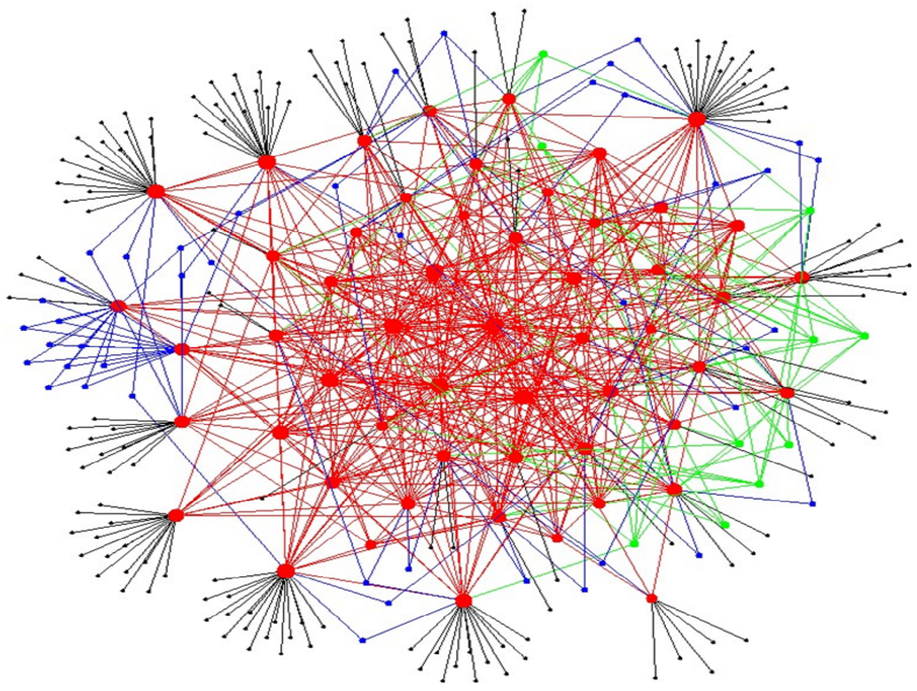
BGP Attack Tree Enumeration

- Broad classification of attacks (IETF drafts):
  - Establish Unauthorized BGP Session with Peer
  - Originate Unauthorized Prefix/Attribute into Peer Route Table
  - Change Path Preference of a Prefix
  - Conduct Denial/Degradation of Service Attack Against BGP Process
  - Reset a BGP Peering Session
  - Send Spoofed BGP Message

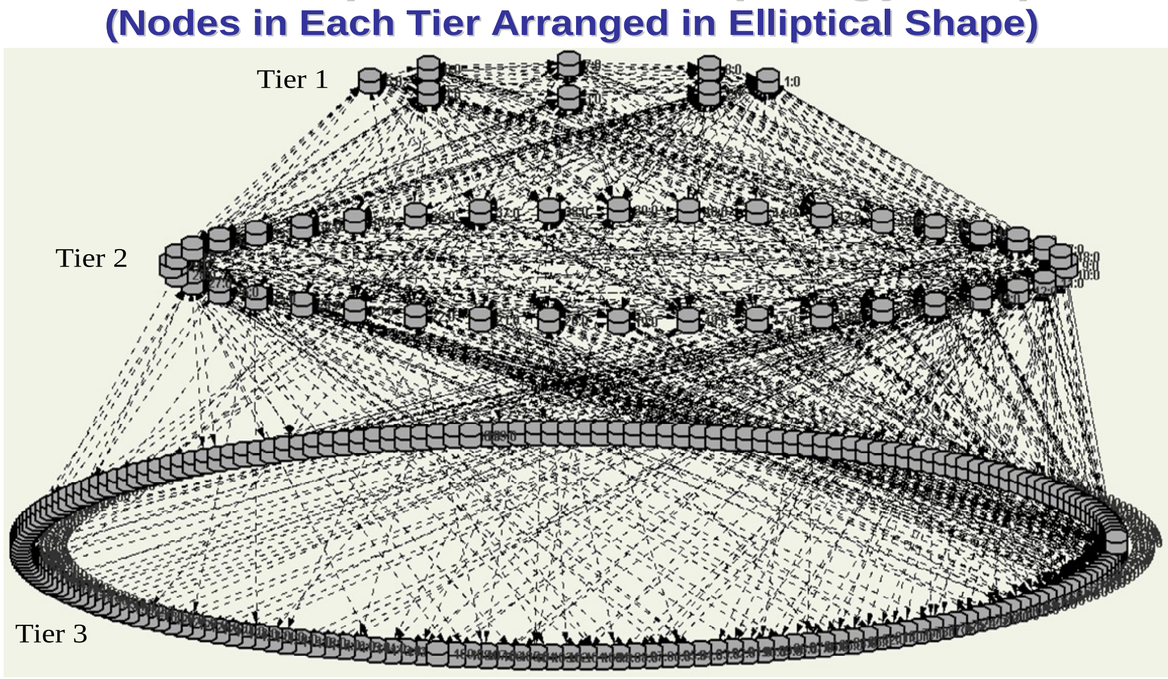
Peering Session Attack Model in Our Simulation Experiments:

- 256 nodes & 753 links – mesh network with three Tiers
- Type of attack: BGP session attacks (by spoofed TCP reset)
- Total attack duration = 500 sec
- # Attack intervals = 50 (each is 10 sec)
- Prob. of success for each attack attempt = 25%

Down-Sampled/Pruned Topology Graph

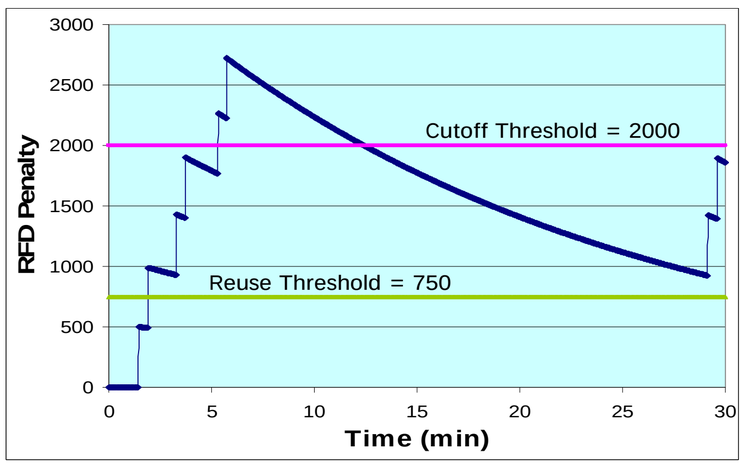


Down-Sampled/Pruned Topology Graph
(Nodes in Each Tier Arranged in Elliptical Shape)



Route Flap Damping (RFD): How It Works

(MRAI = 30 s)



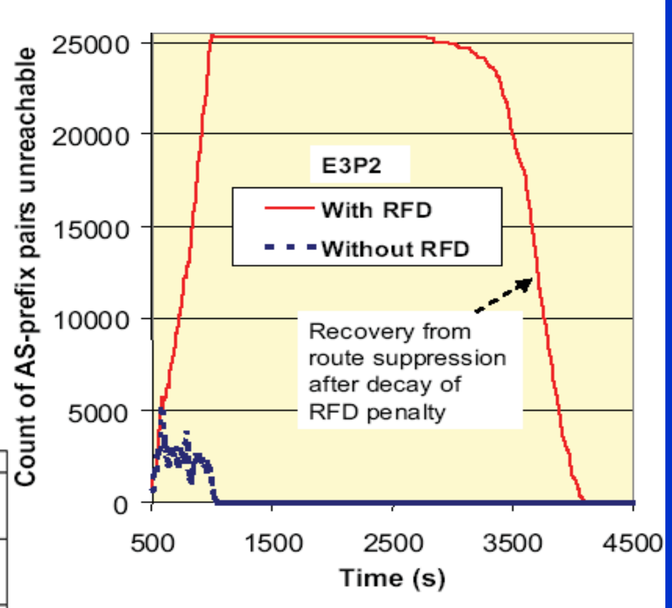
- The update interval is effected by MRAI
- Attackers need to successfully attack one of the BGP peering sessions on the preferred path for the penalty to go higher
- 30 sec MRAI allows enough time for the damaged BGP session to recover within the MRAI
- The waves of attacks would be spaced at intervals equaling approximately MRAI
- To achieve prolonged AS isolation, it is enough if only some of the attacks succeed

Count of AS-Prefix Pairs Unreachable

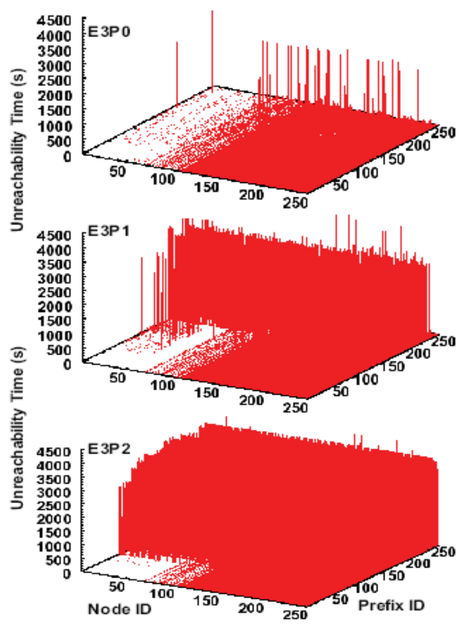
Policy and Topology of Attack:

	Rule	Comments
Policy 1	[U|T]*[D|T]*	All links within a Tier are T (none are P)
Policy 2	{[U|T]*[D|T]*} OR {[U]*[P]?[D]*}	All links within Tier 1 are T, but all most all links in Tier 2 are P's

Experiment	Attack region	Policy
E1P0	All links subjected to attacks	no Policy
E1P1	- do -	Policy 1
E1P2	- do -	Policy 2
E2P0	T1-T1 and T1-T2 links subjected to attacks	no Policy
E2P1	- do -	Policy 1
E2P2	- do -	Policy 2
E3P0	Only T2-T3 links subjected to attacks	no Policy
E3P1	- do -	Policy 1
E3P2	- do -	Policy 2

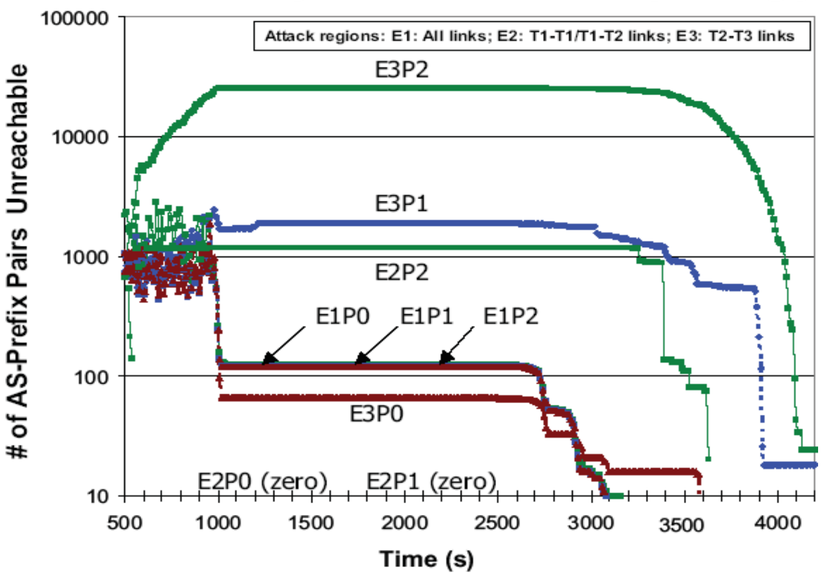


AS-Prefix Unreachability Time Vs. Policy



- As the routing policy gets more restrictive (P0 to P1 to P2), the unreachability under attacks gets worse accordingly.

Unreachable Vs. Time: Sensitivity to Attack-Topology and Policy



- Attacking the peering sessions on the links to stub nodes (as in E3) has the worst impact on unreachability.
- RFD has the effect of prolonging the impact of the attacks

Recommendation: BGP graceful restart can significantly reduce the impact of attacks on peering sessions.