RDJMe.512.28.2023

Radom dnia 22.XI.2023r.

Dr hab. inż. Andrzej Puchalski, prof. URad.
Uniwersytet Radomski
Wydział Mechaniczny
Katedra Mechaniki Stosowanej i Mechatroniki

Opinia

o rozprawie doktorskiej mgra inż. **Marcina Gajdzika**

pt. „ Identification and minimization of threats in embedded systems during the car vehicles maintenance, in accordance with Industry 4.0 concept"

Promotor: dr hab. inż. **Anna Timofiejczuk**, prof. PŚ.

Promotor pomocniczy: dr inż. **Wojciech Sebzda**

Podstawa prawna recenzji: Uchwała Rady Dyscypliny Inżynieria Mechaniczna Politechniki Śląskiej z dnia 27 września 2023 roku.

1. Uzasadnienie podjęcia tematu

Trzecia dekada XXI wieku to kontynuacja niezwykle dynamicznie rozwijanych technologii cyfrowych. Technologie Przemysłu 4.0, takie jak przemysłowy internet rzeczy, uczenie maszynowe, analityka big data znajdują coraz większe zastosowanie w aplikacjach przemysłowych w celu osiągnięcia niezawodności, elastyczności, zwiększonej automatyzacji i lepszej wydajności. Dzięki postępowi inteligencji obliczeniowej, rosnącej przepustowości i możliwościom przetwarzania danych możliwe staje się tworzenie systemów autonomicznych.

Współczesne samochody o stale rosnącej liczbie współpracujących modułów elektronicznych, są przykładami zastosowań technologii, które niosą ze sobą wiele udogodnień i nowych możliwości, ale wiąże się to również z potencjalnymi zagrożeniami obejmującymi możliwość przechwytywania i ingerencji w zbiory danych. Konsekwencja takich ataków jest destabilizacja algorytmów pracy układów mechatronicznych.

Wdrażanie odpowiednich procedur zabezpieczających pojazd przed cyberatakami jest obowiązkiem producentów, także branży samochodowej. Należy reagować na ciągle pojawiające się nowe rodzaje i sposoby zagrożeń.

Niezwykle ważne jest analizowanie potencjalnych zagrożeń w obszarze systemów wbudowanych w pojazdach samochodowych. Analizy uzupełnionej opracowaniem odpowiednich procedur podjął się Autor dysertacji. Motywacją do prowadzenia badań na prezentowany temat był, jest i będzie rozwój samochodów autonomicznych, w których kwestie cyberbezpieczeństwa stawiane są na najwyższym poziomie Za właściwy kierunek badań należy uznać wykorzystanie narzędzi sztucznej inteligencji i uczenia maszynowego, ze szczególnym uwzględnieniem algorytmów głębokich sieci neuronowych, w celu odkrywania ukrytych wzorców i reprezentacji w danych.

Przedstawione wyniki badań potwierdzają wysoki potencjał praktyczny zaproponowanych metod, przewidzianych do wdrożenia w ramach nowych produktów w firmie DRAEXELMAIER.

Rozprawa doktorska jest efektem badań finansowanych przez Ministerstwo Edukacji i Nauki, nr grantu: DWD/3/33/2019.

2. Cel i zakres rozprawy

Głównym celem rozprawy doktorskiej była identyfikacja i opracowanie metod pozwalających na minimalizację potencjalnych zagrożeń wystąpienia ataków na systemy wbudowane w samochodzie.

W celu realizacji postawionych zadań Autor zaplanował i wykonał serie eksperymentów, w których skupił swoją uwagę na różnych aspektach związanych z możliwością podsłuchu i analizach opartych na sztucznej inteligencji do identyfikacji zagrożeń rozpoznawanych na podstawie anomalii.

3. Charakterystyka rozprawy

Recenzowana praca napisana jest w języku angielskim, liczy 119 stron, składa się z 4 rozdziałów, zawiera wykaz najważniejszych skrótów, wykaz rysunków i tablic oraz streszczenia. Literatura obejmuje 73 pozycje, w tym 5 publikacji z lat 2021-2023, w których doktorant jest autorem lub współautorem; w tym rozdział w monografii Advances in Technical Diagnostics II wydanej w roku 2023 przez Springer Nature Switzerland oraz artykuł w materiałach 5th International Conference on Control and Fault-Tolerant Systems, SysTols'21 France.

Praca została przygotowana niezwykle starannie z edycyjnego punktu widzenia.

Kilkustronicowe rozdziały pierwszy i ostatni to odpowiednio wstęp i podsumowanie. We wstępie umieszczono opis tła, celu i 11-to punktowego planu badań, który rozpoczyna przegląd wybranych rozwiązań w systemach wbudowanych w przemyśle motoryzacyjnym, a kończy propozycja kierunków dalszych analiz i badań. We równie zwięzłych wnioskach końcowych Autor przywołuje dwa różne zaproponowane podejścia do tematu ochrony przed atakami hakerskimi na systemy mechatroniczne pojazdu, uznając koncepcję modułów antywłamaniowych za wsparcie dla producentów oryginalnego wyposażenia (OEM).

Rozdział 2. Autor dokonał przeglądu literatury i zasygnalizował kierunki rozwoju układów samochodowych na wybranych przykładach, takich jak układ kierowniczy, hamulcowy, systemy wspomagania kierowcy. Przedstawiono główne funkcjonalności, dla których destabilizacja prawidłowego działania może stwarzać bardzo poważne ryzyko oraz z jakimi rodzajami ataków możemy sobie poradzić z funkcjonalnego punktu widzenia. Powołując się na swoją wcześniejszą publikację Autor szczegółowo opisał klasyfikację zagrożeń z punktu bezpieczeństwa funkcjonalnego: podsłuchiwanie danych, rejestracja i odtwarzanie danych, ataki typu brute-force, zmiany komunikatów magistrali CAN. Przedstawiono przykłady stosowanych ataków na pojazdy mechaniczne oraz opisano aktualnie stosowane zabezpieczenia przed cyberatakami.

W ramach stosowanych obecnie mechanizmów obronnych przed wyrafinowanymi cyberatakami scharakteryzowano szyfrowanie end to end (E2E), uznając szyfrowanie za kluczową i podstawową metodą w dziedzinie bezpieczeństwa informacji i ochrony poufnych informacji przed nielegalnym

dostępem lub przypadkowym ujawnieniem. Autor zwrócił także uwagę na obecność w pojazdach interfejsu diagnostycznego przeznaczonego do diagnostyki zewnętrznej i protokołu Unified Diagnostic Service elektronicznych modułów sterujących (ECU).

Kolejna część rozdziału obejmuje opis najczęstszych zastosowań sztucznej inteligencji w technice samochodowej. Autor skoncentrował uwagę na zaawansowanych systemach wspomagania kierowcy (ADAS), optymalizacji energetycznej, eksploatacji prognostycznej, przetwarzaniu języka naturalnego (NLP), systemach informacyjno-rozrywkowych, wizji maszynowej i cyberbezpieczeństwie.

Rozdział kończy propozycja wykorzystania modeli autoenkoderów, parametryzowanych za pomocą głębokich sieci neuronowych, do realizacji celu rozprawy wyznaczonego przez Autora rozprawy.

Rozdział 3. Autor zaprezentował wykonane badania eksperymentalne i opracowane rozwiązania. Zrealizowano 4 eksperymenty. Ich celem było sprawdzenie możliwości:

- przejęcia kontroli nad modułami sterującymi poprzez rejestrację danych transmisyjnych i odtworzenie scenariuszy poprzez odesłanie zarejestrowanych wcześniej ramek CAN na magistralę CAN,
- równoległego odczytu wartości diagnostycznych, podstawienie wartości sygnałów sterujących za pomocą programowych punktów testowych w sposób niezauważalny dla diagnozowanego pojazdu,
- zamaskowania sygnału kierunkowskazu samochodu w taki sposób, aby kierowca widział na wyświetlaczu aktywny sygnał kierunku, a nie działał kierunkowskaz tylny,
- wykrycia anomalii oznaczającej atak na układ kierowniczy pojazdu z wykorzystaniem algorytmów sztucznej inteligencji, przy założeniu wykorzystania „czarnej skrzynki" (dane są przetwarzane i analizowane, ale sygnały sterujące zawarte w danych są nieznane).

Każde doświadczenie składało się z trzech części: sprawdzenia, czy możliwe jest przeprowadzenie skutecznego ataku na wybrany elektroniczny moduł sterujący, propozycji rozwiązania zwiększającego poziom zabezpieczenia przed atakiem oraz testów walidacyjnych, mających na celu potwierdzenie skuteczności wdrożonych zabezpieczeń.

Całość pracy została podzielona na etapy badawcze, przedstawione w czterech eksperymentach. Autor skupił swoją uwagę na różnych aspektach związanych z możliwością podsłuchu, zakłócenia czy zmiany zawartości ramek podczas transmisji danych poprzez magistralę CAN. Biorąc pod uwagę aktualny stan wiedzy w zakresie transmisji magistrali CAN we współczesnych samochodach, przygotowano kilka koncepcji ataków, które można poddać testom.

Nie jest możliwe uzyskanie zabezpieczenia dającego 100% gwarancję, ponieważ nawet najbardziej efektywne algorytmy zaimplementowane w zabezpieczeniach nie są w stanie w pełni uwzględnić bardzo szybko się rozwijających nowych rodzajów zagrożeń. Rolą autorskich koncepcji przedstawionych w pracy jest minimalizowanie prawdopodobieństwa udanego ataku.

Kolejność i zakres eksperymentów zaplanowano w taki sposób, aby sprawdzić, czy możliwe jest przeprowadzenie skutecznego ataku na elektroniczny moduł wykonawczy, zwiększając poziom trudności w zależności od funkcjonalności, za jaką odpowiadał.

4. Ocena metodyki i programu badań

Opracowany w rozdziale 1 plan badań został w pełni zrealizowany. Autor przedstawił: przegląd aktualnych rozwiązań w systemach wbudowanych w przemyśle motoryzacyjnym, analizę aktualnych zagrożeń cybernetycznych dla systemów wbudowanych, opracowanie własnej koncepcji badawczo-testowej mającej na celu destabilizację normalnej pracy systemów, opracowanie koncepcji zabezpieczeń minimalizujących zagrożenia wynikające z rodzajów badanych ryzyk, rozwiązania mające na celu lepszą ochronę systemów wbudowanych pojazdu przed zagrożeniami oraz nakreślił kierunki dalszych analiz i badań. Na przygotowanym stanowisku badawczym przeprowadzono testy weryfikacyjne.

Efektem rozprawy doktorskiej było opracowanie innowacyjnych koncepcji zabezpieczeń minimalizujących prawdopodobieństwo ataku na systemy wbudowane pojazdu. Autor zaproponował zarówno proste, „stosunkowo tanie", jak i złożone rozwiązania bazujące na algorytmach sztucznej inteligencji.

Do pierwszej grupy zaliczono koncepcję okna czasowego ze znacznikiem czasu, który sprawdza ważność przesyłanych danych, koncepcję operacji XOR oraz rozszerzoną wersją okna czasowego, bazującą na podwójnej negacji bitów w każdym bajcie transmitowanej ramki.

Propozycja zaawansowanego systemu wykrywania anomalii zakłada, że każda wykryta anomalia może wskazywać na trwający atak i wykorzystuje algorytmy sztucznej inteligencji do wykrywania anomalii podczas analizy ruchu na magistrali CAN.

Skrótowy opis systemu diagnostyki modelowej bazującej na autoenkoderze wymaga sprecyzowania i uzupełnienia informacji przez Autora rozprawy. Postępy w uczeniu maszynowym, a zwłaszcza szkoleniu modeli generatywnych otworzyły w ostatniej dekadzie kolejną możliwość rozwoju metod diagnostyki bazującej na modelach. Algorytmy autoenkoderów ewoluowały osiągając możliwość generowania danych syntetycznych poprzez losowe próbkowanie z utajonej podprzestrzeni (Autoenkodery wariacyjne VAE). Ukryta reprezentacja w modelu VAE to wielowymiarowy rozkładu prawdopodobieństwa, który najlepiej określa dane wejściowe. Metody niejawnego modelowania za pomocą sieci takich jak VAE mogą być rozwiązaniem, gdy szybki dostęp do odpowiednio dużej liczbie danych o wysokiej jakości jest niemożliwy lub utrudniony, co jest standardem w systemach mechatronicznych pojazdu.

Powołując się między innymi na swój artykuł, Autor sygnalizuje dodatkową warstwę wymagań związanych z pełnym bezpieczeństwem pojazdu oraz zapewnieniem ochrony człowieka na najwyższym możliwym poziomie wynikających z normy ISO 26262. W jakim stopniu proponowane w dysertacji rozwiązania uwzględniają zapisy tego standardu, w szczególności w zakresie poziomu nienaruszalności bezpieczeństwa ASIL?

W rozprawie zabrakło także odniesienia zaproponowanych koncepcji do szczegółowego opisu architektury komponentów oprogramowania dla przemysłu motoryzacyjnego zawartego w standardzie AUTOSAR, który obsługuje min. zestaw modeli błędów komunikacyjnych i oferuje, omawiane także przez Autora, rozwiązania typu End-to-End (E2E).

5. Wniosek końcowy

Podjęta tematyka metod pozwalających na minimalizację potencjalnych zagrożeń wystąpienia ataków na systemy wbudowane jest niezwykle istotna i aktualna w erze cyberfizycznych systemów w technice motoryzacyjnej. Doktorant wykazał się szerokim zakresem wiedzy. Potwierdził umiejętność korzystania z literatury naukowej, poprawnego wnioskowania, budowy stanowiska badawczego oraz tworzenia i weryfikacji wyników programu badawczego.

Praca zawiera rozwiązanie postawionego problemu naukowego. Praca spełnia wymagania stawiane rozprawom doktorskim w dyscyplinie inżynierii mechanicznej.

Podsumowując niniejszą recenzję pracy doktorskiej Pana mgra inż. Marcina Gajdzika wykonanej pod opieką promotora Pani dr hab. inż. Anny Timofiejczuk, prof. PŚ i promotora pomocniczego Pana dr inż. Wojciecha Sebzdy stwierdzam, że praca doktorska spełnia wymagania określone w Ustawie (z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. 2018 poz. 1668 ze zm.) i wnioskuję do Rady Dyscypliny Inżynieria Mechaniczna Politechniki Śląskiej o dopuszczenie Pana mgr inż. Mateusza Kosiora do publicznej obrony.

Wnioskuję także o wyróżnienie pracy.