Cloud-based Security Research Testbed: A DDoS Use Case

Tomáš Jirsík
Institute of Computer Science
Masaryk University
Brno, Czech Republic
jirsik@ics.muni.cz

Martin Husák
Institute of Computer Science
Masaryk University
Brno, Czech Republic
husakm@ics.muni.cz

Zdenek Eichler
Faculty of Informatics
Masaryk University
Brno, Czech Republic
zdenek.eichler@mail.muni.cz

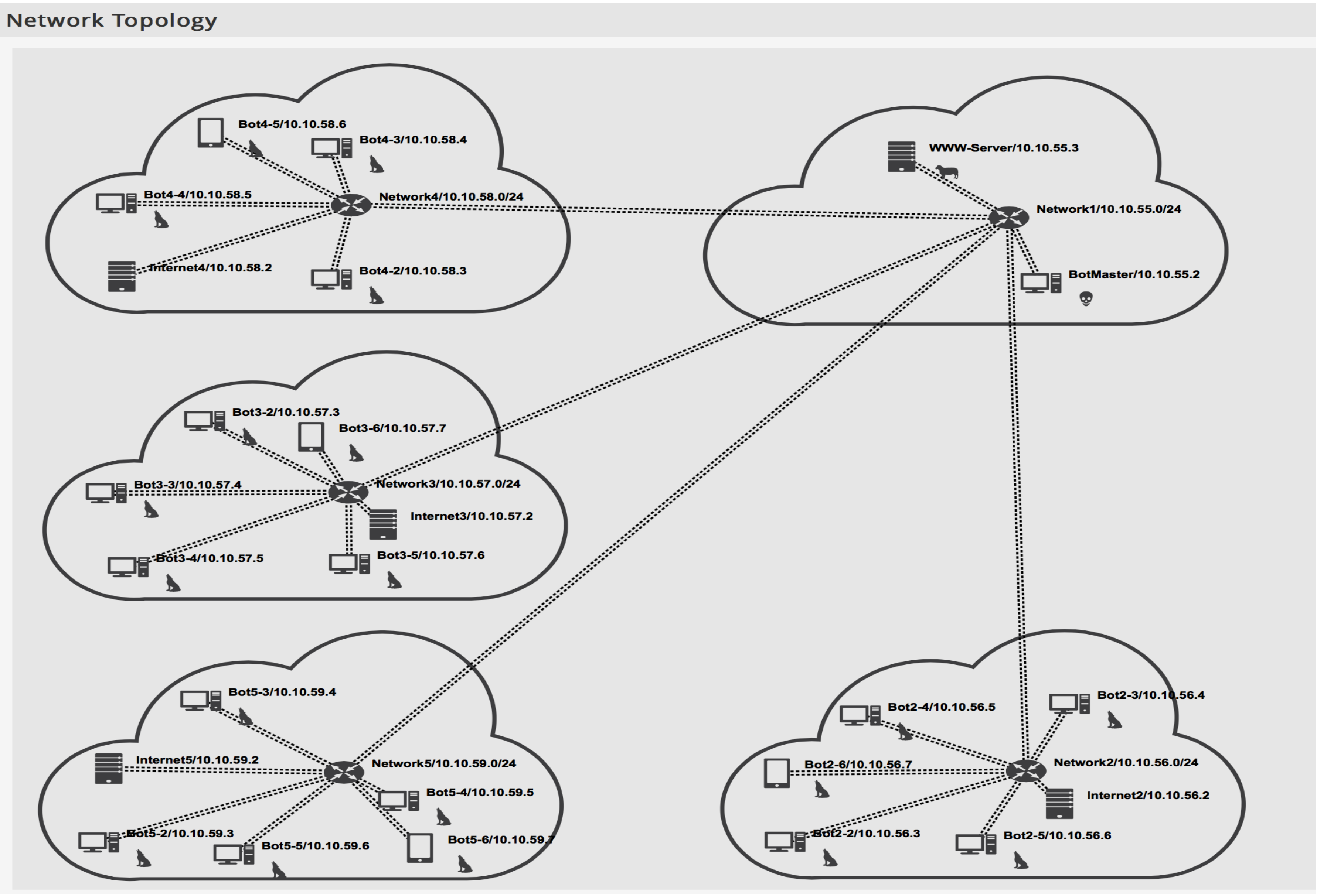
Pavel Čeleda
Institute of Computer Science
Masaryk University
Brno, Czech Republic
celeda@ics.muni.cz

Abstract — We present a cloud-based research testbed designed to aid network security managers. The testbed enables operators to emulate various network topologies, services, and to analyze attacks threatening these systems. A possibility to test results of network management measures is desired, since testing these measures in a production environment is always not possible. We demonstrate a testbed use case, which aids to scrutinize network behavior under attack. Our use case is based on a large DDoS attack which targeted network infrastructure and web servers in Czech Republic in March, 2013.

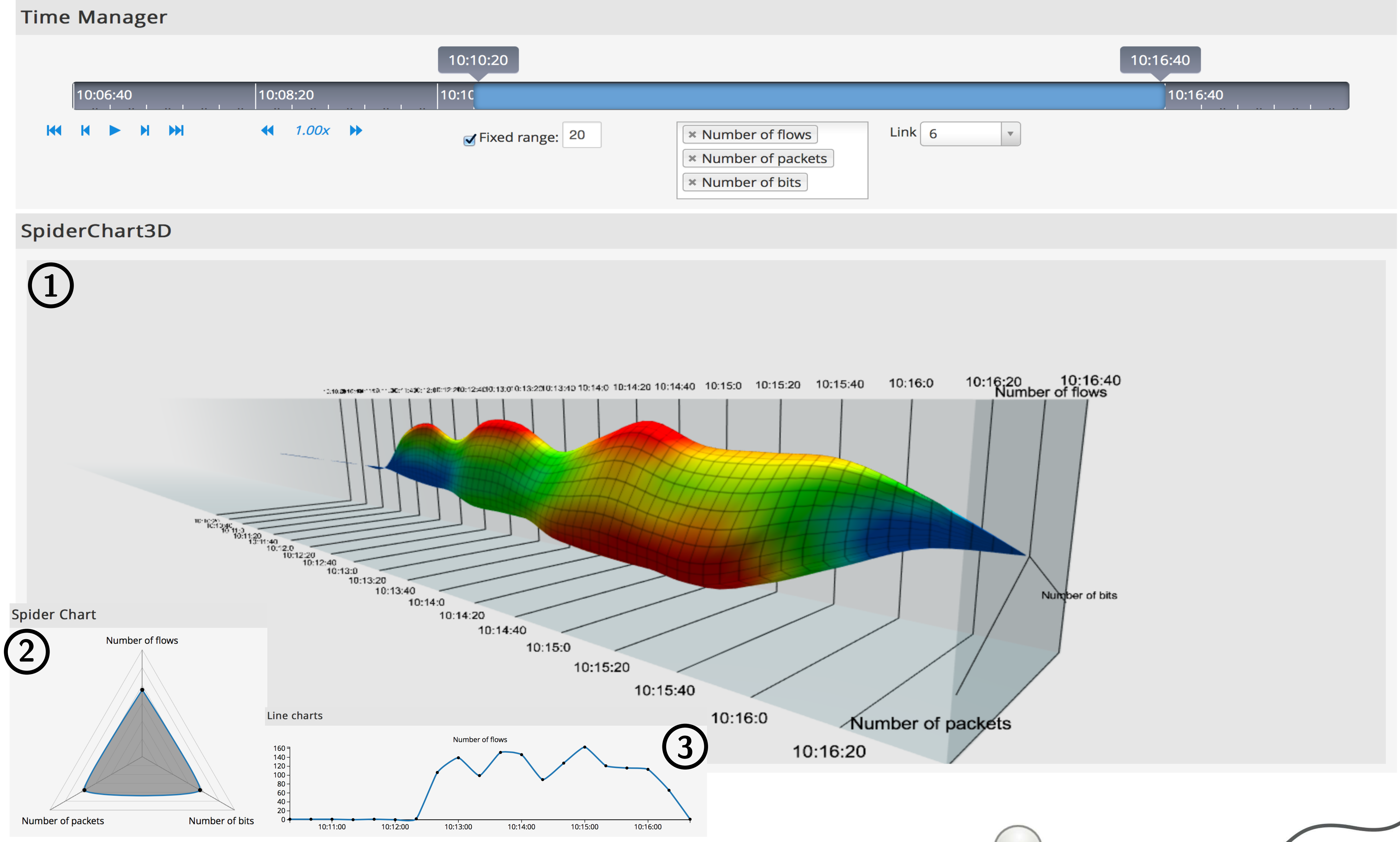
DDoS Simulation

- DDoS Attacks - easy to detect, hard to defend
- Tedbed needed - Cybernetic Proving Ground
- DDoS type - TCP SYN flood
- Based on - DDoS attack on Czech important web servers in March, 2013
- Botnet - commanded by IRC and irssi
- Attacking tool - Low orbit ion cannon (LOIC)

Network Topology



Time Manager


Fixed range: 20
Link: 6
Number of flows
Number of packets
Number of bits

1. 3D sequenced time-ordered radar chart
2. 2D ordinary radar chart
3. Line chart of individual characteristics

DDoS Scenario Timeline

0:00	Start scenario
1:00	Bot master configures bots
2:00	Bot groups 1-4 attack victim
⋮	⋮
6:30	DDoS at full strength
8:30	End of DDoS
11:00	Stop scenario

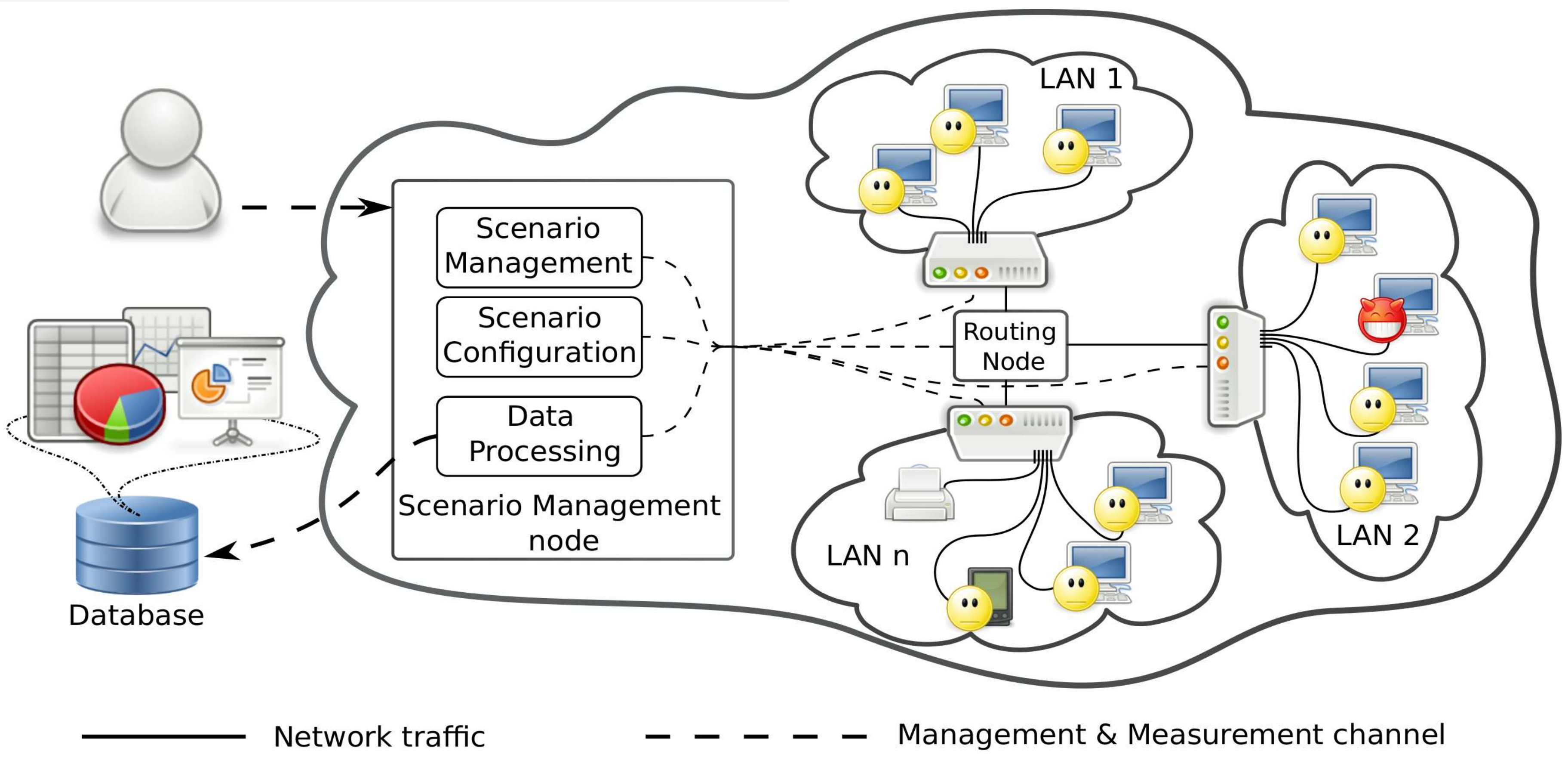
Features

- Simulation of a large network, systems, services and applications
- Cloud environment for repeatable investigation of cyber threats
- Monitoring of network behavior, detection and mitigation of anomalies and attacks
- Automated gathering and processing of data generated during security scenarios
- Creating database of malicious code
- Visualization of significant aspects of the scenarios
- Detailed architecture description in [1]

Visualization

- Web based interface using Liferay Portal
- Interconnected, synchronized portlets displaying various characteristics
- Network topology and traffic visualization

www.muni.cz/ics/kypo



References

[1] D. Kouřil, T. Rebok, T. Jirsík, J. Čegan, M. Drašar, M. Vizváry J. Vykopal. Cloud-based Testbed for Simulation of Cyber Attacks. In Proceedings of NOMS, 2014.

Acknowledgements

This work has been supported by the project "Cybernetic Proving Ground" (VG20132015103) funded by the Ministry of the Interior of the Czech Republic.