Politechnika Opolska

Wydział Elektrotechniki, Automatyki i Informatyki

mgr inż. Piotr Witkowski

Streszczenie rozprawy doktorskiej pt.: „Metody szyfrowania danych w sieciach komputerowych z wykorzystaniem informacji kodowanych w sieci elektroenergetycznej” przygotowanej pod kierunkiem dr hab. inż. Jarosława Zygarlickiego

Celem rozprawy doktorskiej jest analiza możliwości wykorzystania stochastycznego charakteru globalnych fluktuacji częstotliwości harmonicznej podstawowej przebiegu napięcia w sieciach elektroenergetycznych, do opracowania algorytmu generowania i rozpowszechniania liczb losowych, które mogą być stosowane przy implementacjach algorytmów szyfrujących w globalnych sieciach transmisji danych.

W pracy postawiono następująca tezę:

„Wykorzystanie zmiennych w czasie globalnych parametrów rejestrowanych w sieci elektroenergetycznej umożliwia tworzenie niepowtarzalnych kluczy szyfrujących, zwiększających bezpieczeństwo danych przesyłanych w sieciach komputerowych.”

Podczas realizacji prac związanych z rozprawą doktorską, zaprojektowano oraz zaimplementowano stanowiska pomiarowe rozmieszczone w dwóch oddalonych od siebie lokalizacjach. Opracowano i wdrożono oprogramowanie dla utworzonych stanowisk, działających na zasadzie serwerów oraz jednostki typu klient. Miało to na celu opracowanie generatora liczb losowych, który następnie poddano testom zgodnym z wytycznymi NIST.
Praca została podzielona na dziewięć niżej wymienionych rozdziałów:

- rozdział pierwszy to przedstawienie celu i zakresu pracy,
- rozdział drugi stanowi wprowadzenie obejmujący obszar prowadzonych badań oraz uzasadnienie tematu badawczego,
- rozdział trzeci jest studium literaturowym, przedstawiającym wykorzystaną podczas pisania pracy literaturę,
- w rozdziale czwartym przedstawiono opracowany projekt oprogramowania służącego do realizacji badań w pracy. Wykorzystując narzędzia zapożyczone z analizy strukturalnej oraz obiektowej opracowano analityczną koncepcję diagramów systemu informatycznego zaimplementowanego i wykorzystanego na późniejszych etapach realizacji niniejszej pracy. Na początku rozdziału zaprezentowano budowę stanowisk pomiarowych, uwzględniając podział na stanowiska: serwery oraz klient. Przedstawiono szczegółowy dobór narzędzi i urządzeń, zastosowanych do zaimplementowania stanowisk oraz schematy podłączenia urządzeń,
- w rozdziale piątym przedstawiono poszczególne metodyki badań, które zostały wykorzystane podczas prac nad rozprawą doktorską. Skupiono się na szczegółowym opisaniu zastosowanych metod objaśniając procesy przetwarzania sygnałów elektroenergetycznych, doprowadzeniu ich do postaci wspólnej korelacji sygnałowej za pomocą filtrów, generowaniu ciągów liczbowych celem przeprowadzenia testów na ich prawdziwą losowość,
- w rozdziale szóstym przedstawiono wyniki testów statystycznych rekomendowanych przez NIST, wykonanych w celu sprawdzenia czy liczby generowane przez opracowany w rozprawie RNG są liczbami prawdziwie losowymi, mając wykonane podstawowe testy przeprowadzono dalszą analizę statystyczną otrzymanych wyników,
- rozdział siódmy jest podsumowaniem otrzymanych w pracy wyników badań, porównano w nim wyniki badań otrzymane z innych generatorów liczb losowych,
- rozdział ósmy przedstawia wnioski oraz dalsze plany badawcze,

- rozdział dziewiąty stanowi literatura wykorzystana w pracy.