Securitate la nivel fizic folosind caracteristici de timp și tensiune pentru magistrala Controller Area Networks

Teză de doctorat – Rezumat

pentru obținerea titlului științific de doctor la
Universitatea Politehnica Timișoara
în domeniul de doctorat Calculatoare și Tehnologia Informației

autor ing. Lucian-Tudor Popa
conducător științific Prof.univ.dr.ing. Bogdan-Ioan Groza

Septembrie 2023

Controller Area Networks (CAN) sunt încă cele mai frecvent utilizate magistrale de comunicare a datelor în interiorul vehiculelor. Înainte de a fi introduse în anii 1980, dispozitivele electronice din interiorul vehiculelor comunicau prin conexiuni punct la punct, cu fire separate. În contrast cu această metodă, magistrala CAN permite mai multor noduri să transmită și să primească date folosind doar două fire, contribuind la reducerea costurilor și complexității comunicării dintre mai multe noduri. Un alt avantaj al magistralei CAN este fiabilitatea acesteia în cadrul utilizării în autoturisme datorită proprietăților definite de nivelul fizic al comunicării datelor. Datorită fiabilității și eficienței costurilor, magistrala CAN are și actualizări mai recente precum CAN-FD (din 2012) și CAN-XL (din 2018), ceea ce demonstrează prezența de lungă durată în autoturisme a magistralelor CAN și în viitor.

Magistralele CAN sunt folosite ca mediu de comunicare atât pentru sistemele de siguranță (functional safety în automotive), cât și pentru cele care nu sunt legate de siguranță. Una dintre vulnerabilitățile sale majore este legată de securitatea informațiilor transmise între noduri, deoarece, conform standardelor existente, magistrala CAN nu are astfel de particularități. Având în vedere că autoturismele au evoluat de la utilizarea de componente pur mecanice la o combinație între componente electrice, electronice și electro-mecanice în care sunt executate multiple funcții implementate în module software cu utilizarea a diferite sisteme de operare, riscurile în ceea ce privește securitatea datelor transmise pe CAN au crescut și continuă să crească. Există diverse propuneri privind integrarea mecanismelor de securitate pentru Controller Area Networks, atât din lucrări de cercetare, cât și din industria automotive, care au fost folosite și ca bază pentru studiile prezentate în teză. Securitatea Controller Area Network este principala temă de motivare pentru toate lucrările de cercetare care sunt prezentate în teză începând cu Capitolul I care conține motivația autorului pentru subiectele elaborate în teza de doctorat, obiectivele de cercetare, rezultatele obținute și contribuțiile autorului în partea de cercetare.

Mai multe lucrări de cercetare, cum ar fi [1] și [2], au detaliat multiple vulnerabilități privind magistralele CAN care sunt utilizate pentru comunicație între nodurile din autoturisme. În prima lucrare de cercetare [1], autorii au identificat vulnerabilități din punct de vedere al securității în magistrala CAN, cum ar fi lipsa câmpurilor de identificare/autentificare a sursei. De asemenea, aceștia au efectuat diverse atacuri de tip ”sniffing” al pachetelor de date comunicate, atacuri țintite asupra unui singur transmițător și atacuri de tip ”fuzzing” asupra mai multor unități de control electronic (ECU). Checkoway et. al. [2] au analizat și au evaluat o cale de atac furnizată de senzorii de monitorizare a presiunii în pneuri (TPMS), exploatând unitatea de control electronic Telematics ECU pentru a injecta pachete CAN adverse în magistralele din

autoturism unde acesta este conectat.

Având în vedere amenințările identificate în lucrările de cercetare, specificațiile AUTOSAR din industria automotive au inclus funcționalitatea Secure On-Board Communication (SecOC) [3] ca fiind necesară pentru sistemele de siguranță (functional safety) din autoturisme începând cu Versiunea 4.2.2 publicată în 2014, așa cum este descrisă de autori și în [4]. Motivul pentru care funcționalitatea SecOC este cerută de către industria automotive pentru magistrala CAN este protecția comunicației legitime împotriva atacurilor de tip ”injection” și de tip ”replay”. În ultimul deceniu au fost propuse și alte implementări în software pentru securizarea comunicării CAN, cum ar fi utilizarea autentificării mesajelor [5], [6], [7] sau a realocării identificatorilor în timpul comunicației pe magistrala CAN [8], [9], [10].

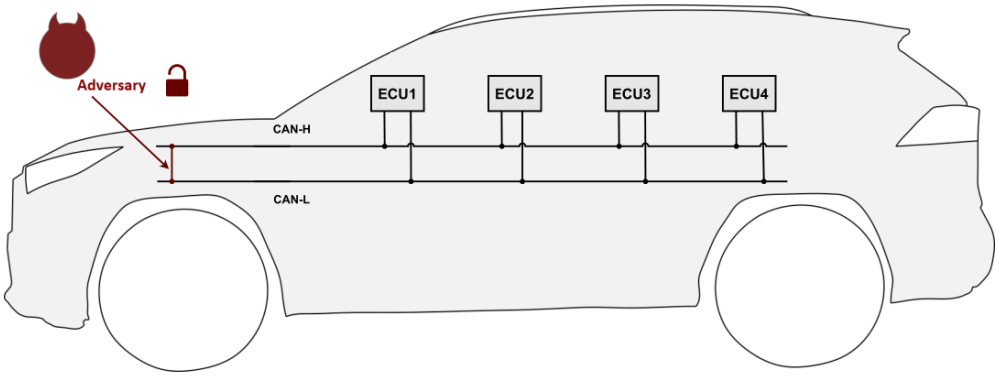

Fig. 1. Atac de tip generic al unui adversar pe magistrala CAN

Un aspect important ce poate fi menționat în prezent este că atacurile pe magistrala CAN au multe implicații negative. De exemplu, în ultimii ani, mai multe vehicule au putut fi furate prin utilizarea de atacuri de tip ”injection” pe magistrala CAN [11]. Acest lucru a fost posibil datorită unei căi de atac care este disponibilă pe magistrala CAN, poziționată aproape de faruri și lângă bara de protecție din față a autovehiculului. Hoții au reușit să deblocheze ușile și să pornească motorul folosind un dispozitiv malițios care poate transmite secvența așteptată de unitățile de control electronic (ECU) a mesajelor pe magistrala CAN. Figura 1 evidențiază un adversar care este conectat la magistrala CAN într-un autoturism și efectuează un atac pe magistrală pentru deblocarea ușilor. Ulterior, posibilitatea de deschidere a ușilor și pornire a motorului prin atacuri pe magistrala CAN a fost raportată ca o vulnerabilitate cunoscută și a fost adăugată la CVE (vulnerabilități și expuneri comune) ca și CVE-2023-29389. Alte probleme recente legate de rețelele de control din autovehicule care au fost, de asemenea, raportate ca vulnerabilități sunt CVE-2017-14937 și CVE-2018-9322. Prima vulnerabilitate este cauzată de accesul previzibil dar nesecurizat la magistrala CAN care afectează unitățile de control electronic (ECU) de tip airbag. A doua vulnerabilitate este raportată pentru unitatea de control electronic de tip infotainment din anumite vehicule BMW care poate fi folosită în mod rău intenționat pentru a injecta mesaje malițioase în magistralele CAN din autoturism.

Obiectivele cercetării. Există mai multe obiective de cercetare prezentate în această teză legate de asigurarea securității rețelelor de comunicație de tip CAN din autovehicule, cum ar fi evaluarea criptografiei cu curbe eliptice pentru CAN, implementarea protocoalelor de schimb de chei ascunse în timp și a protocoalelor de autentificare folosind canale ascunse în timp. Alte obiective de cercetare definite pentru teză sunt reprezentate de amprentarea nodurilor ce transmit pachete CAN folosind caracteristici de timp și de tensiune precum și proiectarea și

evaluarea unei configurații experimentale de tip ”Digital Twin” al unei magistrale CAN dintr-un autoturism. Obiectivele de cercetare ale tezei pot fi rezumate astfel:

1) Revizuirea literaturii de specialitate și a ” state of the art” cu privire la propunerile existente referitoare la asigurarea securității la nivel fizic pentru magistralele de tip CAN, precum și pentru configurațiile experimentale de tip ”Digital Twin” pentru sistemele și magistralele folosite în autoturisme;
2) Evaluarea bibliotecilor software ce oferă posibilitatea schimbului de chei de securitate folosind curbe eliptice pe microcontrolere folosite în sisteme electronice sau electromecanice din autoturisme;
3) Implementarea și evaluarea a patru protocoale de schimb de chei ascunse în timp pentru rețelele de tip CAN, care sunt pe deplin compatibile cu rețelele existente și conforme cu standardele din industria automotive;
4) Implementarea a patru algoritmi de optimizare a timpului când sunt transmise pachetele pe magistrala CAN și evaluarea performanței unui canal de autentificare ascuns în timp în contextul transmiterii optimizate al pachetelor;
5) Colectarea de la patru autoturisme a timpilor de transmisie al pachetelor pentru calculul caracteristicilor de timp al nodurilor transmițătoare și eșantioane de tensiune pentru determinarea caracteristicilor de tensiune în contextul amprentării sistemelor de control electronic sau electro-mecanic din autoturisme (ECU);
6) Evaluarea separării sistemelor de control electronic din nouă autoturisme utilizând caracteristicile de timp (utilizarea întârzierilor determinate între caracteristicile de ceas) și caracteristicile de tensiune (utilizarea a patru informații statistice calculate pe baza eșantioanelor), precum și impactul pe care mediul înconjurător și timpul de funcționare al autoturismelor îl au asupra acestor caracteristici amprentabile;
7) Proiectarea și evaluarea unei configurații experimentale care integrează un ”Digital Twin” pentru funcționalități la nivel de vehicul implementate pe o magistrală de tip CAN folosind cablaje din autoturismul pentru care e realizată configurația experimentală;
8) Evaluarea caracteristicilor de tensiune al magistralei CAN din configurația experimentală implementată pe cablajele din vehicul în comparație cu magistralele CAN din alte configurații experimentale sau din autoturisme în contextul amprentării fizice a nodurilor prin utilizarea caracteristicilor de tensiune.

Contribuții majore. Această teză descrie mai multe implementări de tip software și hardware pentru asigurarea securității rețelelor de tip CAN utilizate în industria automotive. Subiectele care sunt abordate în teză sunt evaluarea bibliotecilor criptografice bazate pe curbe eliptice folosind microcontrolere realizate pentru industria automotive, protocoalele de schimb de chei pentru rețelele de tip CAN, optimizarea transmiterii pachetelor de CAN și autentificarea ascunsă în timp a nodurilor dintr-o rețea CAN, amprentarea sistemelor de control din autoturisme folosind caracteristici de tensiune și de timp ca și caracteristici ale nodurilor conectate la magistrala CAN și realizarea unui design de tipul ”Digital Twin” și evaluarea acestuia în contextul funcționalităților din autoturisme și în contextul amprentării fizice folosind caracteristici de tensiune. Având în vedere obiectivele definite, contribuțiile majore pe care le aduce această teză sunt:

1) Evaluarea temporală a metodelor de securitate utilizând curbele eliptice prin integrarea a trei biblioteci criptografice existente pe un microcontroler utilizat în industria automotive [12];
2) Implementarea și evaluarea protocoalelor de schimb de chei care utilizează pachete CAN pe microcontrolere utilizate în industria automotive [13];
3) Implementarea și evaluarea algoritmilor de optimizare a transmiterii pachetelor pe magistrala CAN și a protocolului de autentificare a canalului ascuns în timp pe

microcontrolere utilizate în industria automotive [14];
4) Colectarea datelor de tensiune și de transmitere al pachetelor de pe magistrala CAN conectată la portul de diagnoză (OBD) din 4 autoturisme [15];
5) Analiza caracteristicilor de tensiune și ale ceasului intern al sistemelor conectate la magistrala CAN din 9 autoturisme [15];
6) Proiectarea și implementarea unui model experimental de tipul ”Digital Twin” pentru o magistrală CAN dintr-un autoturism folosind un cablaj luat de la o mașină [16];
7) Evaluarea caracteristicilor de tensiune ale cablajelor utilizate în diferitele configurații experimentale și cablajele unui autoturism [17].

Aceste contribuții fac parte din lucrări evaluate de recenzori anonimi și publicate în manifestări științifice sau reviste. Evaluarea temporală a primitivelor criptografice implementate prin utilizarea curbelor eliptice pe un microcontroler utilizat în industria automotive a fost realizată în [12]. Trei biblioteci software au fost integrate în codul sursă pentru microcontroler și evaluate în funcție de durata primitivelor criptografice cum ar fi generarea cheilor, semnătura unui mesaj și verificarea semnăturii. Două dintre aceste biblioteci software sunt implementate în limbajul de programare C, în timp ce a treia are atât implementări în C, cât și în C++. Aceste biblioteci software sunt portabile în diferite medii de dezvoltare. Cu toate acestea, timpul necesar pentru metodele ce utilizează curbele eliptice poate fi considerat un neajuns. Pentru a evita acest lucru, patru protocoale pentru schimbul de chei criptografice pe magistrala CAN pe baza caracteristicilor de sincronizare în timp sunt descrise, implementate și evaluate pe un microcontroler utilizat în industria automotive în [13]. Două dintre aceste protocoale se bazează doar pe particularitățile protocolului CAN, și anume, cadre de date/remote și caracteristica de arbitraj al pachetelor, în timp ce celelalte două depind și de componentele hardware interne ale microcontrolerului. O extensie care poate fi aplicată acestor protocoale este prezentată ca o opțiune de îmbunătățire al nivelului de securitate pornind de la o cheie de schimb cu dimensiune și entropie scăzută ca bază pentru generarea unei chei de sesiune cu entropie și dimensiune mai mare. De asemenea, este descrisă pe scurt extensia la un grup de noduri a protocoalelor propuse.

Având în vedere caracteristicile de timp ale pachetelor pentru comunicarea în magistrala CAN și limita câmpului de date al pachetelor sale, o opțiune de implementare a protocoalelor de securitate pe CAN este utilizarea informațiilor de sincronizare referitoare la transmisia și recepția pachetului. Un canal de autentificare ascuns în timp a fost deja descris în [18] și inclus în teza de master a autorului tezei de doctorat. Din păcate, performanța canalului ascuns în timp este redusă de traficul neoptimizat din cauza arbitrajului pachetelor în cazul în care cadrele sunt transmise cu un timp redus între pachete. O îmbunătățire care poate fi luată în considerare pentru canalul ascuns în timp este optimizarea transmiterii pachetelor pe magistrala CAN, lucru prezentat de autorul tezei în [14]. În această lucrare sunt prezentați patru algoritmi de optimizare a transmiterii pachetelor cu detalii legate de valorile optime pentru timpii măsurați între pachete și a valorilor minime și maxime ale acestora. Unul dintre algoritmii de planificare al transmiterii pachetelor este analizat în contextul modelelor de adversar cu trafic optimizat, cât și neoptimizat, cu un singur nod sau cu noduri multiple care implementează protocolul de autentificare. În cadrul lucrării sunt prezentate atât rata de date a canalului de autentificare ascuns în timp cât și nivelul de securitate și impactul algoritmilor de programare transmiterii pachetelor cu mențiunea celor mai nefavorabile momente de recepție al pachetelor cauzate de întârzieri pe magistrala CAN.

Chiar dacă aceste canale ascunse în timp sunt o metodă bună de autentificare a pachetelor transmise pe magistrala CAN, ele transportă cantități mici de entropie iar nivelul lor de securitate este scăzut. Autentificarea transmițătorilor de pachete este posibilă și prin amprentarea fizică, lucru studiat de autorul tezei în [15]. Lucrarea prezintă limitări specifice în ceea ce privește eficiența folosirii caracteristicilor fizice pentru amprentare în cazul utilizării

doar a caracteristicilor de timp sau doar a 1-2 caracteristici de tensiune și efectele schimbărilor de mediu și al utilizării îndelungate al mașinii asupra caracteristicilor fizice colectate inițial. Contribuția majoră a acestei activități de cercetare este numărul de caracteristici fizice colectate și evaluate ca și amprentă a nodurilor transmițătoare, deoarece este realizată pe 9 autoturisme din care sunt identificate 51 de sisteme de control (ECU) folosind un set de date de caracteristici fizice de la ~ 400 de pachete cu identificator de cadru diferit. Valorile determinate ca și caracteristici de timp și caracteristici de tensiune sunt prezentate și într-un material suplimentar în lucrare precum și în teza de doctorat.

Deoarece funcționalitățile la nivel de vehicul sunt de obicei testate pe o configurație experimentală, se recomandă ca setarea să fie cât mai aproape posibil de implementarea reală în mașină. În acest sens, lucrarea de la [16] propune realizarea unui model experimental de tipul ”Digital Twin” pentru unitățile de control electronice (ECU) din industria automotive care comunică pe magistrala CAN. Contribuția acestei lucrări este proiectarea unei configurații experimentale care conține plăci cu microcontrolere utilizate în autoturisme care sunt conectate la o magistrală CAN care face parte din trei cablaje care au fost îndepărtate dintr-un autoturism real. Evaluarea modelelor de tip ”Digital Twin” realizate în lucrare este făcută ca o analiză statistică prin compararea vitezei vehiculului și a turației motorului cu cele colectate de la o mașină reală atunci când este furnizată aceeași intrare pentru ambele sisteme adică starea frânei autoturismului. Ca și posibile aplicații pentru CarTwin [16] sunt sugerate studiile de securitate cibernetică (cybersecurity) și de siguranță funcțională (functional safety). În plus, pe baza rezultatelor din [17], configurația experimentală proiectată pentru CarTwin [16] poate fi utilizată pentru studii de amprentare a nodurilor transmițătoare de pe magistrala CAN folosind caracteristici de tensiune. Asta pentru că, realizând o comparație a configurațiilor experimentale din lucrări anterioare ale grupului de cercetare din care face parte autorul tezei [19], [20] cu condițiile din lumea reală [15], caracteristicile de tensiune ale magistralei CAN din configurația CarTwin [16] sunt foarte apropiate de cele de la magistralele din autoturisme.

Ca un sumar al contribuțiilor, autorul tezei a contribuit la 16 lucrări de cercetare:

1) **L. Popa**, B. Groza, and P.-S. Murvay, "Performance Evaluation of Elliptic Curve Libraries on Automotive-Grade Microcontrollers", in Proceedings of the 14th International Conference on Availability, Reliability and Security, 2019, pp. 1–7,
2) B. Groza, **L. Popa**, and P.-S. Murvay, "TRICKS—Time TRIggered Covert Key Sharing for Controller Area Networks", IEEE Access, vol. 7, pp. 104 294–104 307, 2019,
3) B. Groza, **L. Popa**, and P.-S. Murvay, "CANTO-Covert AutheNtication with Timing channels over Optimized traffic flows for CAN", IEEE Transactions on Information Forensics and Security, vol. 16, pp. 601–616, 2020,
4) **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,
5) **L. Popa**, A. Berdich, and B. Groza, "CarTwin—Development of a Digital Twin for a Real-World In-Vehicle CAN Network", Applied Sciences, vol. 13, no. 1, p. 445, 2022,
6) **L. Popa**, C. Jichici, T. Andreica, P.-S. Murvay, and B. Groza, "Impact of Wiring Characteristics on Voltage-based Fingerprinting in Controller Area Networks", May 2023, accepted for publication at IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI 2023),
7) B. Groza, **L. Popa**, and P.-S. Murvay, "INCANTA-INtrusion detection in

Controller Area Networks with Time-covert Authentication" in Security and Safety Interplay of Intelligent Software Systems: ESORICS 2018 International Workshops, ISSA 2018 and CSITS 2018, Barcelona, Spain, September 6–7, 2018, Revised Selected Papers. Springer, pp. 94–110, 2019,

8) P.-S. Murvay, **L. Popa**, and B. Groza, "Accommodating Time-Triggered Authentication to FlexRay Demands", in Proceedings of the Third Central European Cybersecurity Conference, 2019, pp. 1–6.,
9) B. Groza, **L. Popa**, and P.-S. Murvay, "CarINA-Car sharing with IdeNtity based Access control re-enforced by TPM", in Computer Safety, Reliability, and Security:SAFECOMP 2019 Workshops, ASSURE, DECSoS, SASSUR, STRIVE and WAISE, Turku, Finland, September 10, 2019, Proceedings 38. Springer, pp. 210– 222,
10) B. Groza, H. Gurban, **L. Popa**, A. Berdich, and S. Murvay, "Car-to-Smartphone Interactions: Experimental Setup, Risk Analysis and Security Technologies", in 5th International Workshop on Critical Automotive Applications: Robustness \& Safety, 2019,
11) B. Groza, **L. Popa**, and P.-S. Murvay, "Highly Efficient Authentication for CAN by Identifier Reallocation With Ordered CMACs", IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 6129–6140, 2020,
12) Musuroi, B. Groza, **L. Popa**, and P.-S. Murvay, "Fast and Efficient Group Key Exchange in Controller Area Networks (CAN)", IEEE Transactions on Vehicular Technology, vol. 70, no. 9, pp. 9385–9399, 2021,
13) Groza, **L.Popa**, P.-S. Murvay, Y. Elovici, and A. Shabtai, "CANARY-a reactive defense mechanism for Controller Area Networks based on Active RelaYs.", in USENIX Security Symposium, pp. 4259–4276, 2021,
14) P.-S. Murvay, **L. Popa**, and B. Groza, "Securing the Controller Area Network with covert voltage channels", International Journal of Information Security, vol. 20, no. 6, pp. 817–831, 2021,
15) 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, pp. 668–690,
16) B. Groza, **L. Popa**, T. Andreica, P.-S. Murvay, A. Shabtai, and Y. Elovici, "PanoptiCANs - Adversary-Resilient Architectures for Controller Area Networks", in Computer Security–ESORICS 2022: 27th European Symposium on Research in Computer Security, Copenhagen, Denmark, September 26–30, 2022, Proceedings, Part III. Springer, pp. 658–679.

Teza de doctorat examinează diverse aplicații de securitate și prezintă evaluarea utilizării acestora pentru magistrale de tip CAN. Aplicațiile de securitate utilizează nivelul fizic al magistralei CAN pentru schimb de chei criptografice, autentificarea transmițătorilor de pachete cât și amprentarea acestora. Aceste aplicații sunt, fie comparate cu propunerile existente, punând accent pe îmbunătățirile de performanță, fie analizate în contextul lucrărilor conexe din literatura de specialitate. În cele ce urmează sunt prezentate informații referitoare la celelalte capitole din teză.

Capitolul 2 prezintă fundamentele referitoare la protocolul Controller Area Network cu detalii despre nivelul fizic al magistralei CAN, codificarea biților în funcție de nivelul de

tensiune, tipurile de cadre de date care sunt utilizate precum și câteva informații legate de biții de tip “stuffing”. La începutul capitolului sunt prezentate liniile de transmisie utilizate de sistemele, senzorii și actuatorii din autoturisme pentru a schimba date în timp real precum și nivelurile de tensiune care corespund biților transmiși dar și viteza maximă de transmisie. Un exemplu de biți transmiși pe liniile CAN este prezentat în Figura 2. În acest caz, biții sunt transmiși cu o rată de transmisie de 500 Kbps (timpul unui bit este de 2 μs). Această rată de transmisie de 500 Kbps este utilizată în mod obișnuit în autoturisme. În cele ce urmează, este prezentată structura cadrelor de date standard și extinse transmise pe magistrala CAN referitoare la ordinea biților și stările corespunzătoare pentru arbitraj și control, câmpul de date, suma de control și câmpurile de biți de confirmare (acknowledgment). În același capitol sunt prezentate și cadrele de eroare și stările de eroare definite pentru rețelele CAN. De asemenea, sunt prezentate și tipurile de erori raportate de nodurile care transmit sau recepționează cadrele de date/remote pe magistrala CAN. De exemplu, ca tipuri de erori, sunt definite erori pentru biți, erori pentru suma de control sau erori pentru biții de tip “stuffing”. Cerințele legate de biții de tip “stuffing” precum și alte aspecte privind comunicarea pe magistrala CAN sunt prezentate la sfârșitul celui de-al doilea capitol al tezei.

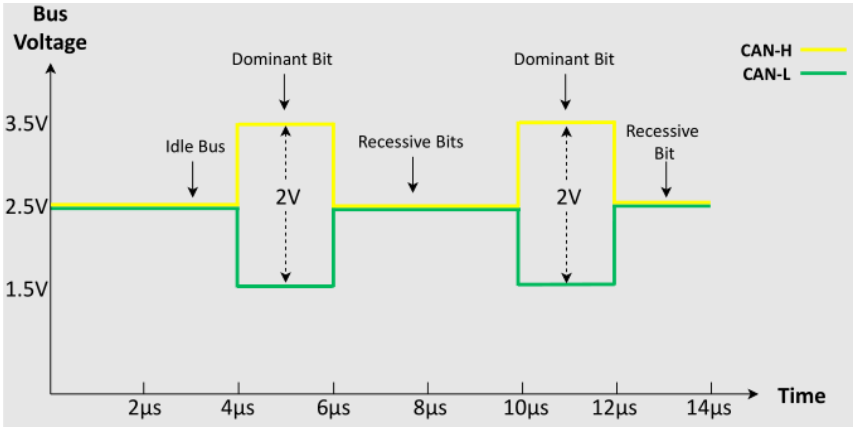

Fig. 2. Tipul biților și nivelul corespunzător de tensiune de pe liniile de date CAN-L și CAN-H ale magistralei CAN în cazul în care timpul unui bit este de 2μs

Capitolul 3 prezintă un mecanism de schimb de chei ascuns în timp pentru rețelele CAN. Capitolul începe cu o prezentare a timpului de calcul necesar în cazul în care este utilizată doar implementarea software a criptografiei cu curbe eliptice pentru schimbul de chei sau semnăturile digitale pe magistrala CAN. Evaluarea timpului de execuție a software-ului pentru schimbul de chei Elliptic Curve Diffie-Hellmann (ECDH) și algoritmii de semnătură digitală Elliptic Curve (ECDSA) este efectuată pe un microcontroler AURIX, utilizat în autoturisme, produs de Infineon. În continuare, în acest capitol sunt prezentate rezultatele experimentale ale implementării a trei biblioteci software de tip ”open-source” în care care sunt implementate primitivele pentru algoritmii de securitate bazați pe curbe eliptice care sunt evaluați. Cu toate acestea, schimbul de chei ECDH necesită transmiterea mai multor cadre CAN până când este realizat schimbul de chei. În cele ce urmează, este descris un protocol de schimb de chei ascuns în timp între două noduri CAN, după ce este prezentat conceptul și studiile din literatura de specialitate care sunt apropiate de concept. Platforma de evaluare utilizată pentru evaluarea protocolului de schimb de chei ascuns în timp este prezentată înainte ca protocolul să fie descris. Protocolul de schimb de chei ascuns în timp poate fi implementat utilizând patru metode diferite de schimb de chei. Prima metodă este negocierea de tipul “Data vs. Remote Frame”, bazată pe

procedura de arbitraj la nivel fizic al magistralei CAN, între pachete de tip date și de tip remote, cu același identificator, transmise de noduri diferite la intervale de timp predefinite. Următoarea metodă propusă pentru schimbul de chei ascuns în timp este Minimax Negotiation. Această metodă este bazată tot pe procedura de arbitraj, dar necesită transmiterea cadrelor de date cu identificatori generați aleator, la intervale de timp fixe, lucru care este prezentat și în Figura 3. Următoarea metodă propusă pentru schimbul de chei ascuns în timp este Time-Triggered Minimax Negotiation. Aceasta se bazează atât pe generarea de valori aleatoare pentru identificatori cât și pe generarea de valori aleatorii pentru intervale de timp din perioade predefinite. Ultima metodă propusă pentru schimbul de chei ascuns în timp este Randomized Time-Triggered Key Exchange. Această metodă se bazează pe un număr predefinit de cadre și de intervale de timp generate aleator în care aceste cadre sunt transmise. În cele ce urmează, metodele propuse pentru schimbul de chei ascuns în timp sunt comparate, comparația fiind raportată la trei caracteristici. Acestea sunt probabilitatea ca un cadru să poată fi utilizat pentru extragerea unui bit din cheia de sesiune, entropia medie și timpul necesar pentru a executa metoda propusă. Deoarece cheia interschimbată de noduri ca rezultat al schimbului de chei ascuns în timp are o entropie mai mică decât cheia utilizată în mod normal în protocoalele criptografice, este propusă și o extensie a ultimelor două metode prezentate prin utilizarea protocolului SPEKE (Simple Password Exponential Key Exchange). Versiunea pentru mai multe noduri (multipartită) a metodelor propuse este descrisă la sfârșitul acestui capitol.

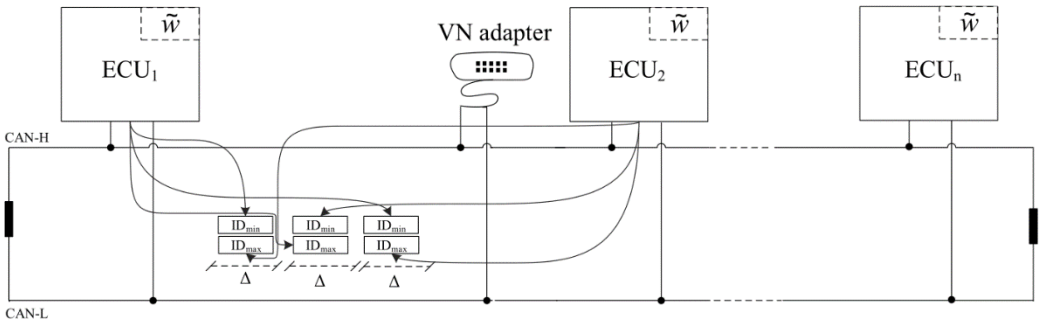

Fig. 3. Structura unei magistrale CAN și una dintre metodele propuse pentru schimbul de chei ascuns în timp

Capitolul 4 prezintă un protocol de autentificare ascuns în timp pentru rețelele CAN, care este îmbunătățit prin optimizarea transmiterii pachetelor. În prima parte a capitolului sunt discutate fundamentele și lucrările din literatura de specialitate cu aceeași temă. De asemenea, sunt prezentate și limitările din lucrările existente dar și îmbunătățirile pe care le aduce propunerea discutată în secțiunile următoare în ceea ce privește optimizarea transmiterii pachetelor. Timpii de recepție, în cel mai defavorabil caz, pentru pachetele transmise pe magistrala CAN sunt discutați ca un fundament teoretic. Valorile determinate teoretic sunt evaluate și practic prin analiza timpilor de recepție al pachetelor de pe o magistrală CAN dintr-un autoturism. Având în vedere întârzierile pe care le poate avea un pachet pe magistrala CAN, de la timpul de transmisie la care acesta este așteptat de nodurile care îl recepționează, până la momentul în care este efectiv trimis și recepționat de celelalte noduri, este propusă optimizarea programării cadrelor pentru depășirea acestor limitări. Configurația utilizată pentru optimizarea programării cadrelor, este realizată printr-un set de date care conține toți identificatorii de cadre, periodicitatea acestora și decalajul de timp care este adăugat la periodicitatea mesajelor. Platforma de evaluare a optimizării transmiterii pachetelor este un echipament utilizat în

industria automotive pentru comunicarea pe magistrala CAN și un microcontroler AURIX, utilizat în autoturisme. Aceasta este descrisă înainte de prezentarea algoritmilor de optimizare a traficului de date pe magistrala CAN. Patru algoritmi de optimizare a transmiterii pachetelor în rețeaua CAN sunt descriși în cele ce urmează. Primul algoritm este cel de alocare simetrică binară (Binary Symmetic Allocation), care este simplu de utilizat și integrat, dar are unele probleme de sincronizare în implementarea practică în comparație cu distribuția teoretică. Cauza acestor probleme de sincronizare este intervalul de timp mic între pachete consecutive. Al doilea algoritm prezentat este cel de alocare aleatorie a căutării (Randomized Search Allocation) care, deși are un spațiu inter-cadre crescut în comparație cu primul algoritm, are probleme de sincronizare în implementarea practică, din aceleași cauze. Următorul este algoritmul Greedy Allocation care este descris atât în varianta cu un singur strat, cât și în variantă multistrat. Varianta Multi-Layer Greedy permite un spațiu inter-cadre de două ori mai mare decât cel din Alocarea Greedy cu un singur strat sau alocarea de căutare aleatorie (Randomized Search Allocation). Rezultatele experimentale pentru implementarea Multi-Layer Greedy sunt conforme cu cele din distribuția teoretică. Ultimul algoritm prezentat este alocarea bazată pe cel mai mare divizor comun (GCD-based Allocation), care permite același spațiu inter-cadre ca și alocarea Greedy Allocation multi-strat (Multi-Layer Greedy). Astfel, implementarea sa practică este conformă cu distribuția teoretică, fără a exista abateri între cele două. Fiecare algoritm este evaluat pe baza minimizării unui factor de calitate care depinde de optimizarea timpului dintre cadre și de valoarea minimă obținută a timpului dintre cadre, pe magistrala CAN.

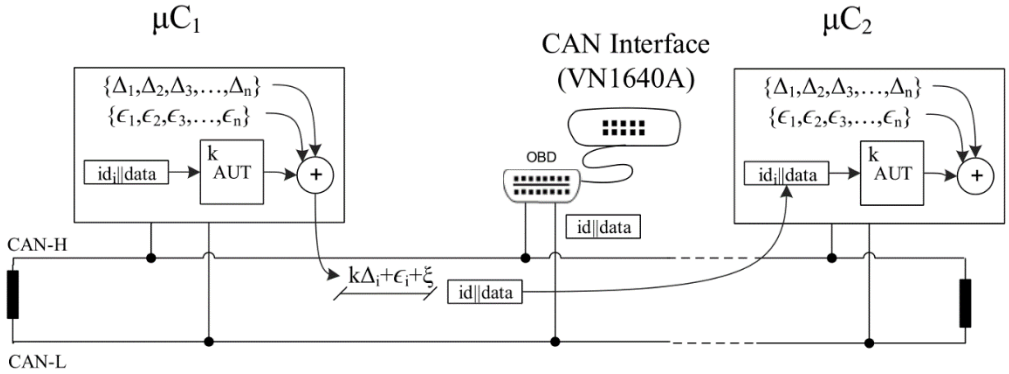

Fig. 4. Structura unei magistrale CAN și canalul de autentificare ascuns în timp cu optimizarea transmiterii pachetelor în rețeaua CAN pentru doi transmițători

După descrierea algoritmilor de optimizare a programării cadrelor, protocolul de autentificare ascuns în timp dintr-o lucrare anterioară a autorului tezei [18] este prezentat împreună cu un model de adversar care este considerat pentru evaluarea performanței protocolului de autentificare. Evaluarea protocolului de autentificare ascuns în timp este făcută în diverse scenarii. Primul scenariu este bazat pe trafic optimizat și un singur transmițător de cadre pe magistrala CAN. Următorul scenariu este bazat atât pe traficul optimizat, cât și pe cel neoptimizat, cu mai mulți transmițători. Scenariul cu trafic optimizat și doi transmițători este prezentat în Figura 4. În cazul mai multor transmițători, sunt propuse acțiuni suplimentare pentru îmbunătățirea performanței canalului de autentificare ascuns în timp. Acestea sunt resincronizarea timpului intern al transmițătorilor și ajustarea ceasurilor care calculează timpul intern. Rata de date a canalului de autentificare și nivelul de securitate al protocolului de autentificare sub acoperire în timp sunt descrise la sfârșitul celei de-a doua secțiuni a acestui

capitol. În secțiunea finală a capitolului, performanța canalului de autentificare ascuns în timp cu optimizarea transmiterii pachetelor este comparată cu alte canale de autentificare ascunse în timp, din alte lucrări publicate în literatura de specialitate.

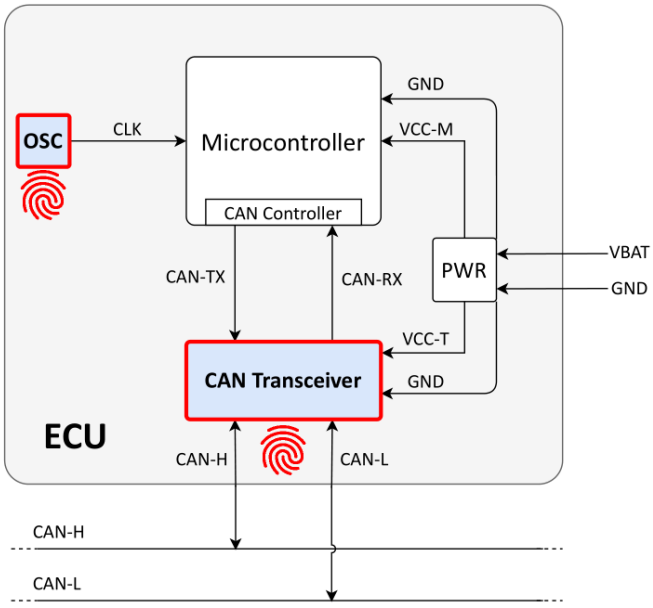

Fig. 5. Diagramă bloc a unei unități de control electronic (ECU) având componentele arhitecturale necesare pentru a comunica pe magistrala CAN ce pot fi utilizate pentru amprentarea fizică

Capitolul 5 prezintă amprentarea fizică a unităților electronice de control (ECU) care comunică în rețelele CAN din interiorul autoturismelor, lucru prezentat și în Figura 5. Prima secțiune a acestui capitol conține detalii legate de lucrările din literatura de specialitate care propun fie amprentarea bazată pe caracteristici de timp sau folosind caracteristici de tensiune pentru nodurile conectate la diferite magistrale CAN. Un sumar al cadrului de colectare al datelor de pe magistrala CAN, datele colectate de autorul tezei din mai multe autoturisme, precum și o comparație între distorsiunile ceasului și caracteristicile de tensiune pentru amprentarea nodurilor transmițătoare sunt, de asemenea, prezentate ca parte a acestei secțiuni. Următoarea secțiune detaliază cadrul teoretic pentru calcularea distorsiunilor de ceas și a caracteristicilor de tensiune care sunt extrase din datele care sunt colectate de la mai multe autoturisme. Există patru caracteristici de tensiune care sunt determinate pentru fiecare transmițător pe baza identificatorului de cadru. Caracteristicile de tensiune care sunt utilizate sunt tensiunea medie și maximă din zona de platou a unui bit dominant, durata unui bit și durata zonei de platou a unui bit dominant. Pentru separarea identificatoarelor de cadrul din același nod transmițător sau din noduri diferite sunt utilizate intra-distanțele și inter-distanțele care sunt definite folosind distanța euclidiană. Secțiunea finală a acestui capitol detaliază valorile obținute pentru fiecare vehicul de pasageri și subliniază limitările în cazul în care este utilizată o singură caracteristică fizică pentru amprentarea transmițătorilor. Separarea pe baza amprentării se face folosind valorile numerice ale caracteristicilor determinate din datele colectate pentru fiecare identificator de cadru. Identificatorii cadrului sunt separați în diferite categorii, cu numele/numărul nodului transmițător, în funcție de caracteristicile de tensiune și de timp obținute. Există 51 de noduri transmițătoare identificate folosind caracteristicile fizice de la 9 autoturisme pe baza datelor colectate pentru aproape 400 de identificatori de cadru. Pentru unele vehicule, cum ar fi Ford Fiesta și Ford Kuga, determinarea caracteristicilor de timp

a fost problematică, deoarece variația timpului de recepție a fost inconsistentă. În setul de date colectat pentru Dacia Logan, există două noduri transmițătoare separate pe baza caracteristicilor de tensiune care au o diferență de caracteriscă de timp de numai 1 ppm (parte per milion). Inter-distanțele și intra-distanțele arată separări între identificatorii de cadru de la același transmițător sau de la transmițători diferiți, dar există mai multe coliziuni în cazul în care este utilizată o singură caracteristică fizică comparativ cu utilizarea mai multor caracteristici fizice. Când toate caracteristicile de tensiune sunt combinate, numărul de coliziuni (asemănări între transmițători) este redus, iar separarea dintre transmițători devine foarte clară. Influența factorilor de mediu (temperatură, timp de funcționare) asupra amprentei fizice este ultimul subiect discutat în acest capitol. Pe baza datelor colectate după pornirea autoturismului și după 1 oră de mers, de la două vehicule diferite, caracteristicile de timp și de tensiune determinate sunt evaluate în raport cu modificările acestora. Întrucât modificările sunt atât pozitive, cât și negative, ceea ce înseamnă că valorile fie au crescut, fie au scăzut după 1 oră, impactul pe care factorii de mediu îl au asupra amprentei fizice nu poate fi generalizat. Acesta este motivul pentru care sunt recomandate actualizări ale amprentelor bazate pe caracteristici fizice pentru a menține valorile colectate cât mai aproape de datele așteptate.

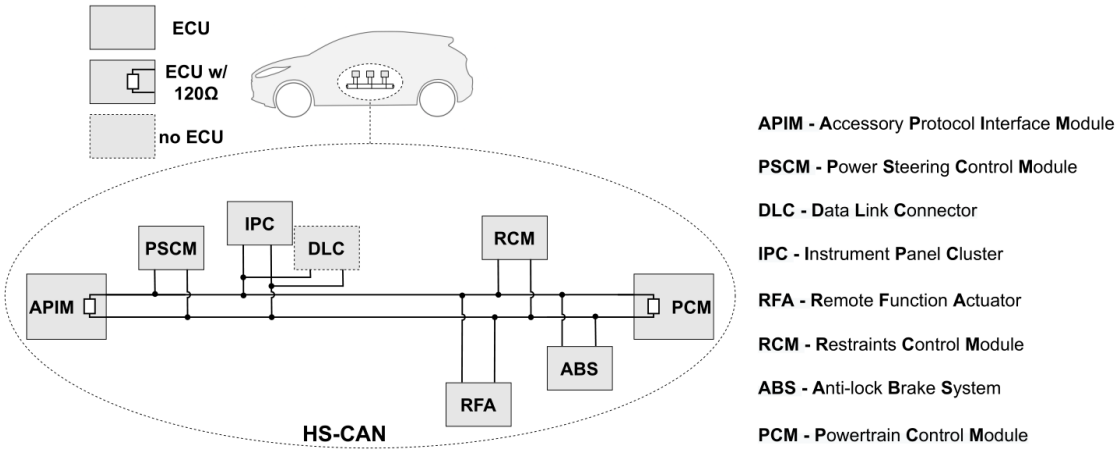

Fig. 6. Prezentare generală a magistralei CAN din autoturism pentru care a fost realizat un model experimental de tipul "Digital Twin"

Capitolul 6 prezintă un model experimental de tipul "Digital Twin" pentru o rețea CAN dintr-un autoturism real. Prima secțiune a acestui capitol începe cu prezentarea motivației pentru proiectarea modelului de tip "Digital Twin" pentru o magistrală CAN precum și a lucrărilor din literatura de specialitate ce adresează acest subiect. Modelul de tip "Digital Twin" se bazează pe modele ale unităților de control electronic (ECU) din autoturism integrate pe plăci ce conțin microcontrolere utilizate în industria automotive care sunt interconectate fizic de o magistrală CAN. Rețeaua CAN este realizată prin firele originale din cablajele care au fost îndepărtate dintr-un autoturism real. Unitățile electronice de control (ECU) de la autoturism și conectarea lor la magistrala CAN din autoturism au fost determinate dintr-o diagramă a manualului de cablare. Cablajul fizic de la autovehicul este descris și în ceea ce privește lungimea firelor și numărul de cabluri secundare legate de cablajul principal. După descrierea implementării fizice din model al magistralei CAN, sunt prezentate și aspectele de proiectare și validare ale modelelor pentru unitățile electronice de control (ECU) care au fost realizate în MATLAB/Simulink. Sistemele modelate și descrise în acest capitol sunt Modulul de Interfață Protocol Accesorii (APIM), Modulul de control al servodirecției (PSCM), Instrumentul de bord

(IPC), Dispozitivul de acționare a funcțiilor de la distanță (RFA), Modulul de control al sistemelor de reținere și airbag (RCM), Sistemul de anti-blocare al frânei (ABS) și Modulul de control al grupului de propulsie (PCM), modele prezentate și în Figura 6. Aceste modele au fost integrate pe microcontrolere utilizate în industria automotive din familia AURIX care sunt produse de Infineon. Dezvoltarea unui program în limbajul de programare C# care furnizează semnale specifice la nivelul vehiculului cerute de unele dintre modele este, de asemenea, descrisă în acest capitol. Integrarea modelelor pe dispozitivele încorporate s-a realizat prin verificarea ieșirilor din magistrala CAN cu cele din MATLAB/Simulink având același set de valori de intrare prevăzute pentru ambele cazuri. Ulterior, viteza vehiculului și turația motorului furnizate de modelele de tip ”Digital Twin” sunt comparate cu viteza vehiculului și turația motorului dintr-un autoturism real. Intrarea care este furnizată modelului CarTwin este starea frânei care automat reduce viteza vehiculului și turația motorului, când este aplicată. Există două condiții de drum care sunt comparate, în care autoturismul real a fost condus, drumurile locale și autostrada. O comparație statistică este realizată prin compararea diferențelor și calculul coeficienților de corelație pentru viteza vehiculului din model și viteza vehiculului din realitate, de pe drum. Aplicațiile posibile pentru modelul de tip ”Digital Twin”, precum și o scurtă comparație cu lucrările din literatura de specialitate sunt prezentate în cele ce urmează. A doua secțiune a capitolului abordează impactul cablajului asupra amprentării folosind caracteristici de tensiune realizate pe rețelele CAN. Mai multe lucrări din literatura de specialitate ce au ca temă același subiect sunt prezentate înainte de descrierea configurației instrumentului de colectare a datelor de tensiune de pe magistrala CAN. Impactul cablajului este evaluat folosind seturi de date din trei modele experimentale cu cabluri diferite și un set de date colectat de la un autoturism real. Caracteristicile care sunt evaluate sunt rata de creștere/scădere a tensiunii (slew rate) pentru un bit dominant, valoarea vârf-la-vârf (peak-to-peak) pe zona platoului de biți și valoarea de la vârf la abaterea medie pătratică (peak-to-RMS) pe aceeași zonă. Având în vedere diferențele dintre cablajele utilizate în modelele experimentale și autoturismele din lumea reală, cablurile ce provin din autoturisme sau care sunt realizate pentru autoturisme sunt cele recomandate pentru a fi utilizate pentru realizarea modelelor experimentale unde intenția este de a colecta eșantioane de tensiune pentru amprentarea nodurilor care comunică pe magistrala CAN. În cazul utilizării altor tipuri de cablare, zgomotul suplimentar indus de cabluri are un impact negativ asupra amprentării.

Pentru a rezuma, această teză prezintă diverse metode de securizare a magistralelor Controller Area Networks care pot fi implementate pe dispozitive utilizare în industria automotive, de la protocoale de autentificare ascunse în timp, care beneficiază de optimizarea programării cadrelor până la amprentarea dispozitivelor fizice folosind caracteristicile de timp și tensiune. De asemenea, este prezentată și o configurație experimentală care este realizată ca un ”Digital Twin” pentru o rețea de control de zonă de vehicule din lumea reală. Impactul cablajului din acest model experimental este evaluat în contextul amprentării bazate pe caracteristici de tensiune, un subiect relevant pentru identificarea transmițătorului și detectarea intruziunilor în rețelele CAN. Există încă multe întrebări deschise cu privire la implementarea securității folosind caracteristici fizice al magistralelor CAN care pot servi ca lucrări sau subiecte viitoare de cercetare. În ceea ce privește canalele de autentificare ascunse în timp, un subiect de cercetare ce rămâne deschis este legat de rata maximă de date care poate fi transmisă și recepționată folosind această metodă de securizare a comunicației. În cazul utilizării caracteristicilor de tensiune sau de timp ca amprente fizice pentru transmițătoarele din rețelele CAN, stabilitatea lor în timp și impactul variațiilor tensiunilor de alimentare sunt posibile direcții de cercetare viitoare pentru această temă. Deoarece modelele de tip ”Digital Twin” sunt un subiect emergent în domeniile auto, acestea pot fi utilizate pentru studii de siguranță raportate la magistrala CAN și securitate cibernetică în contextul automotive. Configurațiile de tip ”Digital Twin” pentru sisteme din autoturisme au nevoie în mod clar de mai multă explorare, deoarece doar câteva lucrări ce au ca temă acest subiect au fost publicate până în prezent.

REFERINȚE

[1] 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 *2010 IEEE Symposium on Security and Privacy*. IEEE, 2010, pp. 447–462.

[2] 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.

[3] *Specification of Secure Onboard Communication*, 4.2.2 edition, AUTOSAR, 2014.

[4] M. Wille, "Automotive security—an overview of standardization in AUTOSAR," *VDI/VW-Gemeinschaftstagung Automotive Security*, 2015.

[5] A. Hazem and H. Fahmy, "LCAP - A Lightweight CAN Authentication Protocol for Securing In-Vehicle Networks," in *10th escar Embedded Security in Cars Conference*, Berlin, Germany, vol. 6, 2012, p. 172.

[6] B. Groza, P.-S. Murvay, A. Van Herrewege, and I. Verbauwhede, "LiBrA-CAN: a Lightweight Broadcast Authentication protocol for Controller Area Networks," in *11th International Conference on Cryptology and Network Security, CANS 2012*, Springer-Verlag, LNCS, 2012.

[7] A.-I. Radu and F. D. Garcia, "LeiA: a lightweight authentication protocol for CAN," in *European Symposium on Research in Computer Security*. Springer, 2016, pp. 283–300.

[8] B. Groza, L. Popa, and P.-S. Murvay, "Highly Efficient Authentication for CAN by Identifier Reallocation with Ordered CMACs," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6129–6140, 2020.

[9] K. Han, A. Weimerskirch, and K. G. Shin, "A practical solution to achieve real-time performance in the automotive network by randomizing frame identifier," *Proc. Eur. Embedded Secur. Cars (ESCAR)*, pp. 13–29, 2015.

[10] A. Humayed and B. Luo, "Using ID-hopping to defend against targeted DoS on CAN," in *Proceedings of the 1st International Workshop on Safe Control of Connected and Autonomous Vehicles*. ACM, 2017, pp. 19–26.

[11] "CAN Injection: keyless car theft," https://kentindell.github.io/2023/04/03/can-injection/, 2023

[12] L. Popa, B. Groza, and P.-S. Murvay, "Performance Evaluation of Elliptic Curve Libraries on Automotive-Grade Microcontrollers," in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, 2019, pp. 1–7.

[13] B. Groza, L. Popa, and P.-S. Murvay, "TRICKS—Time TRIggered Covert Key Sharing for Controller Area Networks," *IEEE Access*, vol. 7, pp. 104294–104307, 2019.

[14] B. Groza, L. Popa, and P.-S. Murvay, "CANTO-Covert AutheNtication with Timing channels over Optimized traffic flows for CAN," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 601–616, 2020.

[15] 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

[16] L. Popa, A. Berdich, and B. Groza, "CarTwin—Development of a digital twin for a real-world in-vehicle CAN network," *Applied Sciences*, vol. 13, no. 1, p. 445, 2022.

[17] L. Popa, C. Jichici, T. Andreica, P.-S. Murvay, and B. Groza, “Impact of Wiring Characteristics on Voltage-based Fingerprinting in Controller Area Networks,” May 2023, *IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI 2023)*.

[18] B. Groza, L. Popa, and P.-S. Murvay, “INCANTA – Intrusion detection in Controller Area Networks with Time-covert Cryptographic Authentication,” in *Security and Safety Interplay of Intelligent Software Systems: ESORICS 2018 International Workshops, ISSA 2018 and CSITS 2018, Barcelona, Spain, September 6–7, 2018, Revised Selected Papers*. Springer, 2019, pp. 94–110.

[19] P.-S. Murvay and B. Groza, “TIDAL-CAN: Differential Timing based Intrusion Detection And Localization for Controller Area Network,” *IEEE Access*, vol. 8, pp. 68895–68912, 2020.

[20] 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.