Streszczenie

Algorytmy detekcji infekcji programów komputerowych inspirowane biologicznymi mechanizmami immunologicznymi

mgr inż. Patryk Widuliński

Systemy komputerowe są w dzisiejszych czasach bardzo popularne. Niestety, wraz ze wzrostem ich popularności pojawili się aktorzy, którzy w różnych celach dążą często do nieuprawnionego dostępu do danych użytkowników. W celu znalezienia odpowiedzi na zagrożenia powstały IDS (ang. intrusion detection systems) - systemy wykrywania intruzji. W ostatnich latach naukowcy zainspirowani byli do znalezienia nowoczesnych rozwiązań pozwalających na wykrywanie intruzji. Badacze zauważyli pewne paralele między celami IDS i biologicznych systemów immunologicznych. Dzięki temu powstały sztuczne systemy immunologiczne (AIS - ang. artificial immune systems). Celem rozprawy była analiza istniejących i opracowanie własnego algorytmu detekcji infekcji programów komputerowych, inspirowanego mechanizmami obronnymi organizmów żywych. Rozprawa stawia tezę, że możliwa jest realizacja algorytmów detekcji infekcji programów komputerowych o właściwościach porównywalnych lub lepszych od znanych rozwiązań, w tym znanych z literatury rozwiązań wykorzystujących AIS. W niniejszej rozprawie doktorskiej przeprowadzono kompleksowy przegląd literatury dotyczącej IDS i AIS, i w szczególności najpopularniejszego algorytmu AIS, jakim jest algorytm negatywnej selekcji (NSA - ang. negative selection algorithm). Zaproponowano następnie własny system wykrywania intruzji, który pozwala na wykrywanie infekcji w systemie operacyjnym. W systemie zaimplementowano metodę losową i metodę wzorców, a następnie przedstawiono autorskie ulepszenie tych metod przy pomocy dodatkowego zbioru receptorów międzykomórkowych. System dogłębnie przetestowano dla szerokiej gamy parametrów wejściowych generacji receptorów, a następnie porównano osiągi z innymi rozwiązaniami znanymi z literatury. Badania eksperymentalne pokazały, że system IDS osiąga wyniki porównywalne lub lepsze od wyników znanych z literatury. Na podstawie badań eksperymentalnych wyciągnięto wnioski, że cel pracy został osiągnięty, a teza dowiedziona. Dalsze badania mogą uwzględniać możliwości naprawy zainfekowanych plików w systemie operacyjnym.