Temat: **„Optimizing Critical Function Placement to Ensure Resilient Network Services — Selected Problems" (pl. Optymalizacja rozmieszczenia funkcji krytycznych dla zapewnienia odporności usług sieciowych — wybrane problemy)**

Streszczenie

Praca dotyczy optymalizacji rozmieszczenia funkcji krytycznych w węzłach sieci dla zapewnienia odporności usług sieciowych. Usługi sieciowe (ang. *network services*) zapewniające użytkownikom możliwość przesyłania danych przez sieć (np. głos, wideo, e-mail, www, rozproszony system plików) są podatne na różnorodne ataki cybernetyczne. Badania prowadzi się w trzech obszarach proponując nowe metody ochrony usług sieciowych i zwiększania ich odporności (ang. *resilience*) na ataki na dostępność. Wszystkie trzy obszary badawcze dotyczą rozmieszczenia krytycznych funkcji sieciowych (ang. *network function*) w węzłach sieci, w sposób zwiększający odporność sieci na wybrane ataki na dostępność.

Pierwszy obszar badań dotyczy rozlokowania sterowników SDN (ang. *Software Defined Network*) w modelu wielu sterowników (ang. *multi-controller design*) oraz identyfikacji węzłów najbardziej podatnych na ataki. Celem operatora jest maksymalizacja przeżywalności sieci, podczas gdy celem atakującego jest minimalizacja przeżywalności sieci. Miarą przeżywalności sieci jest liczba przełączników, które przetrwały atak, czyli takich dla których istnieje ścieżka do kontrolera który przetrwał atak.

Drugi obszar badawczy koncentruje się na rozmieszczeniu czujników wykrywających ataki DDoS (*Distributed Denial of Service*) w węzłach sieciowych. Celem jest minimalizacja (maksymalnego możliwego) niekontrolowanego ruchu sieciowego między danym zestawem źródeł ataku (węzły sieci) i celami ataku (węzły sieci).

Trzeci obszar badawczy podejmuje jednoczesną optymalizację routingu i rozmieszczenia funkcji przetwarzania ruchu (wybór centrów danych) przy budowie łańcuchów funkcji sieciowych (ang. *service chains*) tworzących infrastrukturę usług sieciowych. Wybrane funkcje w łańcuchu mogą mieć charakter ochrony przed atakami (np. firewall, czy system wykrywania intruzów (ang. *Intrusion Detection System*).

W badaniach wykorzystano teorię grafów, programowanie matematyczne oraz teorię gier. Opracowano modele programowania liniowego MIP (ang. \textit{Mixed Linear Programming}) oraz heurystyki dla sieci o dużej skali. Algorytmy zostały zaimplementowane i na podstawie eksperymentów obliczeniowych porównano ich efektywność.

Słowa kluczowe: *sieci sterowane programowo, rozmieszczenie sterowników, wirtualizacja funkcji sieciowych, rozproszony atak na dostępność usługi, rozmieszczenie łańcuchów funkcji sieciowych*

Abstract

The dissertation addresses the optimization of the placement of critical functions in network nodes to ensure the resilience of network services. Network services providing users with data transmission capabilities over the network (e.g., voice, video, e-mail, web, distributed file system) are vulnerable to various cyber-attacks. The three research studies propose new methods of protecting network services and increasing their resilience to attacks on availability. All three research areas concern the deployment of critical network functions in network nodes in a way that increases the network's resilience to selected availability attacks.

The first research area concerns the placement of SDN (*Software Defined Network*) controllers in a multi-controller design model and the identification of nodes most vulnerable to attacks. The goal of the network operator is to maximize network survivability, while the adversary's goal is to minimize network survivability. The measure of network survivability is the number of attack-surviving switches, i.e., those for which there is a path to the attack-surviving controller.

The second research area focuses on placing sensors detecting DDoS attacks (*Distributed Denial of Service*) in network nodes. The goal is to minimize (maximum possible) uncontrolled network traffic between the given set of attack sources (network nodes) and attack targets (network nodes).

The third research area addresses the simultaneous optimization of routing and placement of traffic processing functions (selection of data centers) while building network function chains (*service chains*) that form the network services infrastructure. Selected functions in the service chain may be protective against attacks (e.g., firewall or intrusion detection system).

The research uses graph theory, mathematical programming, and game theory. MIP models (Mixed Linear Programming) and heuristics for large-scale networks were developed. The algorithms were implemented, and based on computational experiments, their effectiveness was compared.

Keywords: *software defined network, control placement problem, network function virtualization, distributed denial of service, service function chaining*