Summary of the doctoral dissertation

Implementation of synchronization algorithms for network devices based on the paradigm of programmable computer networks

Author: M. Sc. Eng. Jaroslaw Homa

Promoter: Prof. Aleksander Nawrat

The thesis and purpose of the PhD thesis is: "It is possible to develop a network attack mitigation system based on a programmable computer network solution." The main goal of the author in his PhD thesis was to develop a system for detecting DDoS type network attacks, based on the SDN solution. The author has developed and implemented a system called STRAINER, the system has a modular structure and consists of three detection modules. Two modules contain AI solutions, including ML machine learning and DL deep learning.

The implementation of the PhD dissertation required a thorough literature review, presenting the current state of knowledge in the field of DDoS attack detection methods using SDN computer networks. Presentation of current research on SDN computer network systems, analysis of network attack mitigation, including DDoS attacks. Overview of network attack detection algorithms, standard method algorithms, AI algorithms, ML machine learning and DL deep learning.

The main task was to fulfill the thesis of the work by developing a solution to the problem, including the creation of an IT system for DDoS attack mitigation based on the SDN network paradigm. The author designed and constructed a system with the working name STRAINER. The built system is based on the SDN concept, with an implemented central network controller, which is integrated with executive modules and detection algorithms implemented in them to detect network attacks. The system has three detection modules, respectively MOD1, MOD2, MOD3. The first module makes detection based on Entropy of network traffic, it is a "light" detection system. MOD2 features an ML machine learning solution with the "Random Forest of Random Forest" algorithm. The last module is the MOD3 module based on the DL deep machine learning mechanism, mainly

used to detect unknown types of network attacks. The system also has IDS probes as anomaly detectors, as well as other necessary subsystems, i.e. data collector, network infrastructure.

The author has performed a number of tests in a laboratory and production environment confirming the effectiveness and detection of DDoS attacks of the STRAINER system.

The complete system was installed, configured and launched in the production environment of the company where the author was carrying out his implementation doctorate