MOTIA Final Conference

Rome - 29 March, 2012

Developing Scientific Foundation for CIIP and Dependency Analysis: Questions for Discussion

Luciano Lenzini
Department of Information Engineering
University of Pisa

Issue

Are there “laws of nature” in cyberspace that can form the basis of scientific inquiry in the previous mentioned fields (i.e. Critical Information Infrastructure Protection)? *Are there mathematical abstractions or theoretical constructs that should be considered?*

I will discuss this issue by making reference to the Internet infrastructure

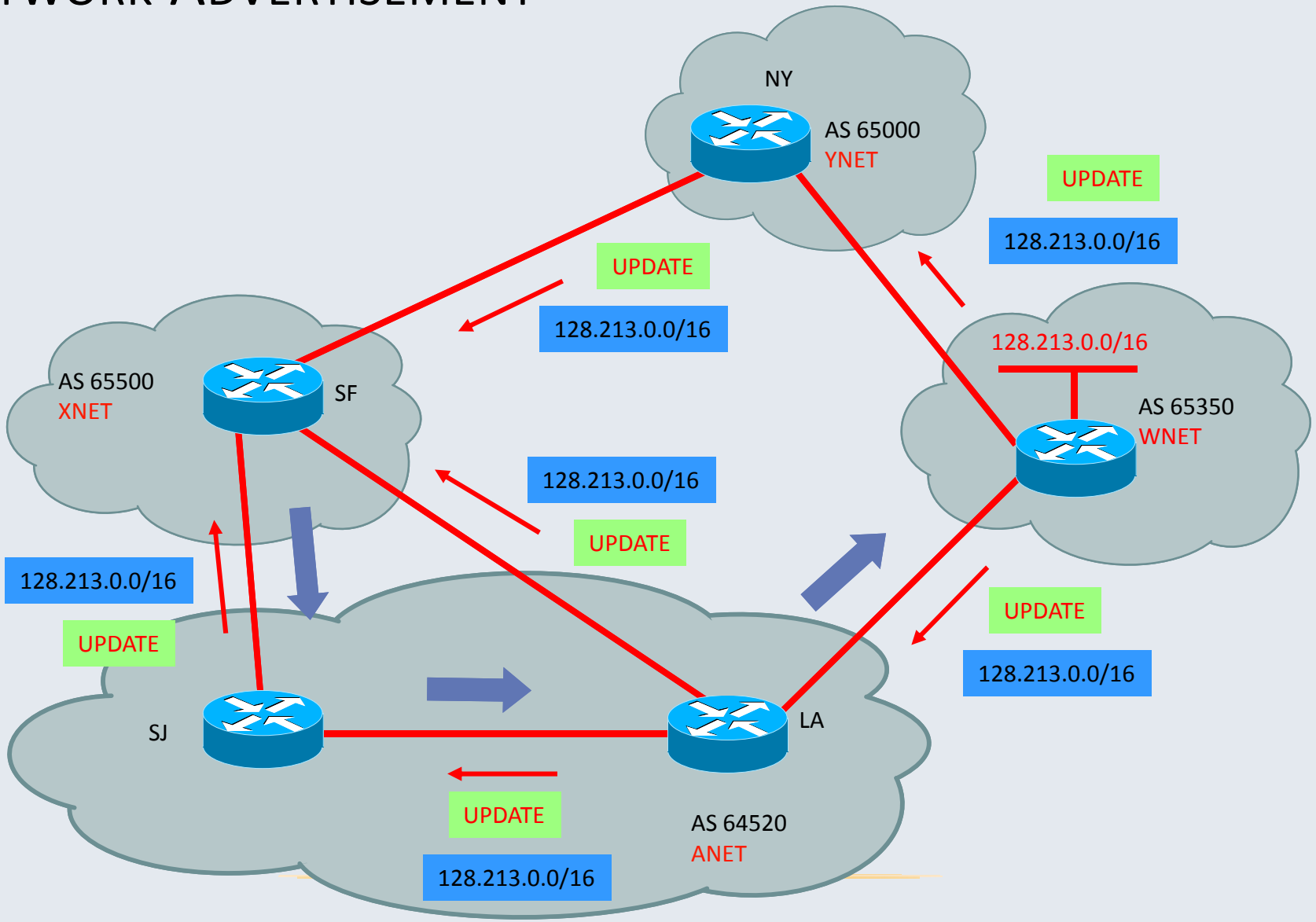
How is the Internet 'Glued' Together?

- ✓ Internet is currently partitioned into more than 40.000 Autonomous Systems (ASes) interconnected via the Border Gateway Protocol (BGP) which is a critical protocols for the Internet

- ✓ BGP was designed long before security became a serious issue for the Internet

BGP retains a number of vulnerabilities

Network Advertisement

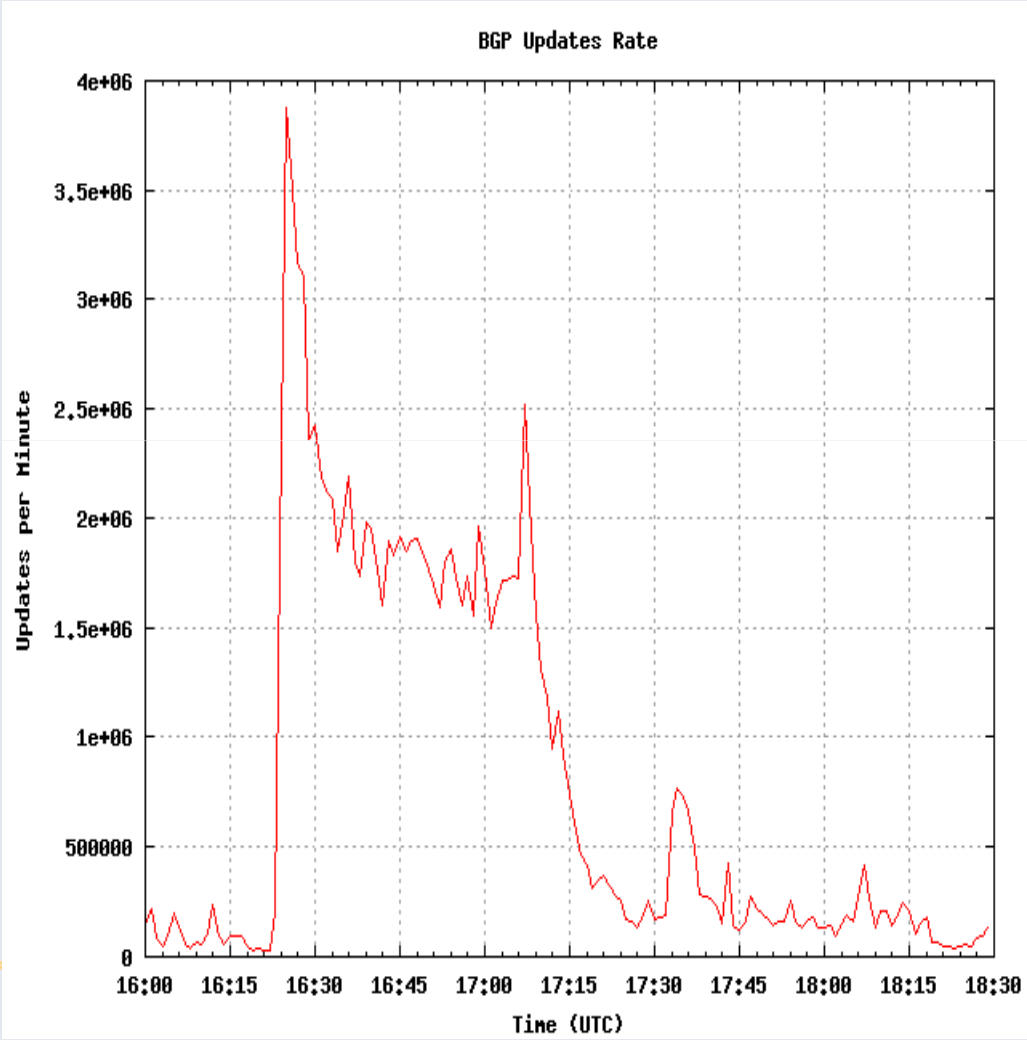


BGP Failures

- ✓ When BGP fails, portions of the Internet may become unusable, thus causing a loss of connectivity between critical portions of the Internet
- ✓ E-mail, e-commerce, and Web accesses would be put out of service for a period of time ranging from minutes to hours!
- ✓ BGP outages could be either
  - *- widespread, affecting large portions of the Internet (e.g. route flapping), or a*
  - *- targeted against a particular network (e.g. denial of service - DoS)*

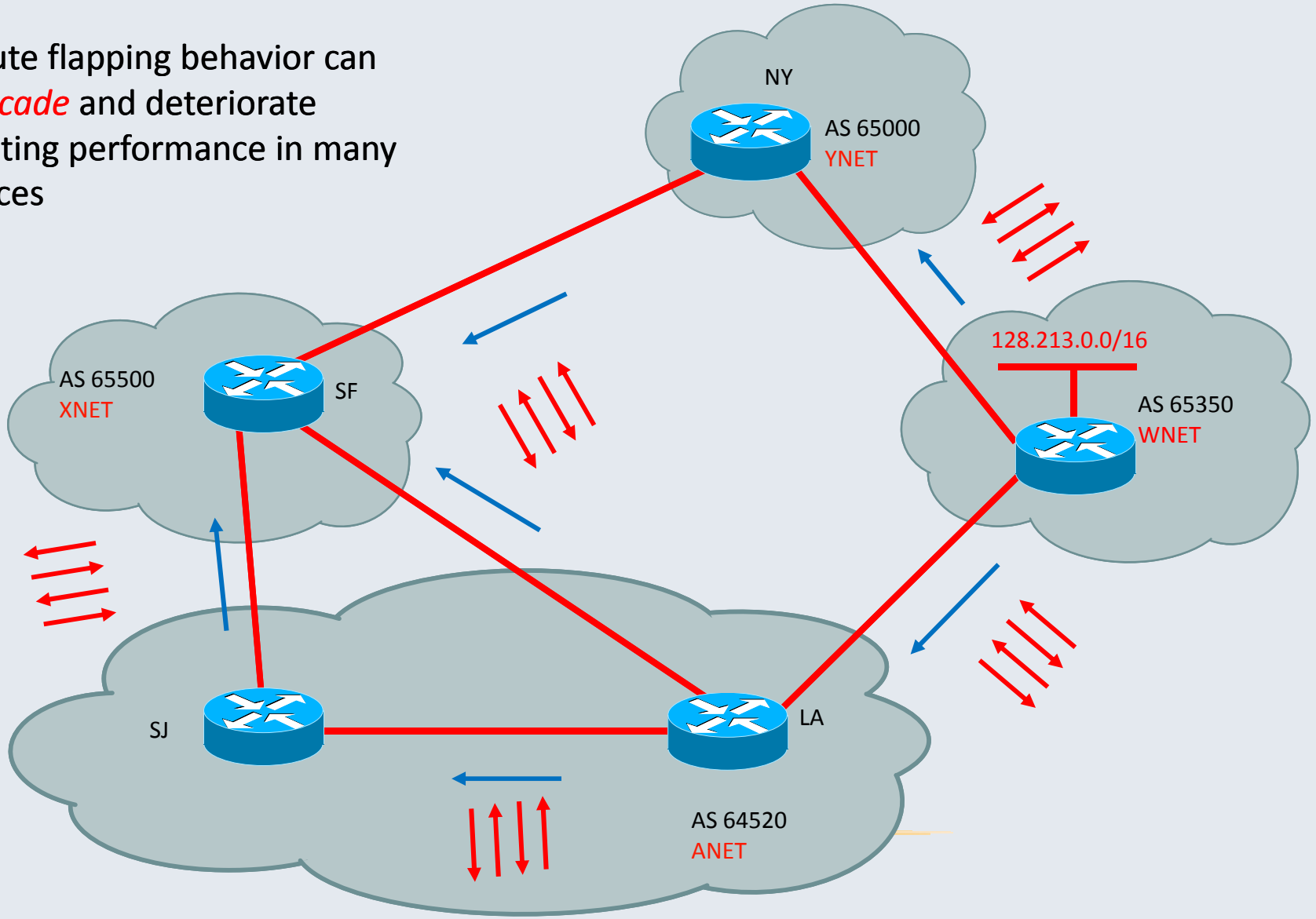
Route Instability

- ✓ *Route Flapping:* occurs when a previously advertised route is withdrawn and then re-announced repeatedly in a short period of time
- ✓ If route flaps happen fast enough the router becomes overloaded, eventually preventing convergence on valid routes



Route Flapping Without Dampening

Route flapping behavior can *cascade* and deteriorate routing performance in many places



Route Instability

- ✓ Route flapping can result in a denial of service (i.e. routers are flooded with more packets than they can handle)
- ✓ The route flap *damping* (RFD) has been designed to prevent routers from thrashing while trying to re-calculate a large number of BGP UPDATEs
- ✓ However, both measurement studies and operational observations show that BGP path exploration can trigger false route damping which leads to prolonged periods of lost network reachability
- ✓ As a result, many networks turned off RFD

Anecdotes of Route Flap Storms

- ✓ April 25, 1997 - small Virginia ISP injected incorrect map into global Internet. Map said Virginia ISP had optimal connectivity to all destinations. Everyone sent their traffic to this ISP. Result: shutdown of Tier-1 ISPs for 2 hours
- ✓ August 14, 199 - misconfigured database server forwarded all queries to ".net" to wrong server. Result: loss of connectivity to all .net servers for few hours
- ✓ More recent events causing route flapping are reported in the Renesys Blog
  - http://www.renesys.com/blog/2009/02/the-flap-heard-around-the-worl.shtml
  - http://www.renesys.com/blog/2010/08/house-of-cards.shtml#more

Best Common Practices at Work

- ✓ Comprehensive BGP security solutions have not yet emerged and current "best common practices" are somewhat
  - *overlapping,*
  - *confusing in scope and applicability, and often*
  - *neglect cost/benefit tradeoffs*

- ✓ Many researchers believe that the Internet may be so hopelessly broken that it could be better to start over, rather than continue to apply band-aids

Long Term Growth Trends in Internet Routing

- ✓ Question 1

  Will the previous problems be exacerbated when the Internet size increases, e.g. double in size?

- ✓ Question 2

  Will the routing system be able to scale and meet the growth of the Internet and its ever-expanding level of demands?

- ✓ Question 3

  What is the ability of the system to produce a stable view of the overall network topology?

Simulative Analysis

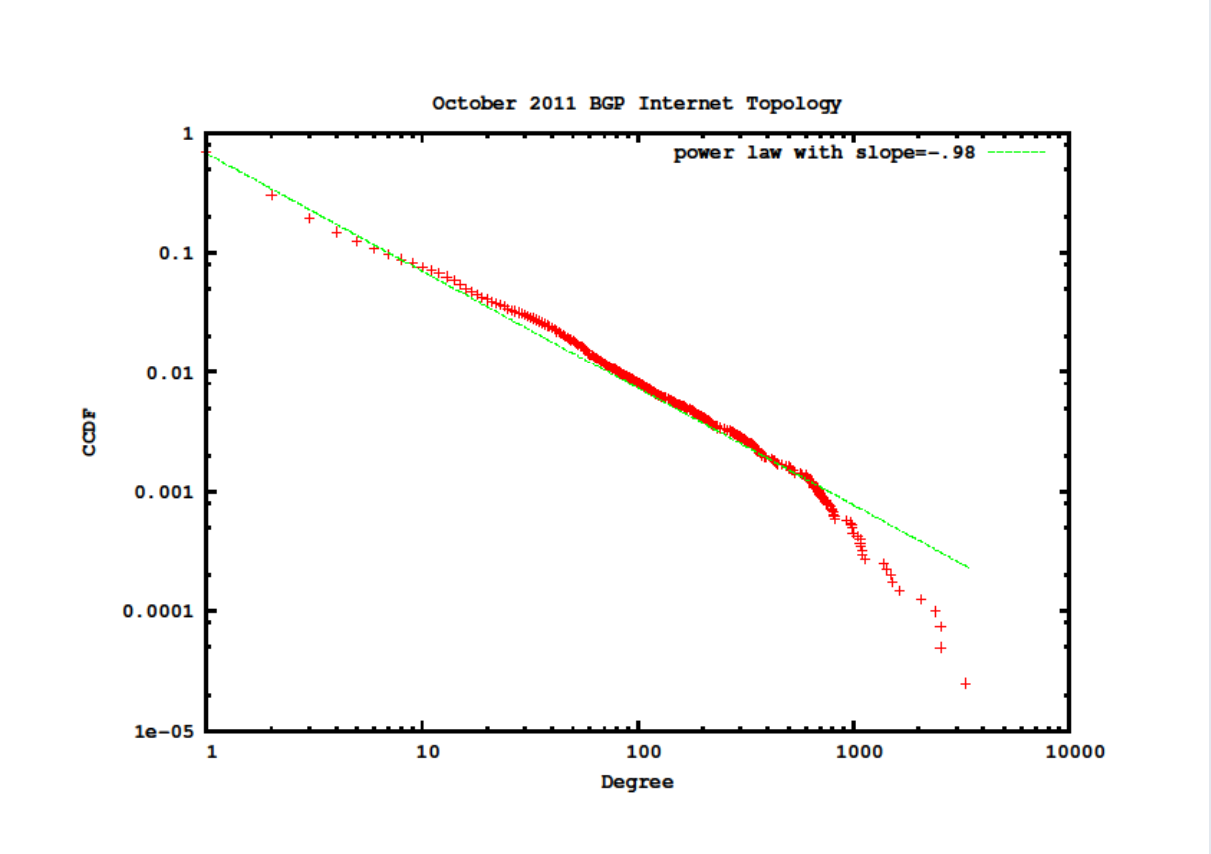
- ✓ We can use simulation to evaluate a proposed BGP security solution before deployment

BUT

this requires an *Internet AS-Level topology* model

Barabasi-Albert Model (Preferential Attachment)

The Barabasi-Albert model (green line) is not adequate to represent the Internet growth at the AS-level of abstraction



CONCLUSIONS

A new (more realistic) model is needed for getting robust results while simulating BGP securiry algorithms

Research is still underway