IOSUD - Universitatea Politehnica Timişoara
Şcoala Doctorală de Studii Inginereşti

Schimb de Cheie și Sincronizare Temporală Securizate pentru Magistrala Controller Area Network

Teză de doctorat – Rezumat

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

Autor: Ing. Adrian-Eugen MUȘUROI
Conducător științific: Prof. Univ. Dr. Ing. Bogdan-Ioan GROZA

Mai 2025

Rețeaua de control de tip magistral Controller Area Network (CAN) a devenit un protocol fundamental în vehiculele moderne definite prin software, datorită costului redus, robusteții și adecvării sale pentru sisteme în timp real. Alături de alte protocoale, precum FlexRay și Ethernet-ul automotive, CAN permite interconectarea unităților electronice de control (Electronic Control Units – ECUs)—dispozitive embedded care gestionează funcțiile automobilului—formând rețele complexe și distribuite în interiorul vehiculului. Prin intermediul acestor rețele, ECUs schimbă date și coordonează operațiuni cu precizie pentru a executa o gamă largă de funcții, bazându-se pe măsurători de la senzori, comenzi ale utilizatorului și algoritmi sofisticați. Astfel, securitatea comunicației CAN este intrinsec legată de siguranța vehiculului, întrucât orice interferență malițioasă poate conduce la comportamente imprevizibile sau incontrolabile care pun în pericol atât pasagerii, cât și ceilalți participanți la trafic. Totuși, în ciuda rolului său critic, protocolul CAN a fost inițial proiectat fără măsuri de securitate încorporate, iar vulnerabilitățile sale au fost demonstrate temeinic de mai bine de un deceniu [1], subliniind necesitatea stringentă de a proteja comunicațiile CAN. Deși au fost propuse diverse soluții și standarde pentru abordarea acestei probleme, prezenta teză se concentrează asupra a două provocări fundamentale încă nerezolvate: (1) proiectarea și implementarea protocoalelor de schimb de chei criptografice în grup, și (2) securitatea mecanismelor de sincronizare temporală—ambele fiind esențiale pentru o comunicare sigură și fiabilă între ECUs conectate prin CAN.

Autentificarea traficului CAN reprezintă o cerință fundamentală de securitate, întrucât absența unor măsuri de protecție lasă sistemul vulnerabil în fața atacurilor de tip replay și spoofing, care pot fi exploatate pentru a obține control neautorizat asupra vehiculului. Numeroase contribuții academice [2–5], împreună cu standardul Secure On-Board Communication (SecOC) dezvoltat în cadrul AUTOSAR [6], susțin utilizarea codurilor de autentificare a mesajelor de tip grup (group Message Authentication Codes – MACs) pentru autentificarea traficului, o abordare justificată de doi factori esențiali. În primul rând, MAC-urile sunt considerabil mai rapide de calculat decât semnăturile digitale, aspect esențial în mediile auto în timp real, unde ECUs sunt supuse unor constrângeri stricte privind capacitatea de procesare și latența. În al doilea rând, MAC-urile au un

impact mult mai redus asupra dimensiunii datelor, ceea ce le face mai potrivite pentru autentificarea mesajelor CAN, care, în majoritatea sistemelor actuale, permit de regulă transport de date limitate la cel mult 64 de octeți[1]. În plus, deoarece CAN utilizează un model de comunicație de tip broadcast, iar mesajele sunt frecvent destinate mai multor receptori, includerea unor MAC-uri individuale pentru fiecare destinatar ar introduce un supracost semnificativ. MAC-urile de grup rezolvă această problemă, permițând autentificarea unui mesaj pentru toți destinatarii vizați printr-un singur MAC, optimizând astfel eficiența comunicației.

Pentru a permite autentificarea prin MAC-uri de grup, este necesară partajarea cheilor simetrice între ECUs implicate, astfel încât toți destinatarii să poată valida același MAC. În mod tradițional, aceste chei sunt injectate în timpul procesului de fabricație al vehiculului sau în cadrul operațiunilor de service, însă această abordare statică prezintă multiple dezavantaje. Deoarece materialul criptografic provine din surse externe, riscul utilizării unor chei slabe sau compromise—ca urmare a erorilor umane sau a defectelor de fabricație—trebuie atenuat printr-o infrastructură robustă, ceea ce conduce la creșterea costului total al sistemului prin necesitatea implementării unor controale avansate de securitate. Mai mult, actualizarea sau înlocuirea cheilor după punerea în funcțiune a vehiculului—de exemplu, în cazurile care implică înlocuirea unui ECU—poate fi imposibilă în afara centrelor de service autorizate. În multe situații, cheile rămân neschimbate pentru perioade îndelungate, ceea ce face imposibilă recuperarea autonomă a vehiculului în urma unor atacuri de extracție a cheilor, cum este cel documentat recent în [7]. Protocoalele de schimb de chei vin în întâmpinarea acestor provocări, permițând ECUs să stabilească autonom și periodic chei secrete partajate, fără a se baza pe date preinstalate. În ciuda potențialului lor, protocoalele de schimb de chei în grup nu sunt încă abordate de standardele actuale, iar deși mai multe studii au evaluat impactul lor computațional și comunicațional în mediile auto, rezultatele sugerează că soluțiile uzuale din alte domenii (precum rețelele enterprise sau cele bazate pe internet) sunt adesea prea costisitoare din punct de vedere al resurselor pentru aplicațiile automotive. Drept urmare, multe lucrări din domeniu continuă să se bazeze pe metode de distribuție a cheilor, mai degrabă decât pe schimburi reale—o abordare care moștenește limitările asociate cu necesitatea pre-partajării secretelor. În consecință, dezvoltarea unor protocoale eficiente de schimb de chei în grup rămâne o direcție deschisă și esențială de cercetare.

Sincronizarea temporală precisă joacă un rol central în susținerea schimbului de chei, a altor protocoale de securitate, precum și a coordonării generale între ECUs. Atunci când ECUs care partajează un magistral CAN sunt sincronizate strâns la o bază de timp comună, acestea pot utiliza marcaje temporale pentru a valida prospețimea mesajelor (așa cum prevede standardul AUTOSAR SecOC) și pentru a alinia cu acuratețe datele senzorilor în aplicații de înaltă precizie, precum fuziunea de senzori (Sensor Fusion). Mai mult, sincronizarea în timp real permite coordonarea eficientă între ECUs aflate pe magistrale diferite și facilitează interacțiunea cu entități externe, cum ar fi alte vehicule sau infrastructura rutieră. Pe lângă aceste beneficii operaționale,

[1] Începând cu 2024, o nouă versiune a standardului CAN — ISO 11898-1:2024 — a introdus CAN XL, care suportă transport de date de până la 2048 de octeți și rate de transfer de date de până la 20 Mbit/s. Totuși, adoptarea CAN XL rămâne limitată, întrucât necesită actualizări semnificative atât ale componentelor hardware, cât și ale software-ului de-a lungul lanțului de aprovizionare din industria auto.

sincronizarea temporală securizată sprijină activități esențiale de securitate, inclusiv verificarea valabilității certificatelor digitale, generarea de jurnale de telemetrie fiabile și realizarea de analize criminalistice (forensic). Toate aceste aplicații depind de integritatea procesului de sincronizare în sine. Deși literatura de specialitate actuală nu oferă propuneri cuprinzătoare privind securizarea sincronizării temporale între ECUs conectate prin CAN, standardul AUTOSAR Time Synchronization over CAN (CanTSyn) [8] integrează totuși anumite mecanisme de securitate. Cu toate acestea, protocolul nu este imediat implementabil, întrucât cadrul său de securitate se bazează pe componente suplimentare care trebuie proiectate și implementate de actori externi, precum producătorul de echipamente originale (Original Equipment Manufacturer – OEM). În plus, standardul se concentrează exclusiv pe sincronizarea la nivelul magistralei, neglijând amenințările de nivel superior care pot apărea la nivelul integrării sistemului. Aceste limitări subliniază importanța continuării cercetării în acest domeniu.

Având în vedere provocările și limitările menționate anterior în ceea ce privește securitatea rețelei CAN, obiectivele urmărite în cadrul acestei lucrări sunt:

1. Implementarea unor protocoale eficiente de schimb de chei pe CAN-FD, utilizând dispozitive embedded de calitate automotive pentru evaluare;

2. Explorarea unor mecanisme alternative de gestionare a cheilor asimetrice ale ECUs, necesare pentru autentificare în cadrul protocoalelor de schimb de chei;

3. Proiectarea unor scheme de extindere scalabile pentru grupuri, care să faciliteze stabilirea cheilor de grup necesare autentificării traficului CAN—o cerință frecvent subliniată atât în literatura academică, cât și în standardele din industrie;

4. Evaluarea și îmbunătățirea securității protocoalelor de sincronizare temporală pe CAN-FD, asigurându-se că măsurile de protecție suplimentare și costurile aferente nu compromit încărcarea sistemului sau precizia necesară aplicațiilor precum fuziunea de senzori;

5. Investigarea unor strategii de implementare practică a protocoalelor de sincronizare temporală, cum ar fi achiziția marcajelor temporale prin Direct Memory Access (DMA), fără întreruperea CPU-ului;

6. Propunerea unei arhitecturi de sincronizare orientate spre securitate, care să abordeze vulnerabilitățile apărute din compromiterea sau imitarea moderatorilor de timp.

Teza este structurată după cum urmează. Capitolul 1 prezintă introducerea și motivația, în timp ce Capitolul 2 oferă fundamentele teoretice relevante pentru conceptele explorate de-a lungul lucrării. Contribuțiile principale sunt împărțite în două părți. Prima parte, tratată în Capitolele 3 și 4, se concentrează pe mecanismele de schimb de chei în rețele CAN. Capitolul 3 explorează schimburi rapide de chei pereche folosind Four$\mathbb{Q}$ ca curbă eliptică de bază, în timp ce Capitolul 4 introduce scheme de extindere pentru grupuri care permit unui număr arbitrar de ECUs să stabilească o cheie comună de grup. A doua parte, analizată în Capitolele 5 și 6, abordează sincronizarea temporală securizată pentru ECUs conectate prin CAN. Capitolul 5 examinează securitatea sincronizării temporale la nivel de magistrală, în timp ce Capitolul 6 extinde

perspectiva la sincronizarea la nivel de sistem, abordând atacuri de nivel superior în topologii tipice ale rețelelor auto. În final, Capitolul 7 prezintă concluziile tezei. În rezumat, contribuțiile principale ale acestei lucrări, aliniate obiectivelor expuse anterior, sunt:

1. Portarea și evaluarea performanței curbei eliptice Four$\mathbb{Q}$ pe microcontrolere de clasă automotive. Rezultatele experimentale pe dispozitive Aurix arată că operațiile Diffie-Hellman și semnăturile digitale bazate pe curba Four$\mathbb{Q}$ sunt de 4–6 ori mai rapide decât operațiile echivalente utilizând curba NIST P-256 [9];

2. Implementarea și analiza comparativă a două protocoale de schimb de chei autentificate: protocolul Station-to-Station (STS) [10], bazat pe criptografie clasică ECC, și protocolul Identity-Based Key Exchange (IBKE) al lui Cao [11]. Protocoalele sunt evaluate în contextul implementării în vehicule, cu accent pe implicațiile privind gestionarea cheilor [9];

3. Proiectarea și evaluarea a trei scheme de extindere pentru chei de grup, bazate pe algoritmul Diffie-Hellman cu curbe eliptice. Varianta cea mai eficientă, integrată cu Four$\mathbb{Q}$, permite stabilirea unei chei de grup între 32 ECUs în mai puțin de 0,6 secunde pe microcontrolere Aurix din gama de bază [9];

4. Dezvoltarea și evaluarea unor îmbunătățiri de securitate pentru protocolul AUTOSAR CanTSyn [8], adresând vectori de atac precum spoofing, delay, replay și forecasting [12];

5. Implementarea unor algoritmi de corecție a ratei ceasului, complementari corecției de offset în sincronizarea temporală AUTOSAR, obținând o acuratețe constantă sub-microsecundă pe hardware Aurix, într-un mediu de testare realist [12];

6. Dezvoltarea unei metode de achiziție a marcajelor temporale utilizând DMA, eliminând dependența de întreruperile CPU și îmbunătățind astfel reziliența și planificabilitatea sistemului [12];

7. Proiectarea și implementarea unui mecanism bazat pe blockchain pentru raportarea securizată a incidentelor din sistemele de detecție a intruziunilor, folosind contracte inteligente pe platforma Ethereum [13];

8. Crearea unui cadru de sincronizare temporală securizat, cu surse de timp redundante, care permite verificarea și detectarea moderatorilor compromiși sau imitați în topologii ce prezintă puncte unice de eșec [14].

Capitolul 3 abordează principala limitare a protocoalelor de schimb de chei utilizate în domeniul automotive: supraîncărcarea computațională, care poate face ca ECUs să devină temporar nefuncționale, afectând negativ comunicarea securizată. Pentru a atenua această problemă, capitolul adoptă Four$\mathbb{Q}$, o curbă eliptică modernă, demonstrată anterior ca având performanțe superioare în comparație cu opțiuni tradiționale precum NIST P-256 în contexte de calcul de înaltă performanță. Prezenta teză extinde evaluarea acestei curbe la platforme embedded specifice industriei auto, inclusiv arhitectura Aurix de la Infineon, frecvent utilizată în vehiculele de producție. Experimentele arată că Four$\mathbb{Q}$ oferă o accelerare de până la șase ori pentru operații de semnătură digitală și ECDH, comparativ cu NIST P-256. Testele comparative cu alte curbe

eliptice de dimensiuni similare din literatură—efectuate pe aceleași platforme hardware ca în [15]—confirmă în plus avantajul de performanță al curbei Four$\mathbb{Q}$, așa cum este ilustrat în Figurile 1 și 2. Pe baza acestei curbe, sunt implementate două protocoale de schimb de chei autentificate. Primul, protocolul Station-to-Station (STS), utilizează certificate digitale convenționale, delegând toate operațiile criptografice asimetrice către ECUs. Această abordare securizează materialul criptografic local, dar presupune existența unor surse de entropie ridicată. Al doilea protocol utilizează criptografie bazată pe identitate, în care autentificarea este derivată din identificatori textuali, în locul certificatelor. În acest caz, o autoritate de încredere gestionează generarea și distribuirea cheilor, reducând cerințele de pe partea ECU, dar necesitând o infrastructură de securitate dedicată. Rezultatele experimentale arată că ambele protocoale ating performanțe similare, permițând ca deciziile privind implementarea să fie ghidate de infrastructura disponibilă. Este de remarcat faptul că ambele soluții depășesc alternativele cunoscute din literatura de specialitate.

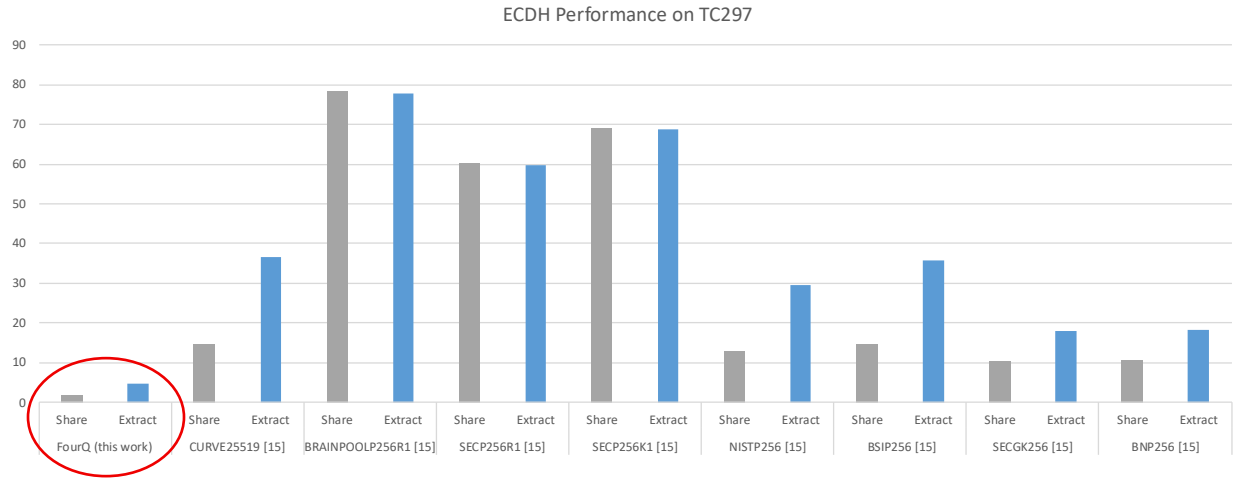

Figura 1: Comparație a performanței între operațiile ECDH bazate pe Four$\mathbb{Q}$ și alte curbe eliptice de dimensiuni similare, evaluate în [15], pe platforma TC297 de la Infineon. Cercul roșu evidențiază avantajul de viteză al Four$\mathbb{Q}$ față de celelalte curbe eliptice.

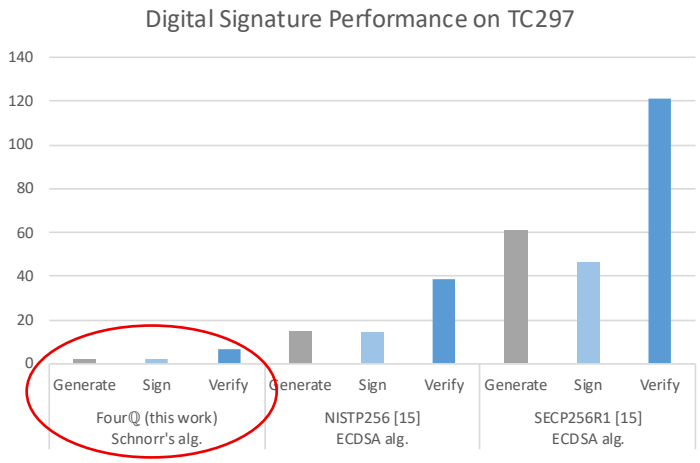

Figure 2: Comparație a performanței între semnătura digitală Schnorr bazată pe Four$\mathbb{Q}$ și ECDSA bazată pe alte curbe eliptice de dimensiuni similare, evaluate în [15], pe platforma TC297 de la Infineon. Cercul roșu evidențiază avantajul de viteză al Four$\mathbb{Q}$ față de celelalte curbe eliptice.

Capitolul 4 continuă pe baza fundamentului stabilit anterior, introducând trei scheme de extindere pentru grupuri în vederea realizării schimburilor orchestrate de chei. Aceste scheme permit mai multor ECUs să ajungă colectiv la un secret partajat, facilitând astfel comunicarea securizată ulterioară. Un ECU Orchestrator de Securitate dedicat (SoECU) supraveghează întregul proces, prevenind inițierile neautorizate care ar putea afecta capacitatea de răspuns a vehiculului. Schema principală, ilustrată în Figura 3, valorifică capacitatea de difuzare (broadcast) a rețelei CAN și introduce conceptul de ECUs logice—entități abstracte compuse din subseturi de ECUs fizice. Schimbul de chei de grup este structurat sub forma unui arbore binar, permițând desfășurarea de operații în paralel la fiecare nivel. De asemenea, sunt stabilite secrete individuale între fiecare ECU și SoECU, pentru o monitorizare îmbunătățită. Cea de-a doua schemă păstrează structura de arbore binar, dar reduce implicarea SoECU, punând accentul pe performanță. A treia utilizează o metodă mai convențională de distribuție a cheilor, dar păstrează canalele secrete cu SoECU.

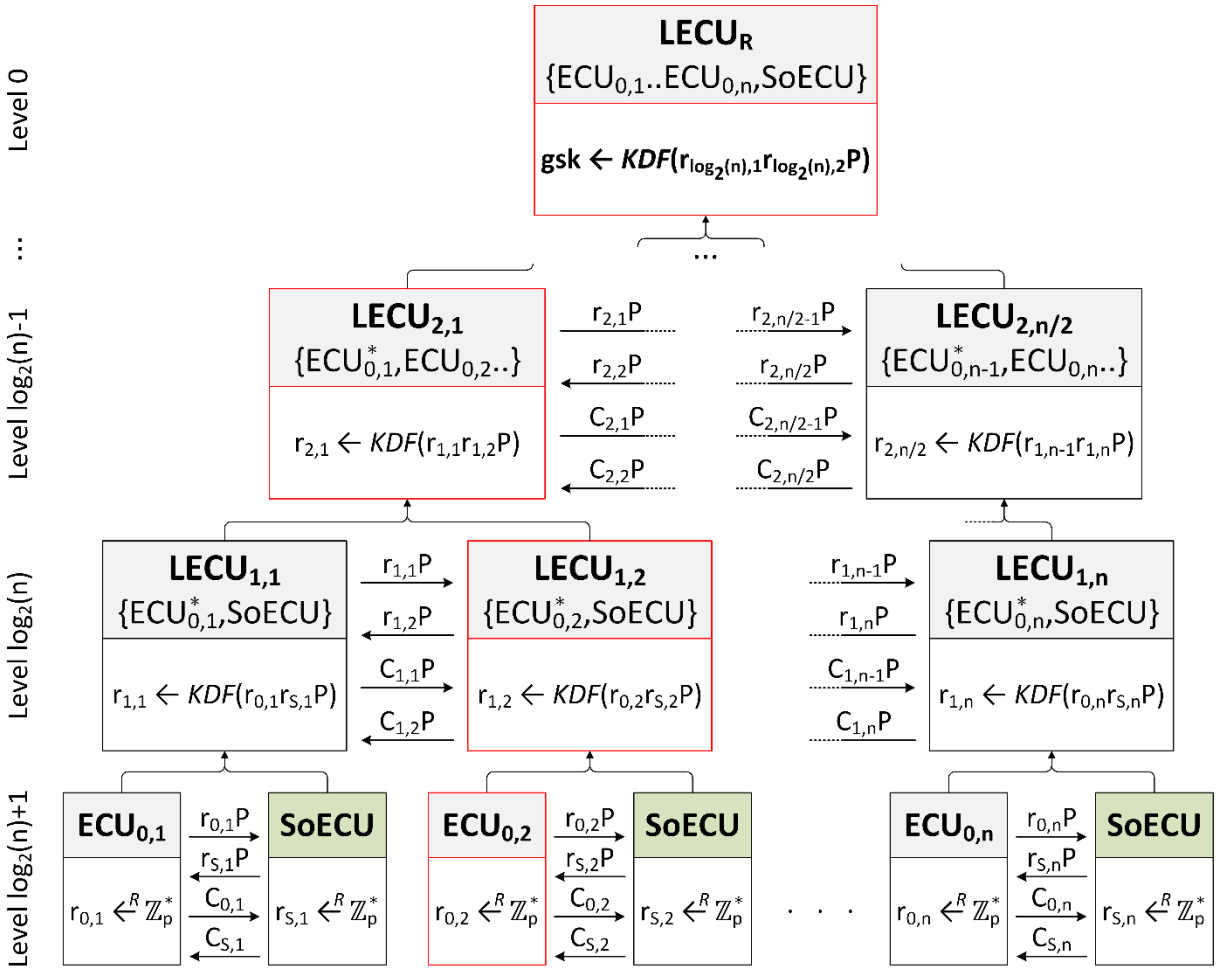

Figure 3: Schimb de chei de grup cu participarea SoECU la formarea fiecărui ECU logic. ECU-urile logice evidențiate cu roșu indică schimburile de chei care trebuie refăcute în cazul compromiterii unui ECU, în acest caz $ECU_{0,2}$.

Toate cele trei scheme sunt evaluate pe baza datelor de timp obținute cu FourQ în Capitolul 3. Rezultatele arată că metoda cea mai rapidă poate conecta în siguranță 32 de ECUs în mai puțin de 0,6 secunde pe microcontrolere din gama de bază, depășind cerințele tipice ale rețelelor CAN. Cea mai sigură variantă obține acordul de grup între 15 ECUs în aproximativ 0,5 secunde, ceea ce o face adecvată pentru scenarii reale. De asemenea, este explorată integrarea cu stack-urile software AUTOSAR, pentru a sprijini implementarea practică.

Capitolul 5 introduce a doua contribuție centrală a acestei teze: sincronizarea temporală securizată. Acesta începe prin analiza protocolului AUTOSAR CAN Time Synchronization [8] în raport cu un model de adversar realist, evidențiind vulnerabilități la atacuri de tip spoofing, replay, întârziere (delay) și anticipare (forecasting). Pentru a contracara aceste amenințări, se propune o versiune întărită a protocolului. Îmbunătățirile cheie includ un mecanism de tip challenge-response pentru validarea prospețimii mesajelor, autentificare multi-MAC pentru a preveni spoofing-ul de către ECUs locale și corecția ratei ceasului pentru o precizie îmbunătățită pe termen lung. Aceste adăugiri vizează amenințări avansate, precum replay dublu și atacuri prin anticipare, menținând în același timp compatibilitatea cu standardul AUTOSAR. Deși adăugarea de mesaje suplimentare ar putea suprasolicita magistrala CAN, evaluările realizate pe baza unor urme reale de trafic provenite de la un vehicul comercial arată că sarcina suplimentară este minimă, chiar și în prezența a 16 subordonate temporale.

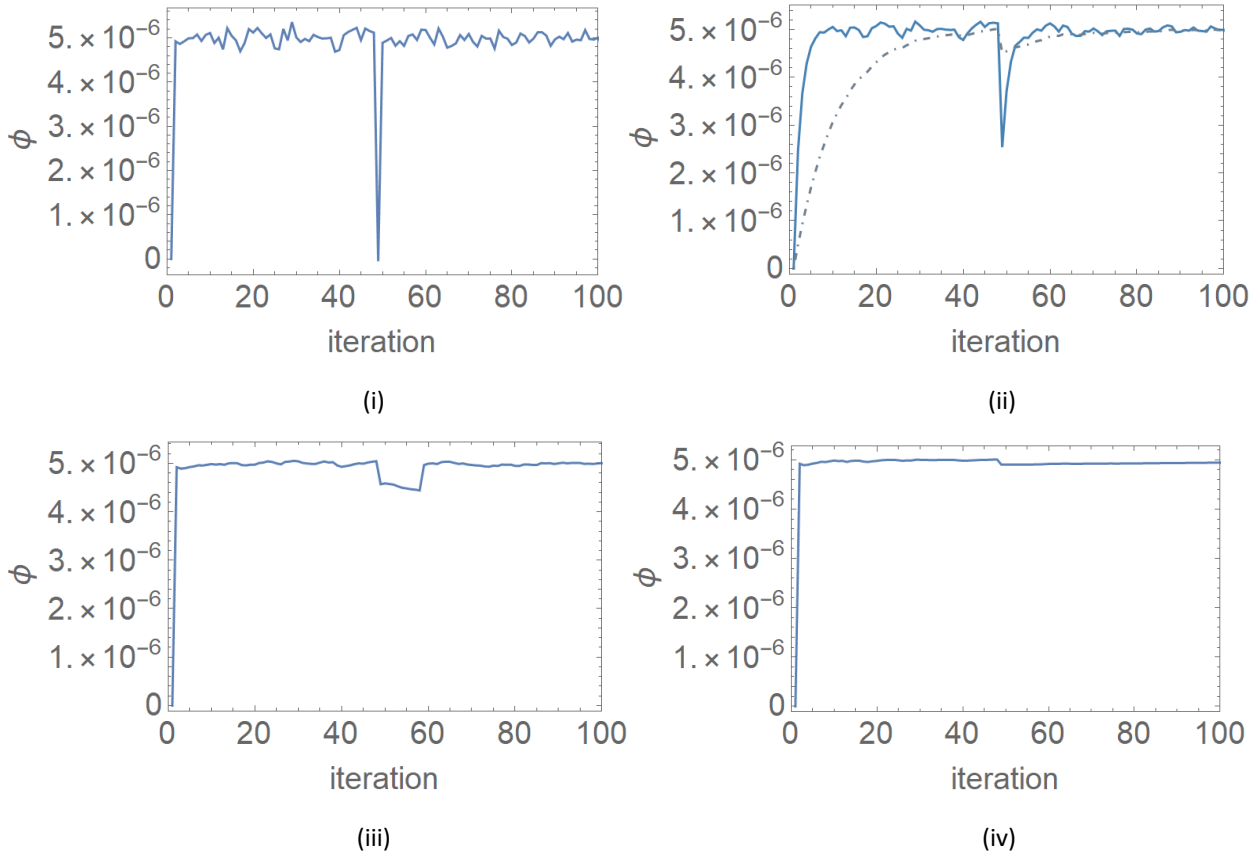

Figure 4: Performanța simulată a algoritmilor de ajustare a frecvenței ceasului: (i) ajustare imediată, (ii) învățare ponderată, (iii) mediere pe fereastră și (iv) mediere continuă, cu zgomot aleator și o anomalie introdusă la a 50-a iterație.

Experimentele arată, de asemenea, că protocolul nemodificat, care se limitează la corectarea offsetului ceasului, poate acumula erori de până la 8 µs la intervale de 1 secundă—valoare care poate fi considerată inacceptabilă pentru unele aplicații sensibile la timp. Versiunea îmbunătățită integrează patru algoritmi de corecție a ratei ceasului, fiecare testat pentru viteza de convergență și robustețe în fața perturbațiilor realiste. Rezultatele unei simulări care prezintă performanțele teoretice ale celor patru algoritmi sunt ilustrate în Figura 4. În timpul testelor, toți algoritmii au menținut erorile de sincronizare sub 1 µs, reprezentând o îmbunătățire semnificativă. Aspectele practice, precum precizia în virgulă mobilă și metodele de ajustare a ceasului, sunt de asemenea abordate. Pentru a elimina dependența de întreruperile CPU în procesul de marcare temporală, se introduce și validează experimental o metodă inovatoare bazată pe DMA, care preia această sarcină de la CPU, îmbunătățind reziliența și planificabilitatea sistemului.

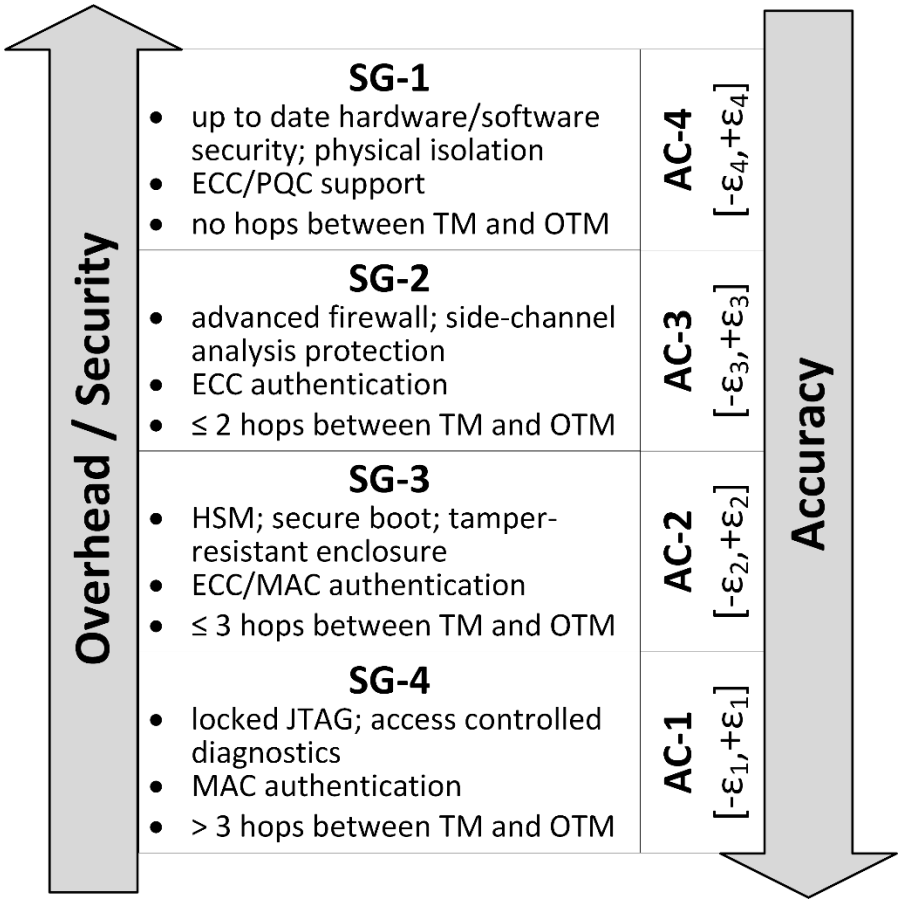

Figure 5: Sistem de evaluare pentru un cadru securizat de sincronizare a timpului, bazat pe costuri de procesare, niveluri de securitate (SG) și clase de acuratețe (AC).

Capitolul 6 extinde problematica sincronizării temporale la nivelul întregului sistem, vizând amenințările provenite de la surse de timp compromise sau imitate, care constituie adesea puncte unice de eșec în rețelele vehiculului. Două scenarii de atac simulate ilustrează riscurile asociate unei sincronizări deficitare: unul implică comenzi de direcție întârziate care pot trece

nedetectate, iar celălalt arată cum un ceas corupt poate induce în eroare un sistem inteligent de intersecție, cu potențialul de a provoca coliziuni. Spre deosebire de arhitecturile tradiționale tolerante la erori, care se concentrează pe fiabilitate, designul propus adoptă o perspectivă orientată pe securitate. Acesta ia în considerare nivele variabile de încredere în sursele de timp, diferențele dintre cerințele de precizie ale ECUs și comportamentele dinamice ale sincronizării. Figura 5 ilustrează relația dintre costul de operare, securitate și acuratețe—factori care sunt utilizați pentru a crea un sistem de evaluare a moderatorilor de timp. Recunoscând faptul că un singur moderator de timp pe magistrala CAN poate fi insuficient, arhitectura propusă permite sincronizarea cu moderatori externi sau de pe alte magistrale prin protocoale independente de magistrală, precum Network Time Protocol (NTP). Pentru a atenua suprasarcina cauzată de comunicarea unu-la-unu specifică NTP, este analizată o strategie de sincronizare colectivă la nivelul întregii magistrale, care reduce costurile de comunicație fără a compromite robustețea sistemului.

Aceste contribuții au fost recenzate și publicate în reviste academice de specialitate. Lista publicațiilor la care autorul a contribuit pe parcursul studiilor doctorale este prezentată mai jos:

1. **A. 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,
2. 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, vol. 20, no. 2, pp. 2029-2041, 2024,
3. T. Andreica, **A. Musuroi**, A. Anistoroaei, C. Jichici, and B. Groza, "*Blockchain integration for in-vehicle CAN bus intrusion detection systems with ISO/SAE 21434 compliant reporting*", Scientific Reports, vol. 14, p. 8169, 2024,
4. **A. Musuroi** and B. Groza, "*Secure Time Synchronization with Submicrosecond Accuracy in Controller Area Networks*", IEEE Transactions on Industrial Informatics, pp. 1-11, 2025.

În concluzie, această teză aduce contribuții semnificative la avansarea securității rețelei CAN, abordând două provocări critice, dar insuficient explorate: schimbul de chei în grup și sincronizarea temporală securizată. Soluțiile propuse îmbunătățesc atât performanța, cât și reziliența, fără a compromite compatibilitatea cu standardele auto consacrate, inclusiv AUTOSAR. Prin evaluări experimentale extinse, desfășurate în condiții realiste și susținute de validare în cadrul procesului de recenzare, această lucrare demonstrează fezabilitatea practică și gradul ridicat de pregătire pentru implementare al abordărilor propuse.

Bibliografie

[1] H. J. Jo and W. Choi, "*A survey of attacks on controller area networks and corresponding countermeasures*", IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 7, pp. 6123-6141, 2022.

[2] Q. Wang and S. Sawhney, "*Vecure: A practical security framework to protect the can bus of vehicles*", Proceedings of the International Conference on the Internet of Things (IOT), pp. 13-18, 2014.

[3] R. Kurachi, Y. Matsubara, H. Takada, N. Adachi, Y. Miyashita, and S. Horihata, "*Cacan-centralized authentication system in CAN (controller area network)*", Proceedings of the 14th International Conference on Embedded Security in Cars (ESCAR 2014), pp. 10, 2014.

[4] G. Bella, P. Biondi, G. Costantino, and I. Matteucci, " *Toucan: A protocol to secure controller area network*", Proceedings of the ACM Workshop on Automotive Cybersecurity, New York, USA, pp. 3-8, 2019.

[5] B. Groza, S. Murvay, A. V. Herrewege, and I. Verbauwhede, "*Libra-can: Lightweight broadcast authentication for controller area networks*", ACM Transactions on Embedded Computing Systems, vol. 16, no. 3, 2017.

[6] AUTOSAR, "*Specification of Secure Onboard Communication Protocol R23-11*", Standard, no. 969, November 2023, accessed: 2025-03-10, available at: https://www.autosar.org/fileadmin/standards/R23-11/CP/AUTOSAR_CP_SRS_CryptoStack.pdf.

[7] W. Melching and G. Hogan, "*My Car, My Keys: Obtaining CAN Bus SecOC Signing Keys*", Presented at Hardwear.io USA, 2024.

[8] AUTOSAR, "Specification of Time Synchronization over CAN R23-11", Standard, no. 674, November 2023, accessed: 2025-03-10, available at: https://www.autosar.org/fileadmin/standards/R23-11/CP/AUTOSAR_SWS_TimeSyncOverCAN.pdf.

[9] A. Musuroi, B. Groza, L. Popa and P.-S. Murvay, "*Fast and efficient group key exchange in controller area networks (CAN)*", IEEE Transactions on Vehicular Technologies, vol. 70, no. 9, pp. 9385-9399, 2021.

[10] W. Diffie, P. C. Van Oorschot, and M. J. Wiener, "*Authentication and authenticated key exchanges*", Designs, Codes and Cryptography, vol. 2, no. 2, pp. 107-125, 1992.

[11] X. Cao, W. Kou, and X. Du, "*A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges*", Information Sciences, vol. 180, no. 15, pp. 2895-2903, 2010.

[12] A. Musuroi and B. Groza, "*Secure time synchronization with submicrosecond accuracy in controller area networks*", IEEE Transactions on Industrial Informatics, pp. 1-11, 2025.

[13] T. Andreica, A. Musuroi, A. Anistoroaei, C. Jichici, and B. Groza, "*Blockchain integration for in-vehicle can bus intrusion detection systems with ISO/SAE 21434 compliant reporting*", Scientific Reports, vol. 14, no. 1, p. 8169, 2024.

[14] A. Musuroi, A. Berdich, and B. Groza, "*A secure automotive architecture for redundant time synchronization*", Submission in progress, 2025.

[15] L. Popa, B. Groza, and P.-S. Murvay, "*Performance evaluation of elliptic curve libraries on automotive-grade microcontrollers*", Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES `19), New York, USA, 2019.