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

Identyfikacja oraz minimalizacja zagrożeń w systemach wbudowanych przy eksploatacji samochodów zgodnie założeniami koncepcji "Przemysł 4.0"

Rozprawa doktorska – streszczenie

Autor: mgr inż. Marcin Gajdzik

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

Opiekun z przemysłu: dr inż. Wojciech Sebzda

Politechnika Śląska, Wydział Mechaniczny Technologiczny

DIP Draexlmaier Engineering Polska Sp. z o.o.

W obliczu dynamicznego postępu w dziedzinie automatyzacji, elektromobilności oraz rosnącego znaczenia Internetu, zwłaszcza Internetu Rzeczy (IoT), fundamentalnym aspektem koncepcji Przemysłu 4.0, jest identyfikacja potencjalnych zagrożeń, które mogą wystąpić w szeroko stosowanych systemach wbudowanych. Szczególnie w sektorze motoryzacyjnym, gdzie niepoprawne działanie systemu może doprowadzić o utraty zdrowia bądź życia ludzkiego ważne jest opracowanie i wprowadzenie strategii i rozwiązań zmierzających do minimalizacji pojawiających się zagrożeń związanych z cyberbezpieczeństwem. Współczesne samochody stają się coraz bardziej zaawansowanymi i zintegrowanymi platformami technologicznymi, które przewyższają tradycyjne pojazdy pod względem funkcjonalności, wydajności i interakcji z otoczeniem. To przykład, jak Przemysł 4.0 transformuje branżę motoryzacyjną, kierując ją w stronę bardziej inteligentnej i zautomatyzowanej przyszłości. W ramach tego konceptu kładzie się szczególny nacisk na synergię zaawansowanych technologii, które są odpowiedzialne za inteligentne zarządzanie rosnącą liczbą modułów wzajemnie się komunikujących. Owa koncepcja nie tylko odzwierciedla ewolucję sektora motoryzacyjnego, ale także symbolizuje postęp w zakresie produkcji przemysłowej. Nowe technologie, które wprowadzane są w dziedzinie motoryzacji i Przemysłu 4.0, niezaprzeczalnie przynoszą liczne korzyści i otwierają nowe możliwości. Niemniej jednak, wprowadzają szereg potencjalnych zagrożeń, takich jak: możliwość kradzieży danych, destabilizacja pracy samochodu, przejęcie kontroli nad pojazdem (lub dowolnym urządzeniem mechatronicznym). Podsumowując, chociaż nowe technologie przynoszą liczne korzyści, nie można ignorować potencjalnych zagrożeń z nimi związanych. Wdrażanie odpowiednich środków bezpieczeństwa, zarówno w zakresie ochrony danych, jak i zapobiegania atakom cybernetycznym, jest kluczowe dla zapewnienia, że nowoczesne pojazdy i urządzenia mechatroniczne będą funkcjonować w sposób bezpieczny i niezawodny. Niezaprzeczalnie, rosnąca popularność samochodów elektrycznych, które są zasilane zaawansowanymi akumulatorami o wysokim napięciu, niesie ze sobą nowe wyzwania z zakresu bezpieczeństwa. W przypadku tych pojazdów, istnieje realne ryzyko, że brak odpowiedniego zabezpieczenia modułu sterującego może umożliwić nieuprawnionym osobom wykorzystanie

pojazdu w sposób niezgodny z jego przeznaczeniem. W związku z tym, kluczowe jest zrozumienie potencjalnych ataków na systemy sterujące wbudowane w samochody i wdrożenie odpowiednich środków bezpieczeństwa w celu ochrony użytkowników. Najpoważniejszymi scenariuszami ataków są te, które prowadzą do przejęcia kontroli nad kluczowymi modułami, takimi jak układ hamulcowy lub systemy stabilizacji pojazdu. Takie sytuacje mogą prowadzić do potencjalnie katastrofalnych konsekwencji, włączając w to wypadki i zagrożenie życia. Dlatego producenci samochodów oraz branża przemysłowa jako całość muszą skoncentrować się na tworzeniu systemów sterowania i zabezpieczeń, odpornych na ataki oraz zdolnych do reagowania na potencjalne zagrożenia w czasie rzeczywistym. W dzisiejszym świecie produkcji przemysłowej, w tym w branży motoryzacyjnej, zapewnienie bezpieczeństwa i odporności na współczesne zagrożenia, w tym cyberzagrożenia, jest niezwykle istotne. Niemniej jednak, niemożliwe jest zapewnienie, że produkt będzie w stu procentach odporny na wszystkie formy ataków. Dlatego konieczne jest podejście proaktywne i całościowe w zakresie zapewnienia bezpieczeństwa produktów mechatronicznych. Podsumowując, wdrażanie odpowiednich procedur i środków bezpieczeństwa jest niezbędne. Elastyczność, reaktywność na zmiany w środowisku zagrożeń i ciągłe doskonalenie stanowią klucz do skutecznego zarządzania ryzykiem i minimalizacji potencjalnych zagrożeń, w tym tych, które jeszcze nie są znane.

Celem pracy było opracowanie procedur i wytycznych, które definiują kierunki dalszych działań. Wykorzystanie systemów sztucznej inteligencji (AI) w monitorowaniu i nadzorowaniu komunikacji pomiędzy systemami wbudowanymi w pojazdach jest zgodne z trendami rozwojowymi w branży. AI może efektywnie analizować dane, wykrywać anomalie i podejrzane działania, co pozwala na szybką reakcję na potencjalne zagrożenia. Jest to szczególnie istotne w kontekście samochodów autonomicznych, gdzie bezpieczeństwo jest absolutnym priorytetem, podobnie jak w przemyśle lotniczym.
Głównym celem badań prowadzonych w ramach tej pracy jest identyfikacja potencjalnych zagrożeń w występujących w systemach wbudowanych stosowanych w przemyśle motoryzacyjnym i opracowanie skutecznych rozwiązań mających na celu zapobieganie tym zagrożeniom. Jednym z kluczowych aspektów badań jest opracowanie metody taniego szyfrowania, która minimalizuje ryzyko destabilizacji pracy samochodu oraz zapewnia integralność i poufność danych w tym kontekście.
W rezultacie, prace badawcze te dążą do stworzenia innowacyjnych rozwiązań opartych o detekcję anomalii z zastosowaniem metod sztucznej inteligencji, które zminimalizują ryzyko destabilizacji pracy samochodu oraz zabezpieczą dane i komunikację pomiędzy modułami wbudowanymi. Jest to istotny krok w kierunku zapewnienia wyższego poziomu bezpieczeństwa w przemyśle motoryzacyjnym, szczególnie w obliczu rosnących zagrożeń związanych z cyberbezpieczeństwem i złożonością współczesnych systemów mechatronicznych.
Prezentowana praca jest efektem badań finansowanych przez Ministerstwo Edukacji i Nauki, projekt nr: DWD/3/33/2019, w ramach którego przyjęto i wdrożono następujący plan działań:
określenie celów badawczych, przegląd literatury w kontekście aktualnych rozwiązań stosowanych w systemach wbudowanych w przemyśle motoryzacyjnym, analiza i identyfikacja aktualnych zagrożeń, w tym zagrożeń cybernetycznych, wybór konkretnych systemów wbudowanych do badań, opracowanie własnej koncepcji badawczo-testowej mającej na celu destabilizację prawidłowego działania systemów, w tym próby całkowitego uniemożliwienia normalnej pracy i przejęcia kontroli nad systemem wbudowanym w pojeździe elektrycznym, przygotowanie stanowiska badawczego, opracowanie koncepcji szyfrowania, implementacja i przeprowadzanie testów weryfikacyjnych w celu oceny skuteczności i wydajności

zaproponowanych rozwiązań, opracowanie koncepcji zabezpieczeń minimalizujących zagrożenia wynikające z rodzajów zidentyfikowanego ryzyka, przeprowadzanie testów weryfikacyjnych po wdrożeniu opracowanych zabezpieczeń, opracowanie koncepcji nadzorcy magistrali CAN z wykorzystaniem metod sztucznej inteligencji, przygotowywanie propozycji i rozwiązań mających na celu lepszą ochronę systemów wbudowanych pojazdu przed zagrożeniami, zdefiniowanie kierunków dalszych analiz i badań.

W początkowych etapach rozwoju przemysłu motoryzacyjnego pojazdy silnikowe były głównie kontrolowane przy użyciu mechanicznych rozwiązań. Jednak w miarę postępu technologicznego i rozwoju przemysłu motoryzacyjnego, zaczęła się stopniowa transformacja, która polegała na inkorporacji elektroniki i systemów sterowania do struktury samochodu. W wyniku tego procesu udział układów mechatronicznych, które łączą elementy mechaniczne z elektronicznymi, znacząco wzrósł kosztem tradycyjnych rozwiązań mechanicznych. Ewolucja od układów mechanicznych do mechatronicznych w przemyśle motoryzacyjnym wynika z coraz wyższych oczekiwań dotyczących osiągów, komfortu, bezpieczeństwa oraz efektywności energetycznej pojazdów. Optymalizacja i integracja elementów sterowanych elektronicznie przyczyniły się do znaczącej poprawy funkcjonalności i wydajności współczesnych samochodów. Typowymi przykładami układów początkowo mechanicznych, a dziś mechatronicznych są układy skręcania i hamowania (na przykładzie hamulca ręcznego). Są to dwa podstawowe moduły sterujące pojazdem. Typowy mechaniczny układ hamulca ręcznego, odpowiadał za możliwość zablokowania tylnych kół, aby zapobiec poruszaniu się pojazdu w trybie parkowania. W przeszłości był to system połączeń za pomocą stalowych linek i regulatorów odpowiedzialny za równomierny rozkład siły hamowania na oba tylne koła. Co ważne, wydajność hamulca musiała zostać zoptymalizowana także pod względem funkcjonalnym, tak aby jego użycie nie wymagało dużej siły. Jego włączenie wymaga reakcji kierowcy. Dźwignię trzeba pociągnąć i przede wszystkim kierowca musi o tym pamiętać. Mechaniczny hamulec ręczny jest sterowany wyłącznie przez kierowcę. Zaletą takiego rozwiązania jest możliwość ręcznego ustawienia siły hamowania i możliwość wykorzystania jej przy próbie wyjścia ze ślizgu bocznego. Następcą mechanicznego hamulca ręcznego jest elektroniczny hamulec postojowy (czasami nazywany elektromechanicznym hamulcem postojowym), będący zaawansowanym systemem mechatronicznym. Sterowanie odbywa się za pomocą sygnałów przesyłanych magistralami transmisyjnymi, dzięki czemu nie ma potrzeby stosowania przewodu łączącego przód i tył pojazdu.

Należy podkreślić, że w współczesnych samochodach systemy mechatroniczne stanowią znaczącą część systemów sterowania. Bez nich, biorąc pod uwagę oczekiwania użytkowników, trudno jest osiągnąć implementację wymaganej funkcjonalności pojazdu. Współcześnie mechatronika odgrywa kluczową rolę w procesie przekształcania pojazdów w inteligentne i efektywne środki transportu, obejmujące zarówno zarządzanie silnikiem, optymalizację automatycznych skrzyń biegów, jak i rozwijanie zaawansowanych systemów wspomagania kierowcy. Głównym celem tych działań jest zwiększanie bezpieczeństwa podróży. Należy podkreślić, że integracja samochodów z systemami Internetu Rzeczy zgodnie z koncepcją Przemysłu 4.0 niesie ze sobą wiele nowych możliwości i udogodnień, ale także liczne zagrożenia, przed którymi samochody muszą być odporne. Dążenie do optymalizacji kosztów i pełnej automatyzacji wiąże się z rozwojem autonomicznych samochodów, które poruszają się coraz szybciej a oczekiwania rynku samochodowego dotyczące przyszłości koncentrują się głównie na obszarach zwiększania odporności na cyberatak. Współcześnie, prowadzący samochód, może na bieżąco sprawdzać informacje dotyczące stanu dróg, korków czy kolizji. Współpraca systemów i czujników, którymi wyposażony jest pojazd, pozwala na szybką reakcję na różne sytuacje, które mogą wystąpić. Dlatego też oczekuje się znacznego udoskonalenia oraz dalszego rozwoju wszystkich mechanizmów unikania kolizji. Urządzenia i rozwiązania takie jak radary czy kamery są znane od dawna, ale zazwyczaj były wdrażane

lokalnie i stosowane do pojedynczych pojazdów. Idea połączenia całej dostępnej infrastruktury drogowej wprowadza istotne zmiany. Zebrane informacje mogą być łączone i analizowane wspólnie, a następnie wykorzystywane w czasie rzeczywistym do zarządzania środowiskiem ruchu drogowego. Współczesne systemy komunikacji pojazdów są traktowane jako części większych ekosystemów, wpisując się w ideę Przemysłu 4.0. W przypadku przemysłu motoryzacyjnego obejmują one takie podejścia jak „vehicle to everything" (V2X) czyli pojęcie odnoszące się do komunikacji między pojazdami a różnymi elementami infrastruktury i urządzeniami w otoczeniu drogowym. To zaawansowany system, który umożliwia pojazdom komunikację z innymi pojazdami (V2V), infrastrukturą drogową (V2I), pieszymi (V2P), siecią (V2N), a także innymi źródłami informacji i danymi. Dzięki V2X, pojazdy mogą wymieniać informacje dotyczące ruchu drogowego, warunków na drodze, sygnalizacji świetlnej, ostrzeżeń przed zagrożeniami i wiele innych, co przyczynia się do zwiększenia bezpieczeństwa i efektywności na drogach.

Odporność na cyberataki w sektorze motoryzacyjnym jest krytyczna dla ochrony życia, danych osobowych, funkcjonalności pojazdów, reputacji marki, zgodności z przepisami prawnymi, stabilności finansowej oraz zrównoważonego rozwoju branży. Innymi słowy, konieczne jest uwzględnienie wszystkich możliwych scenariuszy ataków i przygotowanie odpowiednich środków zaradczych. Jak zaznaczyli (Desnitsky & Kotenko, 2014), specyfika urządzeń wbudowanych wymaga stosowania łączonych mechanizmów ochrony charakteryzujących się odpowiednim poziomem bezpieczeństwa i akceptowalnym zużyciem zasobów. Dlatego zdaje się uzasadnione podejście podwójne do tego problemu. Daje to możliwość stosowania zaawansowanych i kosztownych środków bezpieczeństwa, gdy jest to krytyczne, oraz nisko kosztowych metod zwiększających poziom bezpieczeństwa, gdy jest to wystarczające.

Zagrożenia można klasyfikować różnymi kryteriami. Na przykład, rozważając pochodzenie zagrożeń, można je podzielić na zewnętrzne i wewnętrzne. Z punktu widzenia funkcjonalności można wyróżnić takie rodzaje ataków jak podsłuchiwanie i przechwytywanie danych, destabilizacja czy próby przejęcia kontroli. Przykładowa klasyfikacja zagrożeń została opisana w pracy (Rae & Wildman, 2003), gdzie autorzy podzielili je według typów intruzów. W przypadku ataków rozważanych z funkcjonalnego punktu widzenia (Gajdzik, Sternal, Timofiejczuk, & Przystałka, 2021), zaproponowano następującą klasyfikację: podsłuchiwanie danych, nagrywanie danych i odtwarzanie scenariuszy oraz ataki typu „brute force". W dobie szybkiego postępu technologicznego i nieustannie rosnącej przestrzeni cyfrowej ochrona wrażliwych informacji i krytycznej infrastruktury przed złośliwymi zagrożeniami cybernetycznymi stała się najważniejszym zmartwieniem. W miarę jak ataki cybernetyczne nadal rosną pod względem częstotliwości, złożoności i skutków, instytucje i organizacje na całym świecie są zmuszone wzmocnić swoje mechanizmy obronne. Ogólnie rzecz biorąc, ochrona wrażliwych danych w systemach wbudowanych jest istotna w dzisiejszym świecie, gdzie zagrożenia cybernetyczne stają się coraz bardziej powszechne i zaawansowane. Dlatego rozwijanie odpowiednich mechanizmów bezpieczeństwa staje się priorytetem, zwłaszcza w sektorze motoryzacyjnym. Wprowadzenie mechanizmów ochrony takich jak np. E2E (End to End) było ważnym krokiem w kierunku zabezpieczenia komunikacji krytycznej dla bezpieczeństwa w pojazdach. Wdrażanie E2E po obu stronach nadawcy i odbiorcy pozwala na ochronę przed uszkodzeniami danych i wykrywanie utraconych lub nieprawidłowych sekwencji danych. Kolejnym mechanizmem stosowanym w ochronie informacji w pojazdach jest szyfrowanie. Polega na przekształceniu czytelnych danych w nieczytelne za pomocą matematycznych operacji wykonywanych przez algorytmy kryptograficzne z wyznaczonym kluczem. Autoryzacja kryptograficzna jest stosowana w celu potwierdzenia tożsamości nadawcy danych i zapewnienia integralności przesyłanych informacji. Mechanizmy bezpieczeństwa mogą być realizowane za pomocą oprogramowania, sprzętu lub ich połączenia. Sprzęt często jest używany do przyspieszenia operacji kryptograficznych i jest szczególnie

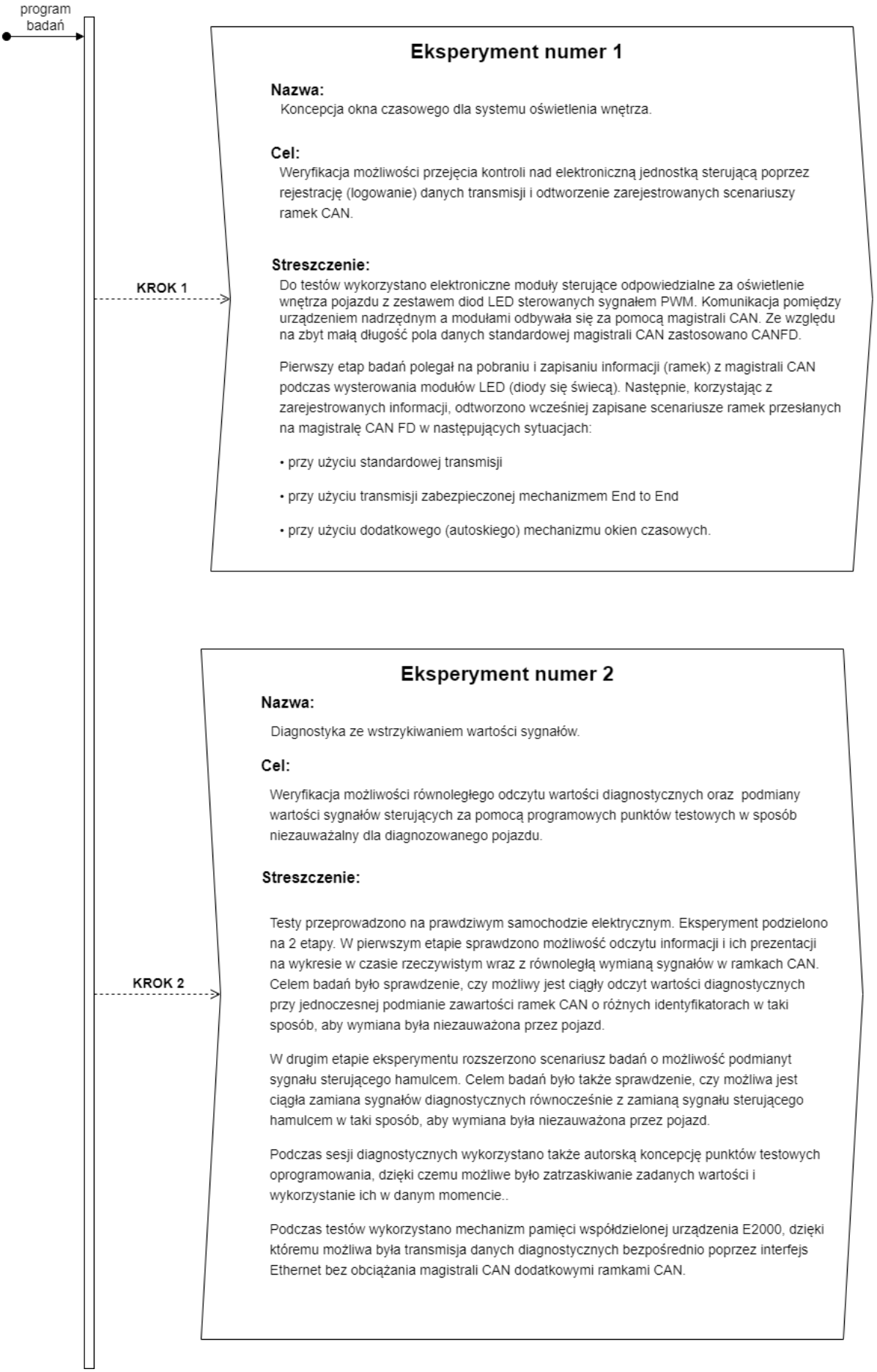
ważny przy zwiększaniu rozmiaru klucza kryptograficznego. Stosowanie specjalnego protokołu komunikacji diagnostycznej UDS (Unified Diagnostic Services) to kolejny przykład zabezpieczenia przed nieautoryzowaną zmianą oprogramowania systemu wbudowanego. Tak samo jak autoryzacja cyfrowa, która jest procesem weryfikacji tożsamości nadawcy danych i potwierdzania integralności przesyłanych informacji. Może być stosowana w systemach wbudowanych do potwierdzania pochodzenia danych i zapewniania niezawodności obrazu oprogramowania przed uruchomieniem lub podczas pobierania z zewnętrznego źródła.

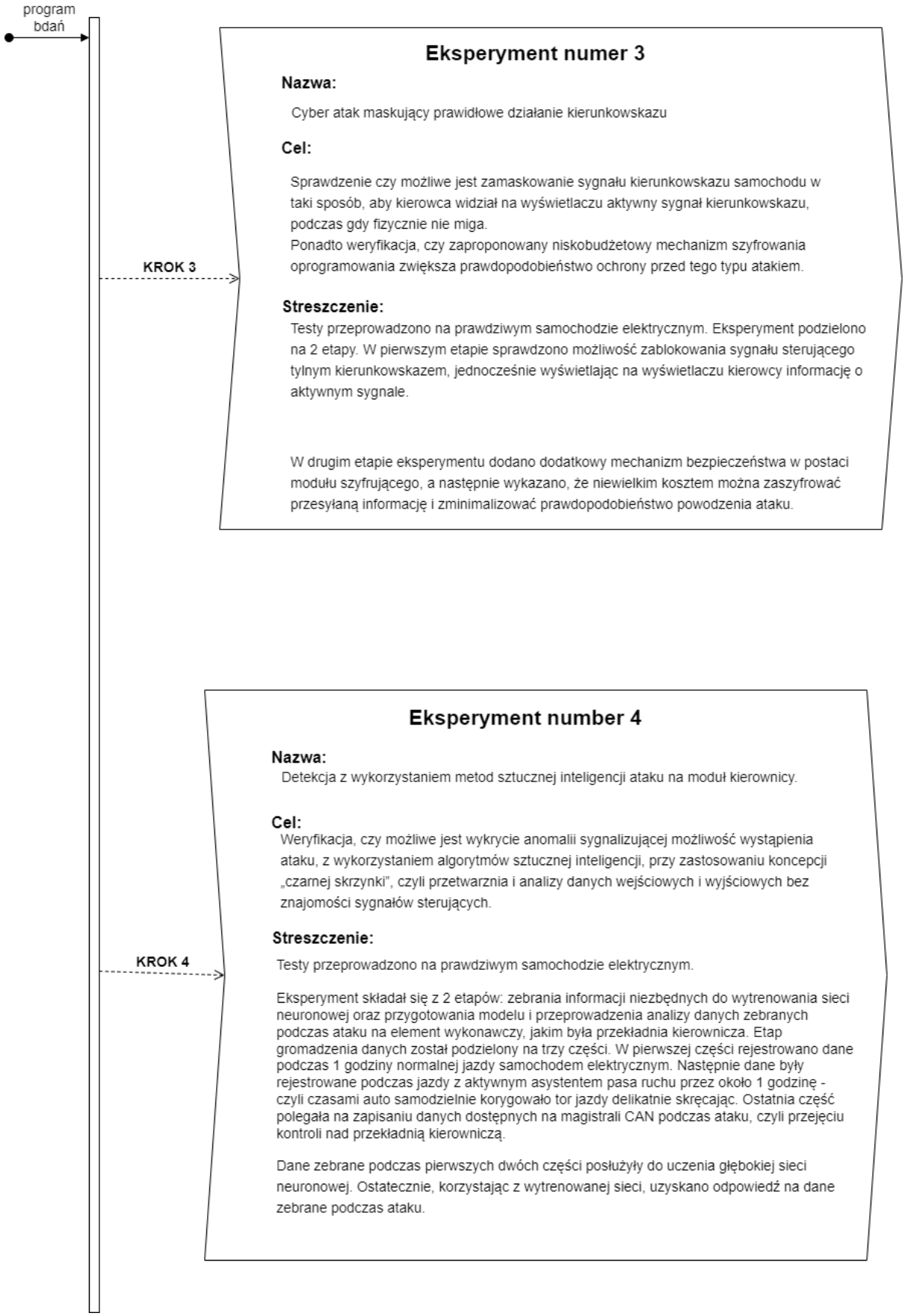
BADANIA EKSPERYMENTALNE

Współczesne pojazdy to bardzo złożone układy mechatroniczne, składające się z kilkudziesięciu, a w przypadku lepiej wyposażonych wersji nawet z ponad stu współpracujących ze sobą elektronicznych modułów sterujących. W procesie sterowania pojazdem w czasie rzeczywistym przesyłane są duże zbiory danych za pomocą magistrali transmisyjnych, przy zachowaniu rygorystycznych wymagań czasowych. Dobrym przykładem rozwoju samochodów w ostatnich latach są zmiany w układzie hamulca ręcznego. W przeszłości był to układ mechaniczny, obecnie jest to układ mechatroniczny. Powszechne wprowadzanie układów elektronicznych zastępujących elementy mechaniczne jest nie tylko efektem rozwoju technologicznego, względów estetycznych i możliwości minimalizacji elementów sterujących, ale także czynników ekonomicznych. Biorąc pod uwagę ilość systemów mechatronicznych stale wymieniających informacje podczas eksploatacji pojazdu można stwierdzić, że obecnie wizja ataku na samochód jest bardzo prawdopodobna i faktycznie zdarza się często. Ataki na układy elektroniczne sterujące modułami wykonawczymi można przeprowadzić na dwa sposoby:

- przejęcie kontroli nad modułem,
- destabilizacja poprawności pracy modułu.

Rozważając ataki opisane powyżej, w ramach projektu doktoranckiego zaplanowano i przeprowadzono 4 eksperymenty. Celem było sprawdzenie możliwości przeprowadzenia skutecznego ataku na wybrany element wykonawczy będący częścią pojazdu. W kolejnych eksperymentach symulowane ataki uporządkowano odpowiednio do rosnącej złożoności implementacji ataku. Począwszy od prostego ataku, polegającego na zapisie transmisji, a następnie jego odtworzeniu (wysłaniu zarejestrowanych ramek na magistralę CAN), poprzez zamianę wartości sygnałów podczas normalnej pracy pojazdu. Udowodniono, że ataki na obecnie produkowane pojazdy, składające się z systemów mechatronicznych, zakończyły się sukcesem. Przeprowadzone badania wykazały, że możliwe jest przejęcie kontroli nad określoną funkcjonalnością pojazdu. W wyniku projektu doktoranckiego zaproponowano nisko kosztowe mechanizmy szyfrowania oprogramowania. Głównym celem realizowanych zadań było znaczne utrudnienie tego typu ataku. Potwierdziły to badania weryfikacyjne. Ostatni eksperyment skupiał się na zastosowaniu i wykorzystaniu algorytmów sztucznej inteligencji do wykrywania ataków na pojazd. Zakładano, że podczas ataku widoczne będą pewne anomalie w sygnałach zawartych w ramkach przesyłanych na magistrali CAN. Do wykrycia anomalii wykorzystano algorytmy głębokiego uczenia się oraz model autoenkodera. W analizowanych danych uwzględniono zależności czasowe. Należy podkreślić, że cały eksperyment przeprowadzono zgodnie z konceptem „czarnej skrzynki”. Zbiór danych został przetworzony i przeanalizowany bez znajomości struktury i charakteru sygnałów. Wszystkie przeprowadzone badania podzielono na cztery eksperymenty przedstawione na Rys. XY1.


program badań
KROK 1
Eksperyment numer 1
Nazwa:
Koncepcja okna czasowego dla systemu oświetlenia wnętrza.
Cel:
Weryfikacja możliwości przejęcia kontroli nad elektroniczną jednostką sterującą poprzez rejestrację (logowanie) danych transmisji i odtworzenie zarejestrowanych scenariuszy ramek CAN.
Streszczenie:
Do testów wykorzystano elektroniczne moduły sterujące odpowiedzialne za oświetlenie wnętrza pojazdu z zestawem diod LED sterowanych sygnałem PWM. Komunikacja pomiędzy urządzeniem nadrzędnym a modułami odbywała się za pomocą magistrali CAN. Ze względu na zbyt małą długość pola danych standardowej magistrali CAN zastosowano CANFD.
Pierwszy etap badań polegał na pobraniu i zapisaniu informacji (ramek) z magistrali CAN podczas wysterowania modułów LED (diody się świecą). Następnie, korzystając z zarejestrowanych informacji, odtworzono wcześniej zapisane scenariusze ramek przesłanych na magistralę CAN FD w następujących sytuacjach:
• przy użyciu standardowej transmisji
• przy użyciu transmisji zabezpieczonej mechanizmem End to End
• przy użyciu dodatkowego (autoskiego) mechanizmu okien czasowych.
KROK 2
Eksperyment numer 2
Nazwa:
Diagnostyka ze wstrzykiwaniem wartości sygnałów.
Cel:
Weryfikacja możliwości równoległego odczytu wartości diagnostycznych oraz podmiany wartości sygnałów sterujących za pomocą programowych punktów testowych w sposób niezauważalny dla diagnozowanego pojazdu.
Streszczenie:
Testy przeprowadzono na prawdziwym samochodzie elektrycznym. Eksperyment podzielono na 2 etapy. W pierwszym etapie sprawdzono możliwość odczytu informacji i ich prezentacji na wykresie w czasie rzeczywistym wraz z równoległą wymianą sygnałów w ramkach CAN. Celem badań było sprawdzenie, czy możliwy jest ciągły odczyt wartości diagnostycznych przy jednoczesnej podmianie zawartości ramek CAN o różnych identyfikatorach w taki sposób, aby wymiana była niezauważona przez pojazd.
W drugim etapie eksperymentu rozszerzono scenariusz badań o możliwość podmianyt sygnału sterującego hamulcem. Celem badań było także sprawdzenie, czy możliwa jest ciągła zamiana sygnałów diagnostycznych równocześnie z zamianą sygnału sterującego hamulcem w taki sposób, aby wymiana była niezauważona przez pojazd.
Podczas sesji diagnostycznych wykorzystano także autorską koncepcję punktów testowych oprogramowania, dzięki czemu możliwe było zatrzaskiwanie zadanych wartości i wykorzystanie ich w danym momencie..
Podczas testów wykorzystano mechanizm pamięci współdzielonej urządzenia E2000, dzięki któremu możliwa była transmisja danych diagnostycznych bezpośrednio poprzez interfejs Ethernet bez obciążania magistrali CAN dodatkowymi ramkami CAN.


program bdań
KROK 3
Eksperyment numer 3
Nazwa:
Cyber atak maskujący prawidłowe działanie kierunkowskazu
Cel:
Sprawdzenie czy możliwe jest zamaskowanie sygnału kierunkowskazu samochodu w taki sposób, aby kierowca widział na wyświetlaczu aktywny sygnał kierunkowskazu, podczas gdy fizycznie nie miga.
Ponadto weryfikacja, czy zaproponowany niskobudżetowy mechanizm szyfrowania oprogramowania zwiększa prawdopodobieństwo ochrony przed tego typu atakiem.
Streszczenie:
Testy przeprowadzono na prawdziwym samochodzie elektrycznym. Eksperyment podzielono na 2 etapy. W pierwszym etapie sprawdzono możliwość zablokowania sygnału sterującego tylnym kierunkowskazem, jednocześnie wyświetlając na wyświetlaczu kierowcy informację o aktywnym sygnale.
W drugim etapie eksperymentu dodano dodatkowy mechanizm bezpieczeństwa w postaci modułu szyfrującego, a następnie wykazano, że niewielkim kosztem można zaszyfrować przesyłaną informację i zminimalizować prawdopodobieństwo powodzenia ataku.
KROK 4
Eksperyment number 4
Nazwa:
Detekcja z wykorzystaniem metod sztucznej inteligencji ataku na moduł kierownicy.
Cel:
Weryfikacja, czy możliwe jest wykrycie anomalii sygnalizującej możliwość wystąpienia ataku, z wykorzystaniem algorytmów sztucznej inteligencji, przy zastosowaniu koncepcji „czarnej skrzynki", czyli przetwarznia i analizy danych wejściowych i wyjściowych bez znajomości sygnałów sterujących.
Streszczenie:
Testy przeprowadzono na prawdziwym samochodzie elektrycznym.
Eksperyment składał się z 2 etapów: zebrania informacji niezbędnych do wytrenowania sieci neuronowej oraz przygotowania modelu i przeprowadzenia analizy danych zebranych podczas ataku na element wykonawczy, jakim była przekładnia kierownicza. Etap gromadzenia danych został podzielony na trzy części. W pierwszej części rejestrowano dane podczas 1 godziny normalnej jazdy samochodem elektrycznym. Następnie dane były rejestrowane podczas jazdy z aktywnym asystentem pasa ruchu przez około 1 godzinę - czyli czasami auto samodzielnie korygowało tor jazdy delikatnie skręcając. Ostatnia część polegała na zapisaniu danych dostępnych na magistrali CAN podczas ataku, czyli przejęciu kontroli nad przekładnią kierowniczą.
Dane zebrane podczas pierwszych dwóch części posłużyły do uczenia głębokiej sieci neuronowej. Ostatecznie, korzystając z wytrenowanej sieci, uzyskano odpowiedź na dane zebrane podczas ataku.

Rys. XY1

Koncepcja okna czasowego dla systemu oświetlenia wnętrza

Celem tego eksperymentu było przeprowadzenie badania porównawczego podatności na atak na moduł wykonawczy sterowany przez magistralę CAN FD. Eksperyment przeprowadzono w trzech scenariuszach:

A. zastosowanie metody okien czasowych do ustalenia ważności sygnałów,

B. korzystania z transmisji z zabezpieczeniem End-to-End,

C. przy użyciu standardowej skrzyni biegów.

Atak polegał na nagraniu transmisji na magistrali CAN w sytuacji gdy moduły LED były wysterowane (diody LED świeciły) i następnie odtworzeniu nagranej transmisji w wybranym momencie.

Element, który został zaatakowany w tym eksperymencie, zaznaczony jest na Rys. XX1 i odpowiada za sterowanie wewnętrznym oświetleniem w samochodzie..

Rys. X1 Moduły oświetlenia wnętrza pojazdu

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

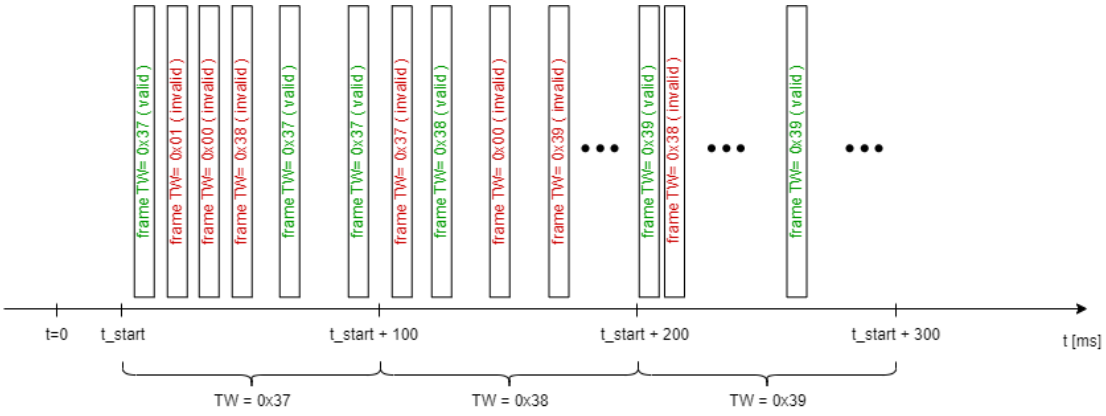


Fig. 1 Koncepcja okna czasowego

Zaproponowane podejście polegające na zaimplementowaniu dodatkowego mechanizmu znacznika okna czasowego znacznie zwiększyło bezpieczeństwo transmisji danych na magistrali CAN. Jak wykazano podczas eksperymentu, skuteczność ataków w przypadku zabezpieczenia metodą okna czasowego spadła do zera. Mechanizm ten zwiększał odporność systemu na ataki polegające na nagrywaniu i odtwarzaniu nagranego scenariusza w celu przejęcia kontroli nad modułem wykonawczym. Analizując wyniki testów prób przejęcia kontroli nad modułem na podstawie wcześniej zarejestrowanych transmisji i ich odtwarzania, można stwierdzić, że w przypadku zastosowania mechanizmu ochrony End-to-End oraz dodatkowego znacznika okna czasowego, przejęcie kontroli nad atakowanym modułem nie było możliwe. Jednakże szansa na udany atak pozostaje realna, jeśli niechciana ramka intruza zostanie wysłana w tym samym oknie czasowym, co pierwotna ramka, aczkolwiek prawdopodobieństwo wystąpienia takiego scenariusza jest małe.

Uzyskane wyniki wskazują na potrzebę prowadzenia dalszych badań w celu określenia optymalnej (minimalnej) długości okien czasowych, zapewniających poprawną transmisję.

Wprowadzenie okna czasowego pomaga określić, czy sygnały w ramce są ważne, czy nie, co zapobiega możliwości późniejszego odtworzenia nagranej wcześniej transmisji. Wskazana została możliwość uzyskania dodatkowej ochrony stosując operację XOR na każdym bajcie pola danych, a sygnały nie są wówczas wysyłane jawnie. Odczytanie pierwotnych wartości jest możliwe po wykonaniu kolejnej operacji XOR na każdym bajcie pola danych.

Jednakże wdrożenie tego rozwiązania wiąże się ze spełnieniem dodatkowych wymagań, m.in. koniecznością zainstalowania zegara czasu rzeczywistego na każdym module oraz synchronizacji zegarów wszystkich modułów na magistrali. Ponadto do przesyłania wartości znacznika okna czasowego należy zastosować nadmiarowe pole danych, co może zmniejszyć pojemność pola danych w ramce CAN. Niemniej jednak w większości przypadków nie jest to krytyczne, ponieważ protokół CAN FD zapewnia możliwość wykorzystania aż 64 bajtów danych w jednej ramce.

Diagnostyka ze wstrzykiwaniem wartości sygnałów

Celem tego eksperymentu była analiza możliwości przeprowadzenia pełnej diagnostyki modułu pojazdu samochodowego w trakcie jego normalnej eksploatacji, czyli w warunkach rzeczywistych. Założono, że dla uzyskania zdefiniowanych warunków testowych konieczne jest wstrzyknięcie informacji i zastąpienie jej w przechwyconych ramkach CAN w czasie rzeczywistym. W przeprowadzonych badaniach wykorzystano mechanizm zatrzaskiwania kluczowych sygnałów z punktu widzenia diagnostyki, odczytu wartości zmiennych, przy zachowaniu oryginalnych cykli czasowych. Dzięki mechanizmowi zatrzaskiwania informacji i wyzwalania w określonym czasie, a następnie odczytywania ich poprzez pamięć współdzieloną, wyeliminowana została konieczność rozbudowy matrycy komunikacyjnej o kolejne ramki debugujące, które zwiększałyby stopień zajętości magistrali. Atakowane elementy samochodu pokazane są na Rys. XX2 i odpowiadają układowi hamulcowemu.

Rys. XX2 Układ hamulcowy

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

Implementacja mechanizmów odczytu wartości w czasie rzeczywistym oraz możliwość wstrzykiwania wartości sygnałów diagnostycznych pozwoliła na odtworzenie dowolnego scenariusza testowego. W tym rozwiązaniu najważniejszą kwestią było to, że nie symulowano sygnałów wejściowych, jak to ma miejsce podczas procesu testowania, ale diagnostyce poddano aktualne wartości rzeczywiste. Dzięki zastosowaniu urządzenia MicroDAQ E2000 możliwe było płynne przesyłanie wszystkich klatek w czasie rzeczywistym do docelowej aplikacji diagnostycznej za pomocą mechanizmu współdzielonej pamięci odczytywanej poprzez interfejs Ethernet. Zastosowanie programowych punktów testowych umożliwiających zatrzaskiwanie wartości umożliwiło także odczyt wartości sygnałów buforowanych. Dodatkowo, równolegle do badań prowadzonych w obu etapach, sprawdzono eksperymentalnie maksymalną liczbę ramek CAN, w których można zmieniać wartości sygnału w sposób niezauważalny dla układu pojazdu. Wyniki uzyskane w 3 seriach nieznacznie różnią się od siebie. Różnice wynikały głównie z zależności czasowych na magistrali CAN, które wpływają na kolejne badane ramki CAN. Długości pola danych w ramkach wahały się od 8 do 64 bajtów. Dodatkowo nie wszystkie ramki charakteryzowały się zaimplementowanym mechanizmem End-to-End Protection (E2E), dlatego nie zawsze konieczne było ponowne przeliczanie sum kontrolnych, co zajmowało dodatkowy czas przetwarzania. Można jednak jednoznacznie stwierdzić, że użyte w testach urządzenie MicroDAQ E2000 pozwoliło w pełni wykonać zadanie zarówno odczytu wartości sygnału, jak i wprowadzenia wartości w wybranym momencie podczas zamiany ramek.

Cyberatak maskujący prawidłowe działanie kierunkowskazu

Głównym celem badań przeprowadzonych w ramach tego eksperymentu było wykazanie, że możliwy jest skuteczny atak na moduł elektroniczny w samochodzie. Celem było przejęcie kontroli nad tylnym kierunkowskazem. Odbyło się to poprzez zamaskowanie informacji przekazywanych kierowcy. Tym samym kierowca włączając kierunkowskaz widzi na wyświetlaczu oczekiwany stan, natomiast tylny kierunkowskaz nie działa. Dodatkowo zaproponowano autorską koncepcję wdrożenia dodatkowego, nisko kosztowego zabezpieczenia systemów transmisji danych. Wykazane zostało, że implementacja takiego zabezpieczenia znacząco utrudnił ataki tego typu. Proponowane rozwiązanie opiera się na programowym podejściu do tematu szyfrowania, bez użycia dedykowanych modułów sprzętowych, co dodatkowo obniża koszty wdrożenia, a także zapewnia łatwą modyfikację

i dostosowanie do szybko zmieniających się technologii. Element atakowany w tym eksperymencie jest zaznaczony na Rys. XX3. i odpowiada tylnemu kierunkowskazowi.

Rys. XX3 Tylny kierunkowskaz

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

W eksperymencie zaprezentowano zastosowanie metod pozwalających na przejęcie kontroli nad elektronicznymi modułami sterującymi bez znajomości układu sterowania danym pojazdem. Zazwyczaj taka wiedza, czyli sygnały sterujące, zawarta jest w tzw. plikach DBC zawierających informację o zdekodowanych wartościach danych rzeczywistych na magistrali CAN w sposób czytelny dla człowieka. W pracy omówiono wybrane metody umożliwiające znalezienie w samochodzie sygnałów sterujących o określonej funkcjonalności. Procedura zawsze zaczyna się od koncepcji rejestrowania informacji sterujących z magistrali CAN, gdy kierunkowskaz jest wyłączony. Kolejnym krokiem jest korekta zebranych danych i przygotowanie listy ramek CAN do wymiany przy włączonym kierunkowskazie. Udowodniono, że możliwe jest znalezienie ciągu bitów sterujących daną funkcjonalnością. Oczekiwanym efektem było znalezienie ramki lub kilku ramek CAN, które po podmianie zawartości pola danych będą wyłączały kierunkowskaz gdy był włączony. Aby zastąpić zawartość ramek, gdy w ramce występuje mechanizm zabezpieczający End-to-End, zastosowano metodę inżynierii odwrotnej, a wszystkie niezbędne wartości kluczy odnaleziono metodą brute-force. W kolejnej fazie eksperymentu, po zawężeniu już listy identyfikatorów ramek, które mogły odpowiadać za sterowanie kierunkowskazem, zastosowano inną metodę, tzw. „heat map", opisaną w (Gajdzik, Sternal, Timofiejczuk i Przystałka, 2021), która pozwoliła na graficzne przedstawienie wartości wszystkich bitów w każdej ramce dla różnych wartości znaczników czasu. W ten sposób odnaleziono sygnały sterujące kierunkowskazem. Wykazano także, że sygnał kierunkowskazu jest inny, niezależny od sygnału stanu migacza , który widoczny jest na wyświetlaczu kierowcy. Po uzyskaniu potwierdzenia przejęcia kontroli, w ostatniej części eksperymentu sprawdzono, czy zastosowanie dodatkowej metody szyfrującej zawartość pola danych ramek CAN będzie w stanie utrudnić skuteczny atak. Niestety nie mając możliwości zmiany oprogramowania modułów w pojeździe zdecydowano się na symulację zdarzenia polegającego na dodaniu funkcjonalności szyfrowania i deszyfrowania informacji. Dokonano tego za pomocą 2 dodatkowych modułów sprzętowych, kodera i dekodera. W praktyce tę samą funkcjonalność uzyskano po zmianie oprogramowania modułów wysyłających i odbierających informacje. Wykazano, że choć zaproponowana metoda taniego szyfrowania programowego nie jest w stanie w pełni zabezpieczyć transmisji przed

potencjalnym dekodowaniem sygnałów przesyłanych magistralą CAN, to znacznie utrudnia to zadanie.
Podsumowując, w trakcie badań udowodniono, że atak na moduł sterujący kierunkowskazem może spowodować bezpośrednie zagrożenie życia, a zaproponowana metoda szyfrowania utrudnia przeprowadzenie tego typu ataku.

Detekcja z wykorzystaniem metod sztucznej inteligencji ataku na moduł kierownicy.

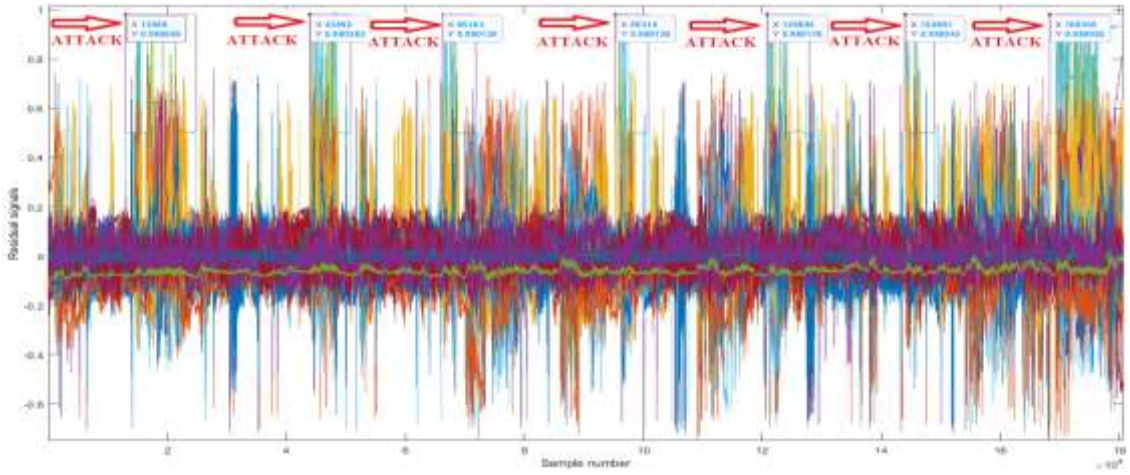
Głównym celem badań przeprowadzonych w ramach tego eksperymentu było wykazanie, że przy pomocy wybranych algorytmów sztucznej inteligencji możliwe jest wykrycie trwającego ataku na elektroniczny moduł sterujący w pojeździe samochodu elektrycznego. Założono, że podczas ataku na pojazd sygnały przesyłane magistralą CAN w postaci bajtów danych wykazują obraz anomalii, czyli wykryty zostanie stan odmienny od oczekiwanego podczas normalnej pracy. Eksperyment przeprowadzono bez dostępu do dokumentacji badanego pojazdu, czyli bez znajomości sygnałów sterujących pojazdem. Biorąc to pod uwagę, zastosowano podejście czarnej skrzynki. Dane rejestrowane z magistrali CAN traktowano jako ciąg bajtów, w których powinny znaleźć się sygnały sterujące. Wypracowane w trakcie badań podejście opierało się na detekcji anomalii z wykorzystaniem głębokiej sieci neuronowej uwzględniającej zależności czasowej, opisanej w szczegółowo w dysertacji. Atakowany element samochodu zaznaczony jest na Rys. XX4 i odpowiada układowi kierowniczemu.

Rys. XX4 Układ kierowniczy

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

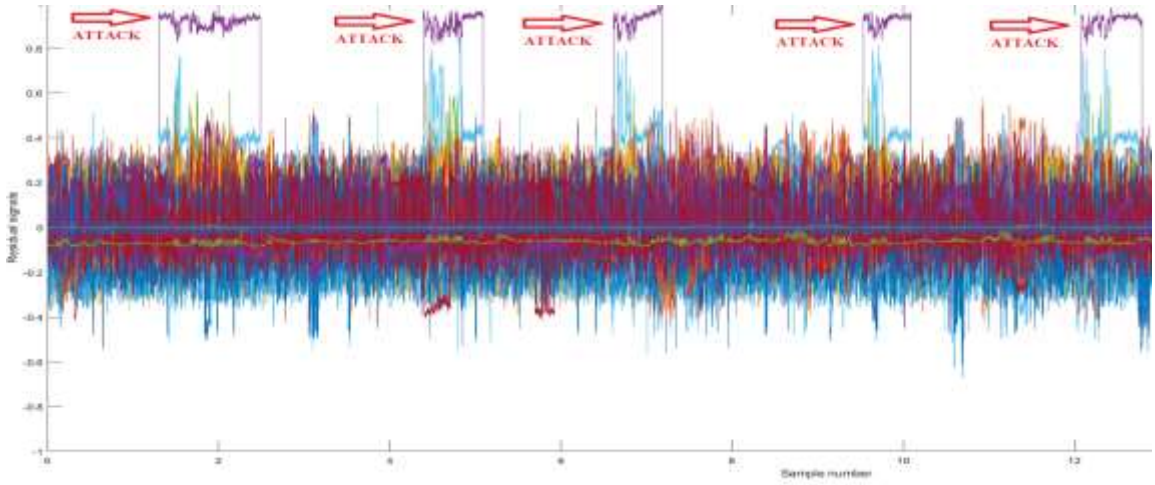
Przez cały czas trwania eksperymentu prowadzono zaplanowaną sekwencję działań mających na celu wykrycie anomalii. Założono, że wykrycie anomalii może stanowić informację o trwającym ataku na samochód. Dane rejestrowano z magistrali CAN połączonej bezpośrednio z układem przekładni kierowniczej. Doświadczenia przeprowadzono podczas jazdy w trybie normalnym i przy włączonym systemie asystenta utrzymania pasa ruchu. Dodatkowo podczas ataku polegającego na przejęciu kontroli nad funkcją skrętu w samochodzie zostały zarejestrowane dane z magistrali CAN. W tym celu zrealizowano realny scenariusz cyberataku z wykorzystaniem dodatkowego urządzenia Microdaq E2000 pracującego w trybie mostu i sterowanego z aplikacji komputerowej poprzez magistralę Ethernet. Udowodniono, że można skutecznie zaatakować nowoczesny samochód elektryczny i przejąć nad nim kontrolę w sposób niezauważalny dla systemu sterowania pojazdem. Po zebraniu danych z magistrali CAN podczas jazdy w zdefiniowanych przypadkach testowych, dane zostały przetworzone w taki sposób, aby możliwa była ich dalsza obróbka zgodna z koncepcja mapy bajtów. Przyjęta wartość 1 milisekundy wynikała z zaproponowanej koncepcji mapy bajtowej, czyli kolejnych

ramek CAN połączonych jako pola danych o rozdzielczości 1ms (koncepcja przedstawiona w dysertacji). Pliki zalogowane dla każdego identyfikatora ramki CAN w sesjach podczas normalnej jazdy (bez ataku) posłużyły do uczenia sieci neuronowej. Następnie podjęto próbę wykrycia anomalii poprzez wprowadzenie danych zarejestrowanych podczas trwającego ataku.



Rys. XX5 Wykrycie anomalii (ataku) za pomocą głębokiej sieci neuronowej w modelu autoenkodera po wytrenowaniu sieci danymi z normalnej jazdy

(Gajdzik, Timofiejczuk, Gnacy-Gajdzik, & Przystałka, 2023)



Rys. XX6 Wykrycie anomalii (ataku) za pomocą głębokiej sieci neuronowej w modelu autoenkodera po wytrenowaniu danymi z normalnej jazdy i aktywnego asystenta utrzymania pasa ruchu

(Gajdzik, Timofiejczuk, Gnacy-Gajdzik, & Przystałka, 2023)

W obydwu przypadkach, tzn. zarówno przy wytrenowaniu głębokiej sieci neuronowej danymi zebranymi podczas normalnej jazdy samochodem jak również podczas jazdy z aktywnym systemem asystenta pasa ruchu wykryte zostały ze 100% skutecznością trwające ataki. Jednak w pierwszym przypadku (patrz Rys. XX5) różnica pomiędzy atakiem a szumem była bardzo mała, natomiast w przypadku drugim (patrz Rys. XX6) z łatwością można zauważyć momenty ataku na jednostkę sterującą.

Podsumowanie eksperymentów i testów weryfikacyjnych. Proponowane podejścia do ochrony samochodów.

Podczas przeprowadzanych eksperymentów, opracowano innowacyjne metody ochrony przed cyberatakami. Rozwiązania te zostały dostosowane do specyficznych wymagań sektora motoryzacyjnego, które obejmują:

- produkcję pewnych modułów w ogromnych ilościach, sięgających milionów jednostek, gdzie ich wpływ na bezpieczeństwo ludzkie jest pośredni, jak w przypadku oświetlenia wnętrza pojazdu.
- istnienie modułów bezpośrednio odpowiedzialnych za kluczowe operacje w pojeździe, takie jak hamowanie, przyspieszanie czy sterowanie.

Aby sprostać tym zróżnicowanym potrzebom, autor zaproponował dwie kategorie rozwiązań wykorzystujących głębokie sieci neuronowe: podejścia ekonomiczne oraz przeznaczone do zabezpieczeń układów realizujących zaawansowane funkcjonalności. Do wykrywania ataków wykorzystano głęboką sieć neuronową z autoenkoderem bazującą na warstwach zawierających bramkowaną jednostkę rekurencyjną (GRU) jako narzędzie do wykrywania anomalii. Dodatkowo udowodniono, że można wykryć ataki, trenując głęboką sieć neuronową danymi zebranymi z magistral pojazdu podczas regularnej jazdy z deaktywowanym asystentem pasa ruchu. Warto zaznaczyć, że w tym przypadku różnica między oczekiwaną wartością na wyjściu sieci a anomalią nie była znacząca. Należy podkreślić, że jeśli sieć została dodatkowo przeszkolona z wykorzystaniem dodatkowego zestawu danych treningowych zebranych podczas jazdy z aktywnym systemem asystenta pasa ruchu, różnica ta była istotna. Eksperyment potwierdził, że dzięki wykorzystaniu głębokich sieci neuronowych możliwe jest wykrywanie ataków z 100% skutecznością, co pozwala na opracowanie odpowiednich strategii na poziomie pojazdu, które mogą zapobiec tego rodzaju sytuacjom lub przynajmniej zminimalizować ich skutki.

Rozwiązania nisko kosztowe

W przemyśle motoryzacyjnym, gdzie produkcja modułów odbywa się w milionach egzemplarzy, kładzie się szczególny nacisk na minimalizację kosztów produkcji pojedynczego modułu. Dlatego, nawet jeśli istnieją skuteczne metody szyfrowania przy użyciu dedykowanego sprzętu, zazwyczaj nie są one implementowane w systemach kontrolujących kluczowe funkcje w pojazdach. Wdrożenie takich metod i urządzeń zwiększa koszty produkcji samochodu. Dlatego w większości przypadków dane na magistralach są przesyłane otwarcie, co tworzy ryzyko niewłaściwego wykorzystania. W kontekście oczekiwań zmniejszenia kosztów i zapewnienia bezpieczeństwa pojazdu, konieczne jest stosowanie prostych metod szyfrowania. Takie podejścia zostały opracowane w ramach projektu doktorskiego i są one wynikiem wcześniej opisanych eksperymentów.

Koncept okien czasowych

Koncepcja zakłada dodanie pewnych informacji, czyli znacznika czasowego, do pola danych ramki CAN. Jego zadaniem jest sprawdzenie poprawność przesyłanych danych. Używana jest w tym celu bieżąca wartość czasu odliczana od momentu uruchomienia całego systemu. Jego początkowa wartość jest określana przez specjalną ramkę CAN, która jest wysyłana przez

urządzenie kontrolujące pozostałe moduły podczas uruchamiania systemu. Następnie znacznik czasowy jest synchronizowany co określony czas (np. co 10 sekund). Domyślnie zajmuje on 1 bajt danych (co oznacza, że mniejsza ilość danych może być przesyłana w jednej ramce CAN), ale może być łatwo rozszerzony do 2 bajtów. Pomysł oraz wyniki weryfikacji zostały opisane w pracy (Gajdzik, Timofiejczuk, & Sebzda, 2021) i omówione w eksperymencie "Koncepcja okna czasowego dla urządzeń oświetleniowych wewnętrznego otoczenia". Testy weryfikacyjne potwierdziły skuteczność tej metody. Stwierdzono, że niemożliwe jest osiągnięcie 100% skuteczności. Jednakże metoda znacząco minimalizuje prawdopodobieństwo udanego ataku. Im krótsze jest okno czasowe i im większa liczba bitów jest przydzielona znacznikowi czasowemu, tym wyższa jest skuteczność opisanej metody. Przyjmując następujące założenia:

- 16 bitów jest używanych do znacznika czasowego
- wartość okna czasowego ustawiona jest na 100 milisekund
- wysyłanie ramek CAN jest możliwe z rozdzielczością 1 milisekundy.

Prawdopodobieństwo przeprowadzenia udanego ataku poprzez odtworzenie ramki jest bliskie 0%.

$$P_{SA} = \frac{1}{65536} * \frac{100ms}{1ms} = 0{,}15\%$$

P_{SA} - Prawdopodobieństwo Udanego Ataku

co przekłada się na skuteczność ochrony wynoszącą 99,85%.

Koncept XOR

Koncepcja jest rozwiniętą wersją "Konceptu okien czasowych". Rozwiązanie to opiera się na podwójnej negacji bitów w każdym bajcie przesyłanej ramki. Dla bitów, które odpowiadają wartości 1 w argumencie, wykonywana jest operacja bitowej negacji, a reszta bitów pozostaje niezmieniona. Operacja jest wykonywana dwukrotnie. W pierwszym kroku wartość operandu to klucz, a w drugim kroku wartość operandu jest związana z oknem czasowym. 8-bitowa wartość klucza jest przechowywana w pamięci nieulotnej każdego ECU podłączonego do magistrali CAN. Odbiornik ramki wykonuje proces odwrotny, tj. najpierw neguje używając wartości okna czasowego jako argumentu, a następnie klucza przechowywanego w pamięci nieulotnej. W poniższej tabeli przedstawiono kolejne kroki proponowanego algorytmu szyfrowania.

Wartość	Wartość szesnastkowa	Wartość dwójkowa
oryginalny bajt	0x7D	01111101
klucz (maska dla negacji)	0xC3	**11**000**11**
zaszyfrowany bajt – krok1	0xBE	10111110
okno czasowe	0xF1	**1111**0001
Finalnie zaszyfrowany bajt	**0x4F**	01001111

Koncepcja modułu przeciwwłamaniowego magistrali CAN wspomaganego algorytmami opartymi na sztucznej inteligencji

Wyniki przeprowadzonych badań prezentowanych w niniejszej pracy wykazały, że istnieje możliwość przejęcia kontroli nad różnymi elektronicznymi modułami sterującymi (ECU). Nawet funkcje krytyczne, takie jak kierowanie czy hamowanie, które powinny być szczególnie

chronione, są podatne na skuteczne ataki. W związku z tym, aby zapewnić ochronę przed możliwymi atakami na magistralę CAN i jednocześnie nie podnosić znacząco kosztów produkcji pojazdów, proponuje się zastosowanie modułu ochrony magistrali CAN. Rozwiązanie to opiera się na wykorzystaniu algorytmów sztucznej inteligencji do wykrywania anomalii w ruchu na magistrali CAN. Głównym założeniem tego podejścia jest przekonanie, że każda wykryta anomalia może potencjalnie wskazywać na trwający atak.

Zaprezentowana koncepcja stanowi kompromis pomiędzy utrzymaniem niskich kosztów produkcji modułu a skutecznym wykrywaniem ataków na magistralę CAN. Dzięki wprowadzeniu tego rozwiązania istnieje możliwość szybkiej reakcji i zapobiegania przejęciu kontroli nad niektórymi modułami pojazdu. Warto podkreślić, że usprawnienie istniejącej architektury transmisji, opartej na magistralach CAN, poprzez dodanie dodatkowego modułu nadzorczego, niesie ze sobą dodatkowe koszty związane z dużą liczbą interfejsów CAN i wymaganą dużą mocą obliczeniową. Niemniej jednak jest to nadal realne rozwiązanie, zwłaszcza w kontekście rosnącej liczby modułów sterowania elektronicznego w nowoczesnych pojazdach.
Koncepcja modułu opracowana w ramach projektu doktorskiego zakłada implementację algorytmów uczenia maszynowego opartych na modelu autoenkodera oraz opracowanej metodzie map bajtów otrzymywanych z magistrali CAN. Szczegółowy opis i weryfikacja tego podejścia zostały przedstawione eksperymencie "Wykrywanie cyberataków na układ kierowniczy przy użyciu sztucznej inteligencji". Podejście to zostało również opisane w pracy autorstwa (Gajdzik, Sternal, Timofiejczuk, & Przystałka, 2021). Testy weryfikacyjne wykazały, że odpowiednio przeszkolona sieć neuronowa była w stanie wykryć próby ataku na system sterowania kierownicą w samochodzie. W czasie testów weryfikacyjnych największy problem pojawił się podczas procesu trenowania sieci neuronowej. Pomimo dużej mocy obliczeniowej i dedykowanej karty graficznej z niezależną pamięcią RAM o pojemności 24 GB, potrzebnych było ponad 20 godzin treningu sieci. Biorąc pod uwagę, że moduł nadzorczy musiałby być w stanie uczyć się w rozsądnym czasie i obsługiwać kilka lub kilkaset interfejsów magistrali CAN, podejście to okazało się zbyt kosztowne. W kontekście obecnie dostępnych rozwiązań z zakresu IT możliwe jest wykorzystanie rozwiązań związanych z "Przemysłem 4.0". Autor opracował zatem koncepcję polegającą na połączeniu modułu ochrony przed włamaniem z systemem chmurowym. W rezultacie wszystkie obliczenia i operacje, które wymagają dużej ilości zasobów, są wykonywane w chmurze. Moduł implementowany w każdym pojeździe przesyła przetworzone dane do systemu chmurowego, gdzie odbywa się proces treningu. Wymagane jest, aby dane były przetwarzane wstępnie ze względu na ich pierwotny duży rozmiar. Istnieje kilka zalet takiego podejścia. Najważniejsza z nich polega na tym, że wszystkie pojazdy są wyposażone w najnowszy model danych zebranych z wszystkich aktywnych pojazdów. Wystarczy, że jeden pojazd zostanie zaatakowany nieznaną dotąd metodą, a dzięki uczeniu w chmurze i rozpowszechnieniu przeszkolonego modelu do modułów nadzorczych w samochodach, każdy samochód staje się odporny na ten nowy rodzaj ataku. Pozwala to być odpornym na dotąd nieznany rodzaj zagrożenia. Dlatego przedstawiona koncepcja jest inteligentnym modelem samouczenia, który jest w stanie skutecznie wykrywać nieznane rodzaje zagrożeń.

Wnioski i plan dalszych badan

Celem badań przeprowadzonych w ramach projektu doktorskiego było opracowanie rozwiązań mających na celu minimalizację zagrożeń w zintegrowanych systemach samochodowych, które kontrolują moduły elektroniczne. W pierwszej części pracy doktorskiej omówiono potencjalne zagrożenia i przykładowe ataki. Autor zidentyfikował ryzyka związane

z cyberbezpieczeństwem w współczesnych samochodach i przeprowadził serię eksperymentów mających na celu atakowanie niektórych zintegrowanych wbudowanych systemów samochodowych. Wyniki tych eksperymentów stanowiły podstawę do zaproponowania oryginalnych rozwiązań dla podjętego problemu.
Współczesny samochód rozumiany jest jako inteligentny pojazd mechatroniczny zintegrowany z systemem zarządzania zgodnym z różnymi aspektami koncepcji "Przemysłu 4.0".
W trakcie badań udowodniono, że w nowoczesnym samochodzie elektrycznym istnieje możliwość przejęcia kontroli nad następującymi modułami sterującymi w pojeździe: oświetleniem wnętrza, kierunkowskazami i funkcją sterowania kierownicą.
Autor pracy doktorskiej zaproponował dwa różne podejścia do tematu ochrony przed atakami:

- niskokosztowe rozwiązania, które obejmują 3 podejścia do zwiększenia poziomu bezpieczeństwa transmisji między modułami sterującymi w pojeździe, minimalizując szanse na przeprowadzenie udanego ataku,
- zaawansowany system detekcji anomalii, które mogą wskazywać na trwający atak, wykorzystujący głębokie uczenie i sieć neuronową do analizy. W weryfikacyjnych testach eksperymentu "Wykrywanie cyberataków na układ kierowniczy za pomocą podejścia opartego na sztucznej inteligencji", udowodniono, że stosując sugerowany model oparty na koncepcji autoenkodera i głębokich sieci neuronowych, osiągnięto wskaźnik wykrywalności ataku wynoszący 100%. Można zatem założyć, że głęboka sieć neuronowa szkolona na danych zawierających nowe rodzaje zagrożeń jest w stanie je wykrywać z bardzo dużym prawdopodobieństwem, nawet bliskim 100%. W związku z tym autor zaproponował zintegrowany system wymiany informacji między pojazdami a systemem chmurowym, który przetwarza dane z wszystkich aktywnych pojazdów. Biorąc pod uwagę fakt, że proces szkolenia głębokiej sieci neuronowej odbywa się w systemie chmurowym, wystarczy, że nowy rodzaj ataku zostanie przeprowadzony nawet na jednym samochodzie, a wszystkie pojazdy staną się odporne na niego. Można stwierdzić, że przedstawiona koncepcja jest zgodna z ideą Przemysłu 4.0, który integruje różne technologie w jednym ekosystemie. Połączenie pojazdów z systemem chmurowym jest celem dalszych analiz i testów.

Należy podkreślić, że rozwiązania przedstawione jako wynik pracy doktorskiej są uniwersalne. Problem badawczy dotyczy cyberataków na moduły sterowania elektronicznego w pojazdach, ale obecnie bardzo wiele procesów przemysłowych jest zautomatyzowanych, co zwiększa ryzyko przeprowadzenia skutecznego ataku na takie struktury. Metody opracowane w ramach projektu doktorskiego mogą być również wdrożone w innych branżach przemysłu.. Współczesne urządzenia to systemy mechatroniczne połączone ze sobą, tworzące sieć. Zaletą jest wzajemna komunikacja i kontrola. Należy podkreślić, że przejęcie kontroli nad takimi systemami lub przynajmniej destabilizacja ich regularnej pracy jest możliwa. Spektrum obszarów, na których może wystąpić taki atak, jest szerokie i stale rośnie. Z drugiej strony istnieje silna potrzeba automatyzacji jak największej liczby procesów przemysłowych. Przyspiesza to produkcję i zwiększa zyski. Biorąc pod uwagę zakłady produkcyjne, przykłady obejmują linie produkcyjne lub centra logistyczne działające jako zautomatyzowane magazyny towarów. Ponadto warto wspomnieć o dynamicznie rozwijającej się branży prywatnych aplikacji inteligentnych domów.
W kontekście nowych technologii, zmieniających się wymagań użytkowników oraz kwestii związanych z bezpieczeństwem, utrzymanie systemów mechatronicznych stanowi wyzwanie o znacznym stopniu skomplikowania. Problem ten wynika z potrzeby zapewnienia diagnostyki w czasie rzeczywistym na żądanie, nawet w przypadku regularnej i bezpiecznej pracy tych systemów. Paradoksalnie, podejścia oparte na diagnostyce w czasie rzeczywistym wprowadzają dodatkowe potencjalne punkty dostępu dla cyberataków.

W niniejszej rozprawie zostały omówione propozycje modułów cyberbezpieczeństwa, zaproponowane jako odpowiedź na te pojawiające się zagrożenia, Zasada działania tych modułów polega na ciągłej analizie rzeczywistych, niezmienionych sygnałów, zakładając, że nie toczy się aktualnie żaden atak. Jedno z podejść wykorzystuje algorytmy sztucznej inteligencji, ze szczególnym naciskiem na sieci neuronowe. W tym kontekście istotnym aspektem jest ciągłe monitorowanie transmisji danych, z głównym celem wykrywania anomalii, rozumianych jako potencjalne oznaki trwającego ataku.
Należy zaznaczyć, że dostosowanie interfejsów komunikacyjnych stanowi istotny aspekt tej koncepcji, zależnie od wykorzystywanych technologii i magistral komunikacyjnych. Jednym z kluczowych atutów przedstawionego podejścia jest możliwość implementacji procesu ciągłego uczenia się. Ten mechanizm pozwala systemowi nieustannie doskonalić swoje zrozumienie norm zachowań, co przekłada się na efektywność w wykrywaniu ataków oraz skuteczną reakcję na potencjalne zagrożenia.