Analysis of BGP Update Surge during Slammer Attack

Mohit Lad
Computer Science Dept,
Univ. of California,
Los Angeles, CA USA
mohit@cs.ucla.edu

Beichuan Zhang
USC/ISI
Arlington, VA. USA
bzhang@isi.edu

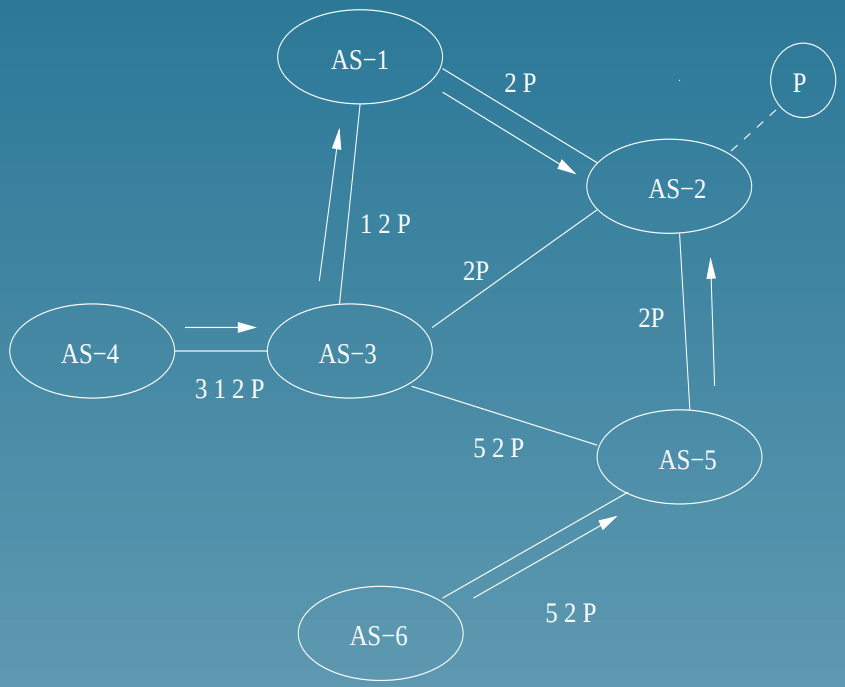
Xiaoliang Zhao
USC/ISI,
Arlington, VA. USA
xzhao@isi.edu

Dan Massey
USC/ISI,
Arlington, VA. USA
masseyd@isi.edu

Lixia Zhang
Computer Science Dept,
Univ. of California
Los Angeles, CA USA
lixia@cs.ucla.edu

December 27, 2003

Background of Border Gateway Protocol



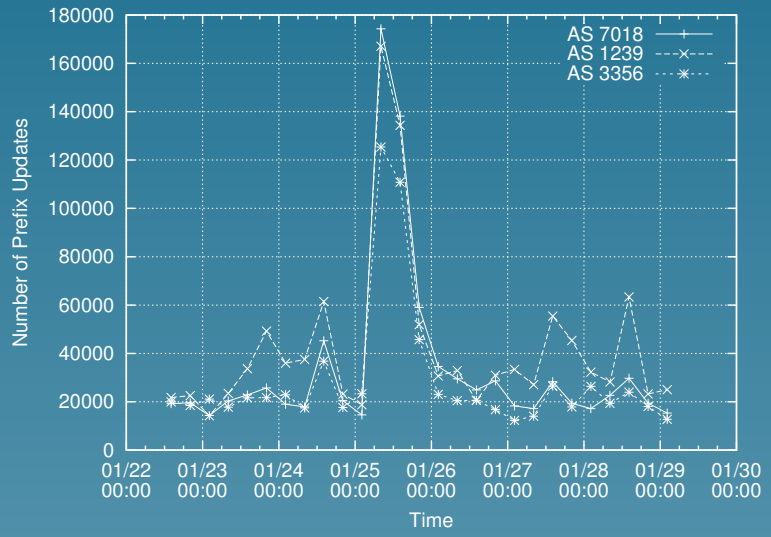
- BGP is a path vector protocol used by AS to exchange routing information.
- Prefix P advertised by AS-2.
- Peers of AS-2 in turn advertise the route to P.
- Note that AS-3 uses a longer path to reach P, though a shorter path exists.

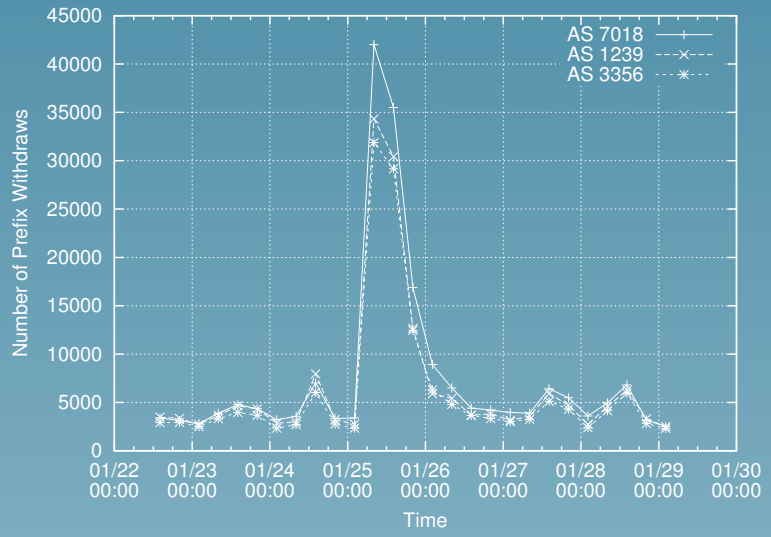
Policies are applied at the incoming routes and outgoing routes.

Background of SQL Slammer Worm attack

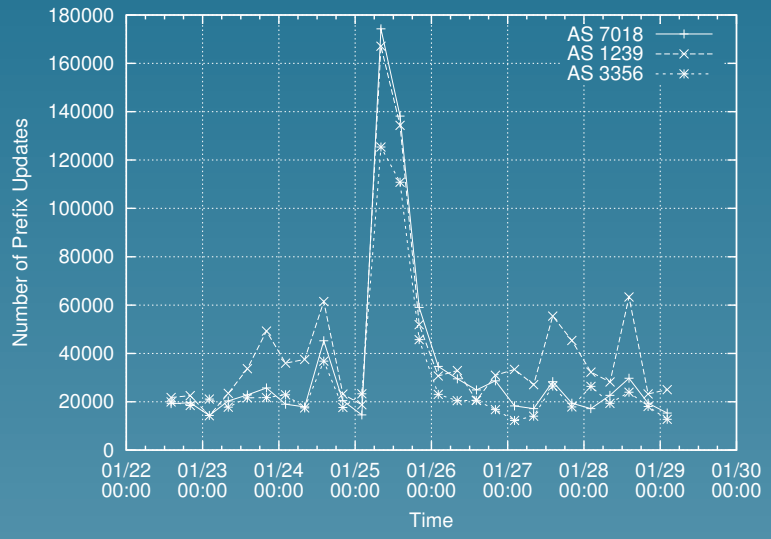
1. Started infecting hosts with known SQL server vulnerability around 5:30 am GMT on Jan 25, 2003
2. Infected machines generated traffic towards seeming random destinations
3. 75,000 hosts were infected in 30 mins, reported as the fastest spreading worm
4. Internet health report: Some AS-AS peering operating above critical thresholds

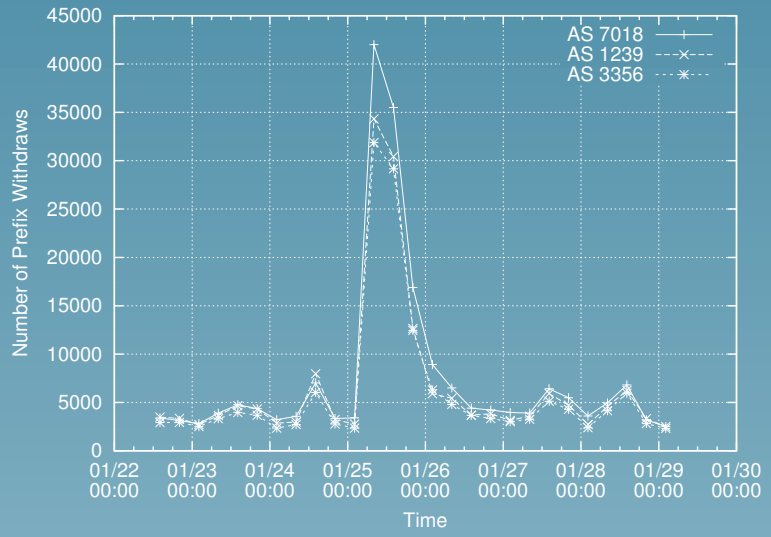
Effect of Slammer on BGP





Effect of Slammer on BGP

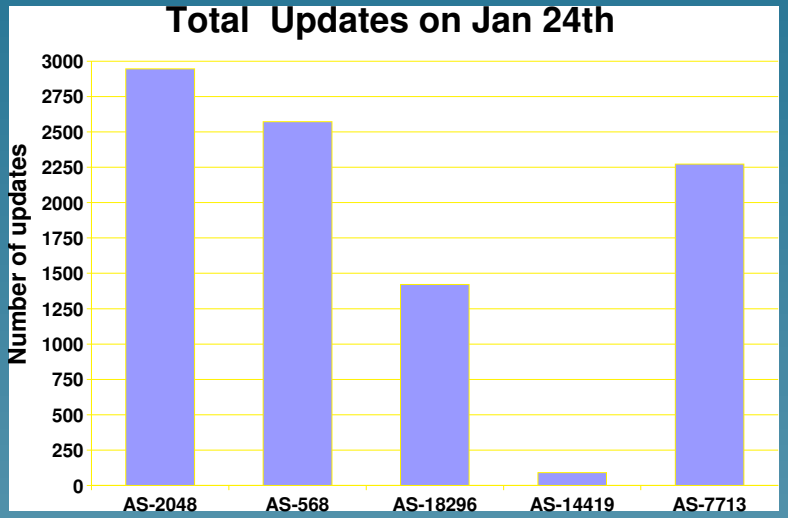


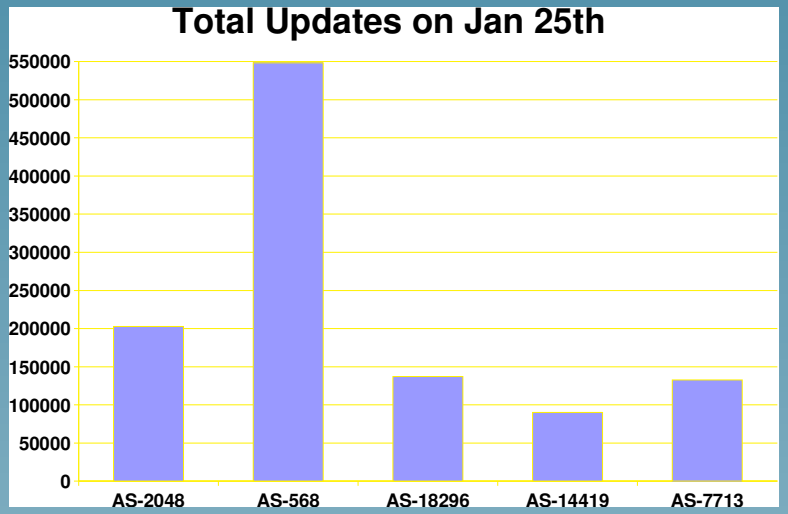


1. The number of updates observed at the BGP monitoring points from RouteViews shows a sharp spike co-inciding with the worm attack

2. The number of withdraw messages also shows a spike compared to other days

Analysis of BGP updates

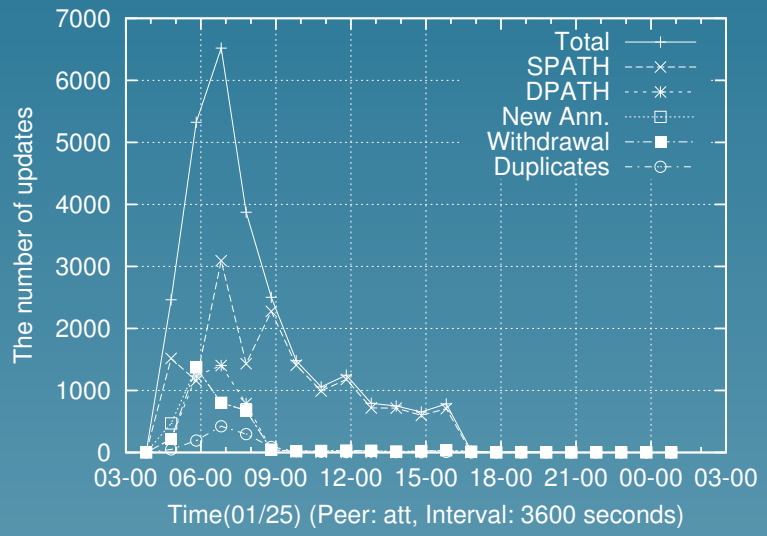




- A small number of ASs contributed a high percentage of updates
- A small set of edge prefixes contributed to a high percentage of updates
- AS 18296 advertising 30 prefixes (0.02% of total prefixes) contributed 1.7% of total updates
- AS 568 and AS 18296 together contributed 5% of the total updates

Classification of updates

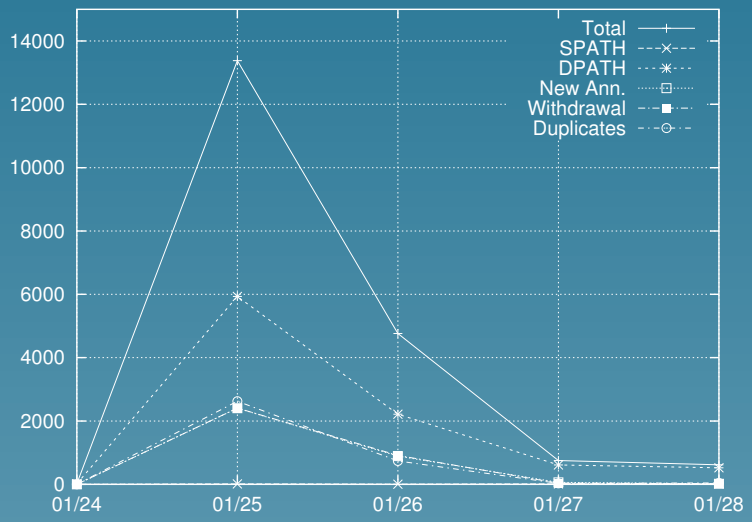
AS 568



1. The AS path did not change for a majority of updates for AS 568

2. Intra-network changes (Aggregator attribute) propagated to the rest of the Internet

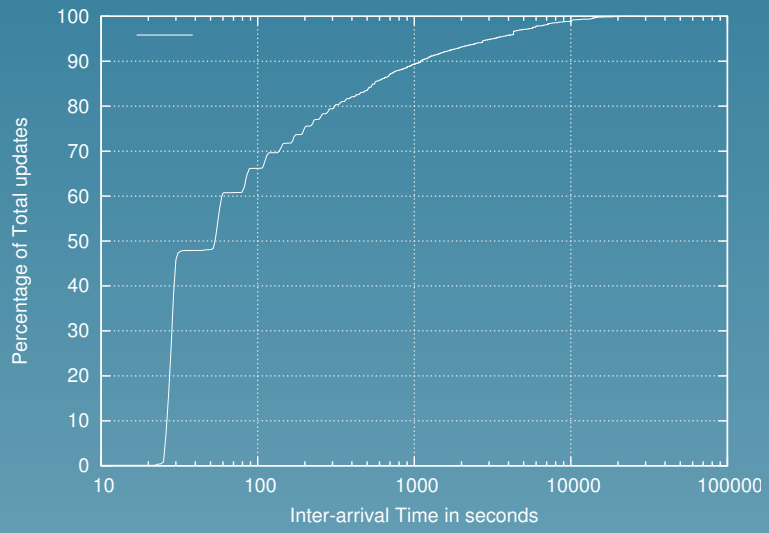
AS 18296



1. Majority of updates for AS 18296 were due to change in AS paths

Summarizing..

- Slammer caused a lot of globally observed BGP update activity on prefixes originating from edge Autonomous Systems like AS 18296, and AS 568.
- Frequent route changes on these prefixes were observed, e.g. for AS 18296 shown below



- Route Flap Damping had been proposed for
  1. Reduce router processing load caused by instability
  2. In doing so, prevent sustained routing oscillations

Enter Route Flap Damping

- Each router maintains a damping penalty per prefix per peering session
- BGP update messages increase the damping penalty, amount of increase may vary based on type of updates
- Penalty also decreases exponentially with time
- If penalty crosses a *supress threshold*, the incoming route is supressed
- When penalty falls below a *reuse threshold*, the route is accepted again

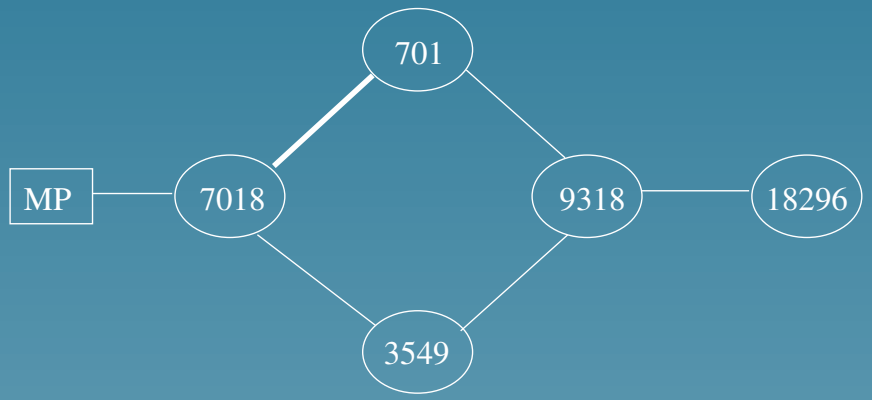
Damping parameters

Damping Parameter	Cisco	Juniper
Withdraw Penalty	1000	1000
Readv. penalty	0	1000
Att. change penalty	500	500
Suppress threshold	2000	3000
Half time (min)	15	15
Reuse threshold	750	750
Max suppress time (min)	60	60

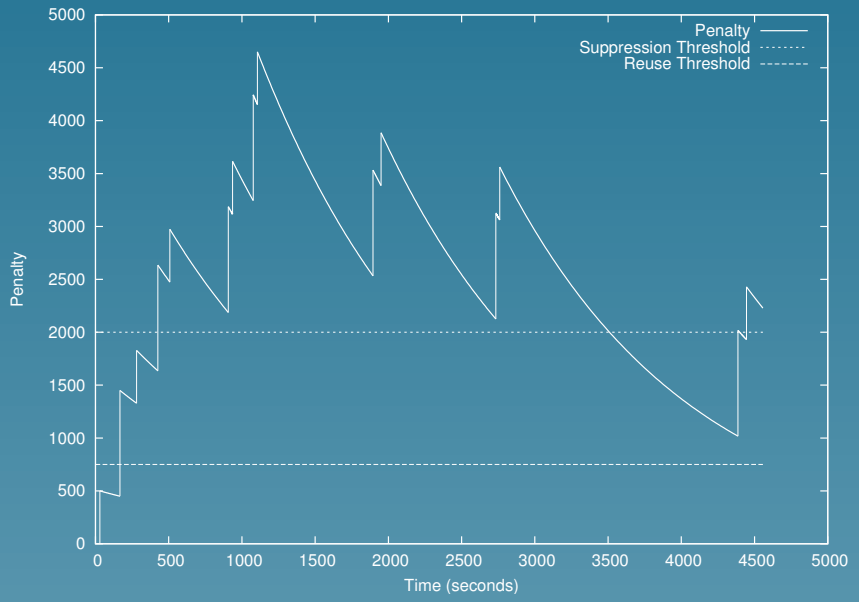
Table 1: Default parameters for route flap damping

Is damping widely deployed in the Internet ?

Case study from BGP logs



(a) Topology in Case 1



(b) Damping Penalty on link between AS 7018 and AS 701

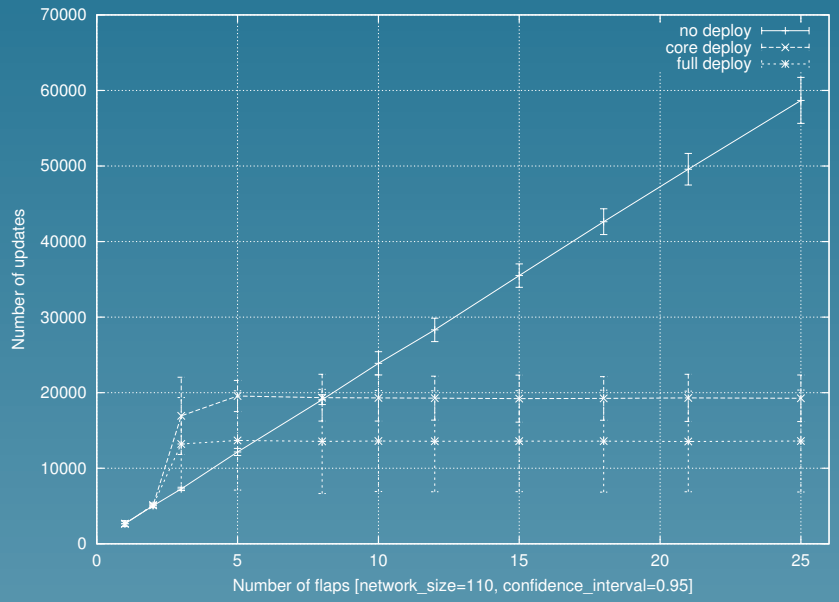
Figure 1: Case study of peering between AS7018 and AS701

Damping could not have been on in some cases.

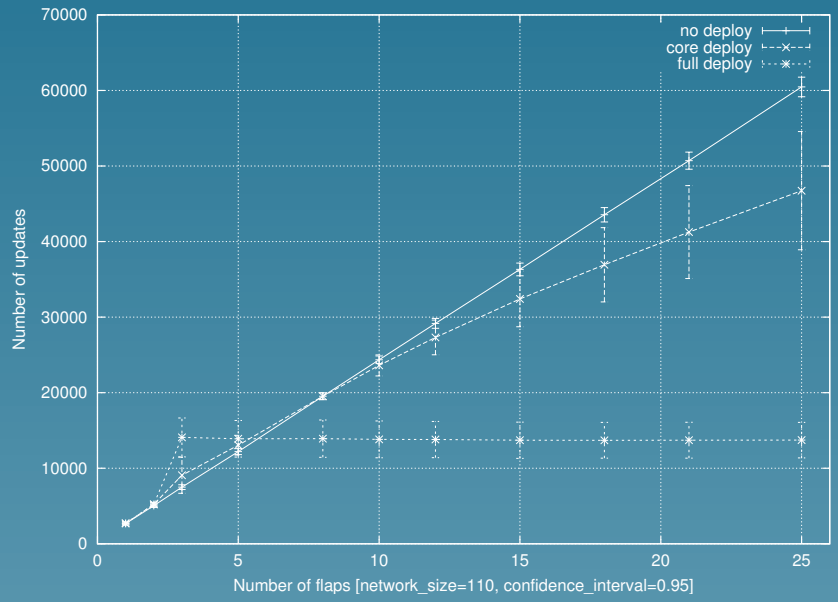
Partial Deployment of Damping: Simulation Setup

- We examined the effectiveness of partial deployment of damping under a Slammer like situation, using a simulation setup on Internet derived topology of 108 nodes
- Randomly chose one AS from topology as *flapping source* and this source withdrew its path every 100 seconds and reannounced every 50 seconds
- Flapping source started withdraw/announce sequence after 1000 seconds, giving the network enough time to converge
- We ran the simulation from 1 to 25 such withdraw/announce sequences

Partial Deployment: Results



(a) Flapping source attached to core



(b) Flapping source attached to edge

Figure 2: Number of Updates

The total number of updates observed with partial deployment and edge instability, does not reduce compared to that with no deployment.

Conclusions

- SQL Slammer attack produced a surge in BGP activity; a small set of edge AS's resulted in a high percentage of these updates
- Local changes should be kept local and not allowed to propagate outside the network
- Need further understanding of the effectiveness of BGP damping under various scenarios

Questions

Further information

- FNIISC project at http://fniisc.nge.isi.edu
- Beyond BGP project at http://www.beyondbgp.net