Sisteme de detecție a intruziunilor pentru magistrale CAN din vehicule comerciale cu comunicație bazată pe SAE J1939

Teză de doctorat – Rezumat
pentru obținerea titlului științific de doctor la
Universitatea Politehnica Timișoara
în domeniul de doctorat Calculatoare și Tehnologia Informației
de
Ing. Camil-Vasile Jichici
Conducător științific: Prof. univ. dr. ing. Bogdan Groza
Septembrie, 2023

Milioane de vehicule grele parcurg sute de kilometri pe autostrăzi în fiecare zi, iar probabilitatea de accidente crește. Datorită acestui lucru, sporirea siguranței participanților la trafic este crucială. În ceea ce privește siguranța, în ultimii zece ani au fost dezvoltate mai multe sisteme de asistență a șoferului, inclusiv avertizarea de coliziune frontală, avertizarea de părăsire a benzii de circulație, dispozitive de blocare a pornirii vehiculului în urma depistării unui șofer sub influența alcoolului, frânarea de urgență autonomă și recunoașterea obiectelor din unghiul mort în timpul deplasării vehiculului. Abilitatea vehiculelor de a fi conduse în mod autonom, fără implicarea umană, este un obiectiv pe termen scurt care este deosebit de important în contextul vehiculelor grele din cauza distanțelor semnificativ de mari pe care trebuie să le parcurgă. Pentru a îndeplini aceste caracteristici, vehiculele grele se transformă, de asemenea, în sisteme ciber-fizice complexe, cu milioane de linii de cod care rulează prin zeci de unități electronice de control și o varietate de senzori, actuatoare, camere și radare. Unitățile electronice de control din vehicule comunică între ele prin diferite interfețe de comunicație, cum ar fi Controller Area Network (CAN), FlexRay și mai recent 100BaseT1 Ethernet, care permite viteze de comunicație substanțial mai mari. Cu toate acestea, în ciuda progreselor recente, magistrala CAN este cea mai utilizată ca și mediu de comunicație, deoarece oferă un raport cost-performanță foarte bun și o soluție fiabilă pentru majoritatea aplicațiilor în timp real. Două versiuni actualizate ale acesteia, CAN-FD [1] și CAN-XL [2], permit rate de transfer mult mai mari dar și câmpuri de date mai mari, care asigură longevitatea protocolului CAN în autoturisme și vehicule grele.

Pe de altă parte, datorită creșterii complexității software, a conectivității și a funcțiilor semi-automatizate, vehiculele devin vulnerabile la atacuri de securitate cibernetică. În consecință, mai multe atacuri au fost raportate de către cercetători în diverse publicații, cum ar fi [3], [4] și [5]. Aceste atacuri pot avea efecte catastrofale atât pentru pasageri, cât și pentru participanții la trafic. Autorii lucrării [3] demonstrează că prin efectuarea de atacuri pe magistrala CAN asupra vehiculelor din lumea reală este posibil ca un adversar să preia controlul mai multor funcții critice ale vehiculului care ignoră complet comenzile șoferului. Exemple de astfel de

acțiuni includ dezactivarea frânelor, deblocarea mașinii, oprirea motorului, etc. Datorită faptului că atacurile demonstrate în [3] necesită o conexiune fizică la magistrala CAN, aplicarea lor în lumea reală poate fi considerată ca fiind una limitată. Pe lângă acest studiu, aceiași autori au demonstrat într-o lucrare ulterioară [4] că atacuri similare pot fi efectuate de la distanță prin stabilirea unei conexiuni cu unitățile de infotainment folosind interfețe wireless precum Bluetooth sau WiFi. Un studiu cuprinzător asupra suprafețelor de atac este oferit de Miller și Valasek în [5].

Indiferent de punctul de acces prin care s-a efectuat atacul, lipsa de securitate a magistralei CAN, care a fost introdusă de către BOSCH în anii 80 [6], este cauza principală a atacurilor menționate anterior. Standardul SAE J1939 [7], dezvoltat de Societatea Inginerilor Automotive în anii 90, este dedicat comunicației CAN în vehiculele grele și completează protocolul standard CAN cu câteva caracteristici specifice care sunt detaliate în capitolul III al tezei. Deoarece protocolul SAE J1939 este construit pe baza protocolului CAN standard, atacuri similare cu cele descrise anterior pot fi efectuate și pe magistralele cu comunicație bazată pe SAE J1939. Un prim exemplu de astfel de atacuri asupra magistralelor CAN conforme cu SAE J1939 a fost propus în [8]. Autorii lucrării [8] demonstrează prin experimente practice pe două vehicule cu comunicație bazată pe SAE J1939, că atacuri asupra funcționalităților critice pentru siguranță cum ar fi accelerarea camionului în timpul mișcării, oprirea frânei de motor, pot fi efectuate prin portul specific J1939 de diagnosticare. Autorii lucrării [9] sunt primii care abordează atacuri asupra protocoalelor de transport specifice SAE J1939 și demonstrează un atac DoS care vizează transmisiile de tip multi-frame. O configurație în care adversarul este conectat la o magistrală CAN conformă cu SAE J1939 și poate intercepta și injecta mesaje malițioase pe magistrala CAN a unui vehicul greu prin portul OBD specific J1939, este prezentată în Figura 1.

Fig. 1. Un vehicul greu care implementează standardul SAE J1939 și instrumentele pentru colectarea de date a traficului de CAN

Având în vedere preocupările pentru siguranța a numeroși pasageri (din interiorul autobuzelor), sau a mărfurilor transportate (din interiorul camioanelor), soluțiile de securitate dez-

voltate pentru sectorul vehiculelor comerciale necesită o atenție deosebită. Cele expuse mai sus stau la motivația din spatele acestei teze. În acest sens, această teză urmărește implementarea sistemelor de detecție a intruziunilor adaptate magistralelor CAN cu comunicație bazată pe SAE J1939.

Obiectivele cercetării. Obiectivul principal de cercetare este implementarea sistemelor de detecție a intruziunilor adaptate la protocolul SAE J1939, care este construit pe baza protocolului CAN și definește nivelurile superioare din stiva de comunicație cum ar fi nivelul de legătură de date sau nivelul de rețea, folosite pentru implementarea funcționalităților din vehicule cu ajutorul magistralelor CAN. Înainte de a trece la soluțiile specifice pentru magistralele SAE J1939, sunt necesare și câteva investigații privind mecanismele de detecție al intruziunilor pentru traficul standard de CAN din autoturisme. Mai precis, obiectivele majore de cercetare ale acestei teze, sunt următoarele:

1) Revizuirea literaturii de specialitate privind lucrările relevante pentru detectarea intruziunilor pe magistralele CAN;
2) Colectarea traficului CAN din autoturisme precum și din vehicule grele cu comunicație bazată pe J1939 pentru a fi folosit în experimente;
3) Evaluarea performanței algoritmilor de inteligență artificială folosiți pentru sisteme de detecție a intruziunilor pe magistralele CAN, precum și fezabilitatea utilizării unor astfel de mecanisme de detecție în aplicații reale din vehicule;
4) Proiectarea și implementarea unei platforme care permite simularea modelelor de adversar și detecția intruziunilor în CANoe;
5) Proiectarea și implementarea unui sistem de detecție și prevenire a intruziunilor care vizează magistralele CAN bazate pe SAE J1939;
6) Analiza atacurilor efectuate la nivelul sistemelor de control ale magistralelor CAN conforme cu SAE J1939 și propunerea unor contramăsuri corespunzătoare.

Contribuții majore. O prezentare generală a contribuțiilor acestei teze este oferită în cele ce urmează. Această teză prezintă mai multe abordări de sisteme de detecție a intruziunilor pentru magistralele CAN, în special pentru magistralele CAN conforme cu SAE J1939. Având în vedere obiectivele de cercetare prezentate mai sus, contribuțiile autorului pot fi rezumate astfel:

1) Traficul CAN a fost colectat de autor de la mai multe vehicule, și anume, 427.660 de mesaje CAN colectate de la un vehicul greu în mișcare care este conform cu standardele de comunicație SAE J1939 [10] și a fost utilizat pentru experimentele din această teză;
2) Traficul CAN a fost de asemenea colectat de către autor pentru mai multe lucrări la care este co-autor sau pe care l-a folosit parțial în lucrările sale ca prim autor, mai exact, 2.488.248 de mesaje CAN colectate de la trei vehicule Dacia Duster diferite [11], [12]; 2.783.265 de mesaje CAN și 90.723 eșantioane de biți de tensiune colectate de la 5 autoturisme [13]; 154.779 mesaje de CAN și 4.021 eșantioane de biți de tensiune colectate de la un vehicul greu cu comunicație bazată pe SAE J1939 [13];
3) Evaluarea rețelelor neuronale în detecția intruziunilor pe magistrale CAN, precum și a performanței lor computaționale pe platforme embedded folosite în industria automotive [14];
4) Implementarea și testarea unei platforme care permite integrarea modelelor de adversar și a sistemelor de detecție a intruziunilor într-un program software standard folosit în industrie, și anume, CANoe [11];
5) Implementarea unui sistem de detecție și prevenire a intruziunilor, adaptat pentru a îndeplini specificațiile J1939. Pentru a demonstra corectitudinea, precum și fezabilitatea utilizării

soluției propuse în vehiculele din lumea reală, este realizată o implementare a conceptului într-o configurație de laborator [10];
6) O implementare specială pentru decodificarea conținutului mesajelor de CAN înainte ca nodurile receptoare să fi setat bitul de confirmare (ACK). Acest lucru face posibilă eliminarea instantanee a intruziunilor fără a fi nevoie de hardware specializat [10];
7) O propunere pentru un mecanism de detecție a atacurilor efectuate la nivelul sistemelor de control care sunt dificil de detectat de către un sistem de detecție de intruziune uzual [15];
8) Dezvoltarea unei mediu experimental care conectează două dintre cele mai utilizate platforme în industrie, CANoe pentru simularea rețelelor vehiculare și respectiv MATLAB pentru proiectarea sistemelor de control [15].

Aceste contribuții se regăsesc într-o serie de articole științifice publicate în diferite reviste și conferințe. Aplicarea rețelelor neuronale ca și sisteme de detecție a intruziunilor pe magistrale CAN a fost explorată de către autor în [14]. Majoritatea experimentelor au fost efectuate pe trafic de CAN generat dintr-o simulare J1939 și o mică parte dintre ele au fost efectuate pe un alt set de date public. Timpul de rulare al algoritmului de detecție a fost evaluat pe trei platforme hardware folosite în industria automotive, pentru a determina dacă soluția propusă ar putea fi utilizată în scenarii din lumea reală. Una dintre platforme reprezintă grupul de dispozitive cu resurse limitate, în timp ce celelalte două sunt candidați pentru dispozitive performante. Având în vedere faptul că atacurile asupra traficului CAN J1939 din [14] au fost generate folosind un script C#, un scenariu mai realist ar fi utilizarea traficului CAN din lumea reală și efectuarea atacurilor folosind o simulare CANoe. Din acest motiv, autorul analizează acest scenariu în [11], unde o platformă este propusă pentru a retransmite traficul CAN colectat de la vehiculele reale și pentru a permite integrarea modelelor de adversar împreună cu sistemele de detecție în cadrul unei simulări bazate pe CANoe. Clasificatorul k-NN a fost investigat ca și sistem de detecție de intruziune în această lucrare [11], însă platforma a fost concepută pentru a suporta orice alt sistem de detecție a intruziunilor. Următoarele două lucrări ale autorului [10], [15] abordează sisteme de detecție de intruziune în contextul magistralelor CAN conforme cu SAE J1939. În prima lucrare [10], autorul propune un sistem de detecție de intruziuni bazat pe două etape și completat de un mecanism de prevenire. În prima etapă se verifică validitatea adreselor criptate. A doua etapă efectuează verificări adecvate ale intervalului de evoluție a parametrilor pentru a detecta chiar și modificări ale unui singur bit în câmpul de date. Deoarece conținutul câmpului de date ale mesajelor CAN este criptat, efectul de avalanșă produs în urma decriptării facilitează identificarea chiar și a celor mai mici intervenții ale adversarului. Mecanismul de prevenire necesită decodificarea fiecărui mesaj CAN (identificatorul și câmpul de date) înainte ca receptorii să confirme recepția corectă prin suprascrierea unui bit dominant în slotul de ACK. Dacă mesajul CAN curent este detectat ca intruziune, acesta este eliminat de pe magistrala CAN prin forțarea intenționată a unui mesaj de eroare. Pentru a demonstra aplicabilitatea practică a soluției, este realizată o implementare a conceptului pe un microcontroler performant din industria automotive. De asemenea, în [15], autorul examinează atacurile asupra magistralelor SAE J1939 efectuate la nivelul sistemelor de control și propune un mecanism de detectare pentru acestea. În plus, această lucrare demonstrează ineficiența sistemelor de detecție bazate pe algoritmi de inteligență artificială în identificarea acestor tipuri de modificări subtile ale câmpului de date și că mecanismele de detectare a schimbărilor sunt mult mai eficiente.

Pe lângă lucrările de cercetare menționate mai sus, care reprezintă nucleul acestei teze, autorul a fost implicat în alte lucrări de cercetare, dintre care cinci au ca și subiect tot securitatea automotive și una abordează împerecherea dispozitivelor mobile (smartphone-urilor) pe baza

unor date extrase din mediu. O abordare eficientă pentru localizarea nodurilor rețelei CAN pe baza întârzierilor de propagare a semnalelor fizice de CAN a fost investigată în [16]. Două conexiuni fizice, una la fiecare capăt al magistralei CAN și doar un front crescător sunt necesare pentru a examina întârzierile de propagare. În această lucrare, autorul a contribuit cu colectarea datelor de tensiune de la o configurație de laborator, precum și cu pregătirea configurației de colectare a datelor în interiorul unui vehicul real, un Renault Megane. O performanță comparativă între dispozitivele bazate pe Android și microcontrolere pentru implementarea mai multor clasificatoare binare ca si sisteme de detecție de intruziune este discutată în [12]. Contribuția autorului tezei la această lucrare ține tot de colectarea traficului CAN de la un SUV, și anume un Dacia Duster, precum și de augmentarea traficului colectat cu atacuri specifice în cadrul unei simulări CANoe. O altă lucrare care este trimisă spre publicare abordează un concept de sistem de detecție a intruziunilor care utilizează infrastructura cloud și dispozitivele bazate pe Android utilizate în vehiculele actuale, care sunt mai puternice din punct de vedere computațional decât micontrolerele. Conceptul include, de asemenea, o echipă de răspuns la incidente care efectuează o evaluare suplimentară a rezultatelor de detecție, iar rezultatul final al acesteia este înregistrat pe Blockchain sub formă de rapoarte care respectă standardul ISO/SAE 21434 [17]. Aici, traficul CAN a fost colectat de la trei vehicule diferite Dacia Duster pentru a demonstra că odată antrenați algoritmii de inteligență artificială pentru una dintre mașini pot fi folositi și la celelalte două mașini în scopul de a detecta intruziuni. Amprentarea fizică a unităților electronice de control bazate pe deviații de ceas de la microcontrollere și date de tensiune extrase de la nivelul fizic este propus în [13]. Analiza efectuată a condus la identificarea a 54 de amprente, adică 54 de unități electronice de control. Pentru evaluare a fost utilizat un set extins de date, care include date colectate de la 9 mașini de pasageri și de la un vehicul cu comunicație bazată pe SAE J1939. Datele de la 5 din cele 9 autoturisme și de la vehiculul greu cu comunicație bazată pe J1939 au fost colectate de către autorul tezei. De asemenea, autorul tezei a contribuit, la o lucrare în care este investigată influența caracteristicilor cablajului asupra amprentelor pe bază datelor de tensiune extrase de la liniile de comunicație CAN [18]. Ca rezultat al acestei cercetări, s-a stabilit că rețelele CAN care se bazează pe cabluri comerciale sau industriale au rata de zgomot și rata de creștere/scădere a tensiunii (slew rate) pentru un bit dominant mai mari decât cele care se bazează pe cabluri folosite în industria automotive. Nu în ultimul rând, autorul tezei a fost membru al proiectului PRESENCE unde a contribuit la o lucrare care abordează împerecherea securizată a dispozitivelor mobile plasate în diverse medii de transport (tramvai, mașină, tren, etc) pe baza datelor extrase de la accelerometru [19].

Per total, autorul tezei a contribuit la 10 articole științifice, dintre care 9 sunt axate pe securitatea automotive și unul este legat de împerecherea securizată a dispozitivelor mobile pe baza datelor extrase de la accelerometru:

1) Camil Jichici, Bogdan Groza, and Pal-Stefan Murvay, “Examining the Use of Neural Networks for Intrusion Detection in Controller Area Networks”, Innovative Security Solutions for Information Technology and Communications: 11th International Conference, SecITC 2018, Bucharest, Romania, November 8–9, 2018, Springer International Publishing, 2019,
2) Camil Jichici, Bogdan Groza, and Pal-Stefan Murvay, “Integrating Adversary Models and Intrusion Detection Systems for In-Vehicle Networks in CANoe”, Innovative Security Solutions for Information Technology and Communications: 12th International Conference, SecITC 2019, Bucharest, Romania, November 14–15, 2019, Springer International Publishing, 2020,
3) Camil Jichici, Bogdan Groza, Radu Ragobete, Pal-Stefan Murvay and Tudor Andreica, “Effective intrusion detection and prevention for the commercial vehicle SAE J1939 CAN

bus", IEEE Transactions on Intelligent Transportation Systems, vol. 13, pp. 17425-17439, 2022,
4) Camil Jichici, Adriana Berdich, Adrian Musuroi, and Bogdan Groza, "Control System Level Intrusion Detection on J1939 Heavy-Duty Vehicle Buses", IEEE Transactions on Industrial Informatics, 2023,
5) Bogdan Groza, Lucian Popa, Pal-Stefan Murvay and Camil Jichici, "CAN-SQUARE-Decimeter Level Localization of Electronic Control Units on CAN Buses", Computer Security–ESORICS 2021: 26th European Symposium on Research in Computer Security, Darmstadt, Germany, October 4–8, 2021, Springer International Publishing,
6) Lucian Popa, Bogdan Groza, Camil Jichici, and Pal-Stefan Murvay, "ECUPrint - Physical Fingerprinting Electronic Control Units on CAN Buses Inside Cars and SAE J1939 Compliant Vehicles", IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1185–1200, 2022,
7) Tudor Andreica, Christian-Daniel Curiac, Camil Jichici, and Bogdan Groza, "Android Head Units vs. In-Vehicle ECUs: Performance Assessment for Deploying In-Vehicle Intrusion Detection Systems for the CAN Bus," IEEE Access, vol. 10, pp. 95161–95178, 2022,
8) Lucian Popa, Camil Jichici, Tudor Andreica, Pal-Stefan Murvay and Bogdan Groza, "Impact of Wiring Characteristics on Voltage-based Fingerprinting in Controller Area Networks", IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI 2023), 2023,
9) Tudor Andreica, Adrian Musuroi, Alfred Anistoroaiei, Camil Jichici and Bogdan Groza, "Blockchain Integration for in-Vehicle CAN Bus Intrusion Detection Systems with ISO/SAE 21434 Compliant Reporting", **(under submission)**,
10) Bogdan Groza, Adriana Berdich, Camil Jichici, and Rene Mayrhofer, "Secure Accelerometer-Based Pairing of Mobile Devices in Multi-Modal Transport", IEEE Access, vol. 8, pp. 9246–9259, 2020.

Această teză investighează diverse sisteme de detecție a intruziunilor pentru magistralele CAN, în special pentru cele implementate în vehiculele grele conforme cu SAE J1939. Abordările utilizate pentru implementarea acestor sisteme variază de la utilizarea algoritmilor de inteligență artificială până la împiedicarea adversarilor prin ascunderea conținutului unui mesaj folosind criptografia simetrică sau realizarea unei analize detaliate la nivelul sistemelor de control. Majoritatea rezultatelor acestei teze se bazează pe trafic de CAN autentic, care a fost colectat de către autorul tezei, fie de la un vehicul comercial (un utilaj agricol modern), fie de la mașini de pasageri (un sedan sau un SUV). O parte din rezultate se bazează pe trafic de CAN generat direct din mediul CANoe, un program software standard în industrie care este utilizat pe scară largă în dezvoltarea rețelelor vehiculare. Pentru a testa și a demonstra că mecanismele de detecție sunt potrivite pentru integrarea lor pe dispozitive din vehicule reale, mai multe măsurători ale duratei de execuție a mecanismelor de detecție sunt efectuate pe microcontrolere. Mai mult, rezultatele de acuratețe în detectarea intruziunilor obținute cu ajutorul soluțiilor propuse sunt comparate cu cele raportate de lucrările aferente de detectare a intruziunilor pentru magistralele CAN cu scopul de a evidenția avantajele oferite de acestea. Pentru fiecare capitol urmează o scurtă descriere generală, menționând unele dintre constatările semnificative.

Capitolul II prezintă o analiză cuprinzătoare a literaturii de specialitate privind soluțiile de securitate propuse pentru magistralele CAN, cu un accent pe sistemele de detecție a intruziunilor și magistralele CAN conforme cu J1939. La final, acest capitol prezintă următoarele metrici: rata pozitiv adevărată (TPR), rata negativ adevărată (TNR), rata pozitiv falsă (FPR), rata negativ falsă (FNR), acuratețea și precizia. Aceste metrici sunt introduse pentru a evalua eficacitatea

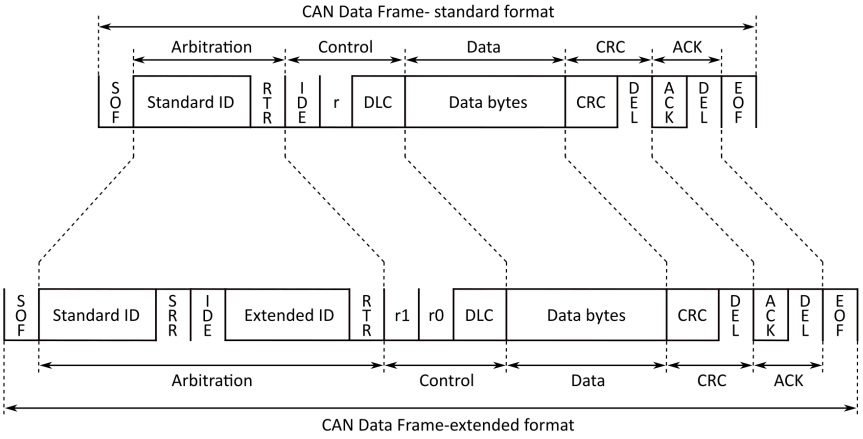

Fig. 2. Formatul standard si extins al unui mesaj de date transmis pe magistrala CAN

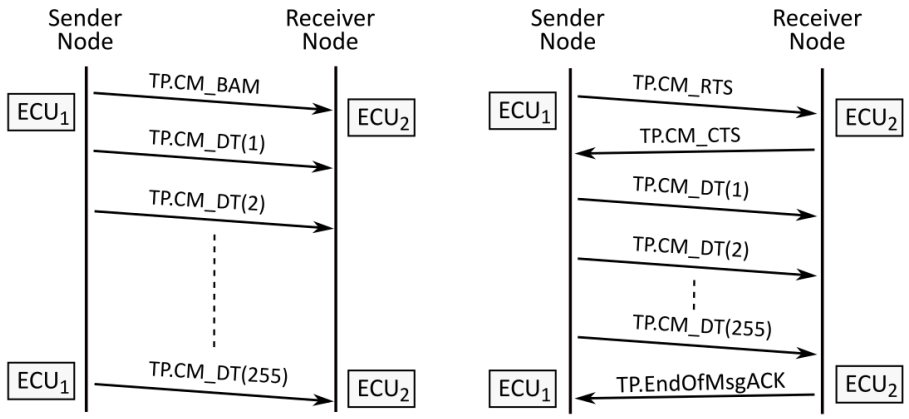

Fig. 3. Broadcast Data Transfer (stânga) and Connection Mode Data Transfer (dreapta) – protocoale de transport folosite în transmisii de tip multi-frame

soluțiilor de securitate propuse în detectarea intruziunilor.

Capitolul III oferă o scurtă descriere a protocolului CAN, concentrându-se pe magistralele CAN conforme cu SAE J1939. Se detaliază nivelul fizic, precum și structura unui mesaj de date. Cele 2 formate, standard și extins, ale unui mesaj de date sunt prezentate în Figura 2. Acest capitol continuă cu o prezentare generală a caracteristicilor specifice SAE J1939, cum ar fi: numerele grupurilor de parametri, protocoalele de transport, defalcarea identificatorului unui mesaj de CAN, precum și procedura de revendicare a adreselor. Protocoalele de transport utilizate în transmisiile de mesaje de tip multi-frame, *Broadcast Data Transfer* și *Connection Mode Data Transfer* sunt descrise în Figura 3. Toate acestea sunt introduse ca noțiuni preliminare pentru implementarea unor sisteme specifice de detecție a intruziunilor, adaptate pentru a respecta specificațiile SAE J1939 și care sunt discutate în capitolele următoare.

Capitolul IV explorează utilizarea rețelelor neuronale ca și sisteme pentru detecția intruziunilor în rețelele CAN. Prima secțiune a acestui capitol începe cu o prezentare a scenariilor care pot fi exploatate de un adversar pentru a obține acces fizic la magistrala CAN prin portul OBD și injectează mesaje malițiose de CAN. Aceeași secțiune detaliază tipurile de atacuri care fac obiectul evaluării sistemului de detecție de intruziune. Următoarea secțiune descrie mediile de dezvoltare utilizate pentru implementarea sistemului de detecție a intruziunilor bazat pe rețele neuronale. Sunt realizate două implementări diferite, una folosește Neural Network Toolbox pusă la dispoziție de platforma MATLAB, în timp ce cealaltă se bazează pe o implementare C++. Prima abordare este preferată, deoarece setul de instrumente pentru rețele neuronale oferit de MATLAB este bine-cunoscut pentru performanța sa, în timp ce a doua este folosită deoarece codul C++ poate fi portat cu ușurință pe micontrolere. Cu toate acestea, se face o verificare pentru a se asigura că rezultate similare de detecție se obțin folosind ambele implementări și într-adevăr acesta este și cazul. Apoi, această secțiune discută pe scurt condițiile de oprire (pentru etapa de antrenament), arhitectura rețelei neuronale, care este prezentată în Figura 4, precum și caracteristicile extrase din traficul CAN, care servesc ca intrări pentru rețeaua neuronală. Rezultatele experimentale în ceea ce privește detecția și performanța de rulare pentru

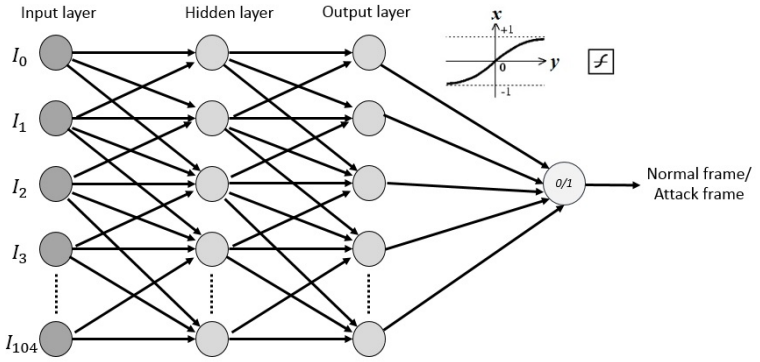

Fig. 4. Structura rețelei neuronale folosită ca sistem de detecție a intruziunilor

sistemul de detecție propus sunt detaliate în secțiunea următoare din acest capitol. Experimentele sunt efectuate pe un trafic care a fost generat folosind o simulare CANoe J1939 și pe un set de date public de CAN. Pentru fiecare tip de atac (retransmisie sau injecții cu date generate aleator în câmpul de date), sunt testate mai multe scenarii în funcție de modul în care traficul de CAN este împărțit între antrenament, validare și testare precum și de modul în care sunt efectuate atacurile, fie pe un singur identificator, fie pe toți identificatorii din trafic. Mai mult, pentru a sublinia compromisul dintre acuratețea rezultatelor de detecție și performanța de rulare, evaluarea este efectuată folosind trei dimensiuni diferite pentru rețeaua neuronală. Performanța de rulare a algoritmului de detectare este măsurată pe trei microcontrolere folosite în industria automotive, unul considerat candidat pentru grupul de dispozitive cu resurse limitate și celelalte două pentru grupul de dispozitive performante. Sistemul de detecție propus are o acuratețe mai slabă în detectarea atacurilor de tip ”replay” (retransmisie), deoarece conținutul mesajelor injectate este același cu cel al mesajelor legitime (timpul de sosire al mesajelor de CAN este singura modalitate de a identifica astfel de atacuri). În ansamblu, experimentele arată că, în ciuda rezultatelor bune în detecția intruziunilor, utilizarea unei astfel de soluții pentru filtrarea

în timp real a traficului de CAN este discutabilă, cel puțin pe microcontrolere cu resurse limitate, deoarece timpul necesar clasificării unui mesaj de CAN este de ordinul a zeci de milisecunde. Acest lucru poate fi considerat un aspect important deoarece majoritatea lucrărilor conexe nu prezintă astfel de rezultate sau utilizează un mediu bazat pe PC-uri cu resurse puternice, care nu reflectă realitatea la nivel de microcontrolere.

O platformă care permite integrarea diverselor modele de adversar pe magistrala CAN, precum și a sistemelor de detecție a intruziunilor în interiorul unei simulări CANoe și oferă în același timp un mediu de testare realist pentru acestea, este prezentat în Capitolul V. Prima secțiune a acestui capitol începe cu o descriere a procedurii folosite de către autorul tezei pentru extragerea traficului de CAN din două autoturisme. Apoi, această secțiune prezintă configurația utilizată pentru colectarea datelor în interiorul vehiculelor, precum și formatul mesajelor CAN înregistrate. Structura rețelei CAN din simularea CANoe și modul în care traficul CAN colectat este utilizat în interiorul acesteia sunt detaliate la sfârșitul acestei secțiuni. A doua secțiune prezintă diverse tipuri de atacuri care au fost integrate în simularea CANoe. Aceste atacuri includ retransmisia mesajelor legitime, injecții cu date generate aleator în câmpul de date, injecții cu date multiplicate folosind un scalar sau la care se adaugă un scalar (tot din câmpul de date), precum și injecții arbitrare. Apoi, această secțiune continuă cu o prezentare a modului în care poate fi utilizată interfața grafică ilustrată în Figura 5, care permite configurarea a diverși parametri pentru atacuri. În secțiunea următoare este prezentat *Statistics and Machine Learning*

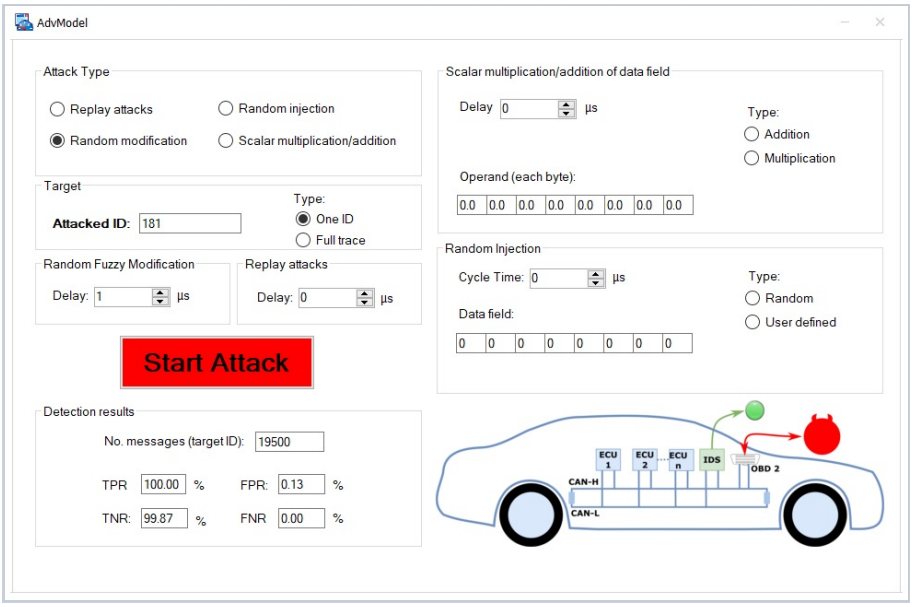

Fig. 5. Interfața grafică pentru utilizator din simularea CANoe

Toolbox oferit de platforma MATLAB, și algoritmul k-NN, folosit ca și sistem de detecție de intruziune. Această secțiune se încheie cu o descriere a intrărilor pentru algoritmul k-NN, care conține următoarele caracteristici extrase din mesajele de CAN: intervalul de timp între sosirea a două mesaje consecutive cu același identificator, precum și conținutul câmpului de date. Nu în ultimul rând, secțiunea experimentală prezintă rezultatele de detecție obținute pentru mai

multe scenarii. Experimentele sunt efectuate pentru a acoperi toate tipurile de atacuri definite anterior. Scenariile testate depind de întârzierea atacului, de ceea ce vizează adversarul (un identificator sau traficul de CAN complet), de câți vecini și ce metrică de distanță sunt utilizate de algoritmul k-NN, precum și de valorile scalare utilizate modificarea câmpului de date. Din cunoștințele autorului, aceasta este prima platformă care permite simularea atât a atacurilor pe magistrale CAN cât și a sistemelor de detecție de intruziune într-un mediu unificat. În același timp, utilizarea unei astfel de platforme este mai sigură deoarece previne orice pericol potențial pentru șoferi sau mașini.

În capitolul VI, este prezentată evaluarea unui sistem de detecție și prevenire a intruziunilor cu scopul securizării magistralelor CAN ale vehiculelor grele care sunt conforme cu standardele SAE J1939. Prima secțiune a acestui capitol rezumă modul în care traficul de pe magistrala CAN conformă cu standardele SAE J1939 este colectat de către autorul tezei prin conectarea la portul de diagnosticare specific SAE J1939 de la un utilaj agricol (un tractor). Această secțiune continuă cu o analiză a caracteristicilor conforme cu SAE J1939 care sunt prezente în traficul de date colectat de pe magistrală. Traficul înregistrat conține 51 de identificatori de mesaje și este transmis de trei unități electronice de control diferite care sunt determinate prin investigarea adreselor sursă unice încorporate în câmpurile de identificare (ID-uri). Conform standardelor SAE J1939, funcția fiecărei unitate electronică de control din rețea este reprezentată după cum urmează: modulul de control al motorului, modulul de control al funcționalităților de ”body” (clima, geamuri, închidere centralizată etc.) și, respectiv, modulul de control al transmisiei. O analiză cantitativă care este bazată pe periodicitatea contabilizată pentru fiecare identificator CAN din mesajele înregistrate, este discutată la sfârșitul acestei secțiuni. Următoarea secțiune prezintă modelul de adversar care include atât atacuri de tip ”replay” (retransmisie), cât și atacuri de modificare al pachetelor. Cu toate acestea, atacurile de modificare urmează o abordare diferită față de cea prezentată în capitolele IV și V, prin aceea că atacurile sunt realizate la nivel de parametri, nu pe întregul câmp de date. Această secțiune prezintă apoi sistemul de detecție a intruziunilor în două etape care a fost conceput pentru a proteja magistralele CAN conforme cu standardele SAE J1939. Prima etapă se bazează pe adresele criptate, adică, sursa mesajelor, precum și adresele de destinație din fiecare câmp de identificare, care sunt criptate folosind algoritmul AES. Motivul din spatele încorporării elementelor de securitate în identificatorii mesajelor CAN este prezentat în cele ce urmează. Conform standardelor SAE J1939, câmpul de date al mesajelor este alocat complet cu parametri specifici SAE J1939, care, la rândul lor, sunt alocați unui grup de parametri. Prin urmare, elementele de securitate sunt împachetate în câmpurile de identificare mai ușor decât în câmpul de date, deoarece utilizarea parametrilor din câmpul de date ca elemente de securitate ar fi în contradicție cu specificațiile din standardele SAE J1939. Prima etapă de detecție a intruziunilor este completată de a doua, care se bazează pe câmpul de date criptat. Acest lucru permite detecția intruziunii chiar și atunci când biți singulari din câmpul de date sunt manipulați, datorită efectului de avalanșă rezultat din decriptarea informației și verificarea ulterioară de plauzibilitate aplicată pentru fiecare parametru specific SAE J1939 transportat de către mesaj. Ulterior, în această secțiune sunt prezentate informații referitoare la cum sunt generate și stocate aceste adrese criptate folosind un arbore binar ordonat și liste circulare. Deoarece aceste adrese trebuie generate ciclic, secțiunea se încheie cu o formalizare a compromisului între periodicitatea generării arborelui de adrese și resursele utilizate (puterea de calcul și capacitatea de stocare). Nu în ultimul rând, secțiunea experimentală oferă o prezentare a timpilor de rulare măsurați pe plăcile de dezvoltare utilizate pentru operațiunile de criptare simetrică (AES) precum și pentru generarea arborelui de adrese. Apoi, secțiunea oferă o privire de ansamblu asupra mecanismului

de protecție activă a mesajelor legitime, care acționează ca un sistem de prevenire al atacurilor. Acest mecanism permite decodificarea conținutului fiecărui mesaj transmis pe magistrala CAN (câmpul de identificare și câmpul de date) înainte ca slotul ACK să fie suprascris de către receptori în cazul recepționării corecte a unui mesaj. În plus, în cazul în care cadrul decodificat este clasificat ca fiind o intruziune, se declanșează procedura de eliminare a acestuia folosind un mesaj de eroare. Pentru a testa și dovedi capacitățile de distrugere a mesajului declanșat de mecanismul de prevenire, se utilizează montajul experimental de laborator prezentat în Figura 6.

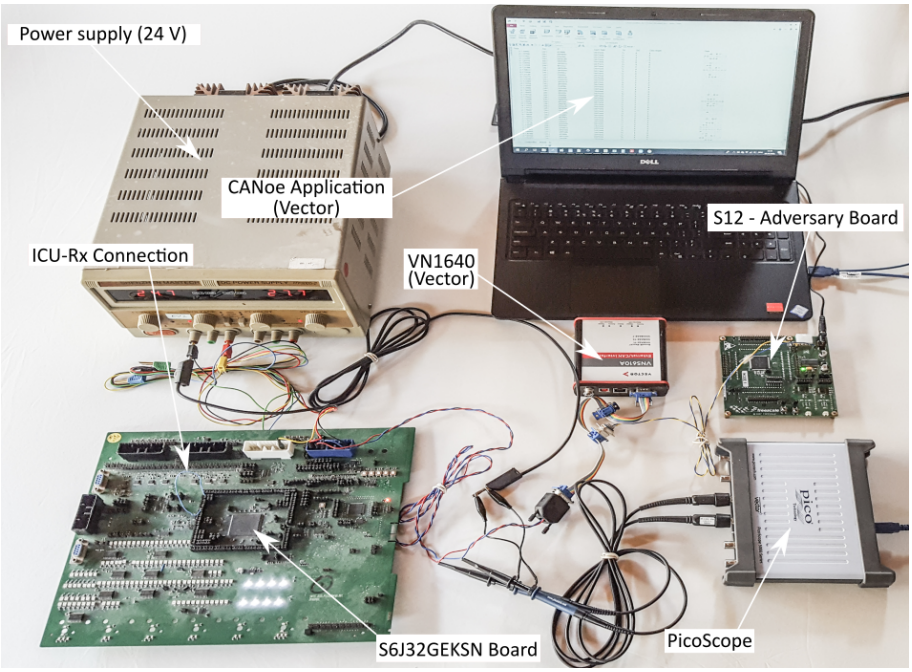

Fig. 6. Configurația experimentală cu dispozitivul VN1640, plăcile de dezvoltare S6J32GEKSN și S12, sursa de alimentare precum și PicoScope pentru monitorizarea comunicației CAN

În finalul acestei secțiuni sunt prezentate rezultatele de detecție a intruziunilor obținute pentru atacurile realizate pe diferiți parametri specifici J1939. De asemenea, este prezentată și o analogie între nivelul de securitate considerat pentru soluția propusă și unul care îndeplinește cerințele specifice AUTOSAR precum ”Secure On-Board Communication (SecOC)” [20]. În general, soluția propusă, care a fost concepută special pentru a îndeplini specificațiile din standardele J1939 s-a dovedit a fi o metodă ce poate fi utilizată atât pentru detectarea în timp real, cât și pentru eliminarea mesajelor care sunt considerate ca intruziuni. Mai mult, după cunoștințele autorului tezei, acesta este primul sistem de detecție și prevenire a intruziunilor adaptat pentru vehicule de mare tonaj cu rețele CAN conforme cu standardele SAE J1939. Abordarea inovatoare pentru decodificarea mesajelor de CAN folosind o metodă bazată pe Input-Capture Unit (ICU) este o altă dezvoltare semnificativă prezentată în acest capitol.

Capitolul VII prezintă un sistem de detecție a intruziunilor la nivelul sistemelor de control din vehicule, adaptat pentru a îndeplini specificațiile din standardele SAE J1939. O prezentare gen-

erală a conexiunii dintre Simulink și CANoe, precum și a modurilor de funcționare combinată a acestora este inclusă în prima secțiune din acest capitol. Ea este, de asemenea, prezentată și în Figura 7. Următoarea secțiune continuă cu o scurtă descriere a simulării din CANoe pentru

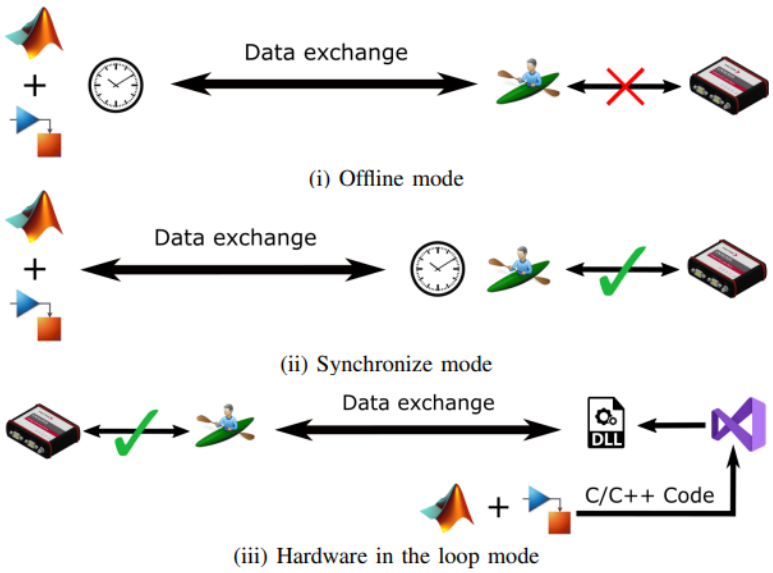

Fig. 7. Interacțiunea CANoe-Simulink – moduri de operare

J1939, a modelelor Simulink folosite precum și a modelului adversar considerat. Modelele Simulink sunt integrate în simularea CANoe și permit predicția următoarelor semnale: viteza vehiculului, distanța parcursă, turația motorului și cuplul. Modelul de adversar este implementat prin atacuri specifice, realizate la nivelul sistemelor de control, cum ar fi: atacuri de tip ”surge”, atacuri de tip ”bias” și atacuri de tip ”geometric”, care nu au fost luate în considerare de către alte lucrări de detecție a intruziunilor pe magistrala CAN până acum. Pe lângă aceste trei tipuri de atac, este luat în considerare și un tip comun de atac, și anume atacul de tip ”fuzzing”. Prima parte a secțiunii experimentale evidențiază comportamentul parametrilor specifici J1939 atunci când sunt realizate astfel de atacuri. Apoi, în această secțiune sunt prezentate rezultatele în ceea ce privește performanța în detecția intruziunilor luate în considerare atât pentru abordările bazate pe învățarea automată, cât și pentru mecanismele de detectare a schimbărilor evoluției parametrilor. O constatare semnificativă din această secțiune arată că, în ciuda eforturilor tot mai mari de a folosi abordări bazate pe învățarea automată pentru sistemele de detecție a intruziunilor, acest tip de algoritmi nu pot identifica modificări minore în câmpul de date ale mesajelor de CAN. Pe de altă parte, pe baza rezultatelor experimentale, mecanismul de detecție a schimbărilor este dovedit a fi mai eficient în detecția unor astfel de atacuri. Pentru fiecare semnal specific J1939, sunt testate mai multe scenarii de atac cu privire la simulări scurte (1000 de cadre CAN) și simulări lungi (1 oră). Pentru fiecare semnal, indiferent de tipul de atac, sunt menținute aceleași valori de ”bias” și ”threshold”. Acest lucru a fost făcut pentru ca scenariile folosite să fie cât mai aproape de condițiile din realitate. În ultima parte a acestei secțiuni este prezentată performanța de rulare a algoritmilor de detecție propuși și prezentați în acest capitol. Rezultatele obţinute arată clar că timpul de rulare al mecanismelor de detecție a schimbărilor

este de la de 2 ori până la de 65 de ori mai mic decât cel necesar pentru execuţia algoritmilor de învăţare automată. Mai mult, nu numai din perspectiva eficienței computaționale, ci și din punct de vedere al capacității de stocare, mecanismul de detectare a schimbării este mai eficient deoarece sunt necesare doar câteva linii de cod pentru implementare lui, în timp ce algoritmii bazați pe învățarea automată necesită utilizarea unei zone de memorie de 10-30 KB.

Capitolul VIII prezintă concluziile tezei de doctorat. Per total, această teză investighează diverse soluții de securitate care vizează magistralele CAN pentru vehicule grele conforme cu standardele SAE J1939, dintre care unele ar putea fi aplicate și magistralelor CAN standard, spre exemplu celor din autoturisme. Aplicabilitatea lor practică a fost testată în diferite configurații de laborator folosind echipamente concepute special pentru industria automotive (microcontrolere, dispozitive VN1640, cabluri CAN, etc.). Ca un rezultat major, această teză prezintă o platformă realistă pentru testarea atacurilor de pe magistralele CAN din vehicule și a sistemelor de dectecție aferente, un sistem de detecție și prevenire a intruziunilor adaptat pentru a îndeplini specificațiile din standardele SAE J1939, o metodă nouă de interpretare a conținutului mesajelor CAN (câmpul de identificare și câmpul de date) înainte de recepția corectă a acestora, precum și un sistem de detecție a intruziunilor proiectat la nivelul de sistemelor de control. Rezultatele acestei teze au fost publicate în reviste și conferințe relevante din domeniul securității, industriei automotive cât și al aplicaților industriale. În general, rezultatele indică faptul că sistemele de detecție a intruziunilor sunt esențiale pentru creșterea securității rețelelor din vehicule și că un astfel de mecanism poate fi implementat eficient în echipamentele dezvoltate în prezent din industrie.

REFERINȚE

[1] "ISO11898-1. Road vehicles — Controller area network (CAN) —Part 1: Data link layer and physical signalling," International Organization for Standardization, Standard, 2nd edition, Dec 2015.

[2] F. Hartwich and R. Bosch, "Introducing CAN XL into CAN Networks," *future*, vol. 11898, p. 1, 2015.

[3] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham *et al.*, "Experimental security analysis of a modern automobile," in *Security and Privacy (SP), 2010 IEEE Symposium on*. IEEE, 2010, pp. 447–462.

[4] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno *et al.*, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," in *USENIX Security Symposium*. San Francisco, 2011.

[5] C. Miller and C. Valasek, "A survey of remote automotive attack surfaces," *Black Hat USA*, 2014.

[6] *CAN Specification Version 2.0.*, Robert BOSCH GmbH, 1991.

[7] "J1939 - Serial Control and Communications Heavy-Duty Vehicle Network," SAE International, Standard, June. 2023.

[8] Y. Burakova, B. Hass, L. Millar, and A. Weimerskirch, "Truck Hacking: An Experimental Analysis of the SAE J1939 Standard," in *10th USENIX Workshop on Offensive Technologies (WOOT 16)*, 2016.

[9] S. Mukherjee, H. Shirazi, I. Ray, J. Daily, and R. Gamble, "Practical DoS Attacks on Embedded Networks in Commercial Vehicles," in *Information Systems Security*, I. Ray, M. S. Gaur, M. Conti, D. Sanghi, and V. Kamakoti, Eds. Cham: Springer International Publishing, 2016, pp. 23–42.

[10] C. Jichici, B. Groza, R. Ragobete, P.-S. Murvay, and T. Andreica, "Effective Intrusion Detection and Prevention for the Commercial Vehicle SAE J1939 CAN Bus," *IEEE Transactions on Intelligent Transportation Systems*, 2022.

[11] C. Jichici, B. Groza, and P.-S. Murvay, "Integrating Adversary Models and Intrusion Detection Systems for In-vehicle Networks in CANoe," in *International Conference on Information Technology and Communications Security*. Springer, 2020, pp. 241–256.

[12] T. Andreica, C.-D. Curiac, C. Jichici, and B. Groza, "Android Head Units vs. In-Vehicle ECUs: Performance Assessment for Deploying In-Vehicle Intrusion Detection Systems for the CAN Bus," *IEEE Access*, vol. 10, pp. 95 161–95 178, 2022.

[13] L. Popa, B. Groza, C. Jichici, and P.-S. Murvay, "ECUPrint—Physical Fingerprinting Electronic Control Units on CAN Buses Inside Cars and SAE J1939 Compliant Vehicles," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1185–1200, 2022.

[14] C. Jichici, B. Groza, and P.-S. Murvay, "Examining the Use of Neural Networks for Intrusion Detection in Controller Area Networks," in *International Conference on Security for Information Technology and Communications*. Springer, 2019, pp. 109–125.
[15] C. Jichici, A. Berdich, A. Musuroi, and B. Groza, "Control System Level Intrusion Detection on J1939 Heavy-Duty Vehicle Buses," *IEEE Transactions on Industrial Informatics*, pp. 1–13, 2023.
[16] B. Groza, P.-S. Murvay, L. Popa, and C. Jichici, "CAN-SQUARE – Decimeter Level Localization of Electronic Control Units on CAN Buses," in *Computer Security–ESORICS 2021: 26th European Symposium on Research in Computer Security, Darmstadt, Germany, October 4–8, 2021, Proceedings, Part I 26*. Springer, 2021, pp. 668–690.
[17] "ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering," International Organization for Standardization, Standard, 1st edition, Aug 2021.
[18] L. Popa, C. Jichici, T. Andreica, P.-S. Murvay, and B. Groza, "Impact of Wiring Characteristics on Voltage-based Fingerprinting in Controller Area Networks," in *2023 IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI)*. IEEE, 2023, pp. 000 231–000 236.
[19] B. Groza, A. Berdich, C. Jichici, and R. Mayrhofer, "Secure Accelerometer-Based Pairing of Mobile Devices in Multi-Modal Transport," *IEEE Access*, vol. 8, pp. 9246–9259, 2020.
[20] *Specification of Secure Onboard Communication*, R20-11 ed., AUTOSAR, November 2020, no. 654.