Report of
Complex Networks Monitoring and Security and
Fraud Detection for Enterprises (CoNeSec)
track of WETICE 2017

Grzegorz Kolaczek
Faculty of Computer Science and Management
Wroclaw University of Science and Technology
Wroclaw, Poland
Grzegorz.Kolaczek@pwr.edu.pl

Krzysztof Juszczyszyn
Faculty of Computer Science and Management
Wroclaw University of Science and Technology
Wroclaw, Poland
Krzysztof.Juszczyszyn@pwr.edu.pl

Abstract — The CoNeSec track aims to bring together
leading researchers and practitioners from both the complex
networks monitoring and modelling community and the
communication systems security, in order to focus on innovative
research contributions that address both the use of network
analysis in the field of fraud detection and security maintenance
to address the design of highly secured systems. This paper
reports on the motivations of the track.

I. MOTIVATION AND SCOPE

As fraud and security breaches are becoming more
frequent and sophisticated, traditional security solutions are
not able to protect company assets. The problems which must
be solved to provide high-security level for data and users of
enterprise computer systems is related to analysis and
correlation of large amounts of real-time data from network
and security devices. The high-level context of data is often a
crucial element in the way of successful management of
internal and external security threats or improvement of
incident response time and compliance reporting. The network
monitoring can be performed by various types of intrusion
Detection systems which monitor and analyze network traffic
to detect, identify, and report on suspicious activity or
intrusions. But new security threats can be recognized only
when we provide an efficient way for pattern/anomaly
recognition on larger volumes and a greater variety of data.
Another critical issue for each enterprise is to detect and
prevent fraudulent activities by internal or external parties.
This is why for security application we need new methods and
tools to Improve risk assessment and associated scoring by
building sophisticated machine learning models that can take
into account hundreds or even thousands of indicators and
complex patterns introduced by the cooperation of systems
and people and detectable only on using higher levels of
network dependencies.

The purpose of this track is two-fold: Firstly, the track
offers a forum for scientists and engineers to exchange ideas
on novel analytical techniques using network log data. Secondly, the track has a thematic focus on emerging
technology for a complex network, security, and privacy.

II. ACCEPTED PAPERS

The papers submitted to the track have undergone a thorough
review process. Each paper has been reviewed by at least two
members of the program committee. At the end of the review
process, the following six papers have been accepted for
publication and presentation at the conference:

• Structural analysis and link prediction in dynamic
networks of Web services(full paper): the paper presents
a model of dynamic networks of Web services, which
allows to define and analyze the patterns of execution of
Web services. This concept is illustrated by an
experiment involving two service repositories, which
provide services in service composition framework.

• Bringup a NetFPGA setup for projects at Wroclaw
university of Technology (full paper): the paper describes
possibilities of utilization of NetFPGA 1G cards with
modern operating systems and research laboratories.
Moreover, the limitations resulting from the NetFPGA
has no longer been supported by FPGA chip producer
have been described. Authors prepared the low-level
software to perform network analysis and measurements
and integrate the NetFPGA card with polish national
network research testbed PL-LAB and Wroclaw node of
European consortium FIWARE Lab. Application
prepared in this way allows performing high accurate
measurements in experiments related with resources
consumption in distributed service based systems.

ACKNOWLEDGMENT

The track organizers sincerely express their gratitude to the
program committee members for their thorough effort on
setting up the track and reviewing submitted papers.