Raport științific final

Proiect de cercetare PN-III-P1-1.1-PD-2016-1198
Creșterea securității și evaluarea vulnerabilităților pentru rețele standardizate utilizate în industrie

Security **E**nhancements and **V**uln**E**rability assessment for industry-standard **N**etworks (**SEVEN**)

Autor

ș.l.dr.ing. Pal-Ștefan MURVAY

Universitatea Politehnica Timișoara

Iunie 2020

Prezentul raport descrie activitatea științifică desfășurată în cadrul proiectului de cercetare *PN-III-P1-1.1-PD-2016-1198, Creșterea securității și evaluarea vulnerabilităților pentru rețele standardizate utilizate în industrie (Security enhancements and vulnerability assessment for industry-standard networks - SEVEN)* aferentă întregii perioade de desfășurare mai 2018 – iunie 2020.

În conformitate cu propunerea de proiect, de-a lungul perioadei de desfășurare a proiectului au fost abordate următoarele obiective științifice:

O1: Evaluarea vulnerabilităților prezente în protocoale de comunicare standardizate utilizate în industrie

O2: Designul unor mecanisme de securitate pentru contacararea vulnerabilităților protocoalelor utilizate în industrie

O3: Designul unor sisteme de detecție a intruziunilor în rețele standardizate utilizate în industrie

O4: Analiza impactului de performanță a mecanismelor de securitate studiate .

Deși constituie un obiectiv separat, analiza de performanță propusă prin obiectivul O4 a fost realizată în strânsă legătură cu dezvoltarea fiecărui mecanism de securitate din cadrul obiectivelor O2 și O3. Rezultatele științifice obținute prin abordarea acestor obiective au fost diseminate prin articole publicate în conferințe și jurnale în domeniu. Astfel, în cadrul proiectului au fost realizate 6 lucrări științifice, dintre care 4 sunt articole prezentate la conferințe și publicate în volumele dedicate acestor evenimente, iar 2 sunt articole acceptate spre publicare (unul fiind deja publicat, iar al doilea aflat în curs de publicare) în reviste ISI cu factor de impact aflate în categoria Q1 a domeniului de referință. Lista completă a lucrărilor realizate în cadrul proiectului este disponibilă pe pagina web dedicată (http://www.aut.upt.ro/~pal-stefan.murvay/projects/SEVEN/publications.html).

În continuare prezentăm sintetic activitățile și rezultatele obținute în cadrul fiecărui obiectiv al proiectului, făcând referire la lucrările științifice asociate fiecărei activități. Detalii tehnice suplimentare se regăsesc în lucrările asociate.

O1: Evaluarea vulnerabilităților prezente în protocoale de comunicare standardizate utilizate în industrie

1. Descrierea obiectivului

În conformitate cu propunerea de proiect, în cadrul acestui obiectiv a fost prevăzută analiza unor protocoale de comunicare folosite în rețele standardizate în industrie cu scopul identificării de noi potențiale vulnerabilități. S-au avut în vedere în principal protocoale de comunicare pentru care problematica securității nu a fost încă abordată sau pentru care studiile existente nu prezentau o analiză cuprinzătoare. Pentru o analiză cuprinzătoare au fost luate în considerare aspecte specifice de la toate nivelele prezentate în specificația protocoalelor.

2. Activități realizate în cadrul obiectivului

A1.1 Analiza vulnerabilitatilor din protocoale pentru retele standardizate in industrie

În conformitate cu planul de realizare a proiectului, această activitate a fost definită pentru îndeplinirea obiectivului O1. Această prima etapă a proiecului a constat în analiza unor protocoale de comunicare industriale standardizate utilizate în diverse sectoare ale industriei. S-a avut în vedere identificarea de vulnerabilități care ar putea să faciliteze realizarea unor atacuri încă necunoscute. Ca subiect al studiului au fost alese două protocoale de comunicare pentru care analizele de securitate erau fie inexistente fie insuficient de amănunțite. Primul dintre acestea, FlexRay, este un protocol e comunicare dezvoltat pentru industria auto și folosit în rețelele interne ale autovehiculelor. Cel de-al doilea, DeviceNet, este utilizat în sisteme industriale de control. În cele ce urmează detaliem rezultatele obținute în urma analizei acestor protocoale.

i. Analiza vunlerabilităților protocolului FlexRay

FlexRay este un protocol de comunicare ce a fost dezvoltat pentru nevoile specifice ale domeniului automotive cu accent pe asigurarea transmiterii la timp a mesajelor necesare funcționării corecte a sistemelor critice pentru siguranță. Utilizarea protocolului FlexRay în aplicații cu un rol important în asigurarea siguranței în exploatarea autovehiculului a constituit un factor determinant în alegerea acestuia pentru analiză. În urma analizei specificației au fost identificate o serie de atacuri care pot afecta funcționarea sistemelor bazate pe comunicare FlexRay. În continuare, înainte de prezentarea atacurilor descriem caracteristici ale protocolului ce fac posibile aceste atacuri.

Protocolul FlexRay implementează un model de comunicare de tip time-triggered, în care transmiterea mesajelor este organizată în cicli de comunicare repetitivi. În cadrul fiecărui ciclu de comunicare FlexRay sunt definite două segmente în care nodurile pot transmite mesaje: segmentul static și segmentul dinamic. Segmentul static este alcătuit din unități elementare, egale ca dimensiune, numite sloturi. Fiecare slot poate fi alocat unui singur nod din rețea pentru transmiterea de mesaje. Segmentul dinamic a fost conceput pentru a permite transmiterea mesajelor cauzate de apariția unor evenimente, mesaje a căror transmise nu trebuie să fie ciclică. Spațiul de transmisie din acest segment se alocă în mod dinamic.

Specificația protocolului FlexRay acoperă nivelul fizic și nivelul data-link. Funcționalitatea de la aceste două nivele este implementată de către un transceiver FlexRay și respectiv controller-ul FlexRay. Transceiverul transformă informația din forma ei digitală în semnale fizice transmise pe cele două linii de comunicare folosite îndeplinind în același timp și funcția inversă de traducere a semnalelor fizice în formă digitală. Controllerul este responsabil de implementarea protocolului de comunicare la nivel logic.

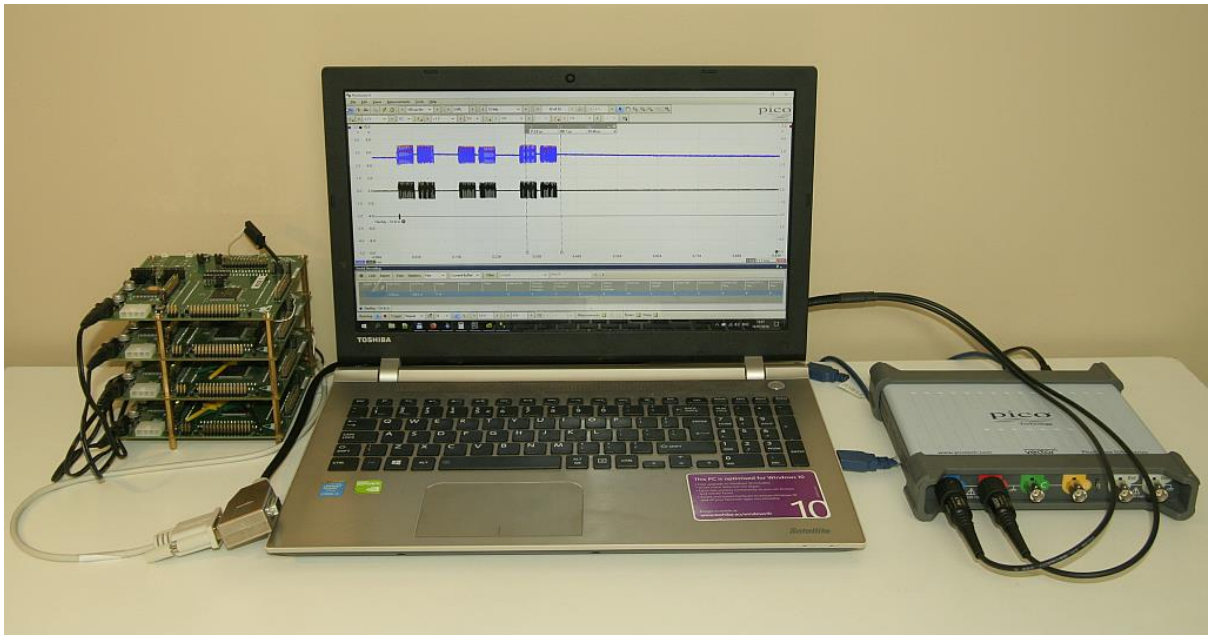

Figura 1. Sistemul experimental utilizat pentru implementarea atacurilor asupra protocolului FlexRay [1]

Din perspectiva securității, specificația protocolului FlexRay nu prevede funcționalități intrinseci pentru a asigura acest aspect al comunicării. Pentru a identifica posibilitățile de atac asupra comunicării folosind protocolul FlexRay, am evaluat atât atacuri care pot fi realizate doar prin intermediul transceiverului cât și atacuri ce utilizează controllerului pentru a genera și transmite mesaje. Ca urmare a analizei, au fost identificate o serie de atacuri de tip DoS (Denial of Service) și spoofing (falsificarea de mesaje) a căror fezabilitate a fost testată pe

sistemul experimental, ilustrat în Figura 1. Acest sistem de test constă într-o rețea FlexRay cu 4 noduri și o componentă folosită pentru analiza traficului. Fiecare din cele patru noduri ale rețelei a fost construi pe baza unei placi de dezvoltare EVB9S12XF512E echipată cu microcontroller S12XF512 și transceivere FlexRay TJA1080A, în timp ce pentru analiza traficului a fost folosit un echipament PicoScope conectat la un PC.

Analizând efectul pe care îl au asupra comunicării, atacurile identificate pot să fie împărțite în 3 categorii:

- **DoS pentru întreaga comunicare** - prevenirea completă a transmiterii de mesaje. Acest tip de atac se bazează pe sistemul FlexRay de detecție a erorilor. Acesta face ca nodurile să inceteze transmisia în cazul în care frame-urile folosite ca referință pentru sincronizare nu sunt recepționate corect pe durata unui număr dat de cicli de comunicare. Atacul poate fi realizat folosind oricare din cele două abordări menționate anterior. Folosind controlul direct al transceiverului se poate genera un nivel dominant constant (corespunzător fie pentru 0 logic fie pentru 1 logic) pe canalul de comunicare. generând coliziuni și făcând imposibilă interpretarea corectă a datelor transmise. Efectul final este pierderea sincronizării și, în cele din urmă, încetarea comunicării. Cea de-a doua variantă de implementare a atacului se folosește de controllerul FlexRay pentru a rezerva toate slot-urile de transmisie și a le ocupa cu frame-uri. Rezultatul, similar primei abordări, este incapacitatea nodurilor legitime de a transmite mesaje fără a cauza coliziuni fapt care duce la pierderea sincronizării și oprirea comunicării. O variantă optimizată a atacului constă în transmiterea mesajelor doar în sloturile rezervate pentru frame-urile folosite în sincronizare. Efectele atacului sunt redate în Figura 2 ce ilustrează cele trei variante ale atacului. Zona marcată cu fundal verde conține un ciclu de comunicare în care atacul nu este prezent. În toate cele trei cazuri atacul începe odată cu zona redată pe fundal roșu ce marchează durata de timp necesară pentru a determina terminarea comunicării. După cum se poate observa, cea de-a treia variantă de atac prezintă cel mai mic impact asupra aspectului unui ciclu normal de comunicare.
- **DoS direcționat** – presupune împiedicarea recepționării corecte doar pentru anumite mesaje, alese de atacator, fără a produce încetarea completă a transmisiunilor în rețea. Pentru realizarea atacului folosind doar transceiverul FlexRay este necesară implementarea la nivelul aplicației a unei rutine pentru identificarea intervalului în care se transmite mesajul țintă în cadrul ciclul de comunicare, pentru generarea adecvată a

coliziunilor. În varianta de atac ce folosește controllerul, atacatorul trebuie doar să ocupe cu un mesaj propriu slotul alocat mesajului țintă. Pentru mesajele transmise în segmentul dinamic nu se poate cunoaște momentul transmisiei. Astfel pentru a împiedica transmisia unor mesaje din acest segment atacatorul trebuie să asigure transmisia continua a mesajului de atac rezultând într-o serie suplimentară de transmisii pe lângă cele care colizionează cu mesajul țintă. Efectele atacului în cele două abordări sunt ilustrate în Figura 3 ce reprezintă pe fundal verde forma unui mesaj normal, iar pe fundal roșu forma mesajului atacat.

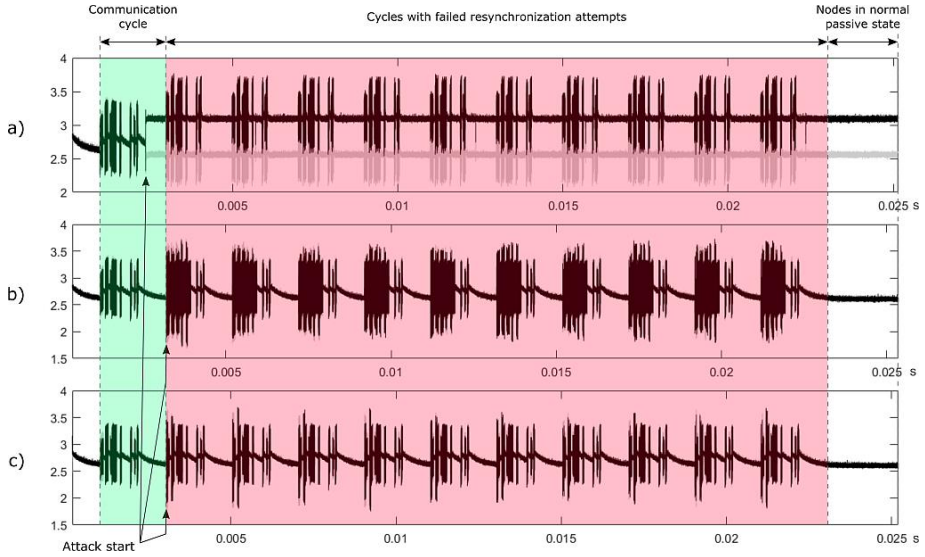

Figura 2. Atacuri de tip DoS pentru întreaga comunicare: a) folosind transceiverul, b)folosind controllerul pentru a ocupa toate sloturile, c) folosind controllerul în varianta optimizată [1]

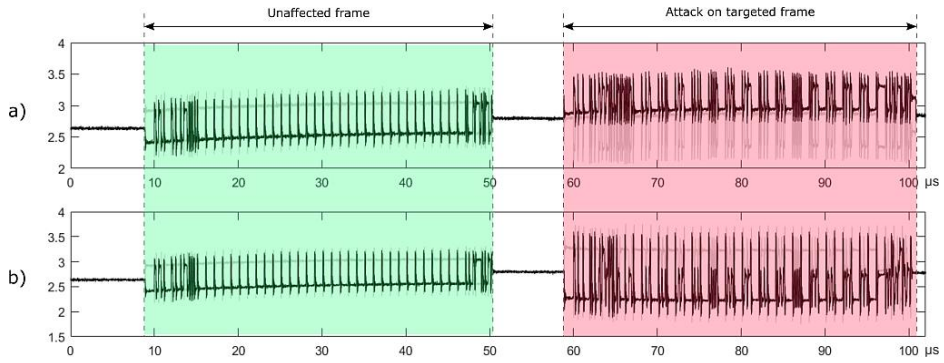

Figura 3. Atacul de tip DoS direcționat: a) folosind transceiverul, b) folosind controllerul [1]

- **Falsificarea mesajelor** – presupune transmiterea de către atacator a unor mesaje menite să pară că sunt transmise de către unul din nodurile legitime ale rețelei. În ceea ce privește mesajele transmise în segmentul static, falsificarea nu este posibilă atâta timp cât nodurile legitime transmițătoare ale acestor mesaje sunt active în rețea. Transmiterea unui mesaj de atac în sloturile statice rezervate ar duce la coliziuni facând

imposibilă transmiterea unui mesaj corect. În ceea ce privește sloturile dinamice, falsificarea de mesaje este posibilă atâta timp cât mesajul legitim nu este transmis. Transmiterea mesajului legitim odată cu cel falsificat va produce coliziuni și imposibilitatea interpretării corecte a mesajului.

ii. *Analiza vulnerabilităților protocolului DeviceNet*

DeviceNet este un protocol de comunicare, membru al familiei de protocoale Common Industrial Protocol (CIP), devoltat pentru a fi folosit în sisteme industriale de control. CIP reprezintă specificația comună a familiei de protocoale ce implementează nivelele superioare ale modelului OSI. Pentru nevelul fizic, data-link și rețea fiecare protocol prezintă o implementare diferită. DeviceNet folosește Controller Area Network (CAN) pentru a implementa nivelul fizic și data-link. Studiul securității protocolului CAN a constituit un subiect intens studiat datorită folosirii sale pe scară largă în domeniul automotive, fiind cunoscut faptul că este vulnerabil la atacuri de tip DoS și spoofing. În studiul DeviceNet ne-am axat pe identificarea vulnerabilităților specifice nivelelor superioare ale protocolului adăugate peste nivelele de bază ale CAN.

În urma analizei protocolului DeviceNet au fost identificate o serie de atacuri care, după tipologie, se încadrează în două categorii: atacuri de tip DoS și spoofing (falsificare). DeviceNet implementează un model de comunicare bazat pe conexiuni. O bună parte din atacurile identificate sunt legate de mecanismele de realizare a conexiunilor. Atacurile identificate sunt următoarele:

- Atacuri DoS:
    - Prevenirea accesului la rețea
    - Prevenirea conexiunilor prin UCMM (Unconnected Message Manager)
    - Închiderea conexiunilor prin UCMM
    - Prevenirea și închiderea conexiunilor prin clasa de conexiune
    - Epuizarea conexiunilor posibile
    - Prevenirea utilizării setului de conexiuni predefinit
    - Perturbarea transmisiunilor fragmentate
- Mesaje falsificate:
    - Modificarea caracteristicilor conexiunii
    - Falsificarea datelor transmise.

Toate aceste atacuri sunt posibile datorită lipsei mecanismelor de securitate atât în ceea ce privește protocolul CAN cât și elementele specifice DeviceNet. Privind din perspectiva nivelelor de baze ale protocolului CAN, toate aceste atacuri sunt realizate prin falsificarea mesajelor standard CAN. Modul de realizare pentru fiecare din aceste atacuri este descris pe larg în lucrarea [2], redactată pe baza rezultatelor obținute în cadrul analizei de securitate.

3. Rezultate asociate obiectivului

Conform planului de realizare propus pentru activitatea asociată acestui obiectiv am preconizat diseminarea rezultatelor sub forma unei lucrări științifice într-o conferință relevantă în domeniu. Rezultatele obținute în cadrul acestui obiectiv sunt prezentate în două lucrări prezentate în cadrul unor conferințe de specialitate în domeniul securității și publicate în volumele dedicate acestora. Articolele publicate sunt:

- Pal-Stefan Murvay, Bogdan Groza, ***Practical security exploits of the FlexRay in-vehicle communication protocol***, The 13th International Conference on Risks and Security of Internet and Systems (CRISIS 2018), pp. 172-187, Springer, 2018
- Pal-Stefan Murvay, Bogdan Groza, ***A brief look at the security of DeviceNet communication in industrial control systems***, Proceedings of the Central European Cybersecurity Conference 2018, pp. 5:1-5:6, ACM, 2018.

O2: Designul unor mecanisme de securitate pentru contacararea vulnerabilităților protocoalelor utilizate în industrie

1. Descrierea obiectivului

Acest obiectiv se referă la designul unor mecanisme de securitate menite să prevină posibile atacuri realizate pornind de la vulenrabilitățile protocoalelor folosite în rețele industriale. Datorită particularităților specifice fiecărui sector industrial și fiecărui protocol de comunicare, în cadrul acestui obiectiv propunem identificarea unui caz specific penru care să se definească mecanisme de securitate menite să asigure obiective de securitate (de ex. managementul cheilor, authentificare sau confidențialitate).

2. Activități realizate în cadrul obiectivului

A2.1 Designul unor mecanisme de securitate menite să contracareze vulenrabilitățile protocoalelor de comunicare utilizate în industrie

Pentru acest obiectiv cercetarea s-a concentrat pe identificarea și implementarea unor mecanisme de securitate pentru protocolul FlexRay. După cum am arătat în cadrul obiectivului

O1, protocolul FlexRay prezintă o serie de vulnerabilități care fac posibilă implementarea de atacuri de tip DoS în principal și falsificarea mesajelor în anumite condiții. Importanța asigurării securității în comunicare pemtru protocolul FlexRay este subliniată de utilizarea acestuia cu precădere în aplicații responsabile de siguranță în exploatarea autovehiculelor.

Primul obiectiv de securitate abordat a fost schimbul de chei pentru a dezvolta un mecanism sigur și eficient care să asigure distribuirea cheilor necesare pentru realizarea altor obiective de securitate precum autenticitatea sau confidențialitatea. Ca o a doua direcție de cercetare privind securitatea în rețele FlexRay am abordat analiza unui mecanism dezvoltat să asigure autenticitate în comunicare. Prezentăm în continuare rezultatele obținute pentru cele două direcții abordate.

i. Schimb de chei eficient pentru rețele FlexRay folosind layerul fizic

Introducerea unui mecanism de securitate, în rețele pentru care securitatea nu a fost luată în considerare la momentul designului inițial, aduce după sine, de cele mai multe ori, încărcarea rețelei cu traficul de date suplimentar necesar implementării noului mecanism. În cadrul acestei activități ne-am propus să dezvoltăm, pentru protocolul FlexRay, un mecanism care să limiteze încărcarea suplimentară a canalului de comunicare. Astfel, soluția pe care o propunem folosește caracteristici specifice nivelului fizic pentru a implementa schimbul de chei într-un segment rar folosit al ciclului de comunicare FlexRay.

Comportamentul nivelului fizic al protocolului FlexRay este definit pe baza a două tipuri de semnale: dominante (“0” și “1” logic) și recesive (ce indică starea Idle). Nivelul fizic FlexRay implementează funcția ȘI-cablat. Astfel, generarea concomitenta, pe canalul comun de comunicare, a unui semnal dominant și a unui semnal recesiv va avea ca rezultat un semnal dominant. Mecanismul pe care îl propunem se bazează pe o soluție similară propusă de Mueller și Lothspeich [3] pentru rețele CAN. Folosind comportamentul de circuit ȘI-cablat al nivelului fizic, procedura prin care două noduri pot stabili un secret comun. Această procedură este exemplificată în Figura 4 și constă în următorii pași: (a) fiecare nod generează o secvență de numere aleatoare; (b) secvența generată se modifică prin adăugarea, după fiecare bit din secvența originală, a unui nou bit reprezentând opusul celui original (în lipsa acestui pas nodurile ce transmit biți dominanți nu pot determina valoarea transmisă de nodul partener); (c) secvențele de biți sunt transmise simultan de cele două noduri implicate în schimbul de chei în același timp cu citirea rezultatului; (d) fiecare nod înlătură acei biți din secvențele inițiale care sunt considerați compromiși în urma transmisiei (datorită celui de-al doilea pas, un adversar

poate identifica cazurile în care ambele noduri transmit aceeași valoare); (e) la finalul procedurii fiecare nod va deține o secvență identică cu inversa secvenței deținute de nodul partener.

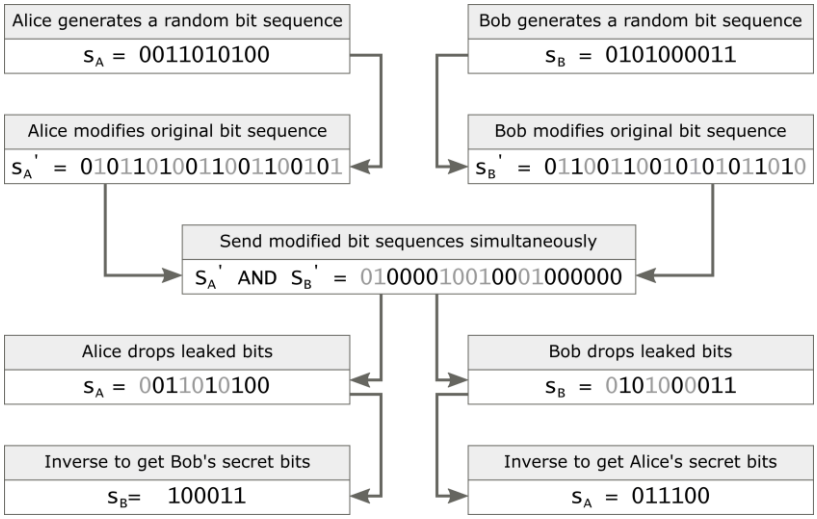

Figura 4. Exemplificarea procedeului de stabilire a unui secret comun pentru secvențe de 10 biți aleatori

Întroducerea mecanismului propus pentru shimbul de chei păstrând în același timp compatibilitatea cu nodurile care nu implementează acest mecanism se poate realiza doar prin evitarea generării de erori care să perturbe transmisiunile implementate conform specificației de bază FlexRay. Pentru aceasta propunem implementarea transmisiunilor necesare schimbului de chei în segmentul *Symbol window* al ciclului de comunicare FlexRay. Acest segment este folosit rar pentru transmisiuni speciale utilizate în inițierea și testarea procesului de comunicare. Ca alternativă la utilizarea acestui segment am investigat și varianta utilizării spațiului nefolosit din cadrul segmentului dinamic al fiecărui ciclu de comunicare. Deși încalcă reguli de transmisiunie impuse prin specificația FlexRay, am demonstrat experimental fezabilitatea acestei alternative fără efecte negative asupra comunicației atâta timp cât nodurile rețelei nu implementează mecanisme suplimentare de management al erorilor la nivelul aplicației. Propunerea noastră pentru formatul transmisiunii secvenței de biți precum și protocolul utilizat pentru inițierea procedurii sunt descrise pe larg în lucrarea redactată pentru această activitate [4], lucrare acceptată spre publicare în revista IEEE Transactions on Vehicular Technology.

Evaluarea experimentală a soluției propuse pentru asigurarea schimbului de chei într-o rețea Flexray a fost realizată pe baza a două configurații experimentale. Prima are la bază o platforma cu microcontroller din familia S12XF ce oferă performanțe de nivel mediu spre slab în timp ce a doua configurație utilizează platforme bazate pe microcontroller TriCore

caracteristice pentru aplicații ce necesită performanțe ridicate. Cele două configurații experimentale, precum și instrumentele utilizate pentru analiza traficului sunt prezentate în Figura 5.

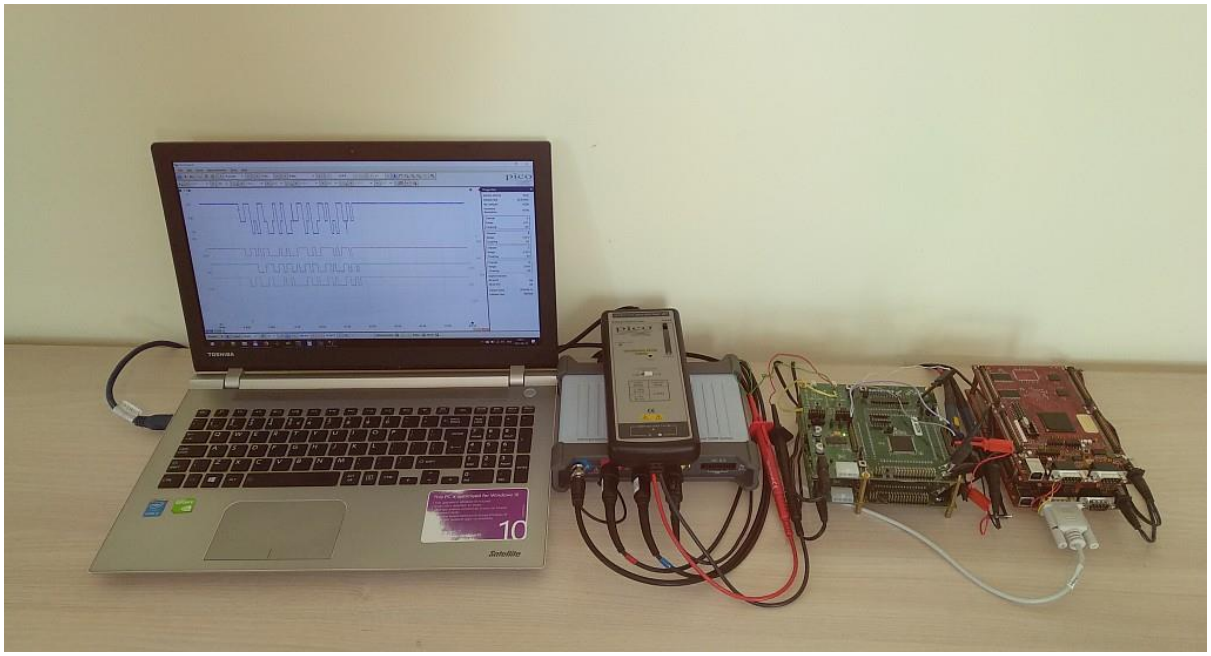

Figura 5. Lanțul experimental utilizat pentru implementarea și testarea metodologiei propuse pentru asigurarea schimbului de chei

Fezabilitatea implementării mecanismului propus a fost testată cu succes pe cele două configurații experimentale. În Figura 6 și Figura 7 sunt ilustrate semnalele generate în timpul schimbului de chei între două noduri S12XF și respectiv TriCore.

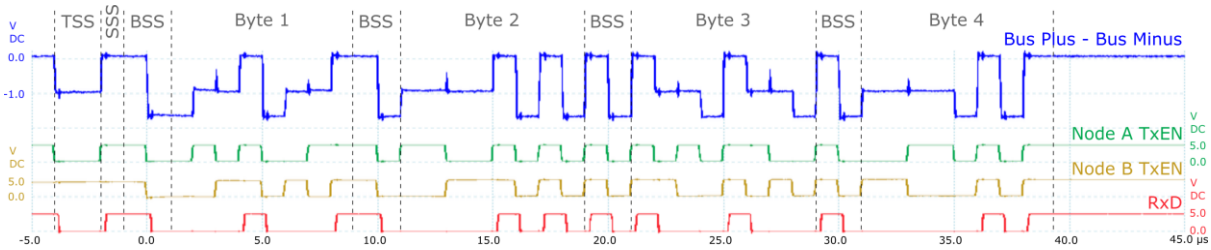

Figura 6. Semnalele generate pe durata schimbului de chei între două noduri S12XF

Rezultatele experimentale privind performanțele obținute de mecanismul propus pentru realizarea schimbului de chei într-o rețea FlexRay corespund obictivului O4 și sunt prezentate în secțiunea dedicată acestui obiectiv.

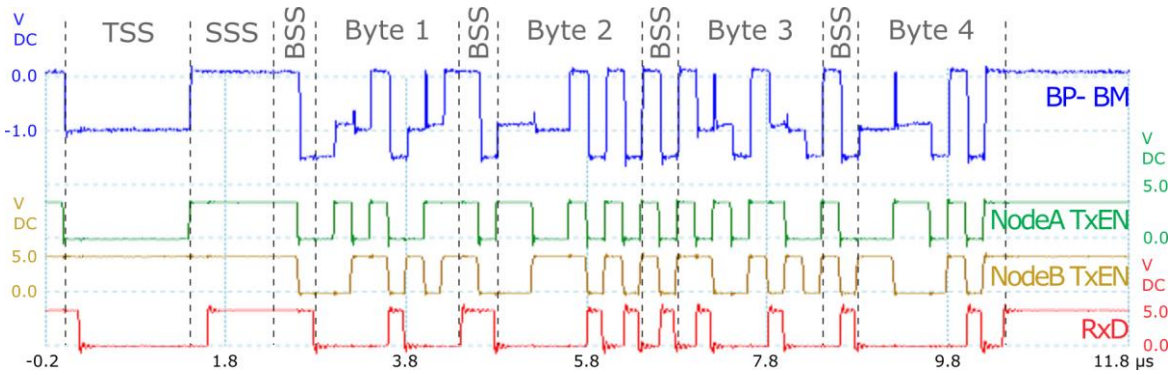

Figura 7. Semnalele generate pe durata schimbului de chei între două noduri TriCore

ii. Autentificare în regim time-triggered pentru rețele FlexRay

Ca o a doua direcție de cercetare, având ca scop asigurarea securității pentru comunicarea în rețele FlexRay, am abordat problema asigurării autenticității. Și în acest caz, principala provocare o constituie limitarea întârzierilor suplimentare introduse în procesul de comunicare datorită noilor mecanisme dezvoltate. Respectarea termenlor limită impuse pentru transmiterea mesajelor este extrem de importantă întrucât FlexRay deservește în principal sisteme critice pentru siguranța vehiculului. În plus, mecanismul de autentificare trebuie să se conformeze modelului de comunicare time-triggered implementat de FlexRay ce presupune transmiterea mesajelor conform unui ciclu de comunicare cu o lungime prestabilită, marea parte a mesajelor transmise fiind mesaje ciclice. Conform exemplelor de aplicații reale analizate, cele mai scurte intervale de repetiție ale mesajelor FlexRay pot să fie de ordinul milisecundelor (de ex. 1, 2,5, 5ms).

Soluția propusă, prezentată pe larg în [5], ia în considerare o serie de elementele în cadrul activității de design a unui protocol de autentificare dedicat rețelelor FlexRay. Aceste aspecte sunt următoarele:

a) **Distribuirea cheilor.** Am propus ca distribuirea cheilor pentru fiecare sesiune de utilizare a vehiculului să se realizeze în perioada în care vehiculul nu este utilizat, pentru a evita încărcarea suplimentară a canalului de comunicare în timpul utilizării normale. Procesul de generare și distribuire a cheilor este realizat de un nod master. Distribuirea sigură cheilor se realizează pe baza unui alt set de chei provenind din lanțuri one-way pre-programate pe fiecare nod în timpul producției vehiculului și partajate cu nodul master.

b) **Utilizare adaptabilă a algoritmilor criptografici.** Am propus alegerea algoritmilor utilizați, pentru fiecare tip de mesaj, în funcție de intervalul de repetiție al acestuia în vederea minimizării timpului necesar procesării algoritmilor criptografici asociați. Astfel, pentru un

anumit interval de repetiție se poate alege un algoritm criptografic ce oferă un nivel suficient de securitate pentru durata dată.

c) **Trunchierea tag-urilor de autentificare.** O abordare uzuală pentru minimizarea încărcării suplimentare a canalului de comunicare în protocoalele de autentificare propuse pentru domeniul automotive o reprezintă trunchierea tag-urilor de autentificare. Conform recomandărilor NIST, am folosit truncherea tagurilor la 32 biți.

d) **Transmiterea tag-urilor de autentificare.** Pentru transmiterea tag-urilor de autentificare am propus două abordări: transmiterea acestora în același frame cu datele autentificate sau transmiterea, într-un frame separat, a tuturor tag-urilor generate de un nod pe durata unui ciclu de comunicare.

e) **Sincronizare temporală.** Protocolul de autentificare propus se bazează pe protocolul TESLA, utilizat în rețele de senzori, a cărui securitate se bazează pe existența sincronizării temporale între nodurile participante la comunicare. Prin designul său, protocolul FlexRay asigură deja această cerință sincronizarea între noduri fiind obligatorie pentru menținerea comunicării într-o rețea FlexRay.

După cum am menționat anterior, protocolul de autentificare propus pentru FlexRay se bazează pe binecunoscutul protocol TESLA. Acesta folosește chei din lanțuri one-way pentru a autentifica mesaje transmise la intervale prestabilite de timp utilizând coduri MAC (coduri de autentificare a mesajelor). Cheile sunt mai apoi făcute publice în următorul segment de timp pentru a se putea verifica autenticitatea mesajelor transmise în segmentul precedent. Dezavantajul acestei abordări este reprezentat de autentificarea întârziată. Din acest motiv am propus o a doua variantă a protocolului în care lanțurile de chei one-way sunt distribuite nodurilor implicate în comunicare înainte de începerea utilizării lor pentru autentificare. Astfel, nodurile receptoare pot verifica autenticitatea mesajul de îndată ce acesta este primit împreună cu tag-ul de autentificare.

Pentru evaluarea experimentală a protocolului propus fost realizat un model experimental simplificat, bazat pe plăci de dezvoltare cu microcontroller S12XF. Parametrii configurați pentru comunicarea FlexRay au fost aleși în conformitate cu exemple reale identificate în literatura de specialitate. Rezultatele experimentale referitoare la performanțele obținute sunt prezentate în secțiunea dedicată obiectivului O4.

3. Rezultate asociate obiectivului

Rezultatele științifice obținute în cadrul acestui obiectiv sunt detaliate în 2 articole dintre care unul a fost acceptat și prezentat în cadrul unei conferințe de specialitate în domeniul securității, iar al doilea a fost acceptat pentru publicare la un jurnal de referință pentru industria producătoare de vehicule (IEEE Transactions on Vehicular Technology – factor de impact 5,339, categoria Q1).

- Pal-Stefan Murvay, Lucian Popa, Bogdan Groza, ***Accommodating Time-Triggered Authentication to FlexRay Demands***, The third Central European Cybersecurity Conference (CECC 2019), pp. 1-6, 2019
- Pal-Stefan Murvay, Bogdan Groza, ***Efficient Physical Layer Key Agreement for FlexRay Networks***, acceptată pentru publicare în IEEE Transactions on Vehicular Technology, 14 pages, 2020.

O3: Designul unor sisteme de detecție a intruziunilor în rețele standardizate utilizate în industrie

1. Descrierea obiectivului

Ca o a doua linie de apărare împotriva atacurilor, acest obiectiv propune designul și implementarea unor sisteme de detecție a intruziunilor pentru rețele standardizate utilizate în industrie. Ca sursă de informație pentru detecția intruziunilor se propune utilizarea datelor provenite de la nivelele inferioare ierarhic ale arhitecturii rețelei. Se vor avea în vedere în particular rețele utilizate în domeniul automotive și utilizarea datelor de la nivelul fizic.

2. Activități realizate în cadrul obiectivului

A2.2 Designul unor sisteme pentru detectia intruziunilor in rețele industriale

În cadrul acestei activități au fost abordate două direcții de cercetare ambele având ca țintă protocolul CAN, protocol utilizat pe scară largă în rețele intra-vehiculare cât și ca nivel de bază pentru protocoale utilizate în sisteme industriale de control (de ex. CANopen și DeviceNet). Prima direcție abordată propune utilizarea informațiilor oferite de nivelul data-link al CAN care sunt disponibile la nivelul aplicației. A doua variantă abordată se bazează doar pe utilizarea informațiilor de la nivelul fizic al protocolului CAN.

i. Detecția intruziunilor bazată pe informații de la nivelul aplicației

În cadrul acestei activități s-a pornit de la dezvoltarea unui sistem care să permită testarea de atacuri și analiza traficului în rețele CAN. Implementarea realizată se bazează pe

CANoe, un mediu folosit în mod curent în industria automotive pentru simularea și testarea rețelelor intra vehiculare. CANoe oferă funcționalități ce facilitează analiza traficului sau generarea de trafic atât în timp real prin conectarea directă la rețeaua internă a vehiculului cât și în mod off-line pentru secvențe de trafic deja înregistrate. CANoe permite de asemenea integrarea de noi funcționalități implementate în alte medii de analiză a datelor precum Matlab facilitând transformarea mediului CANoe într-o unealtă avansată de analiză a traficului având ca scop detecția intruziunilor în rețele automotive. Simularea atacurilor a fost realizată utilizând modelul atacatorului definit în CANoe și traficul de date înregistrat în vehicule reale. Modelul definit acoperă cele mai des raportate tipuri de atac asupra rețelelor CAN: replay și spoofing. Au fost implementate funcționalități care să permită variante avansate ale acestor atacuri beneficiind de mecanisme automate pentru transmiterea cu o periodicitate prestabilită a mesajelor de atac și diferite tipuri de modificări asupra câmpului de date.

Sistemul de detecție a intruziunilor a fost implementat prin integrarea în CANoe a unor funcționalități de analiză a datelor disponibile în Matlab prin intermediul toolbox-ului pentru statistică și machine learning. Rutine de analiză implementate în Matlab pot fi exportate sub formă de fișiere .dll permițând integrarea funcționalităților în alte aplicații precum CANoe. Pentru analiza datelor, în vederea detecției de intruziuni, a fost ales algoritmul k-NN fiind soluția utilizată în general când informațiile despre datele analizate sunt limitate. Cu excepția mesajelor standardizate folosite pentru diagnoză, descrierea conținutului mesajelor prezente în rețelele CAN nu este în mod uzual făcut public de către producători. Astfel, utilizarea k-NN este potrivită pentru clasificarea frame-urilor transmise pe o magistrală CAN, singurele informații disponibile despre acestea la nivelul aplicației fiind conținutul efectiv al frame-ului (identificatorul, lungimea mesajului și câmpul de date) precum și intervalul de repetiție al mesajelor ciclice care poate să fie determinat prin analiza traficului.

Evaluarea mecanismului de detecție a intruziunilor s-a realizat in perspectiva ratei de succes în detecție. Rezultatele experimentale obținute sunt prezentate în articolul asociat acestui subiect [6] și în secțiunea dedicată obiectivului O4.

ii. Detecția intruziunilor bazată pe caracteristici ale nivelului fizic

A doua direcție de cercetare abordată în scopul dezvoltării unui sistem de detecție a intruziunilor pentru rețele CAN s-a axat pe analiza semnalelor fizice generate pe liniile de comunicație. Abordarea pe care o propunem se bazează pe viteza de propagare a unui semnal printr-un conductor electric pentru identificarea transmițătorului. Durata de timp necesară unui

semnal pentru a parcurge un anumit segment de conductor este determinată de lungimea acelui segment de conductor dar și de caracteristicile fizice ale nodurilor conectate de-a lungul segmentului. Așadar, diferența de timp între momentul când un semnal ajunge la un capăt al segmentului de linie monitorizat și momentul când acesta ajunge la celălalt capăt va depinde de poziția de la care a fost transmis semnalul. Numim această valoare timp de propagare diferențial și o folosim pentru caracterizarea poziției nodului transmițător. Mecanismul propus, numit TIDAL-CAN (differential Timing Based Intrusion Detection and Localization for CAN), este nou, el ne mai fiind utilizat în scopul identificării nodurilor într-o rețea cablată. Figura 8 ilustrează influența poziției transmițătorului asupra timpului de propagare a unui semnal înspre capetele unui canal de comunicare CAN cu o lungime de 5m.

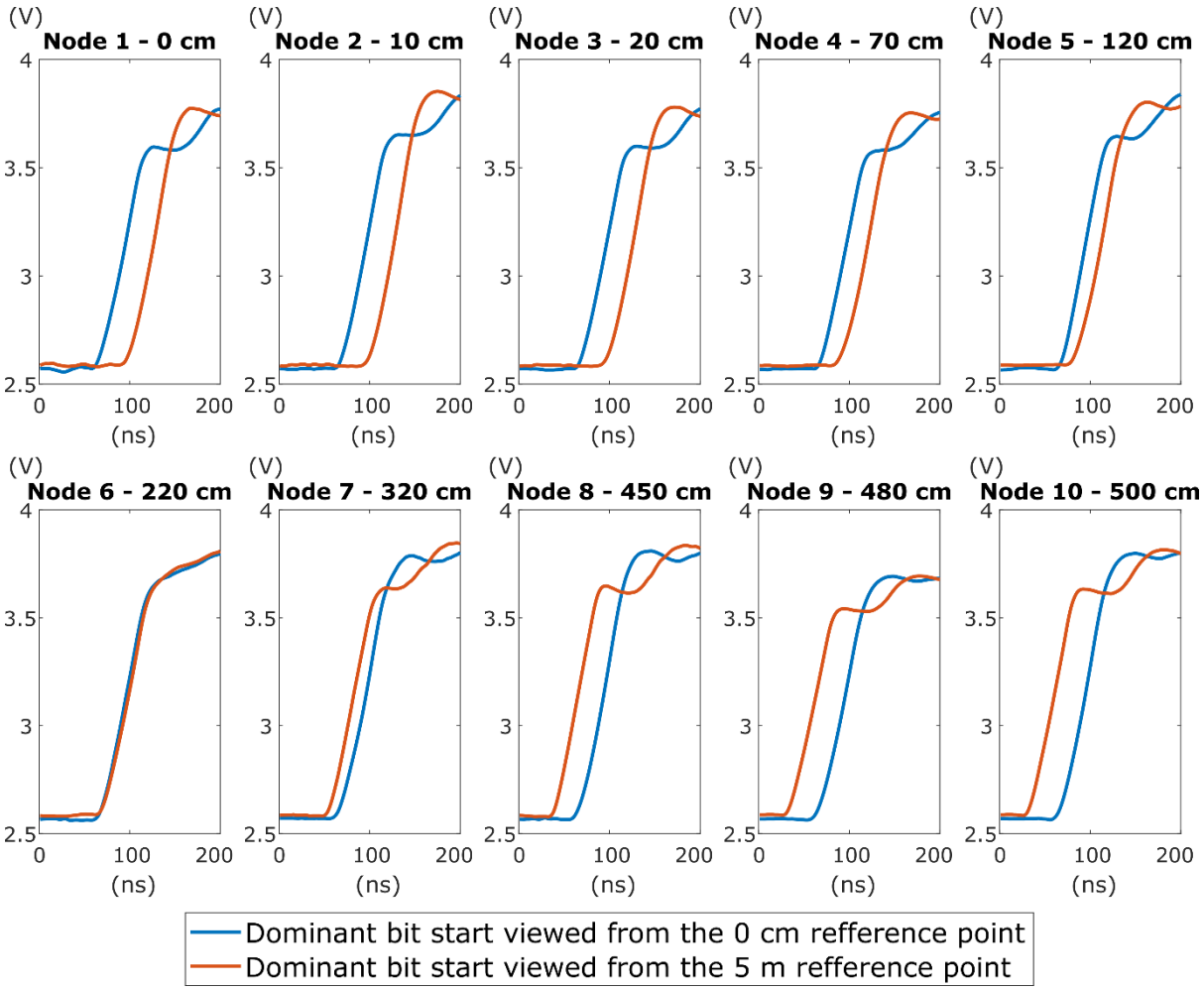

Figura 8. Variația timpului de propagare a unui semnal către capetele unei linii CAN în funcție de poziția transmițătorului

În articolul redactat pentru acest subiect [7], propunem două abordări pentru estimarea timpului de propagare corespunzator fiecărui nod cunoscut din rețea. Prima abordare se bazează pe existența unui model al canalului de comunicare. În acest caz acuratețea estimărilor depinde de calitatea și complexitatea modelului utilizat. Estimările obținute folosind un model

echivalent simplificat al canalului de comunicare sunt apropiate de valori reale măsurate, pentru distanțe de propagare mai mari de 2m după cum ilustrează Figura 9. Aceste rezultate sugerează faptul că îmbunătățirea modelului utlizat poate crește acuratețea estimărilor realizate pe baza acestuia.

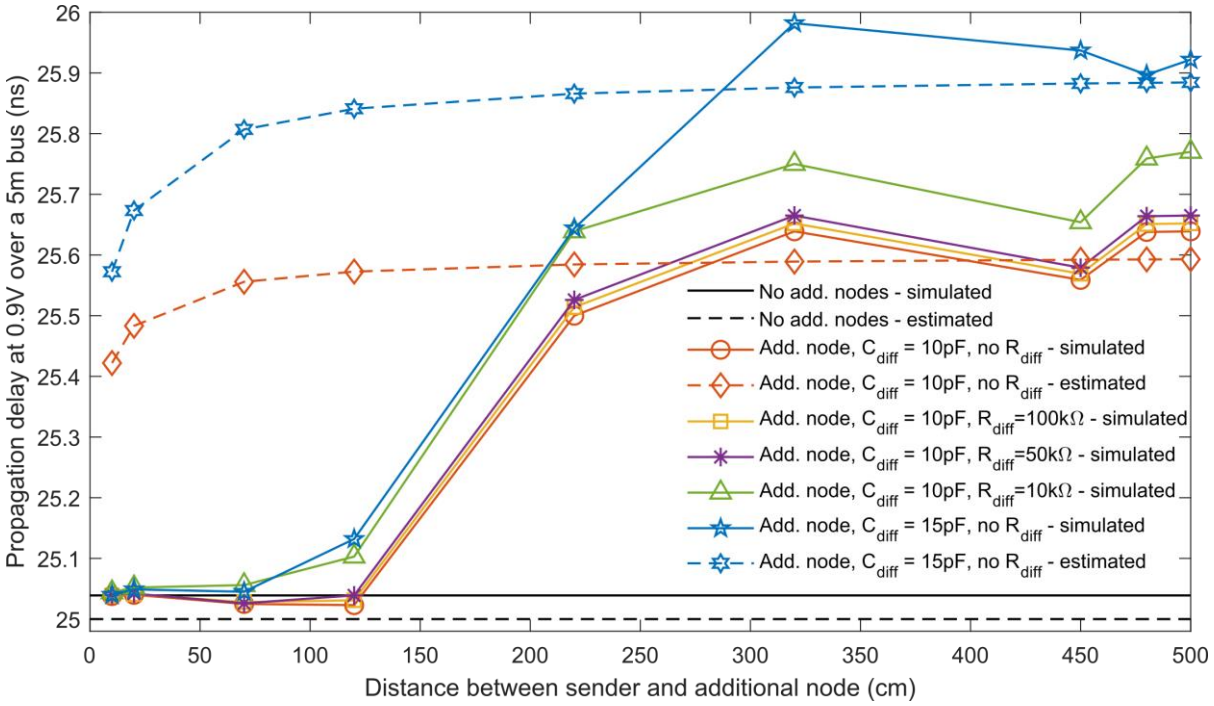

Figura 9.Timpul de propagare estimat pe baza modelului simplificat și timpul de propagare măsurat pentru diferite configurații

Abordarea alternativă pe care am utilizat-o pentru estimarea timpului de propagare diferența se bazează pe amprentarea caracteristicilor nodurilor. Astfel, pentru fiecare nod cunoscut din rețea se realizează o amprentă ce constă în timpul de propagare diferențial caracteristic pe baza unui set de transmisiuni folosit în faza de amprentare. Estimarea timpului de propagare pentru un mesaj dat se face mai apoi pe baza amprentei aferente nodului cunoscut ca transmițător al acelui tip de mesaj.

Caracteristicile fizice care determină întârzieri în propagarea semnalelor CAN sunt direct dependente de localizarea pe bus a nodului transmițător. Acest fapt constituie un avantaj al utilizării acestei abordări, în comparație cu alte propuneri pentru detecția intruziunilor în rețele CAN, întrucât oferă posibilitatea localizării nodului transmițător. Prin corelarea poziției nodului transmițător cu tipul mesajului transmis se poate determina dacă mesajele transmise sunt legitime (au fost transmise de nodul cunoscut ca transmițător legitim). Folosind această corelare se poate mai apoi determina dacă mesajul este transmis de către un nod legitim sau dacă un nod atacator (un nod existent compromis sau un nou nod introdus în rețea) încearcă să

transmită mesaje menite să fie trimise de către alte noduri. Un dezavantaj, comun mecanismelor de detecție a intruziunilor bazate pe caracteristici fizice, este imposibilitatea identificării mesajelor de atac când acestea sunt transmise de pe un nod compromis care este transmițătorul legitim al acestor mesaje.

Evaluarea funcționării principiului propus pentru detecția intruziunilor a fost realizată folosind o rețea de test cu o lungime de 5m, în care punctele de conexiune ale nodurilor au fost instalate la poziții fixe prestabilite față de unul din capetele rețelei. Întregul stand experimental ce include rețeaua cu 10 noduri conectate, sistemul de achiziție și cel de analiză sunt ilustrate în Figura 10. Setul de noduri folosit în evaluarea experimentală include o serie de dispozitive de interfațare USB-CAN precum și transceivere conectate la o placă de dezvoltare. Evaluarea performanțelor acestui mecanism sunt prezentate în capitolul dedicat obiectivului O4.

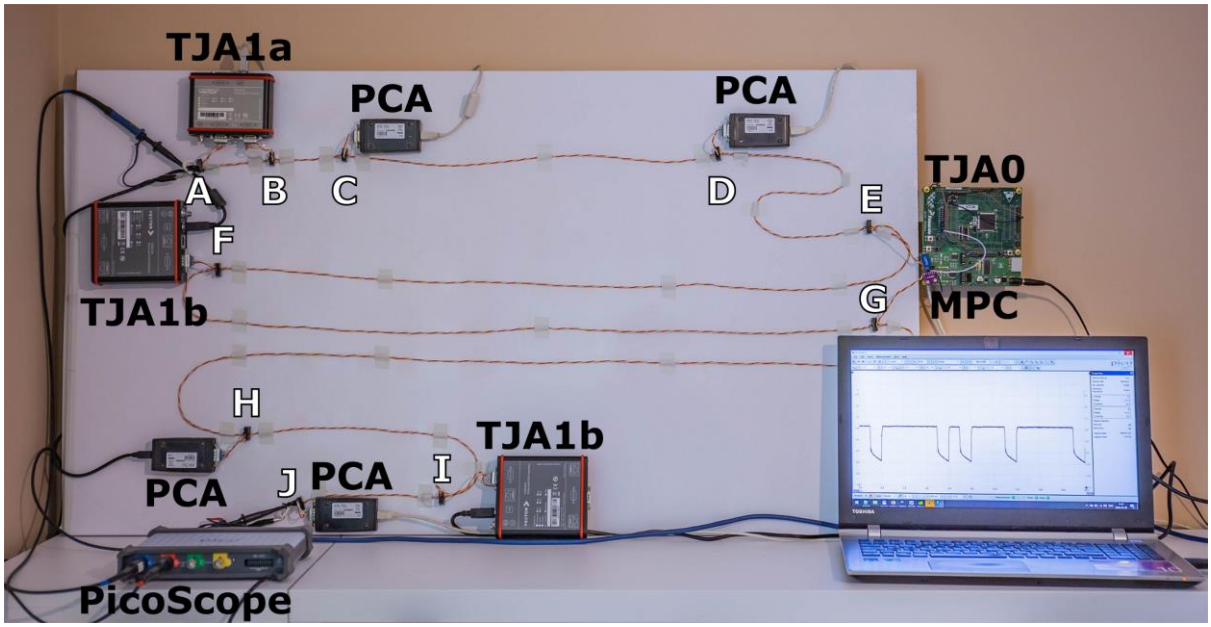

Figura 10. Model experimental pentru evaluarea sistemului de identificare a intruziunilor bazat pe layerul fizic

3. Rezultate asociate obiectivului

Rezultatele științifice obținute în cadrul acestui obiectiv sunt incluse în 2 articole. Unul dintre acestea a fost acceptat și prezentat în cadrul unei conferințe de specialitate în domeniul securității, iar al doilea a fost acceptat și publicat în revista IEEE Access aflată în categoria Q1 și având factorul de impact 3,745.

- Camil Jichici, Bogdan Groza, Pal-Stefan Murvay, ***Integrating Adversary Models and Intrusion Detection Systems for In-Vehicle Networks in CANoe***, The 12th

International Conference on Security for Information Technology and Communications (SECITC 2019), pp. 241-256, 2019.

- Pal-Stefan Murvay, Bogdan Groza, ***TIDAL-CAN: differential Timing based Intrusion Detection And Localization for Controller Area Network***, IEEE Access, Volume 8, pp. 68895 – 68912, 2020

O4: Analiza impactului de performanță a mecanismelor de securitate studiate

1. Descrierea obiectivului

Introducerea unor mecanisme de securitate aduce după sine modificări în performanța sistemului pe care acestea îl deservesc. Efectele asupra performanței provin din întârzieri cauzate de introducerea unor costuri computaționale și de comunicare suplimentare. Acest obiectiv este complementar obiectivelor O2 și O3 și urmărește analiza performanței pentru fiecare din mecanismele de securitate dezvoltate în cadrul acestor obiective. În analiza de performanță se vor urmări aspecte precum costul computațional, consumul de memorie și impactul asupra comunicației luând în considerare eventuale compromisuri între performanță și nivelul de securitate.

2. Activități realizate în cadrul obiectivului

A3.1 Analiza impactului de performanta pentru mecanismele de securitate investigate

În cadrul acestei activități a fost realizată analiza de performanță pentru toate mecanismele de securitate propuse în activitățile de design din cadrul proiectului. Prezentăm în continuare rezultatele obținute în această analiză pentru cele 4 mecanisme propuse.

i. Schimb de chei eficient pentru rețele FlexRay folosind layerul fizic

În cadrul analizei de performanță realizate pentru mecanismul dedicat schimbului de chei [4] au fost testate într-o primă fază ratele de transmisie ce pot fi atinse pe fiecare din cele două configurații implementate pentru schimbul de chei cât și compatibilitatea transmisiunilor speciale introduse cu noduri care nu implementează mecanismul de schimb de chei. Folosind configurația experimentală bazată pe platforma S12XF rata maximă de transfer atinsă a fost de 1 Mbit/s, limitarea fiind dată în acest caz de performanțele limitate ale microcontroller-ului. În cazul configurației ce folosește noduri cu microcontroller TriCore performanța platformei nu constituie o limitare pentru viteza maximă de generare a semnalelor. Cu toate acestea, rata maximă de transfer posibilă în segmentul Symbol window se situează în jurul valorii de 5 Mbit/s datorită unor limitări ale transceiver-elor FlexRay care, conform specificației, fac

imposibilă detecția tranzițiilor între stări recesive și dominante la utilizarea unor rate de transfer mai mari.

Pentru testul de compatibilitate a mecanismului de schimb de chei cu noduri ce nu implementează mecanismul nou introdusa fost realizată o configurație de rețea mixtă folosind cele două tipuri de platforme. Ca urmare a testului, al cărui rezultat asupra comunicării este ilustrat în Figura 11, am demonstrat că noul tip de trafic poate coexista cu traficul standard FlexRay. Nodurile FlexRay pot sesizează existența, în segmentul Symbol window, a unor transmisiuni non-conforme cu definiția standardului. Aceste neconcordanțe nu sunt însă încadrate, de către controllerul FlexRay, în categoria erorilor în urma cărora trebuie oprită comunicarea. Singura acțiune realizată este informarea nivelului aplicației despre existența acestor neconcordanțe, fiecare nod fiind responsabil de implementarea unor eventuale măsuri specifice nedefinite în standard. Același comportament a fost observat și în cazul în care transmisiunile corespunzătoare schimbului de chei ocupă spațiul liber din segmentul dinamic demonstrând compatibilitatea noului mecanism propus cu rețele FlexRay existente.

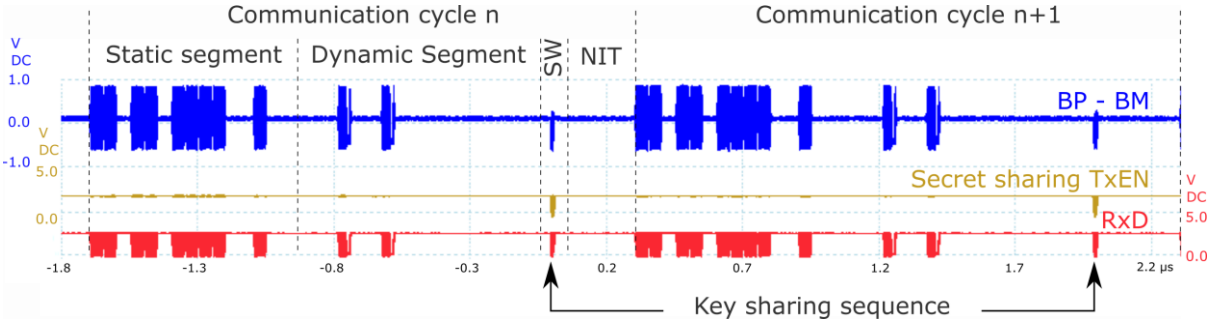

Figura 11. Semnalele FlexRay generate în cadrul testului de compatibilitate

Am evaluat de asemenea și timpul necesar pentru realizarea schimbului de chei între două noduri folosind mecanismul propus. Ca alternativă comparativă am analizat durata schimbului de chei, pe aceeași platformă, folosind algoritmul Diffie-Hellman bazat pe curbe eliptice. Testele au fost realizate folosind configurația bazată pe platforma TriCore întrucât resursele limitate ale platformei S12XF nu permit implementarea schimbului de chei Diffie-Hellman. În Tabel 1 sunt prezentate duratele de timp necesare pentru realizarea schimbului de chei între două noduri folosind cele două variante comparate. Valorile prezentate acoperă atât întârzierile date de componena computațională cât și timpul necesar transmiterii de mesaje considerând diferite variante de configurare a comunicației FlexRay. Valorile prezentate

demonstrează că metoda propusă este considerabil mai rapidă decât abordarea unui mecanism clasic utilizat în rețele de calculatoare.

	ECDH		**Metoda propusă**		
	SECP192R1	**SECP256R1**			
	Cheie 128 biți		**Cheie 128 biți**	**Cheie 192 biți**	**Cheie 256 biți**
MAPO= 31 SWAPO= 63	414.24 ms	696.25 ms	5.107 ms	10.091 ms	10.123 ms
MAPO= 31 SWAPO= 31	414.24 ms	696.25 ms	5.047 ms	5.079 ms	10.047 ms
MAPO= 20 SWAPO= 20	414.21 ms	696.22 ms	0.095 ms	5.058 ms	5.090 ms
MAPO= 10 SWAPO= 10	414.18 ms	696.19 ms	0.081 ms	5.039 ms	5.071 ms
MAPO= 5 SWAPO= 5	414.16 ms	696.18 ms	0.073 ms	5.030 ms	5.062 ms

MAPO – gdMinislotActionPointOffset
SWAPO – gdSymbolWindowActionPointOffset

Tabel 1. Durata schimbului de chei folosind algoritmul Diffie-Hellman bazat pe curbe eliptice în ciomparație cu varianta propusă

ii. Autentificare în regim time-triggered pentru rețele FlexRay

Pentru evaluarea modului în care este afectată comunicarea într-o rețea FlaxRay prin introducerea protocolului de autentificare propus am analizat întârzierile introduse datorită execuției primitivelor criptografice cât și de transmiterea tag-urilor de autentificare. Conform rezultatelor experimentale [5], performanța computațională a platformei utilizate constituie limitarea principală în ceea ce privește viteza de comunicare în regim autentificat. Acest aspect este ilustrat și în Figura 12 care prezintă timpul total necesar pentru execuția algoritmului criptografic și transmisia mesajului autentificat pentru diferite primitive criptografice. Deși cazul graficului din partea dreaptă a figurii a necesitat transmiterea a două frame-uri cu lungime mai mare decât în cazul graficului din partea stângă, influența asupra întârzierii totale a transmisiilor suplimentare este nesemnificativă.

Rezultatele obținute arată că utilizarea protocolului propus este fezabilă însă pentru asigurarea transmisterii la timp a mesajelor este necesară realizarea nodurilor rețelei pe baza unor platforme capabile să ofere nivelul de performanță necesar atât pentru implementarea funcționalităților de bază cât și pentru transmiterea mesajelor fără depășirea termenelor de transmisie specificate.

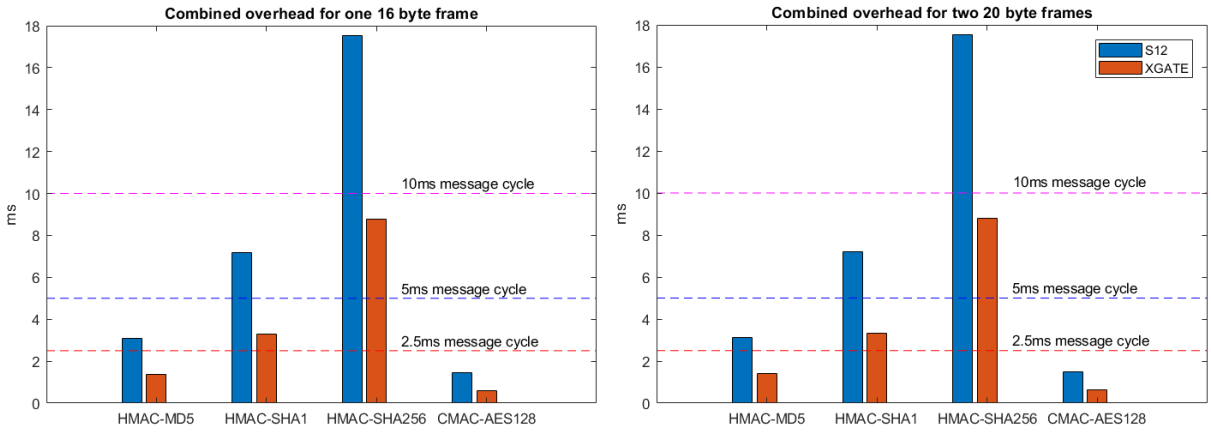

Figura 12. Intârzierea totală cauzată de introducerea protocolului de autentificare propus

iii. Detecția intruziunilor bazată pe informații de la nivelul aplicației

Pentru testarea mecanismului de detecție a intruziunilor a fost folosit un set de date real înregistrat de pe rețeaua interna a unor vehicule. Au fost simulate diferite tipuri de atacuri, pe baza datelor de trafic pre-înregistrat, folosind modelul adversarului implementat în CANoe.

În prima fază a evaluării s-a urmărit identificarea de atacuri asupra unui anumit tip de mesaj reprezentat de identificatorul acestia. În cazul atacurilor de tip replay, rata de detecție a atacurilor se situează în jurul valorii de 100% pentru varianta clasică a atacului cu o reducere a ratei de detecție la valori situate între 51 și 85% pentru atacuri elaborate ce presupun controlul strict al momentului la care este transmis mesajul de atac. Pentru atacuri ce constau în injectarea mesajelor aleatoare rata de detecție este de 100%. Pentru variante avansate ale acestui tip de atac ratele de detecție variază între 100% și ~54% în funcție de varianta atacului și valoarea utilizată pentru temporizarea mesajului de atac. Ratele de detecție pot fi îmbunătățite prin realizarea detecției pe baza a două modele, fiecare antrenat pentru una din caracteristicile mesajului.

O a doua etapă a evaluării a constat în aplicarea mecanismului de detecție pentru un sistem în care atacatorul pote folosi orice tip de mesaj. Rezultatele obținute în acest caz sunt similare cu cele obținute pentru analiza limitată la mesajele cu un anumit identificator prezentând doar o scădere de aproximativ 2% a ratei de detecție.

iv. Detecția intruziunilor bazată pe caracteristici ale nivelului fizic

Pentru evaluarea performanțelor mecanismului propus s-a avut în vedere în mod special efectul caracteristicilor referitoare la configurația rețelei asupra timpului de propagare diferențial. Astfel, s-au avut în vedere modurile prin care atacatorul poate alege să construiască

atacul: printr-un nod compromis, prin înlocuirea fizică a unui nod în rețea, prin introducerea unui nod în rețea sau prin efectuarea de modificări multiple asupra rețelei. Atacurile realizate prin noduri compromise, în care structura rețelei nu este alterată, sunt detectate în procent de 100% localizarea nodului folosit de atacator fiind evidentă în această situație. Aceste atacuri sunt reprezentate de transmiterea unor mesaje care nu au ca transmițător legitim nodul compromis.

Atacurile ce folosesc înlocuirea unui nod legitim cu unul controlat de atacator introduc schimbări în caracteristicile fizice ale canalului de comunicare ce se reflectă asupra timpului de propagare diferențial caracteristic pentru fiecare nod din rețea. Figura 13 ilustrează aceste efecte în cazul aceleiași configurații de rețea considerând noduri atacatoare diferite. Prima coloană din fiecare grafic ilustrează comportamentul nodurilor din rețea în configurația inițială și este urmată de rezultatul înlocuirii unuia din nodurile originale cu nodul atacator. Magnitudinea variației timpului de propagare diferențial caracteristic nodurilor legitime diferă în funcție de asemănarea caracteristicilor fizice ale nodului înlocuit cu cele ale nodului atacator. Totuși, în ambele cazuri aceste diferențe sunt vizibile și vor determina semnalarea prezenței unei intruziuni.

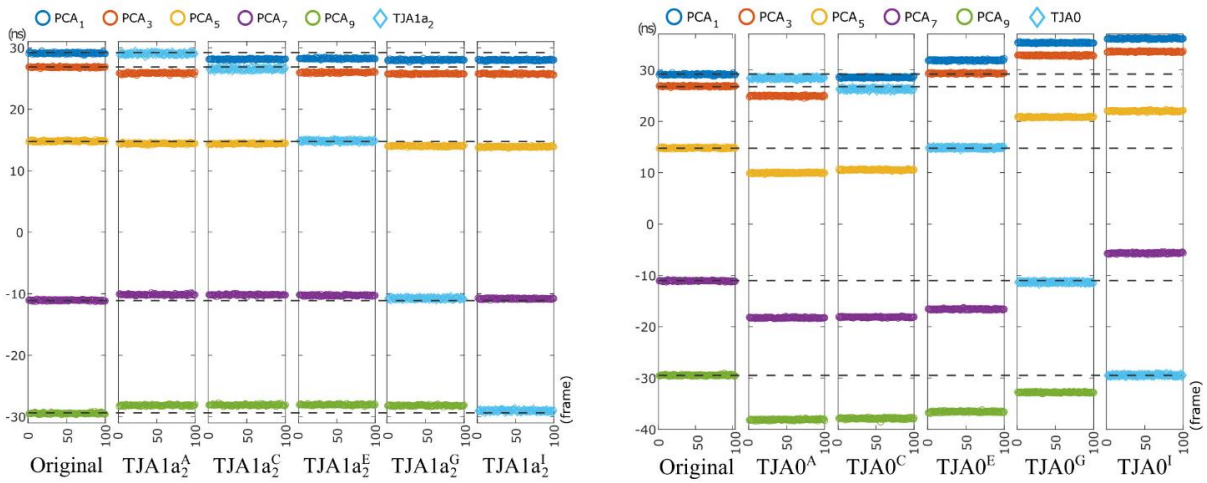

Figura 13. Efectele atacului prin înlocuirea unui nod asupra timpului de propagare diferențial

Introducerea unui nou nod în rețea afectează într-un mod similar timpul de propagare diferențial al nodurilor legitime după cum este ilustrat în Figura 14. Diferența majoră, care ajută nu numai la identificarea prezenței unui atac ci și la deosebirea tipurilor de atac, constă în prezența unei benzi suplimentare în graficul timpilor de propagare diferențiali construit pe baza mesajelor transmise în rețea. Având în vedere faptul ca pentru mesaje stransmise de către același nod timpul de propagare diferențial măsurat variază într-un interval restrâns, sistemul

de detecție a intruziunilor va identifica prezența unui număr mai mare de noduri decât cel așteptat (un nod suplimentar în cazul testului realizat).

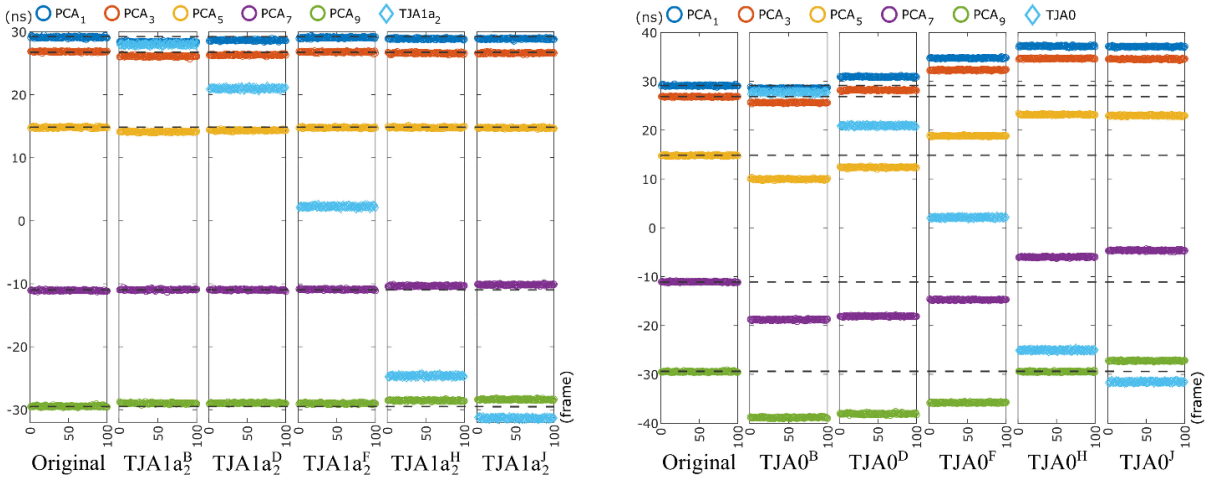

Figura 14. Efectele introducerii unui nou nod asupra timpului de propagare diferențial

Atacurile ce presupun modificări multiple asupra rețelei pot fi detectate datorită efectelor pe care schimbările le au asupra timpilor de propagare diferențiali corespunzători nodurilor legitime. Totuși în acest caz devine imposibilă identificarea modificărilor efectuate asupra rețelei prin simpla analiză a timpilor de propagare diferențiali.

Au fost evaluați de asemenea și alți factori ce pot afecta mecanismul de detecție a intruziunilor. Pentru rate de eșantionare ale semnalelor de peste 250MS/s, mecanismul TIDAL-CAN poate deosebi transmisiuni provenind de la noduri situate la distanțe relative, unul față de celălalt, de peste 10cm. Folosind rate de eșantionare de 62,5MS/s distanța minimă posibilă între noduri crește la 20cm. În ceea ce privește rata de transmisie utilizată pentru rețeaua CAN, testele realizate au arătat că aceasta nu influențează abilitatea de a deosebii nodurile transmițătoare.

Un alt aspect analizat a fost posibilitatea estimării localizării nodului transmițător pe baza timpului diferențial măsurat pentru fiecare mesaj transmis. Pentru 5 configurații diferite de rețea au fost realizate estimări folosind interpolarea liniară. Rezultatele obținute demonstrează că în majoritatea cazurilor, folosind această metodă simplă, se pot estima pozițiile nodurilor transmițătoare cu o eroare de 10cm. În unele cazuri eroarea crește până la 40cm oferind totuși posibilitatea identificării segmentului de rețea în care se află transmițătorul unui anumit mesaj.

3. Rezultate asociate obiectivului

Rezultatele privind analiza de performanță au fost publicate în lucrările asociate obiectivelor O2 și O3, amintite în capitolele precedente, însoțind detaliile privind designul celor 4 mecanisme de securitate propuse.

Concluzii

Obiectivele acestui proiect de cercetare au fost propuse ca urmare a necesității creșterii nivelului de securitate pentru rețelele standardizate utilizate în diverse sectoare ale industriei. Pentru a sublinia această necesitate, am demonstrat existența vulnerabilităților în rețele FlexRay folosite în interiorul vehiculelor și rețele industriale de control bazate pe protocolul DeviceNet prin semnalarea de noi vunlerabilități. Ca măsuri de protecție împotriva unor atacuri au fost propuse o serie de mecanisme de atacuri pentru protocolul FlexRay, specific industriei auto, și pentru protocolul CAN, utilizat atât în industria auto cât și in alte sectoare ce folosesc sisteme industriale de control. Astfel, în cazul protocolului FlexRay am propus un mecanism nou ce permite realizarea schimbului de chei între două noduri ale rețelei într-o manieră eficientă. De asemenea am propus și analizat un protocol de autentificare pentru rețele FlexRay. În contextul rețelor bazate pe protocolul CAN ne-am axat pe problematica detecției de intruziuni. Primă abordare propusă bazată pe analiza traficului folosind algoritmi de Machine Learning a fost utilizată cu succes în detecția mesajelor de atac acoperind o gamă variată de atacuri. Totodată am demonstrat posibilitatea utilizării timpului de propagare diferențial pentru semnale CAN produse de un nod al rețelei ca bază pentru identificarea și localizarea transmițătorului în vederea detecției de intruziuni. Mecanismele propuse au fost evaluate experimental în vederea analizei performanței.

Conform propunerii de proiect și a planului de realizare am estimat ca rezultate două lucrări (câte una pentru fiecare din cei doi ani ai proiectului) prezentate în cadrul unor conferințe relevante în domeniu și transmiterea spre publicare a unei sau două lucrări în jurnale cu factor mare de impact. Rezultatele științifice obținute în cadrul proiectului au fost disemnate în 4 lucrări prezentate în cadrul unor conferințe în domeniul securității (publicate în volumele dedicate conferințelor). Am realizat de asemenea 2 lucrări acceptate spre publicare în două jurnale din categoria Q1, din care unul este deja publicat în revista *IEEE Access* (având factorul de impact 3,745), iar al doilea se află în curs de publicare în revista *IEEE Transactions on Vehicular Technology* (factor de impact 5,339). Realizările privind publicarea de articole depășesc astfel estimările inițiale.

Referințe

[1] Pal-Stefan Murvay, Bogdan Groza, *Practical security exploits of the FlexRay in-vehicle communication protocol*, presented at The 13th International Conference on Risks and Security of Internet and Systems (CRISIS 2018), 2018

[2] Pal-Stefan Murvay, Bogdan Groza, *A brief look at the security of DeviceNet communication in industrial control systems*, Proceedings of the Central European Cybersecurity Conference 2018, pp. 5:1-5:6, ACM, 2018.

[3] A. Mueller and T. Lothspeich, *Plug-and-secure communication for CAN*, CAN Newsletter, pp. 10–14, 2015.

[4] Pal-Stefan Murvay and Bogdan Groza, *Efficient Physical Layer Key Agreement for*

FlexRay Networks, acceptată pentru publicare, IEEE Transactions on Vehicular Technology, 14 pages, 2020.

[5] Pal-Stefan Murvay, Lucian Popa, Bogdan Groza, *Accommodating Time-Triggered Authentication to FlexRay Demands*, The third Central European Cybersecurity Conference (CECC 2019), pp. 1-6, 2019

[6] Camil Jichici, Bogdan Groza, Pal-Stefan Murvay, *Integrating Adversary Models and Intrusion Detection Systems for In-Vehicle Networks in CANoe*, The 12th International Conference on Security for Information Technology and Communications (SECITC 2019), 2019.

[7] Pal-Stefan Murvay, Bogdan Groza, *TIDAL-CAN: differential Timing based Intrusion Detection And Localization for Controller Area Network*, IEEE Access, Volume 8, pp. 68895-68912, 2020