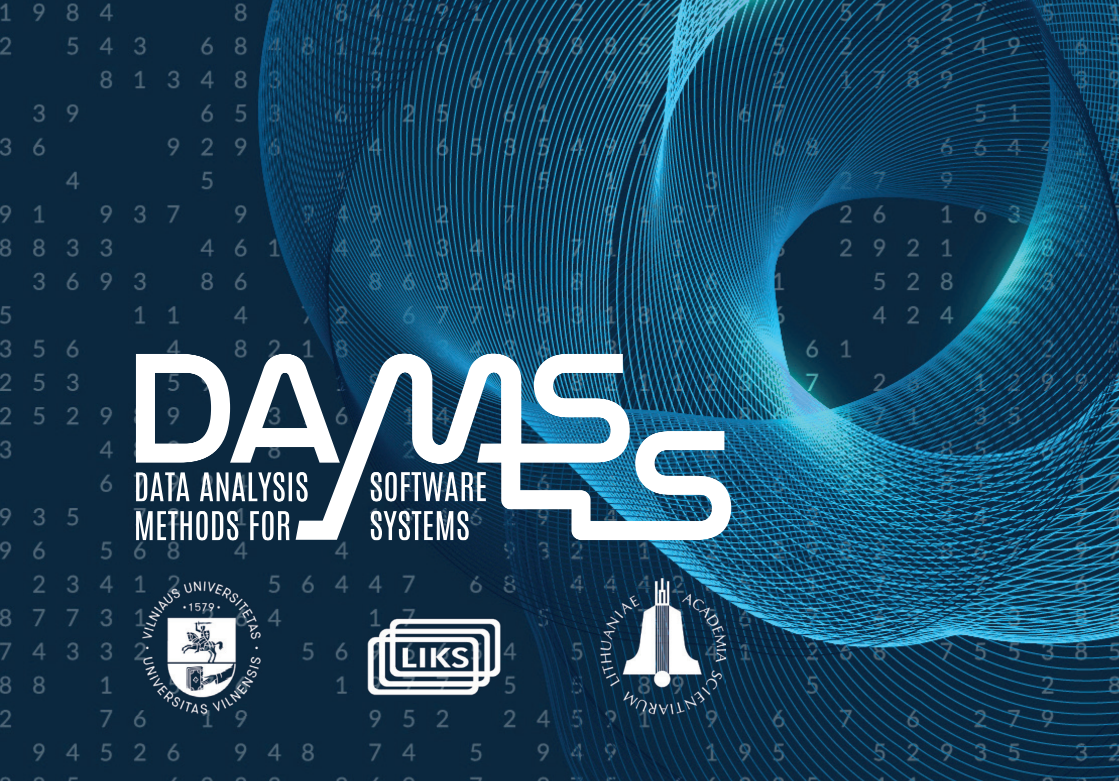

DAMSS
DATA ANALYSIS METHODS FOR SOFTWARE SYSTEMS
VILNIAUS UNIVERSITETAS · 1579 · UNIVERSITAS VILNENSIS
LIKS
ACADEMIA SCIENTIARUM LITHUANIAE

15th Conference on

DATA ANALYSIS METHODS for Software Systems

November 28–30, 2024

Druskininkai, Lithuania, Hotel "Europa Royale"
https://www.mii.lt/DAMSS

Co-Chairmen:

Prof. **Gintautas Dzemyda** (Vilnius University, Lithuanian Academy of Sciences)
Dr. **Saulius Maskeliūnas** (Lithuanian Computer Society)

Programme Committee:

Dr. **Jolita Bernatavičienė** (Lithuania)
Prof. **Juris Borzovs** (Latvia)
Prof. **Janis Grundspenkis** (Latvia)
Prof. **Janusz Kacprzyk** (Poland)
Prof. **Ignacy Kaliszewski** (Poland)
Prof. **Bożena Kostek** (Poland)
Prof. **Tomas Krilavičius** (Lithuania)
Prof. **Olga Kurasova** (Lithuania)
Assoc. Prof. **Tatiana Tchemisova** (Portugal)
Assoc. Prof. **Gintautas Tamulevičius** (Lithuania)
Prof. **Julius Žilinskas** (Lithuania)

Organizing Committee:

Dr. **Jolita Bernatavičienė**
Prof. **Olga Kurasova**
Assoc. Prof. **Viktor Medvedev**
Laima Paliulionienė
Assoc. Prof. **Martynas Sabaliauskas**
Prof. **Povilas Treigys**

Contacts:

Dr. Jolita Bernatavičienė
jolita.bernataviciene@mif.vu.lt
Tel. (+370 5) 2109 315
Prof. Olga Kurasova
olga.kurasova@mif.vu.lt

https://doi.org/10.15388/DAMSS.15.2024

ISBN 978-609-07-1112-5 (digital PDF)

Evidence-Based Network Flow Modelling and Assessment for Cyber Security

Virgilijus Krinickij, Linas Bukauskas

Institute of Computer Science
Vilnius University

virgilijus.krinickij@mif.vu.lt

In the rapidly evolving landscape of cybersecurity, real-time detection and alignment of network incidents and anomalies have become critical. Traditional methodologies for incident detection often rely on offline PCAP file analysis, which is not feasible in the context of modern network environments where real-time assessment is paramount. Additionally, many current techniques suffer from inherent limitations due to data buffer and window size constraints, reducing their effectiveness in capturing and aligning incidents across asynchronous network flows. The increasing complexity of cyber attacks, combined with the volume of network traffic, demands highly efficient, real-time solutions for anomaly detection that are both scalable and responsive to evolving threats. The core challenge addressed in this research is the inadequacy of current algorithms and methods for network flow alignment to process the volume and speed of real-time network flows. Algorithms such as Dynamic Time Warping (DTW), Needleman-Wunsch, and others – commonly used in sequence alignment – are applied in this context to align and detect anomalies in network flows. However, these algorithms are traditionally computationally expensive, requiring significant processing power. This work explores an innovative approach to incident and anomaly detection in real-time network flows using machine learning algorithms coupled with asynchronous alignment techniques. Unlike traditional methods, which struggle with computational overhead and delays due to their reliance on synchronous data windows, the proposed solution leverages asynchronous network flows to simulate cyber incidents in synthetic scenarios. These simulations allow the machine learning models to dynamically adapt to the evolving nature of network traffic without being constrained by static buffer sizes or fixed time windows. The paper dem-

onstrates how applying asynchronous alignment techniques to real-time network flows can provide a robust framework for detecting anomalies and cyber incidents more effectively. We evaluate these algorithms' performance under synthetic, simulated cyber attack scenarios, highlighting their strengths and weaknesses in terms of speed, accuracy, and computational efficiency. By focusing on the dynamic nature of modern network traffic, we present a novel methodology that can significantly enhance the capability of cybersecurity systems to detect and respond to incidents in real time without the need for pre-captured data such as PCAP files. Ultimately, this research addresses the growing need for real-time, asynchronous network flow assessment using machine learning in cybersecurity, providing an effective solution to the limitations of current incident alignment techniques. This approach improves the speed and accuracy of incident detection and offers a scalable model that can be applied in diverse network environments. We demonstrate the effectiveness of our approach through experimental evaluations using real-world network flows. Overall, our work contributes to advancing the field of network traffic analysis by introducing a novel approach that addresses the limitations of traditional synchronous methods and provides a foundation for more robust and adaptive cyber security solutions.