Prof. dr hab. inż. Krzysztof Wawryn
Wydział Elektroniki i Informatyki
Politechnika Koszalińska
ul. Śniadeckich 2, 75-453 Koszalin

Koszalin, 21 kwietnia 2022 roku

Opinia
o rozprawie doktorskiej mgr inż. Patryka Widulińskiego
pt: " *Algorytmy detekcji infekcji programów komputerowych inspirowane biologicznymi mechanizmami immunologicznymi* "

Rozprawa zawiera pięć rozdziałów oraz bibliografię. W rozprawie mgr Widuliński podejmuje temat poszukiwania infekcji w zasobach komputerowych za pomocą algorytmów naśladujących immunologiczne mechanizmy organizmów żywych. Jest to temat ważny z punktu widzenia rozwoju nowoczesnych metod detekcji infekcji komputerowych znanych w literaturze jako „Intrusion Detection Systems". Obejmuje on aktualne zagadnienia zgodne z trendami światowymi i nawiązuje do najnowszych badań w tej dziedzinie, bowiem algorytmy detekcji zagrożeń znajdują współcześnie wiele praktycznych zastosowań przede wszystkim w ochronie programowych zasobów w komputerach (IDS) jak i przesyłanych za pomocą rozległych sieci komputerowych (NIDS).

Przedmiotem badań podjętym w rozprawie przez mgr Widulińskiego było poszukiwanie algorytmów detekcji intruzów atakujących zasoby programowe komputera. Projektanci oprogramowania zwalczającego zagrożenia systemów komputerowych pochodzące z cyberprzestrzeni zmagają się z coraz to nowymi wyzwaniami. Dlatego poszukują niekonwencjonalnych rozwiązań. Od kilku lat preferowane są rozwiązania z zakresu sztucznej inteligencji. Wykorzystuje się w nich matematyczne modele różnych funkcji biologicznych organizmów żywych. Okazuje się, że nawet bardzo proste modele pozwalają na uzyskiwanie bardzo dobrych rezultatów w różnych praktycznych zastosowaniach. Tak jest w przypadku sztucznych sieci neuronowych, algorytmów ewolucyjnych czy algorytmów odpornościowych naśladujących odpowiednio działanie systemu nerwowego, mechanizmów dziedziczenia cech czy odporności organizmów żywych. Dlatego dotychczasowe rozwiązania detekcji infekcji oprogramowania komputerów są wbogacane o algorytmy wzorowane na wybranych mechanizmach immunologicznych.

Celem pracy było opracowanie nowego algorytmu detekcji infekcji programów komputerowych, inspirowanych mechanizmami obronnymi organizmów żywych, a tezą, że możliwa jest realizacja algorytmów detekcji infekcji o właściwościach porównywalnych lub lepszych od znanych rozwiązań w tym znanych z literatury rozwiązań wykorzystujących sztuczne systemy immunologiczne. Cel i teza pracy wraz z uzasadnieniem podjęcia badań na podstawie analizy istniejących rozwiązań detekcji infekcji programów komputerowych naśladujących biologiczne mechanizmy obronne Autor rozprawy przedstawił w rozdziale 1.

Dla osiągnięcia celu i udowodnienia tezy pracy mgr Widuliński wykorzystał wybrane mechanizmy stosowane w biologicznych systemach immunologicznych do poszukiwania infekcji komputerowych. Przedstawienie opracowanego algorytmu oraz wyników swoich badań Autor rozpoczął od wprowadzenia w rozdziale 2 pojęć z zakresu bezpieczeństwa systemu komputerowego, metod wykrywania infekcji programów komputerowych, w tym także za pomocą algorytmów naśladujących mechanizmy obronne organizmów żywych. W wyniku analizy istniejących rozwiązań zaproponował własny algorytm wykrywania infekcji

Zasadnicza część pracy jest zawarta w rozdziałach 3 i 4. W rozdziale 3 mgr Widuliński wykorzystał rozważania teoretyczne dotyczące poszukiwania nowych, oryginalnych metod detekcji zagrożeń w systemach komputerowych, do opracowania własnego algorytmu o praktycznym zastosowaniu. W opracowaniu algorytmu detekcji infekcji programów komputerowych Autor zastosował jedną z metod stosowanych przez mechanizmy immunologiczne. Jest to metoda selekcji negatywnej wzorowana na działaniu limfocytów typu T, która za pomocą receptorów limfocytów rozpoznaje intruzów w organizmach żywych. Do wyznaczania zbioru receptorów wykorzystana została metoda podziału szablonów na własne i obce, przy czym szablony obce zostawały wybrane jako receptory do poszukiwania intruzów. Metody wykorzystujące szablony ulegały w ostatnich latach licznym modyfikacjom. Mgr Widuliński opracował własną modyfikację algorytmu. Polega ona na zastosowaniu, oprócz zbioru receptorów podstawowych, dodatkowego zbioru receptorów międzykomórkowych zwiększających wykrywalność infekcji. Wyjaśnił także jaki jest wpływ jego modyfikacji nie tylko na większą skuteczność wykrywania zagrożeń, ale także złożoność obliczeniową i zajętość pamięci komputera. W przypadku opracowanej metody dokonał dodatkowo własnej oryginalnej minimalizacji redukującej receptory nadmiarowe. Skutkuje to mniejszą zajętością pamięci i zmniejszeniem czasu wykrywania infekcji. Uzasadnił również konieczność wykonania licznych badań eksperymentalnych potwierdzających przewidywane efekty detekcji infekcji jak to ma miejsce w istniejących rozwiązaniach literaturowych.

Rezultaty działania opracowanego algorytmu detekcji infekcji w programach komputerowych mgr Widuliński zweryfikował badaniami eksperymentalnymi zaprezentowanymi w rozdziale 4. W badaniach przeprowadził liczne testy wyznaczające wykrywalność infekcji, zajętość pamięci i czas wykrywania infekcji. Testy zostały przeprowadzone dla każdego z trzech parametrów oddzielnie dla różnych wartości wielkości receptorów i progów aktywacji. Zostały one przedstawione w licznych tabelach i skomentowane wnioskami o optymalnych wartościach tych wielkości dla danego programu. W celu końcowej weryfikacji opracowanych algorytmów Autor porównał ich działanie ze znanymi rozwiązaniami dla stosowanych w literaturze plików testowych ze względu na skuteczność wykrywania zagrożeń, złożoność obliczeniową i zajętość pamięci komputera. Wyniki badań potwierdzają zalety proponowanych przez Autora rozwiązań. Spełniają więc warunek określony w tezie pracy.

W rozdziale 5 mgr Widuliński przedstawił wnioski końcowe i wymienił zalety opracowanego algorytmu detekcji infekcji programów komputerowych inspirowanego mechanizmami odpornościowymi organizmów żywych.

Podsumowując stwierdzam, że praca stanowi nową pozycję z zakresu algorytmów rozpoznawania zagrożeń w systemach komputerowych i może inicjować inne prace tego typu. Do osiągnięć autora wnoszących wkład do nauki należą:

- opracowanie algorytmu wyznaczania receptorów za pomocą wzorców zmodyfikowanego o wyznaczanie receptorów międzykomórkowych,
- opracowanie algorytmu optymalizacji liczby receptorów prowadzącą do minimalizacji zajętej pamięci,
- eksperymentalne badania porównawcze następujących algorytmów z algorytmami zaproponowanymi w literaturze ostatnich kilku lat dla następujących parametrów:
  - wykrywalności infekcji,
  - szybkości działania,
  - zajętości pamięci.

Biorąc pod uwagę wyżej wymienione osiągnięcia w mojej opinii cel pracy został osiągnięty, a teza dowiedziona.

Konkluzja

Mając na uwadze osiągnięcia mgr inż. Patryka Widulińskiego, nowatorski charakter rozprawy oraz poznawcze i praktyczne znaczenie wyników według mojej opinii praca spełnia wymagania stawiane rozprawom doktorskim przez obowiązujące przepisy i wnioskuję o dopuszczenie jej do dalszych etapów przewodu.