ЦЕНТР
ПРИКЛАДНЫХ
ИССЛЕДОВАНИЙ
КОМПЬЮТЕРНЫХ
СЕТЕЙ

2013
CEE-SEC(R)
Разработка ПО

Моделирование WAN-сетей для исследования вредоносного ПО

Антоненко Виталий

ЦПИ КС, программист-разработчик

24 октября 2013

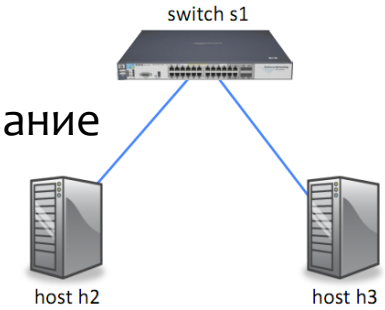
Мотивация

Создание среды разработки и отладки приложений для контроллера ПКС сети.

Разработка системы моделирования сетевой структуры и сетевой активности.

Моделирование компьютерной сети

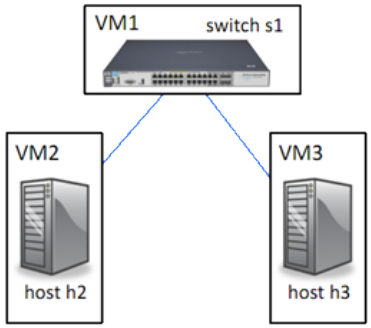
Физическое оборудование



ЗА:
- высокая степень доверия

ПРОТИВ:
- плохая масштабируемость

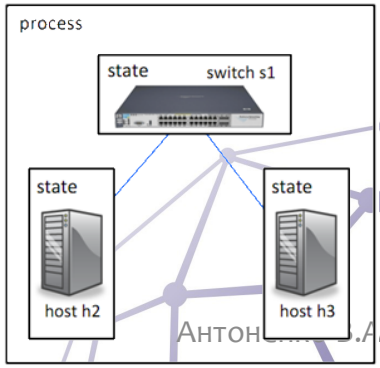
Эмуляция



ЗА:
- высокая степень доверия
- нет необходимости закупки оборудования

ПРОТИВ:
- высокие требования к ресурсам

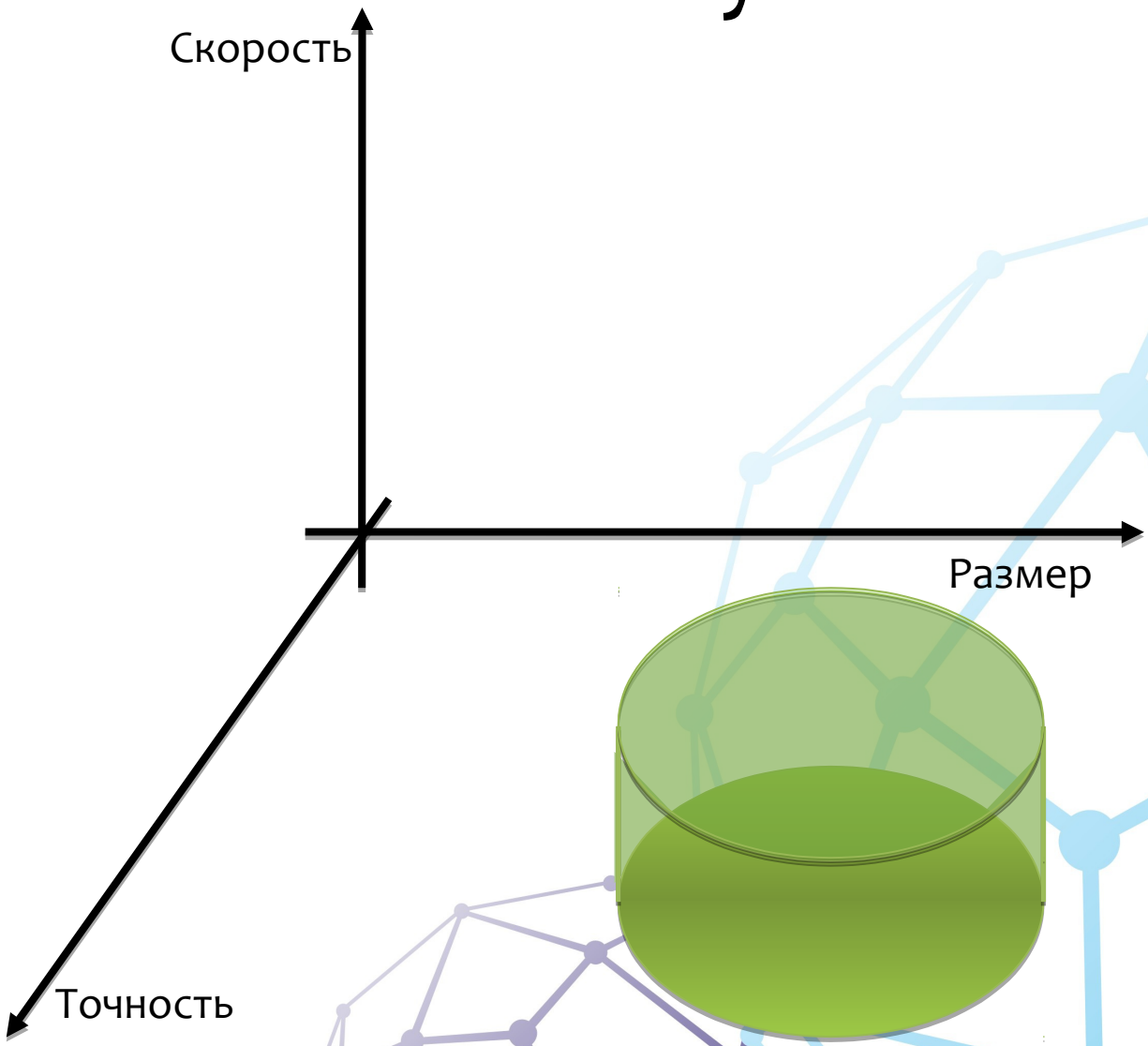
Моделирование



ЗА:
- пониженные требования к ресурсам

ПРОТИВ:
- необходимость доказывать корректность и адекватность модели

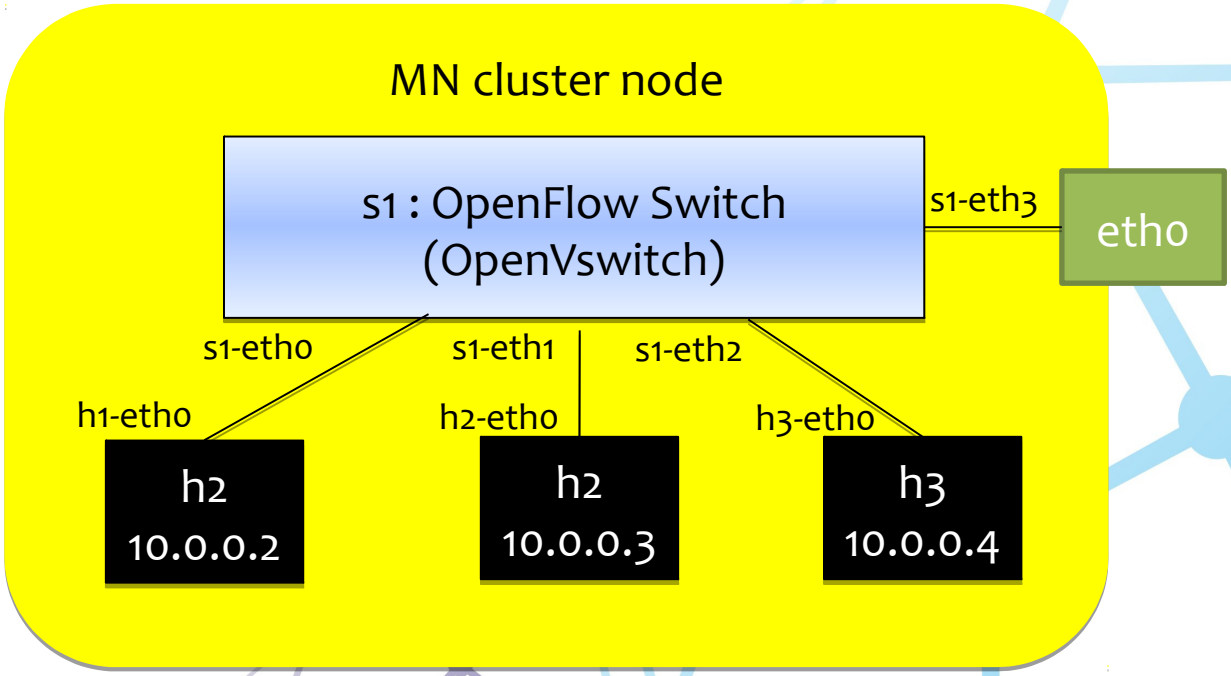
Что хотелось получить?



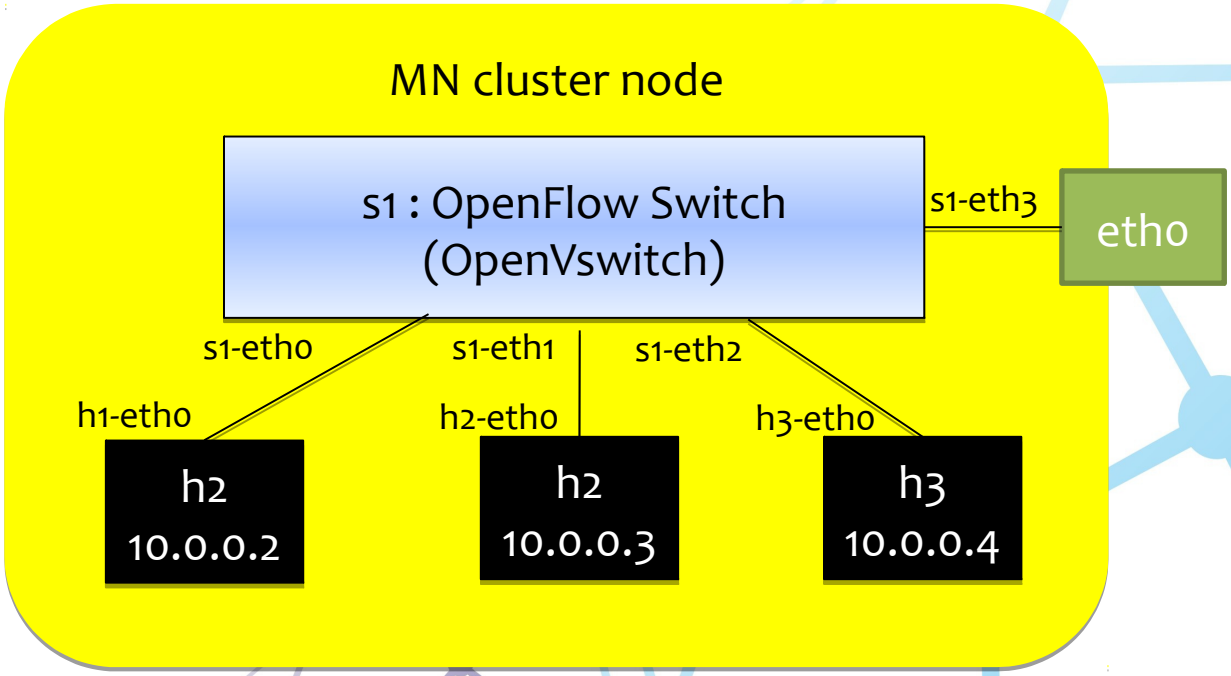
Решение – MNCE (Mini Network Cluster Edition)

- Виртуальная сеть на локальном ПК или кластере компьютеров
- Гибкое создание топологии сети
- Масштабируемое решение
- Возможность моделирования сети регионального масштаба

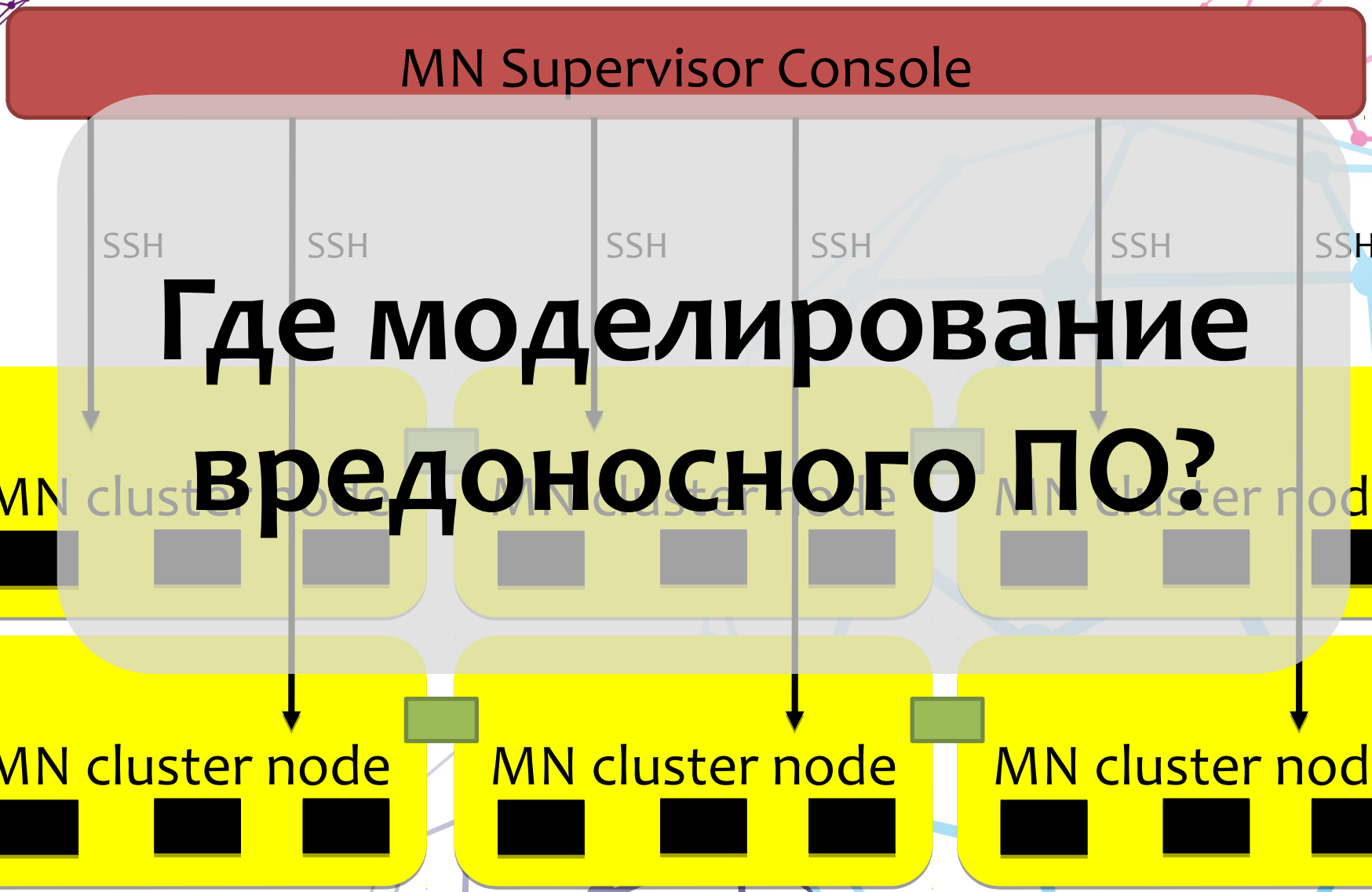
Архитектура MNCE



Архитектура MNCE



Архитектура MNCE

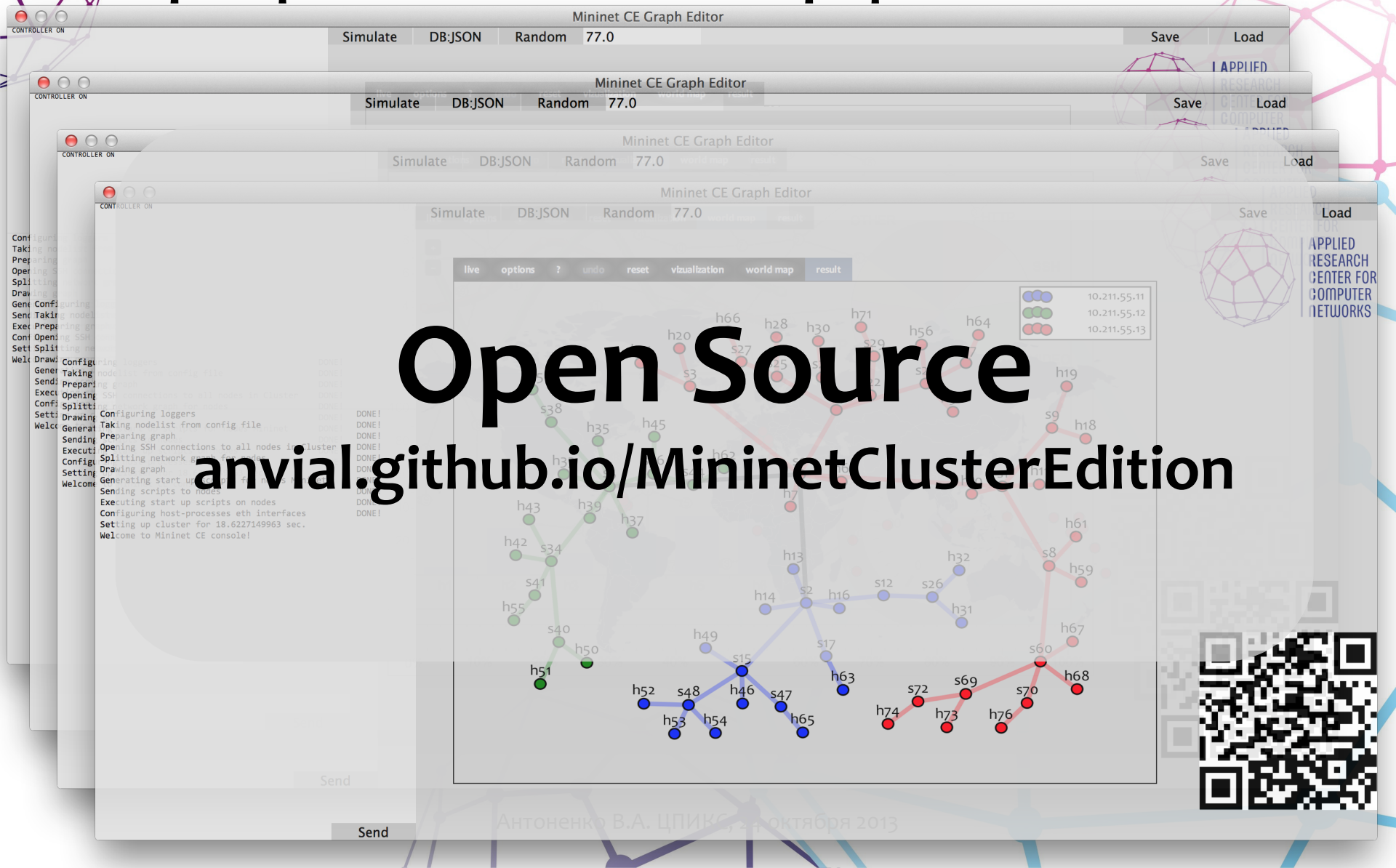


Где моделирование вредоносного ПО?

Распространения сетевого червя

Как это все визуализировать?

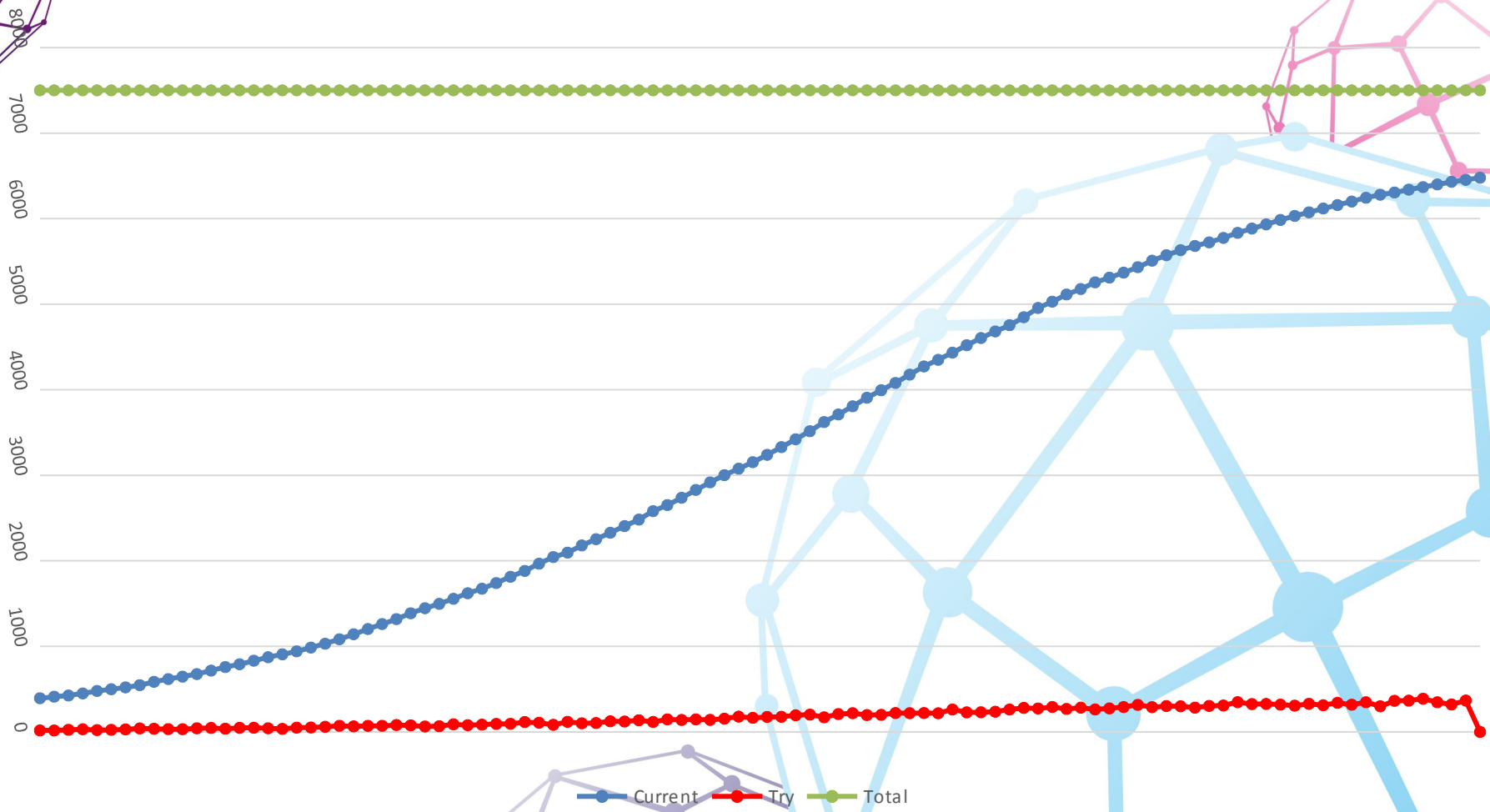
Графический интерфейс MNCE



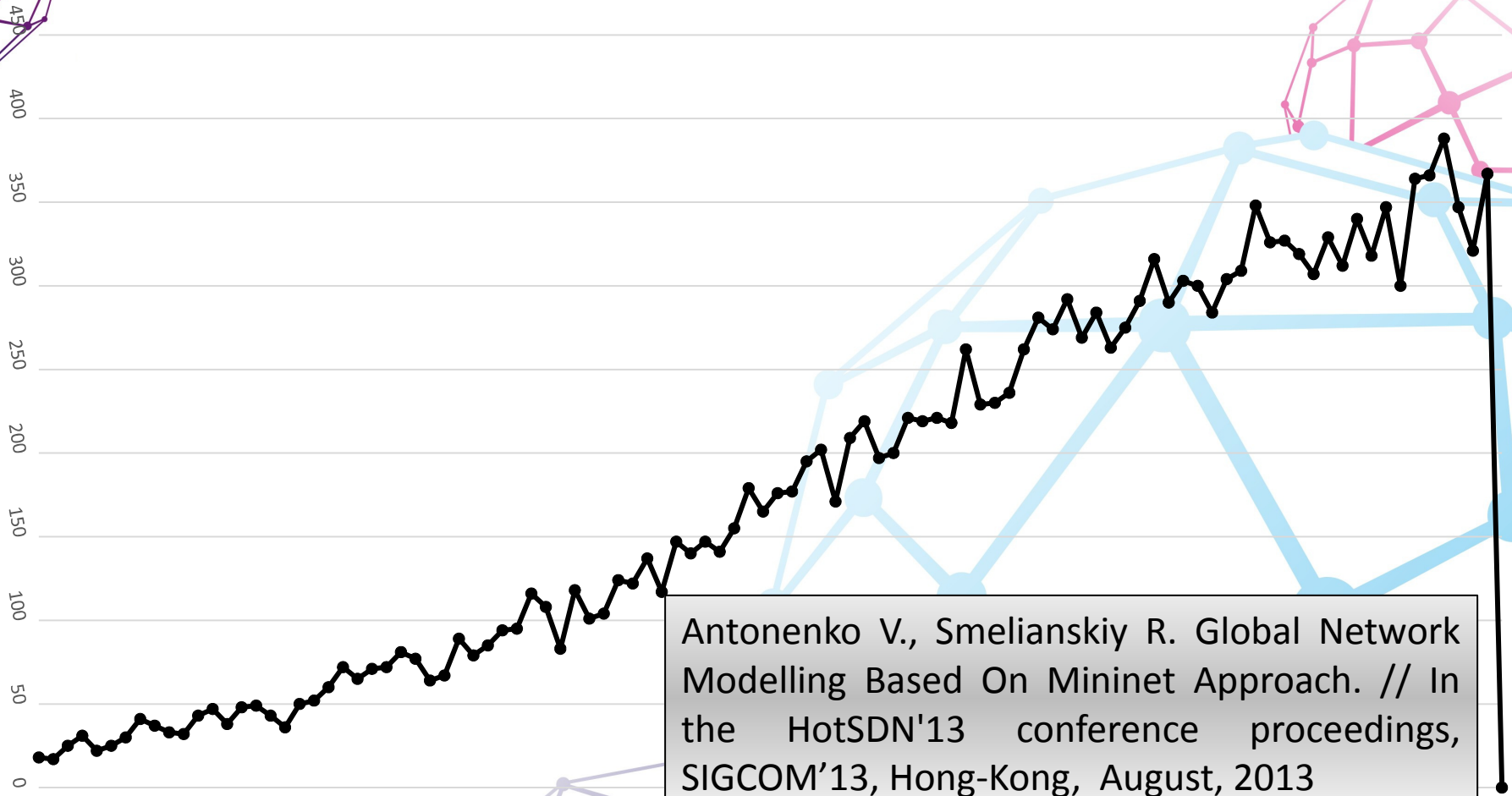
Open Source

anvial.github.io/MininetClusterEdition

Распространение червя Sasser

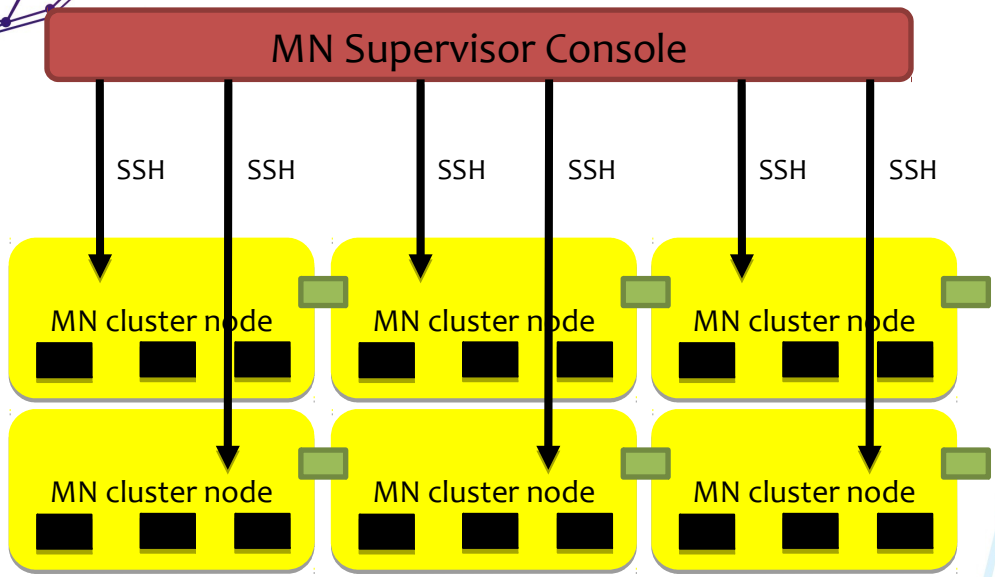


Распространение червя Sasser



Antonenko V., Smelianskiy R. Global Network Modelling Based On Mininet Approach. // In the HotSDN'13 conference proceedings, SIGCOM'13, Hong-Kong, August, 2013

Масштаб сети MNCE



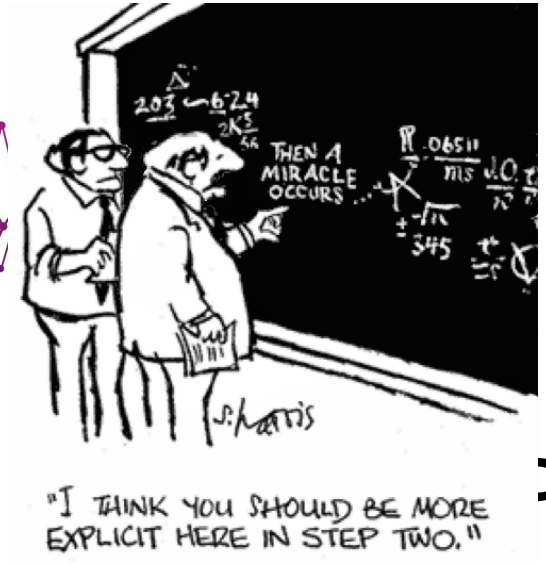
Количество процессов хостов на одном узле кластера: до **2000**

Количество процессов хостов на одном узле кластера при проведении экспериментов: от 250 до **1000**

Количество улов кластера на одном сервере: **15**

Количество доступных серверов: **2**

ИТОГО: ~ 30 тыс. узлов в графе сети



ы?

Антоненко Виталий

vantonenko@arccn.ru

APPLIED RESEARCH CENTER FOR COMPUTER NETWORKS

www.arccn.ru

@arccnnews

anvial.github.io/MininetClusterEdition

Спасибо за внимание!

Антоненко Виталий
vantonenko@arccn.ru

www.arccn.ru

@arccnnews

anvial.github.io/MininetClusterEdition