



Contribution ID : 33

Type : Talk

Preliminary study on artificial intelligence methods for cybersecurity threat detection in computer networks based on raw data packets

Wednesday, 5 June 2024 13:55 (25)

Most of the methods of the intrusion detection systems for cybersecurity threats detection in computer networks are based on traffic flow characteristics. However, this approach may not fully exploit the potential of deep learning algorithms to directly extract features from raw packets. Moreover, it impedes real-time monitoring due to the necessity of waiting for the processing pipeline to complete and introduces dependencies on additional software components.

In this paper, we investigate deep learning methodologies capable of detecting attacks in real-time directly from raw packet data within network traffic. Our investigation utilizes the CICIDS2017 dataset, which includes both benign traffic and prevalent real-world attacks, providing a comprehensive foundation for our research.

Primary author(s) : OGONOWSKI, Aleksander (National Centre for Nuclear Research); Mr ŻEBROWSKI, Michał (National Centre for Nuclear Research); ĆWIEK, Arkadiusz (National Centre for Nuclear Research)

Presenter(s) : OGONOWSKI, Aleksander (National Centre for Nuclear Research); Mr ŻEBROWSKI, Michał (National Centre for Nuclear Research)

Session Classification : High Performance Computing

Track Classification : High Performance Computing