Politechnika Śląska
Wydział Automatyki, Elektroniki i Informatyki
Kierunek Informatyka

Rozprawa doktorska

Implementacja algorytmów synchronizacji urządzeń sieciowych bazujących na paradygmacie programowalnych sieci komputerowych

Autor: mgr inż. Jarosław Homa
Promotor: prof. dr hab. inż. Aleksander Nawrat
Promotor pomocniczy: dr inż. Krzysztof Daniec

Gliwice, 2023

Streszczenie rozprawy doktorskiej

Implementacja algorytmów synchronizacji urządzeń sieciowych bazujących na paradygmacie programowalnych sieci komputerowych

Autor: mgr inż. Jarosław Homa

Promotor: Prof. dr hab. inż. Aleksander Nawrat

Teza i cel pracy doktorskiej brzmi: „Możliwe jest opracowanie systemu mitygacji ataków sieciowych, opartego o rozwiązanie programowalnych sieci komputerowych". Głównym celem autora w pracy doktorskiej było opracowanie systemu do wykrywania ataków sieciowych typu DDoS, opartego o rozwiązanie SDN. Autor opracował i wdrożył system pod nazwą STRAINER, system posiada budowę modularną, składa się z trzech modułów detekcyjnych. Dwa moduły zawieraj rozwiązania sztucznej inteligencji AI, w tym uczenia maszynowego ML, jak i głębokiego uczenia maszynowego DL.

Realizacja rozprawy doktorskiej wymagała gruntownego przeglądu literaturowego, zaprezentowanie aktualnego stanu wiedzy w zakresie metod wykrywania ataków DDoS z wykorzystaniem sieci komputerowych SDN. Przedstawienie aktualnych badań dot. systemów sieci komputerowych SDN, analiza mitygacji ataków sieciowych z uwzględnieniem ataków DDoS. Przegląd algorytmów wykrywania ataków sieciowych, algorytmów opartych o standardowe metody, algorytmów sztucznej inteligencji AI, uczenia maszynowego ML i głębokiego uczenia maszynowego DL.

Głównym zdaniem było spełnienie tezy pracy poprzez opracowanie rozwiązania problemu, w tym utworzenie systemu informatycznego mitygacji ataków DDoS opartego o paradygmat sieci SDN. Autor zaprojektował i skonstruował system o roboczej nazwie STRAINER. Zbudowany system oparty jest o koncepcję SDN, z zaimplementowanym centralnym kontrolerem sieci, który zintegrowany jest z modułami wykonawczymi, zaimplementowanymi w nich algorytmami detekcyjnymi do wykrywania ataków sieciowych. System posiada trzy moduły detekcyjne odpowiednio MOD1, MOD2, MOD3. Pierwszy moduł dokonuje detekcji w oparciu o Entropie ruchu sieciowego, jest „lekkim" systemem detekcji. MOD2 zawiera rozwiązanie uczenia maszynowego ML z algorytmem „Random Forest of Random Forest". Ostatni moduł to moduł MOD3 oparty o mechanizm głębokiego uczenia maszynowego DL, służący głównie do wykrywania nie znanych rodzajów ataków sieciowych. System posiada również sondy IDS, w roli detektorów anomalii, jak również niezbędne inne podsystemy tj. kolektor danych, infrastruktura sieciowa.

Autor wykonała szereg testów w środowisku laboratoryjnym i produkcyjnym potwierdzających skuteczność działania i detekcji ataków DDoS systemu STRAINER.

Kompletny system została zainstalowany, skonfigurowany i uruchomiony w środowisku produkcyjnym przedsiębiorstwa, w którym autor realizował doktorat wdrożeniowy