Malware models for network and service management

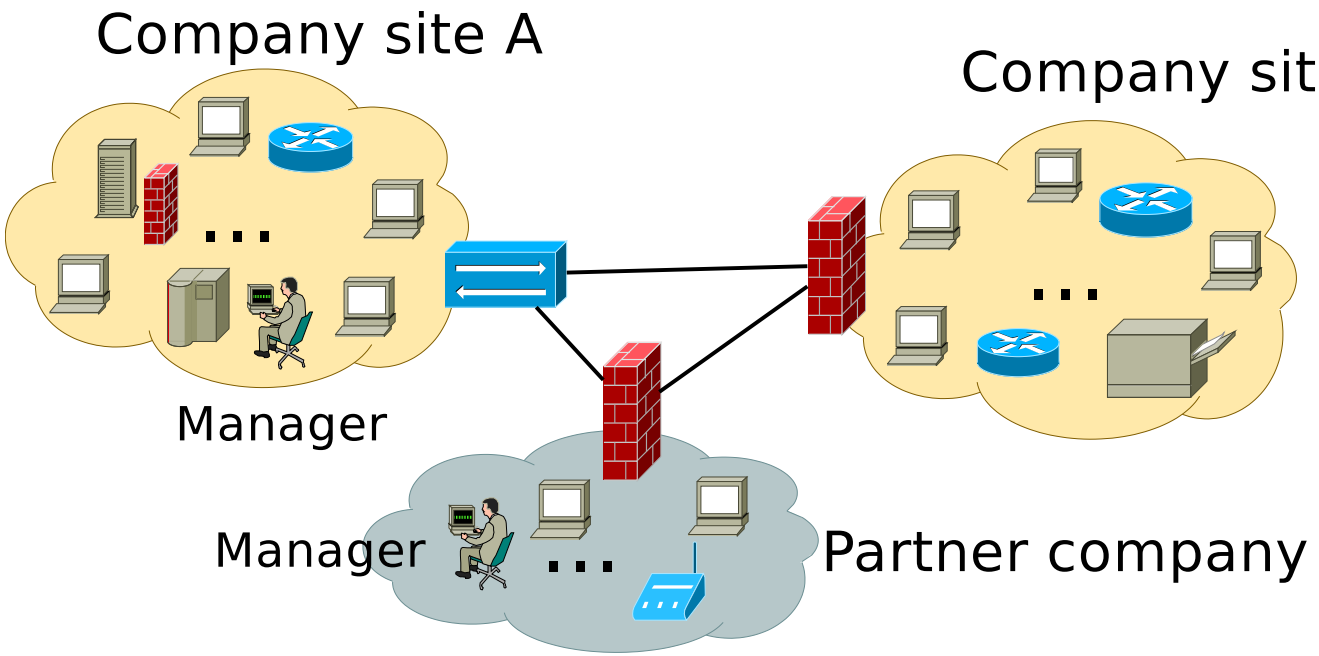
Jérôme François, Radu State and Olivier Festor

MADYNES EMANICS CNRS CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE Nancy-Université

LORIA, Campus Scientifique - BP 239 - 54506 Vandoeuvre-lès-Nancy, France

Efficient and scalable management plane

- Number of devices to be managed
- Diversity of devices to be managed
- management domain boundaries are not clear
- an hostile environment: firewall, addresses translators
  $\longrightarrow$ difficult to reach the devices to be managed



Malware based management

- the creators of malware faced the same problems
- the botnets
  - compromised machines waiting for instructions from the master
  - IRC network, very useful to send a request to all bots
  - simple communication exchange
  - the applications are various
  - the scalability: huge botnets were already observed (400 000 bots)

$\longrightarrow$ adapt the botnets for network management

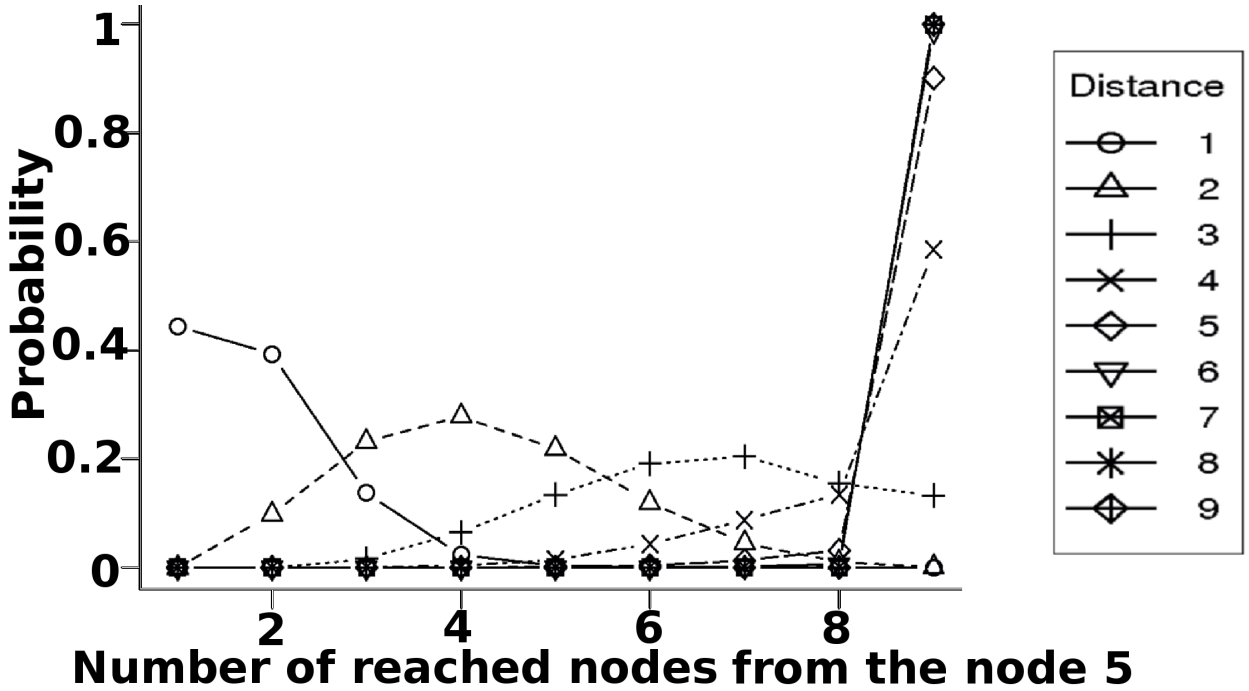
How to evaluate the malware benefits ?

- many papers describe the power of malware and above all the botnets
- network management need to know the performances of a such system
- a company need to know the performance of its management plane
  - probability to reach 90% of the devices
  - time needed to update 95% of the computers
- creation of the management botnet $\longrightarrow$ choose the right topology

$\longrightarrow$ need to have a mathematical model of a botnet

Our model

- bots connected randomly and uniformly on the servers
  $\longrightarrow$ consider only the servers
- N ($= 10$) servers form a random tree
- the probability to reach a subset of N from a given node at a given distance



Future works

- add parameters like network failures
- observe more metrics like overload or time needed to perform a global management operation
- use these metrics to optimize the management plane
- evaluate a botnet based management framework: an implementation on a realistic testbed