

Emergency Slice and In-Network DPI as application of network virtualization

Japan-EU Workshop on Future Internet/New Generation Network

Aki Nakao

University of Tokyo

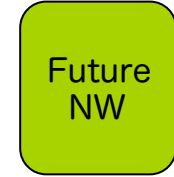
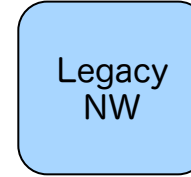
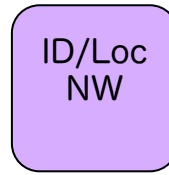
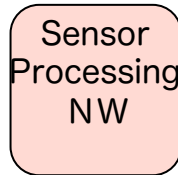
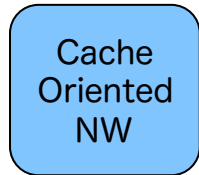
2012/1/19

Our Vision: “Flexibly Programmable” Network

Slice 1

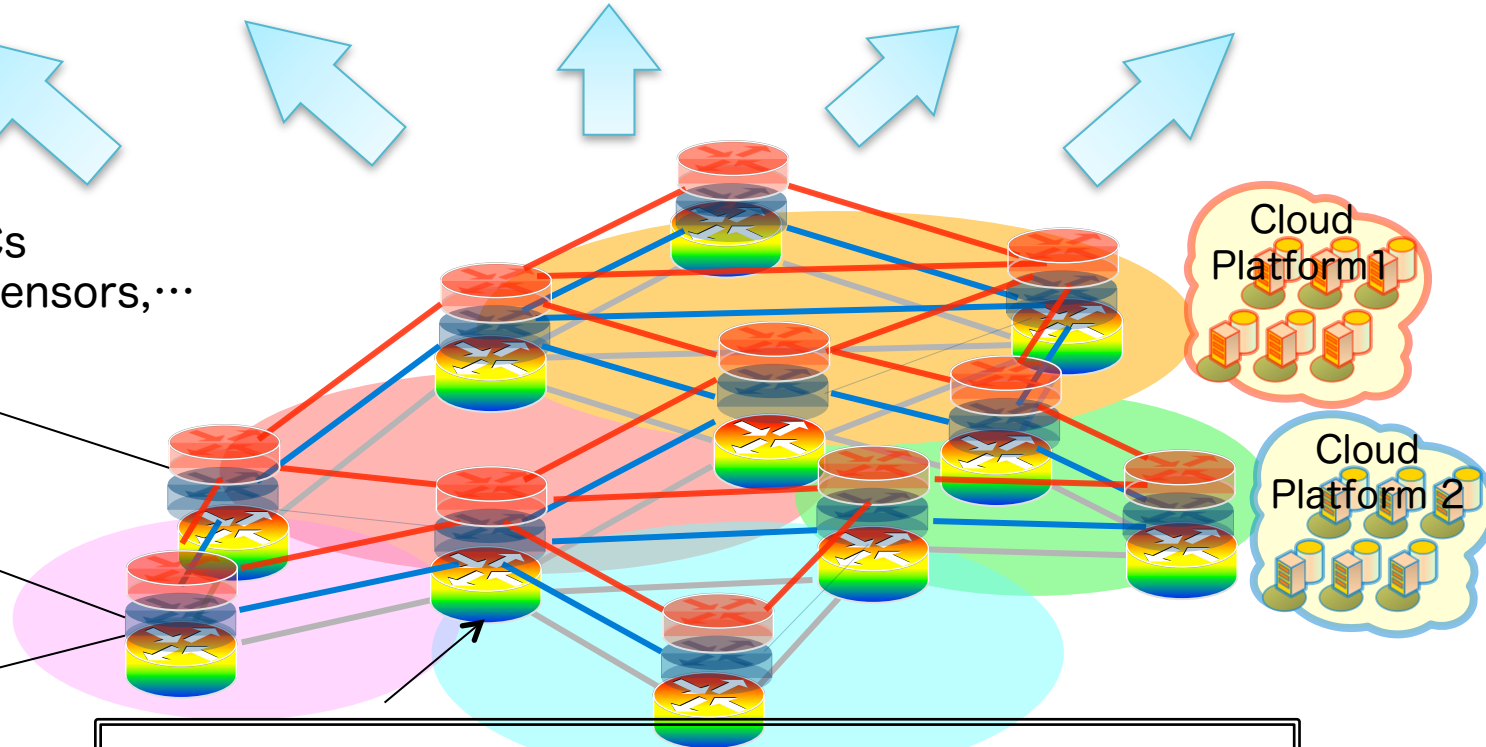
Slice 2

Slice N



“Slices” accommodate diverse NWs

Handsets, PCs
Appliances, Sensors,...



Network Virtualization Infrastructure



Benefit of Network Virtualization #1

Network Slicing
for **Public Safety** and for **Emergency**

Allocating Resources for Emergency

❖ Dilemma of “Inflexible” Infrastructure

If resources **reserved** and nothing happens, **wasted**.



If resources **not reserved** and anything happens, **troublesome**.

We need a slice of resources to be allocated on demand!
And protocols do not have to be a standard one!



Benefit of Network Virtualization #2

In-Network DPI
(Deep Packet Inspection)

Spam: More than Just a Nuisance

- 95% of all email traffic
- As of August 2007, **one in every 87 emails** was a phishing attack
- Targeted attacks** on rise
 - 20k-30k unique phishing attacks per month

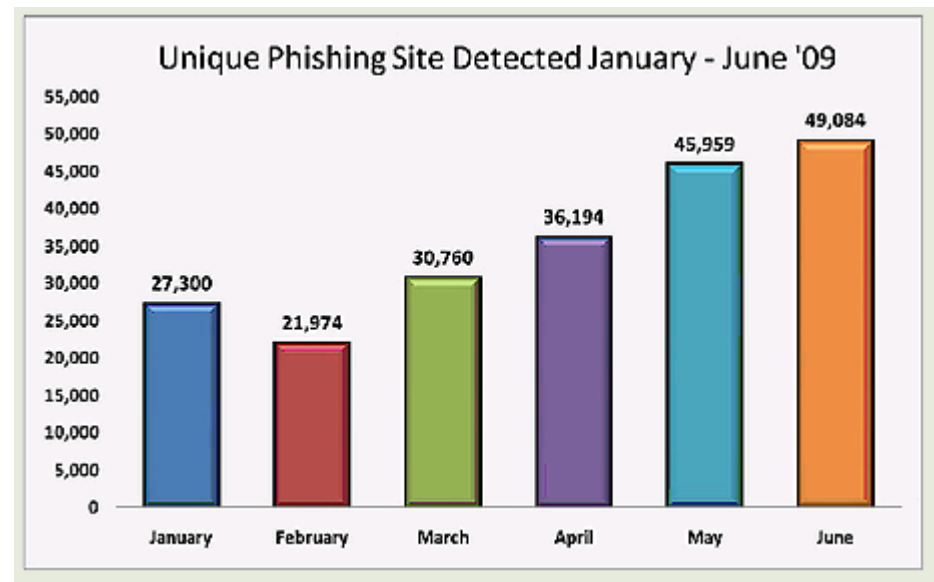
**One bot-infected PC =
600,000 spam messages a day**

Rustock, Xarvester top the list as most efficient spam-spewing bots

By Gregg Keizer

April 22, 2009 12:00 PM ET

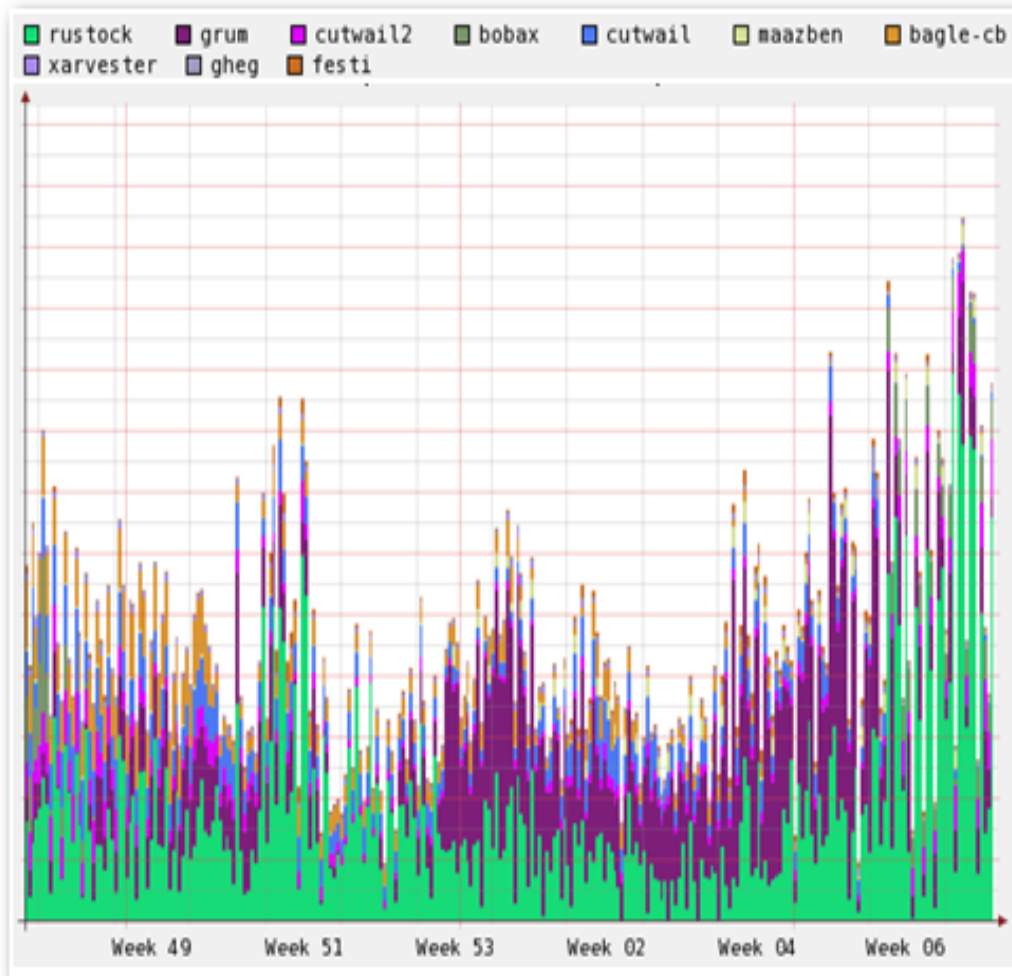
Computerworld - Some bot-infected PCs can crank out as many as 25,000 spam messages per hour, new research released today claimed.



Source: APWG

(Nick Feamster's Talk @UTokyo)

Top-10 Spamming BotNets



BotNet	Size	# of Spams
Grum	600K	40B
Bobax	100K	27B
Pushdo	1.5M	19B
Rustock	2M	17B
Bagle	500K	14B
Mega-D	50K	11B
Maazben	300K	2.5B
Xarvester	60K	2.5B
Donbot	100K	800M

<http://www.techrepublic.com/>

“Botnets” rent bots on the black market for **\$0.03 per week**

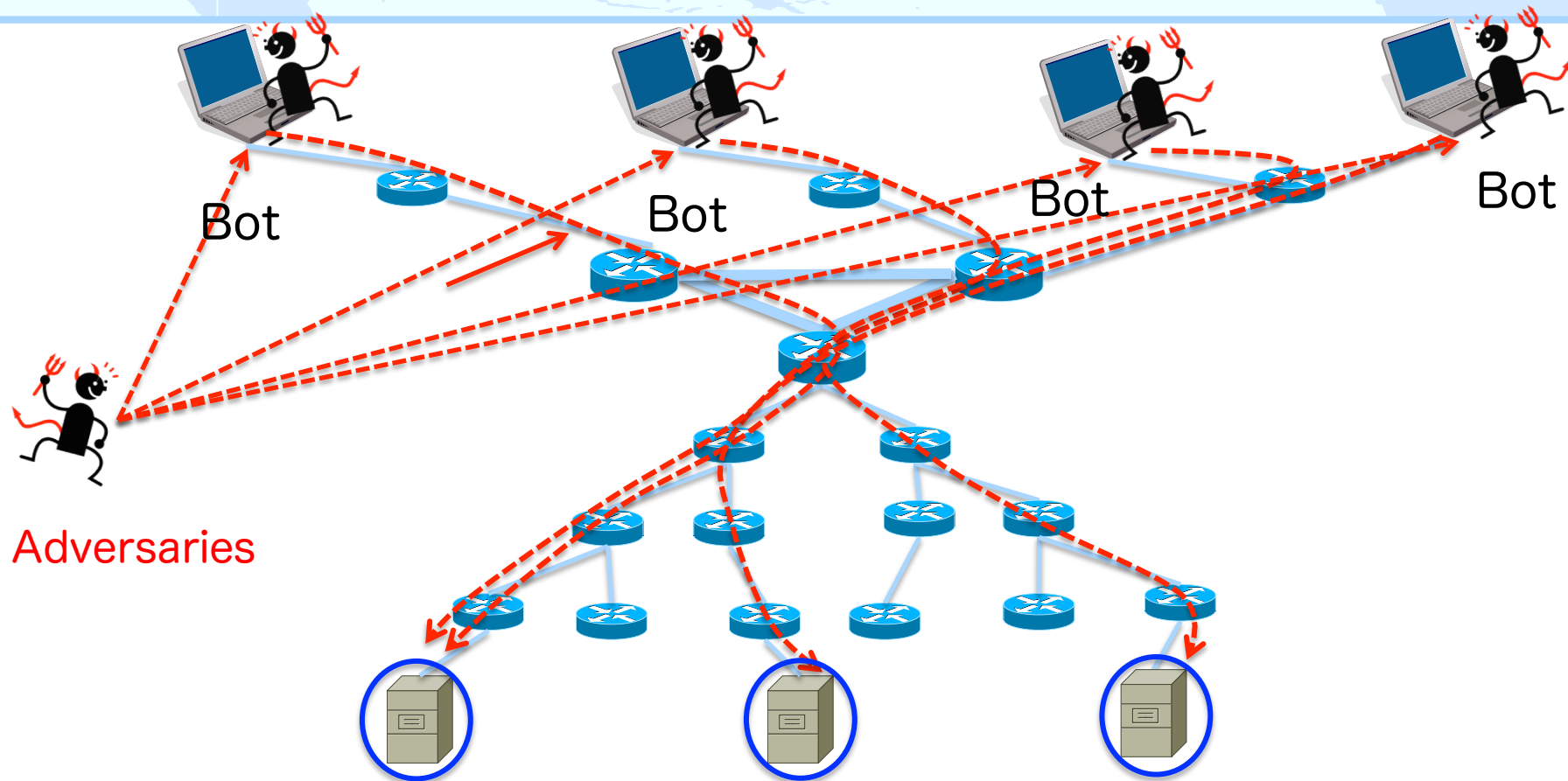
PAXSON, V. private communication, December 2008.

Above the Clouds: A Berkeley View of Cloud Computing 2009

\$5,000 per day for a botnet of 50,000 to 70,000 PCs

The New Front Line, Michael Lesk, Martin R. Stytz, Roland L. Tropé

Problems of BotNet Detection At Network Edges



Problem 1 : Similar SPAMs are detected independently at edges

→ Redundant processing

Problem 2: Hard to utilize temporal correlation Among SPAMs

→ Under-utilizing collective behaviors

In-Network DPI : BotNets Detection In the Network

	Advantage	Disadvantage
Proposal	1. Redundant DPI Elimination	<u>Require Fast Processing</u>
	2. Utilize Temporal Correlation	
Prior Art	Tolerate Slow Processing	Cannot Exploit Collective Behavior



Challenges

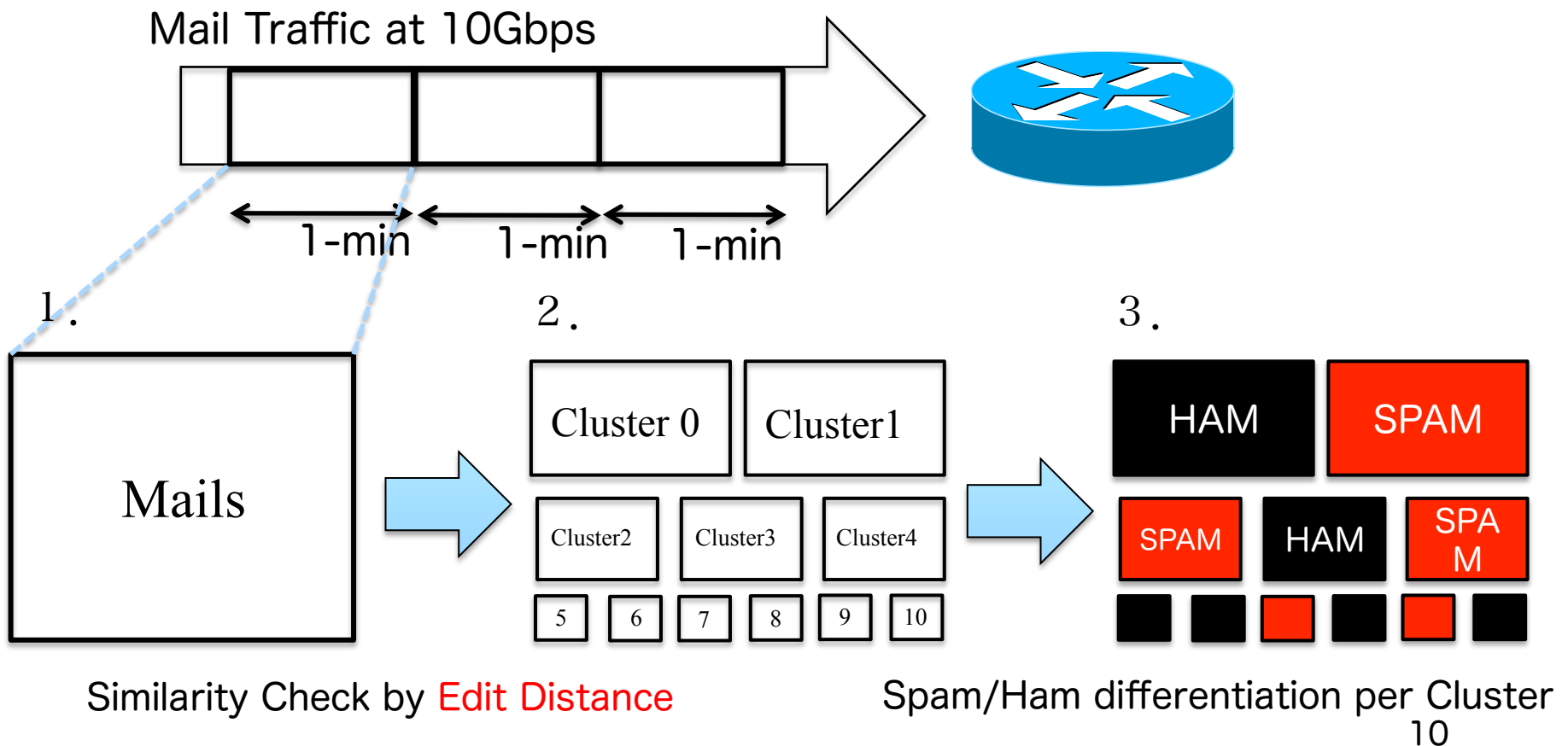
1. Simple Clustering Similar Emails Using **Edit Distance**
2. Acceleration of Clustering using **GPGPU**
3. Fast Spam / Ham Differentiation

Our Methodology

1. Divide Email traffic into 1-minute blocks
2. Clustering based on Edit-Distance
3. Spam/Ham differentiation per block

GPGPU based
Fast In-Network DPI
Real-Time BotNet Detection

86% Success at 10Gbps



Conclusion

In-Network Processing for Future Network Security

- ⊕ Emergency and Public Safety Network Slice
 - ⊠ Dynamic Allocation/Revocation of Resources
 - ⊠ Dynamic Introduction of New Protocols/Services
- ⊕ In-Network DPI
 - ⊠ SPAM Filtering / BotNets Detection as an example
 - ⊠ Redundant Processing Elimination
 - ⊠ Temporal Correlation / Collective Behavior Exploitation

We are looking for partners ...

<http://www.nakao-lab.org>
<http://nakao.iii.u-tokyo.ac.jp>
nakao@iii.u-tokyo.ac.jp