Interactive Analysis of Cyber Defence Mechanisms Against DDoS Attacks

Demonstration at Ciena booth #933

Ralph Koning, Ben de Graaff, Paola Grosso, Robert Meijer, Cees de Laat

SARNET

SARNET, Secure Autonomous Response NETworks, is a project funded by the Dutch Research Foundation. The University of Amsterdam, TNO, KLM, and Ciena conduct research on **automated methods against attacks** on computer **network infrastructure**.

Analysing DDoS Defence Mechanisms

In this demonstration we let the viewers interactively **analyse DDoS defence strategies**. The touch table interface shows a virtual **network under attack** and a revenue graph. During the attack the revenue will decrease because the successful transactions are disrupted by the malicious traffic. We **challenge the viewer to defend** against the attacks by monitoring and changing network aspects, such as link state and bandwidth, and **minimise the impact** on the revenue.

The system **records** and **analyses** the viewers' solutions and **ranks** the solution based on multiple aspects, including **revenue recovery**. In this way the system **learns** the **most optimal defence against the attack** and can apply them automatically.
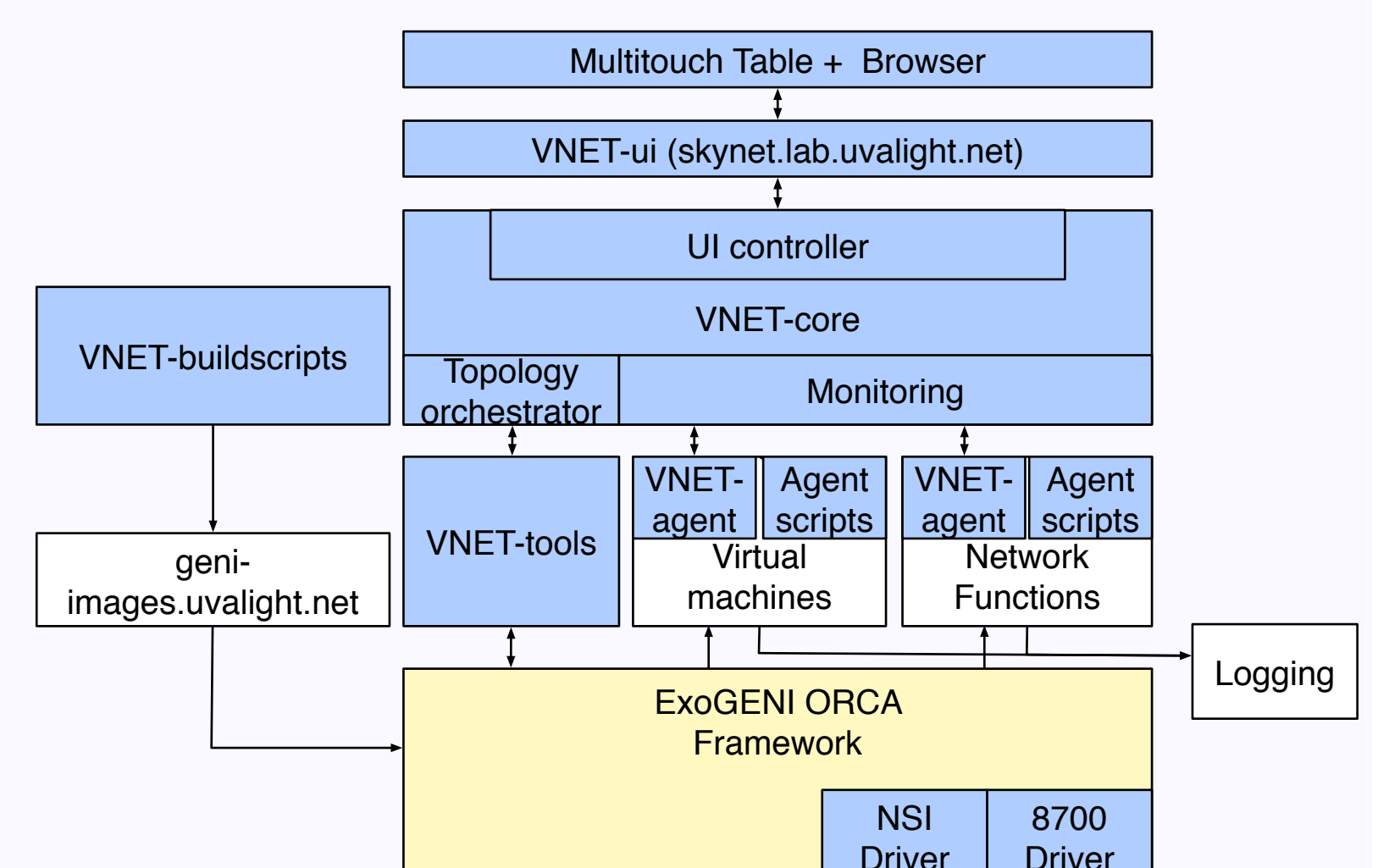
The viewer will learn the following;

• Anti DDoS solutions are not trivial;
• DDoS defence is an iterative proces;
• Tools are needed for effective DDoS response.
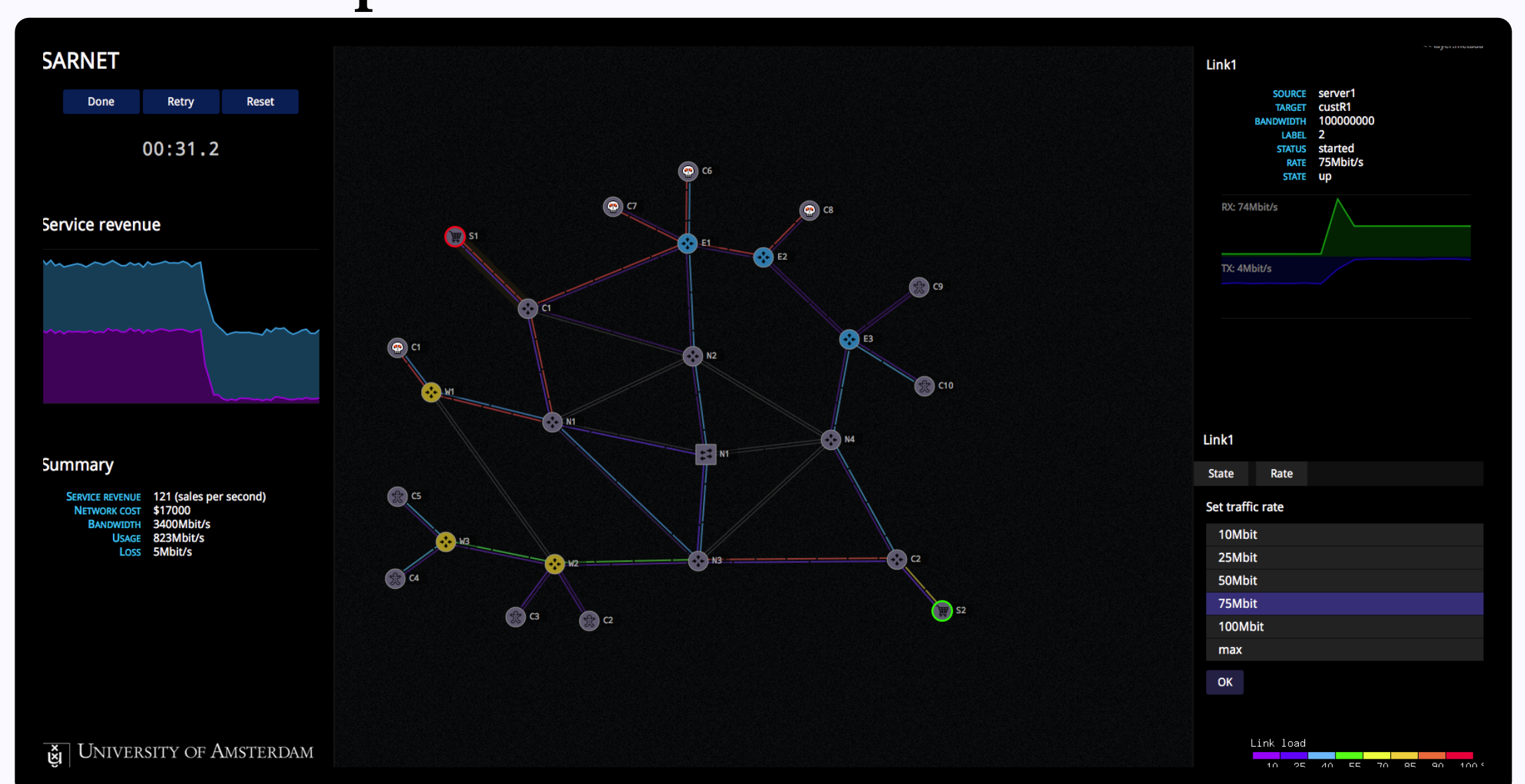
Infrastructure and visualisation

For the demo we use **real** and **realistic** attacks that are executed on top of **ExoGENI,** an international federated cloud testbed. A **Ciena 8700** switch is used at the UvA and Ciena sites to provide additional traffic isolation. For control, data collection, and visualisation we use the **VNET** framework, which is specifically developed to visualise attack scenarios.

Ralph Koning <R.Koning@uva.nl>, Ben de Graaff <b.degraaff@uva.nl>, Paola Grosso <P.Grosso@uva.nl>, Cees de Laat <delaat@uva.nl>
http://sne.science.uva.nl | http://www.delaat.net/ | http://sarnet.uvalight.net