dr hab. inż. Aleksandra Świetlicka
Instytut Automatyki i Robotyki
Politechnika Poznańska
60-965 Poznań, ul. Piotrowo 3A

Poznań, dn. 4.08.2023 r.

Recenzja rozprawy doktorskiej mgr. inż. Piotra Witkowskiego pt. „Metody szyfrowania danych w sieciach komputerowych z wykorzystaniem informacji kodowanych w sieci elektroenergetycznej"

1. Podstawy formalne

Niniejsza recenzja napisana została na podstawie Uchwały Rady Naukowej Dyscypliny Automatyka, Elektronika, Elektrotechnika i Technologie Kosmiczne Politechniki Opolskiej z dnia 1 czerwca 2023 r. o powołaniu recenzentów w ww. rozprawie doktorskiej. Recenzja przygotowana została na podstawie Ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz.U. 2018 poz. 1668). Rozprawa mgra inż. Piotra Witkowskiego napisana została w języku polskim, pod kierunkiem promotora dr hab. inż. Jarosława Zygarlickiego, prof. uczelni oraz promotora pomocniczego dr hab. inż. Aleksandry Kawala-Sterniuk, prof. uczelni.

2. Zakres tematyczny rozprawy

Doktorant w rozprawie analizuje możliwość wykorzystania entropii pochodzącej z nieprzewidywalnych zjawisk obserwowanych w zarejestrowanych przebiegach czasowych napięcia do stworzenia metod szyfrowania danych w globalnych sieciach informacyjnych. Opracował nową metodę generowania liczb losowych opartą na entropii zmiennych częstotliwości harmonicznych napięcia elektroenergetycznego. Bezpieczeństwo metody opiera się na filtrach o określonych parametrach, co wymaga znajomości tych parametrów przez atakującego, aby odczytać przesyłane dane. Praca rozważa również inne techniki zabezpieczeń przed dostępem osób trzecich.

W rozprawie Doktorant przedstawił przegląd literatury dotyczący parametrów jakości energii elektrycznej oraz metod szyfrowania. Przeprowadzone przez Doktoranta badania wykazują, że niechciane parametry, takie jak entropia wywołana zmiennością częstotliwości harmonicznej podstawowej napięcia elektroenergetycznego, mogą być wykorzystane w kryptografii poprzez wprowadzenie nowych algorytmów szyfrowania lub modyfikację istniejących rozwiązań.

Doktorant przedstawił następującą tezę rozprawy:
„Wykorzystanie zmiennych w czasie globalnych parametrów rejestrowanych w sieci elektroenergetycznej umożliwia tworzenie niepowtarzalnych kluczy szyfrujących, zwiększających bezpieczeństwo danych przesyłanych w sieciach komputerowych".

Podjęta tematyka badawcza jest istotna ze względu na kilka powiązanych ze sobą aspektów:

- Ochrona poufności danych: W sieciach komputerowych, szczególnie w Internecie, wiele informacji jest przesyłanych przez publiczną infrastrukturę, co oznacza, że są one narażone na ryzyko podsłuchu przez niepożądane osoby. Szyfrowanie danych

A. Św.

zapewnia, że tylko osoby posiadające odpowiedni klucz mogą odczytać przesyłane informacje, co zabezpiecza je przed nieuprawnionym dostępem.

- Zapewnienie integralności danych: Szyfrowanie danych w sieciach komputerowych pomaga również w zapewnieniu integralności informacji. Pozwala to wykryć wszelkie próby zmiany lub manipulacji danych podczas ich przesyłania. W przypadku próby modyfikacji danych, szyfrowanie powoduje, że dane stają się nieczytelne lub niepoprawne, co sygnalizuje możliwość naruszenia.
- Ochrona przed atakami typu "man-in-the-middle": Ataki typu "man-in-the-middle" polegają na podsłuchiwaniu i przekierowywaniu komunikacji pomiędzy dwoma stronami komunikującymi się ze sobą. Szyfrowanie danych utrudnia tego rodzaju atak, ponieważ atakujący nie będzie w stanie odczytać treści przesyłanych wiadomości.
- Bezpieczne transakcje online: Szyfrowanie danych jest niezwykle istotne dla bezpieczeństwa transakcji online, takich jak płatności kartami kredytowymi czy bankowymi. Bez odpowiedniego szyfrowania, dane karty kredytowej lub konta bankowego mogą zostać skradzione przez cyberprzestępców.
- Ochrona przed ransomware: Ransomware to rodzaj złośliwego oprogramowania, które blokuje dostęp do danych lub systemu i żąda okupu w zamian za przywrócenie dostępu. Szyfrowanie danych może pomóc w minimalizacji ryzyka utraty danych w wyniku takich ataków.

Integracja szyfrowania z sieciami elektroenergetycznymi może stanowić istotny element infrastruktury cyberbezpieczeństwa. W miarę jak przemysł staje się coraz bardziej zautomatyzowany i cyfrowy, zwiększa się ryzyko ataków na infrastrukturę energetyczną. Szyfrowanie danych w sieciach elektroenergetycznych może pomóc w ochronie przed cyberatakami i utrzymaniu stabilności dostaw energii.

Podsumowując, szyfrowanie danych w sieciach komputerowych jest kluczowym elementem w zapewnieniu poufności, integralności i bezpieczeństwa informacji, a także w ochronie infrastruktury krytycznej, takiej jak sieci elektroenergetyczne, przed potencjalnymi zagrożeniami.

3. Struktura rozprawy

Praca ma 127 stron, składa się z 9 rozdziałów, obejmujących Cel i zakres pracy, Wprowadzenie, Studium literaturowe, Projekt systemu, Metodologię badań, Wyniki – NIST, Podsumowanie, Wnioski oraz Literaturę.

W rozdziałach 1 i 2 Doktorant przedstawia cel i zakres pracy oraz uzasadnienie podjętej tematyki wraz ze zdefiniowaniem tezy rozprawy.

Rozdział trzeci obejmuje przegląd literaturowy.

W rozdziale czwartym Autor rozprawy omawia stworzony koncept oprogramowania, służącego do prowadzenia badań opisanych w pracy. Doktorant opracował analityczną koncepcję diagramów systemu informatycznego, które zostały wdrożone i wykorzystane w kolejnych fazach realizacji celu pracy. W początkowej części rozdziału przedstawił projekt stanowisk pomiarowych, podzielonych na sekcje: serwery oraz klient. Wnikliwie opisał dobór narzędzi i sprzętu, który posłużył do implementacji tych stanowisk, a także przedstawił schematy połączeń między urządzeniami.

W piątym rozdziale Doktorant przedstawił poszczególne strategie badawcze, które były wykorzystane podczas prowadzenia prac nad rozprawą. Skupił się na szczegółowym omówieniu zastosowanych metod, wyjaśniając procesy przetwarzania sygnałów

A. Św.

elektroenergetycznych, konwersji ich do wspólnej formy korelacji przy użyciu filtrów oraz generowaniu sekwencji liczbowych w celu przeprowadzenia testów na ich losowość.

W rozdziale szóstym Autor przedstawił wyniki testów statystycznych rekomendowanych przez NIST, zaproponowanego generatora liczb losowych.

Ostatecznie w rozdziałach 7 i 8 Doktorat podsumowuje uzyskane wyniki, redaguje wnioski oraz przedstawia plan dalszych badań.

Rozdział 9 stanowi spis literatury cytowanej w rozprawie.

4. Uwagi szczegółowe

Podczas czytania pracy nasunęło mi się kilka następujących uwag:

1) Autor w pracy pisze o istnieniu 15 testów NIST służących do sprawdzenia działania generatorów liczb losowych w aplikacjach kryptograficznych, jednak testuje tylko 5 z nich, bez wyjaśnienia dlaczego reszta nie została wykorzystana.
2) Czy na podstawie opisu we wstępie do rozdziału 4 można utworzyć schemat, który obrazowałby realizowane w pracy zagadnienie?
3) Rysunek 4.4 przedstawia, jak sądzę, zdjęcie „stanowiska klient", jednak tuż nad nim przeczytać można, że będzie on przedstawiać pewien schemat blokowy. Czy taki schemat blokowy można dodatkowo narysować?
4) Załączniki 1 i 2 oraz rysunki 4.5 - 4.15 przedstawiają diagramy; oprócz generalnego opisu teoretycznego tych diagramów w pracy zabrakło ich dokładnego opisu – odniesienia się do przedstawionych rysunków.
5) Macierz CRUD ma za zadanie zaprezentować relacje pomiędzy zbiorami danych i procesami, w których są one wykorzystywane. Tabele 4.1 - 4.9 mają przedstawiać macierze CRUD procesów elementarnych, jednak w zasadzie nie niosą żadnej praktycznej informacji. Czy jest możliwość utworzenia pełnej macierzy CRUD, która obrazowałaby cały proces?
6) Autor rozprawy nie cytuje żadnych swoich prac naukowych, jednak w Bazie Wiedzy Politechniki Opolskiej widnieją dwie prace. Czy oznacza to, że Doktorant nie ma żadnych prac związanych bezpośrednio z tematyką rozprawy?
7) W pracy znaleźć można liczne usterki językowe, kilka przykładów:
   - Autor rozprawy cytuje m.in. prace Autora Kuwałka, jednak w tekście wielokrotnie pisze o Piotrze Kuwalku.
   - Wręcz nagminne są drobne literówki, co sprawia wrażenie, że praca została napisana w pośpiechu; np. *stochastycznyczne* (drugi paragraf streszczenia), *jest udoskonalaniu* (strona 11, 8 linia od dołu, powinno być: jest na udoskonalaniu), *w oparciu liczbę badań* (strona 15, 8 linia od góry, powinno być: w oparciu o liczbę badań), *EKG. Można* (strona 17, 15 linia od góry, powinno być: EKG, można), *pozwoliło eliminację* (strona 17, 17 linia od góry, powinno być: pozwoliło na eliminację), itd.
   - Autor używa słów potocznych, zapożyczonych, np. *XOR-owanie* (strona 18, linia 14).
   - Równania powinny być numerowane z użyciem nawiasów.
   - Funkcje takie jak mod (modulo) powinny być zapisane czcionką prostą a nie kursywą.

5. Wnioski końcowe

Rozprawa doktorska poświęcona jest aktualnemu i istotnemu z punktu widzenia bezpieczeństwa w sieciach komputerowych, zagadnieniu szyfrowania danych. Jest ono kluczowym elementem w zapewnieniu poufności, integralności i bezpieczeństwa informacji,

A. Sh.

a także w ochronie infrastruktury krytycznej, takiej jak sieci elektroenergetyczne, przed potencjalnymi zagrożeniami.

Podsumowując, można stwierdzić, że pomimo pewnych uszczerbków, przedstawiona rozprawa doktorska spełnia wymagania Ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz stopniach i tytule w zakresie sztuki (Dz.U. 2003 nr 65 poz. 595) stawiane rozprawom doktorskim i wnoszę do Rady Naukowej Dyscypliny Automatyka, Elektronika, Elektrotechnika i Technologie Kosmiczne Politechniki Opolskiej o dopuszczenie jej do publicznej rozprawy.

A. Świetlicka

.....

dr hab. inż. Aleksandra Świetlicka