



# Evaluating Resilient Consensus with DetelLab

Mark Yampolskiy (Vanderbilt University)

Work with: Xenofon Koutsoukos and  
Yevgeniy Vorobeychik

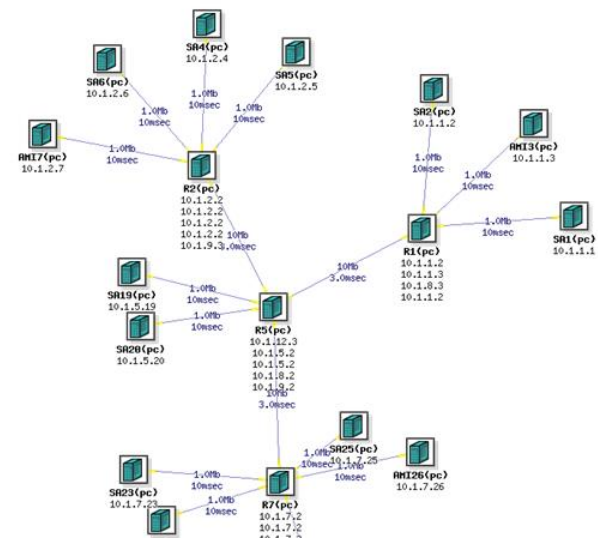


# Realistic Network Topology

## Advantages/Disadvantages

- \* Advantages
  - \* Application layer attacks
  - \* Network layer effects, e.g., background traffic
  - \* Network attacks, e.g., DDoS
- \* Disadvantages
  - \* Time consuming
  - \* Scalability

## Network Topology



# Emulation in DeterLab – Procedure

- \* Procedure
  - \* Define NW topology in DeterLab and deploy node software
  - \* Run experiments. Collect results as per-node log files
  - \* Save log files on a dedicated computer for evaluation purpose
  - \* Import log files in MATLAB and analyze results
- \* Key features
  - \* Node software: PERL program
  - \* Communication between nodes: over TCP/IP
  - \* Synchronization of rounds: SYNC messages from dedicated node
  - \* Overlay topology defined in node's software

# Network Effects/Attacks in DeterLab

The screenshot displays the SEER (SEcurity Emulation and Research) interface. On the left, a tree view under 'Controls' includes categories like Configuration, Traffic, Attack, Malware, Defense, Analysis, and Other. The 'Attack' category is expanded, showing options like Botnet, Packet Flooder, and Malware. The main panel shows configuration for an 'Attack Source' with nodes A1, A2, and A3. The 'Basics' section includes a target A4 and protocol tcp. The 'Rate Info' section has a flood type of pulse and various rate settings. The 'UDP/TCP' section includes port ranges and TCP flags. A network diagram on the right shows nodes A1, A2, A4, and S0 connected to a central router lan1. The interface also features a 'Start' and 'Stop' button at the bottom.

Background Traffic can be generated

Supported Attacks

- Packet Flooding
- User-Defined Malware can be added

Traffic Monitoring and Analysis Tools available

# Results

