Raport științific

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

Etapa Nr.2 Designul unor mecanisme de securitate pentru retele industriale

Autor

ș.l.dr.ing. Pal-Ștefan MURVAY

Universitatea Politehnica Timișoara

Noiembrie 2019

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 etapei nr. 2, *Designul unor mecanisme de securitate pentru rețele industriale*.

Raportul prezintă, într-o manieră sintetică, rezultatele obținute, în timp ce detaliile tehnice suplimentare se regăsesc în lucrările asociate. Rezultatele științifice obținute în cadrul acestei etape sunt detaliate în 2 lucrări acceptate și prezentate anul acesta în cadrul unor conferințe de specialitate în domeniul securității, un articol transmis pentru publicare la un jurnal de referință pentru industria producătoare de vehicule (IEEE Transactions on Vehicular Technology – factor de impact 5,339, categoria Q1). Un al doilea articol de jurnal se află în curs de pregătire pentru a fi transmis spre publicare la un jurnal din categoria Q1 sau Q2. Articolele publicate]n anul 2019, disponibile pe pagina web a proiectului (http://www.aut.upt.ro/~pal-stefan.murvay/projects/SEVEN/publications.html), sunt:

- Pal-Stefan Murvay, Bogdan Groza, *Accommodating Time-Triggered Authentication to FlexRay Demands*, The third Central European Cybersecurity Conference (CECC 2019), 2019
- 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.

Activitatea principală prevăzută în această prima etapă a proiecului a constat în identificarea unor soluții pentru probleme de securitate prezente în protocoale de comunicare industriale standardizate utilizate în diverse sectoare industriale. În conformitate cu activitățile propuse în contractul de finanțare pentru această etapă a proiectului cercetarea s-a desfășurat pe două direcții principale. Pe de o parte s-a avut în vedere designul unor mecanisme de securitate ale unor protocoale de comunicare utilizate în industrie (activitatea 2.1 din contractul de finanțare, respectiv obiectivul O2 din propunerea de proiect). A doua direcție de cercetare a avut ca scop designul unor sisteme pentru detecția intruziunilor în rețele industriale (activitatea 2.2 din contractul de finanțare, respectiv obiectivul O3 din propunerea de proiect). Secțiunile următoare detaliază rezultatele obținute în cadrul fiecărei din aceste activități principale. Pentru a asigura continuitate direcției de cercetare abordate în analiza vulnerabilităților din prima

etapă a proiectului, protocoalele de comunicare ce au stat la baza activităților din această a doua etapă au fost FlexRay și CAN. Spre deosebire de protocolul FlexRay, CAN nu a constituit subiectul direct al analizei vulnerabilităților în prima etapă a proiectului fiind studiat DeviceNet [2] – un protocol de nivel înalt ce are la bază protocolul CAN. Pentru această a doua etapă a proiectului am ales să ne orientăm spre identificarea unor soluții pentru protocolul CAN care să poată fi aplicate pentru toate protocoalele de nivel inalt bazate pe acesta.

1 Activitate 2.1 - Designul unor mecanisme de securitate menite să contracareze vulnerabilitățile protocoalelor de comunicare utilizate în industrie

Pentru acest obiectiv cercetarea s-a concentrat pe identificarea și implementarea unor mecanisme de securitate pentru protocolul FlexRay. Așa cum am prezentat în primul raport de cercetare asigurarea securității pentru comunicarea realizată folosind protocolul FlexRay este importantă deoarece acesta deservește cu precădere aplicații responsabile de siguranță în exploatarea autovehiculelor. Specificația protocolului FlexRay nu prevede mecanisme specifice pentru asigurarea securității lucru care face posibile o serie de atacuri de tip DoS și falsificarea mesajelor așa cum am demonstrat experimental în lucrarea [1].

Primul aspect abordat a fost dezvoltarea unui mecanism sigur și eficient pentru a asigurarea schimbului de chei intre participanții la comunicare într-o rețea FlexRay. O a doua direcție de cercetare privind securitatea în rețele FlexRay a constat în analiza unui mecanism care să asigure autenticitate în comunicare. Prezentăm în continuare rezultatele obținute pentru cele două direcții abordate.

1.1 Schimb de chei eficient pentru rețele FlexRay folosind layerul fizic

Problema principală adusă de introducerea unui mecanism de securitate, în rețele pentru care securitatea nu a fost luată în considerare la momentul designului inițial, este încărcarea suplimentară a rețelei cu mesajele corespunzătoare mecanismului nou introdus. În cazul FlexRay ne-am propus să dezvoltăm un mecanism care să ofere o încărcare limitată a canalului de comunicare.

Soluția propusă [3] pentru asigurarea schimbului de chei se folosește de implementarea nivelului fizic ce definește două tipuri de semnale: dominante și recesive. Dacă un semnal dominant este generat în același timp cu unul recesiv pe canalul comun de comunicare, rezultatul vizibil pe acel canal va fi semnalul dominant. Astfel, pentru două noduri care transmit

concomitent semnale un canal de comunicare FlexRay va implementa funcția ȘI-cablat (considerând că semnalul dominant corespunde lui “0”, iar cel recesiv lui “1”). Designul nostru se bazează pe o soluție similară propusă de Mueller și Lothspeich [4] pentru rețele CAN.

Plecând de la această caracteristică a nivelului fizic, procedura prin care două noduri pot stabili un secret comun, exemplificată în Figura 1, constă în următorii pași:

- fiecare din cele două noduri generează o secvență de numere aleatoare
- nodurile modifică secvența generată adăugând după fiecare bit din secvență un nou bit reprezentând opusul celui original; acest pas este necesar pentru cazul în care un nod transmite un bit dominant (“0”) pentru a-i permite acestuia să identifice valoarea bitului transmis de nodul partener
- secvențele de biți sunt transmise simultan de cele două noduri
- fiecare nod înlătură acei biți din secvențele inițiale care sunt considerați compromiși în urma transmisiei; ca o consecință a celui de-al doilea pas, un adversar poate identifica cazurile în care ambele noduri transmit aceeași valoare fie ea dominantă (”0”) sau recesivă (“1”)
- la finalul procedurii fiecare nod va avea o secvență egală cu inversa secvenței deținute de nodul partener.

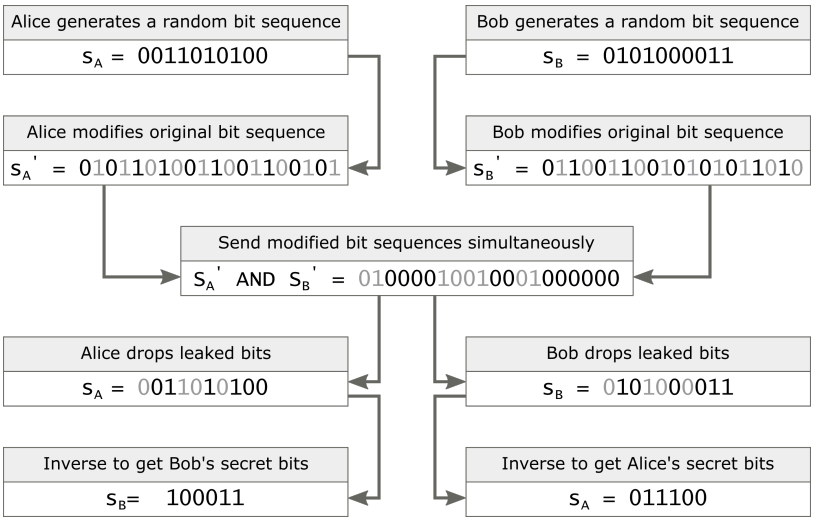

Figura 1. Exemplificarea procedeului de stabilire a unui secret comun pentru secvențe de 10 biți aleatori

Datorită restricțiilor date de specificația protocolului FlexRay, aplicabilitatea metodei prezentate, păstrând compatibilitatea cu alte noduri ce nu o folosesc, este limitată la un singur segment din ciclul de comunicare: Symbol window. Lucrarea aflată în evaluare pentru

publicare în jurnal [3] descrie pe larg propunerea noastră pentru formatul transmisiunii secvenței de biți precum și protocolul utilizat pentru inițierea procedurii.

Soluția propusă pentru asigurarea schimbului de chei într-o rețea Flexray a fost implementată pe două configurații experimentale. Prima este bazată pe o platforma cu microcontroller din familia S12XF ce oferă performanțe de nivel mediu spre slab. Pentru a doua implementare am utilizat 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 2.

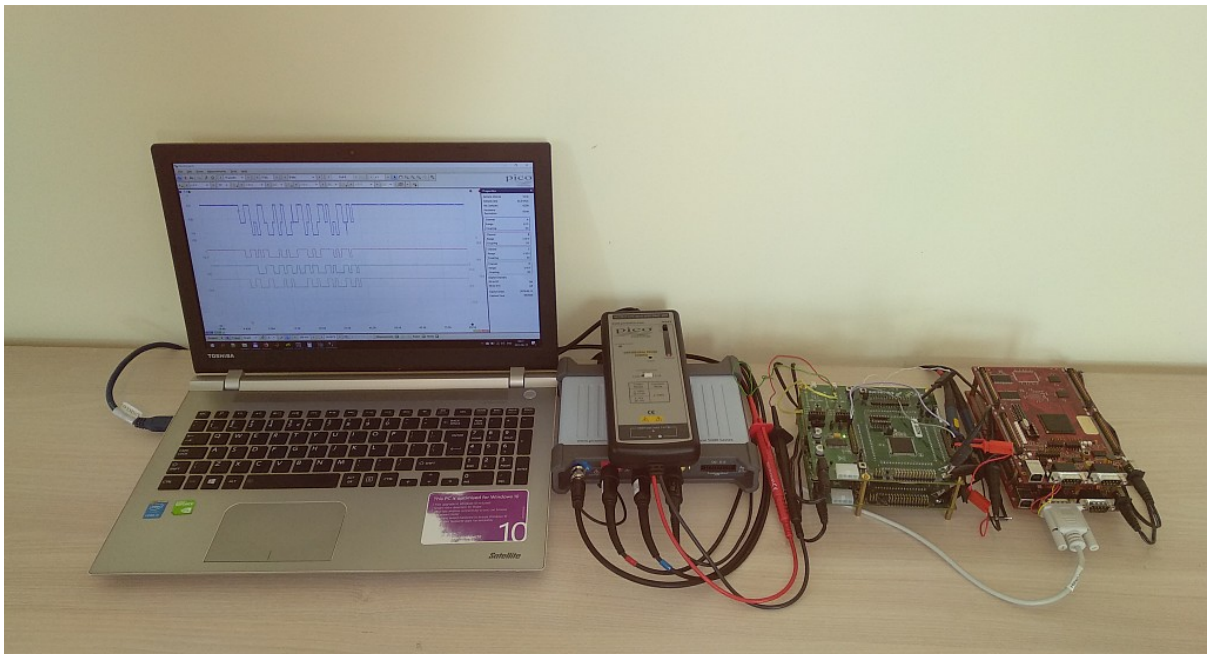

Figura 2. Lanțul experimental utilizat pentru implementarea și testarea metodologiei propuse pentru asigurarea schimbului de chei

Au fost testate atât ratele de transmisie ce pot fi atinse pe fiecare din cele două configurații pentru schimbul de chei cât și compatibilitatea transmisiunilor speciale introduse cu noduri care nu implementează mecanismul de schimb de chei.

Pe platforma S12XF a fost atinsă o rată maximă de transfer de 1 Mbit/s datorită performanței limitate a microcontroller-ului. În cazul TriCore performanța platformei nu constituie o limitare. Totuși, rata maximă de transfer posibilă în segmentul Symbol window se situează în jurul valorii de 5 Mbit/s datorită unor limitări intrinseci în designul transceiver-elor FlexRay care fac imposibilă detecția tranzițiilor între stări recesive și diminante la utilizarea unor rate de transfer mai mari. Figura 3 ilustrează schimbul de chei realizat la 5 Mbit/s între două noduri bazate pe microcontroller TriCore.

Testul de compatibilitate cu noduri ce nu implementează mecanismul de schimb de chei a demonstrat că noul tip de trafic poate să coexiste cu traficul standard FlexRay. Nodurile FlexRay sesizează existența, în segmentul Symbol window, a unor transmisiuni nedefinite în standard dar nu consideră aceste neconcordanțe ca fiind suficient de grave pentru a opri comunicarea. Singura acțiune este informarea nivelului aplicației despre existența acestor neconcordanțe fiind responsabil de implementarea unor eventuale măsuri specifice nedefinite în standard.

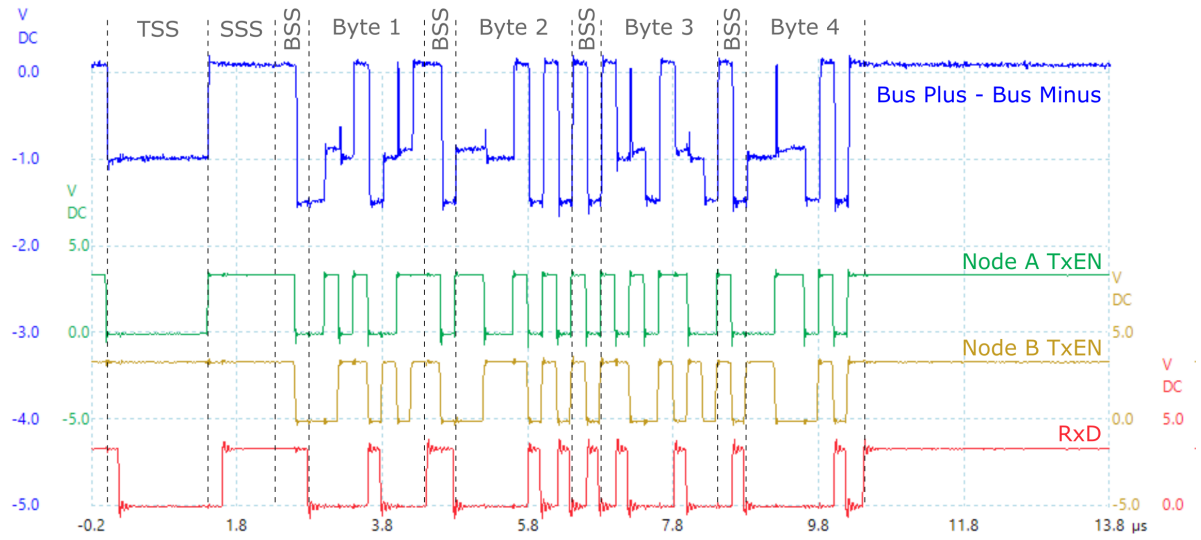

Figura 3. Semnalele generate pe durata schimbului de chei între două noduri TriCore la o rata de transfer de 5Mbit/s

1.2 Autentificare în regim time-triggered pentru rețele FlexRay

A doua direcție de cercetare abordată pentru asigurarea securității pentru comunicarea în rețele FlexRay a fost asigurarea autenticității [5]. Principala provocare în dezvoltarea unui mecanism de autentificare o constituie respectarea termenlor limită impuse pentru transmiterea mesajelor. Fiind dezvoltat pentru aplicații în care lipsa recepției mesajelor la termene prestabilite poate afecta siguranța, FlexRay implementează un model de comunicare time-triggered. Transmiterea mesajelor are loc conform unui ciclu de comunicare cu o lungime prestabilită în cadrul căruia sunt definite două segmente în care se pot transmite mesaje: segmentul static și segmentul dinamic. Segmentul static este cel care asigură transmiterea mesajelor ciclice. Conform exemplelor de aplicații reale analizate, cele mai mici intervale de repetiție ale mesajelor în cadrul ciclilor de comunicare sunt de ordinul milisecundelor (de ex. 1, 2,5, 5ms).

În cadrul prezentului proiect au fost abordate elementele de bază pentru designul unui protocol de autentificare pentru comunicare în rețele FlexRay după cum urmează:

1. **Distribuirea cheilor.** Pentru a reduce încărcarea adițională a canalului de comunicare, în regimul normal de funcționare, am propus ca distribuirea cheilor pentru fiecare sesiune de utilizare a vehiculului să se realizeze în perioada în care vehiculul nu este utilizat. Generarea și distribuirea cheilor este realizată de un nod master. Cheile distribuite sunt criptate folosind un alt set de chei provenind din lanțuri one-way pre-programate pe fiecare nod în timpul producției vehiculului.

2. Utilizare adaptabilă a algoritmilor criptografici. Pentru a reduce timpul necesar pentru execuția algoritmilor criptografici propunem alegerea algoritmilor utilizați, pentru fiecare tip de mesaj, în funcție de intervalul de repetiție a mesajelor ciclice. Pentru fiecare interval se poate alege un alrogitm ce oferă suficientă securitate pentru durata intervalului.

3. Trunchierea tag-urilor de autentificare. O abordare uzuală în protocoalele de autentificare propuse pentru domeniul automotive o reprezintă trunchierea tag-urilor de autentificare pentru a reduce încărcarea suplimentară a canalului de comunicare. Conform recomandărilor NIST, am folosit truncherea tagurilor la 32 biți.

4. 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 tuturor tag-urilor generate de un nod pentru un ciclu de comunicare ca un frame separat.

5. Sincronizare temporală. Protocolul de autentificare propus se bazează pe protocolul TESLA utilizat în rețele de senzori. Unul din elementele pe care se bazează securitatea acestuia este existența sincronizării temporale între noduri. Prin designul său, protocolul FlexRay asigură deja această cerință sincronizarea între noduri fiind obligatorie pentru menținerea comunicării într-o rețea FlexRay.

Protocolul de autentificare. Varianta de bază a protocolului 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 folosind coduri MAC (coduri de autentificare a mesajelor). Cheile sunt mai apoi făcute publice în următorul interval de timp pentru a se putea verifica autenticitatea mesajelor. 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 a-priori nodurilor implicate în comunicare. Astfel nodurile receptoare pot autentifica mesajul de îndată ce acesta este primit împreună cu tag-ul de autentificare.

Pentru a evalua influența introducerii unui astfel de protocol într-o rețea FlexRay au fost analizate întârzierile introduse atât de execuția primitivelor cryptografice cât și de transmiterea

tag-urilor de autentificare. Evaluarea experimentală a fost realizată pe un model experimental simplificat, construit pe plăci de dezvoltare bazate pe platforma S12XF. Experimentele au arătat [5] că performanța platformei utilizate constituie și în acest caz cea mai mare limitare pentru viteza de comunicare în regim autentificat. Acest aspect este ilustrat și în Figura 4 în care fiecare din cele două grafice prezintă timpul total necesar pentru calculul primitivei criptografice și transmisia mesajului autentificat pentru diferite primitive criptografice. Deși cazul graficului din partea dreaptă a necesitat transmiterea a două frame-uri cu lungime mai mare decât în cazul graficului din partea stângă, influența asupra întârzierii totale este nesemnificativă.

Rezultatele obținute arată că utilizarea protocolului propus este fezabilă alegând, pentru fiecare funcționalitate, platforme capabile să ofere nivelul de performanță necesar pentru transmiterea mesajelor la intervalele de timp specificate.

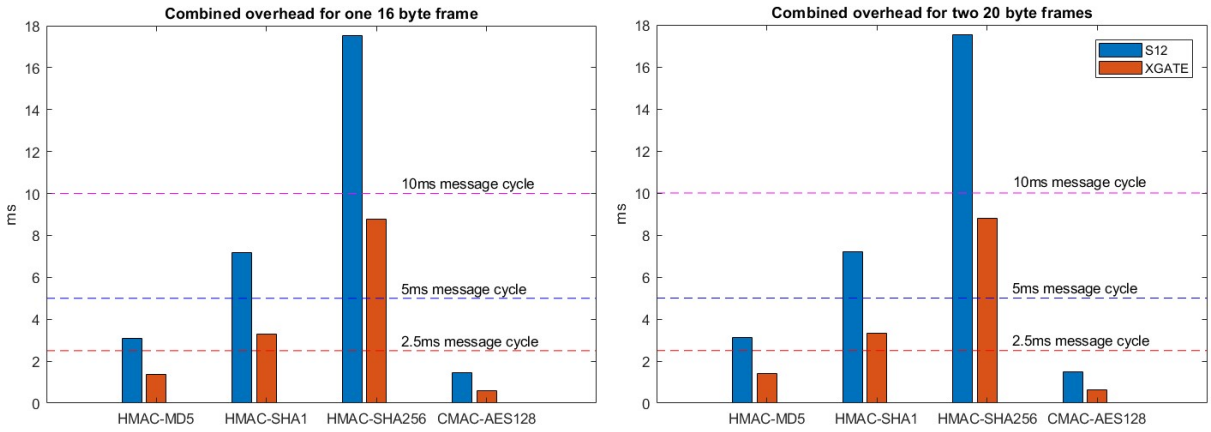

Figura 4. Intârzierea totală cauzată de introducerea protocolului de autentificare propus

2 Activitate 2.2 - Designul unor sisteme pentru detectia intruziunilor in rețele industriale

După cum am precizat anterior, pentru această activitate a proiectului cercetarea s-a axat detecția intruziunilor pentru rețele bazate pe protocolul CAN. În cadrul acestei activități au fost abordate două direcții: detecția intruziunilor bazată pe informații de la nivelul aplicației și detecția bazată pe nivelul fizic.

2.1 Detecția intruziunilor bazată pe informații de la nivelul aplicației

În cadrul proiectului, pentru această primă abordare, a fost propus conceptul implementării unui sistem care să permită testarea unor atacuri și analiza traficului pentru detecția de intruziuni în CANoe, un mediu folosit în mod curent în industrie pentru simularea și testarea

rețelelor in-vehicle. CANoe permite implementarea facilă a unor funcționalități de analiză a traficului sau de generare de trafic atât în timp real prin conectarea directă la rețeaua interna a vehiculului cât și în mod off-line pentru secvențe de trafic înregistrate. În plus, existența posibilității de integrare a unor funcționalități din alte medii de analiză a datelor precum Matlab poate transforma CANoe într-un mediu avansat de analiză a traficului și detecție a intruziunilor în rețele automotive.

Pentru realizarea de atacuri a fost definit modelul atacatorului incluzând cele mai comune tipuri de atac asupra comunicației CAN raportate în literatură: replay și spoofing. Au fost luate în considerare și variante de atac care să permită transmiterea automată cu periodicitate prestabilită a mesajelor de atac și diferite tipuri de modificări asupra câmpului de date.

Pentru sistemul de detecție a intruziunilor s-a optat pentru integrarea în CANoe a unor funcționalități de analiză a datelor disponibile în Matlab. Prin intermediul toolbox-ului pentru statistică și machine learning, Matlab oferă o serie de algoritmi ce folosesc machine learning pentru a rezolva probleme de regresie sau clasificare. Rutine de analiză implementate în Matlab pot fi exportate sub formă de fișiere .dll permițând integrarea funcționalităților în alte aplicații precum CANoe.

Ca algoritm pentru analiza datelor a fost ales k-NN fiind soluția utilizată în general când informațiile despre datele analizate sunt limitate. Exceptând mesajele standardizate folosite pentru diagnoză, descrierea conținutului mesajelor prezente în rețelele CAN nu este în mod uzual făcute publice 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 (lungimea mesajului și câmpul de date) precum și temporizarea mesajelor ciclice.

Testarea algoritmului de detecție pe atacuri introduse într-un set de date real înregistrat de pe rețeaua interna a unor vehicule a demonstrat rate de detecție de peste 90% pentru 60% din tipurile de atac testate și peste 80% pentru 77% din atacuri. Aceste rezultate demonstrează utilitatea abordării propuse în detecție unor tipuri de atac și sugerează necesitatea utilizării mai multor algoritmi de detecție pentru acoperirea unui spectru mai larg de atacuri.

2.2 Detecția intruziunilor bazată pe layerul fizic

A doua direcție de cercetare pentru identificarea intruziunilor într-o rețea CAN s-a axat pe analiza semnalelor fizice generate pe liniile de comunicație. Principiul pe care îl propunem nu a mai fost utilizat în scopul identificării nodurilor într-o rețea cablată. Designul sistemului de

detecție a intruziunilor propus se bazează pe viteza de propagare a unui semnal printr-un conductor electric. Durata de timp necesară unui semnal pentru a parcurge o anumită secțiune de conductor este direct proporțională cu lungimea acelei secțiuni. Așadar, analizând diferența de timp între momentul când un semnal ajunge la un capăt al conductorului și momentul când acest ajunge la celălalt capăt, putem estima poziția de la care a fost transmis semnalul.

Avantajul utilizării acestui principiu, în comparație cu alte propuneri bazate pe layerul fizic pentru detecția intruziunilor în rețele CAN, este dat de posibilitatea localizării nodului transmițător. Prin identificarea poziției nodului transmițător se poate determina dacă mesajul transmis este unul din mesajele pe care acel nod are "dreptul" să îl transmită. Astfel se poate determina dacă un nod compromis sau un nod introdus în rețea (spre exeplu prin portul de diagnoză) încearcă să transmită mesaje aparținând altor noduri.

Pentru demonstrarea funcționării conceptului enunțat a fost realizată o rețea de test în care punctele de conexiune ale nodurilor au fost instalate la distanțe prestabilite față de unul din capetele rețelei. Figura 5 ilustrază standul experimental cu 5 noduri conectate. Semnalele generate de noduri instalate în toate punctele de conexiune ale rețelei au fost capturate de la cele două capete ale rețelei folosind un osciloscop. Pentru estimarea localizării nodului transmițător, s-a calculat mai apoi defazajul între cele două semnale capturate pentru fiecare transmisie.

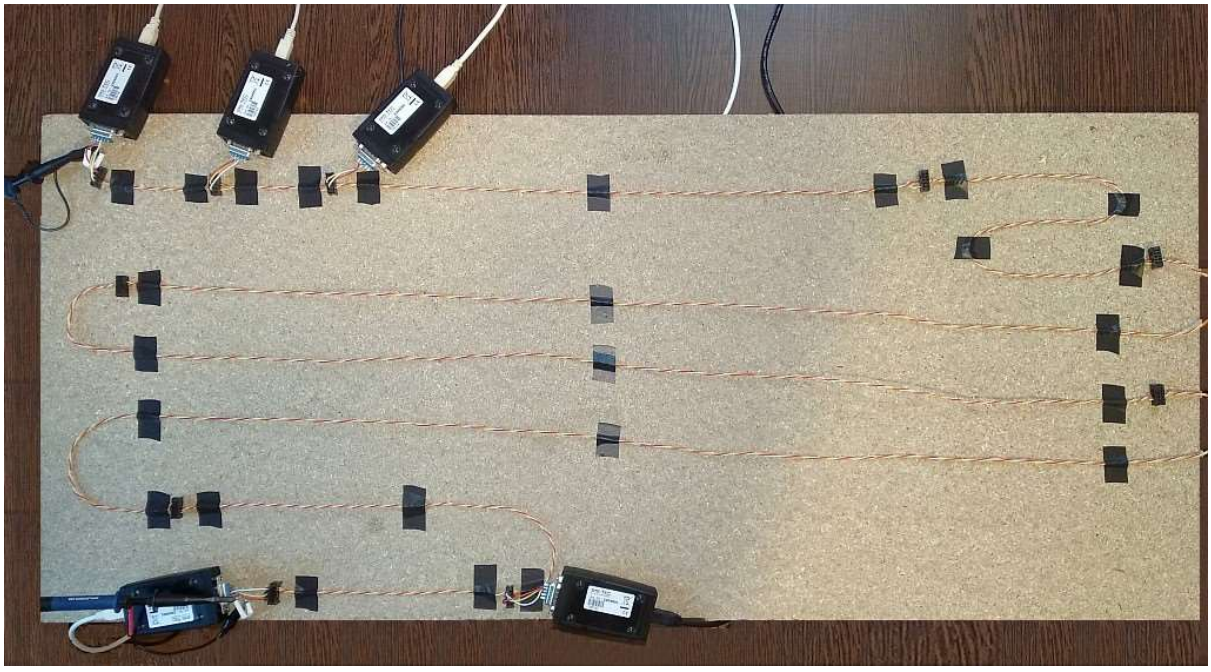

Figura 5. Model experimental pentru evaluarea sistemului de identificare a intruziunilor bazat pe layerul fizic

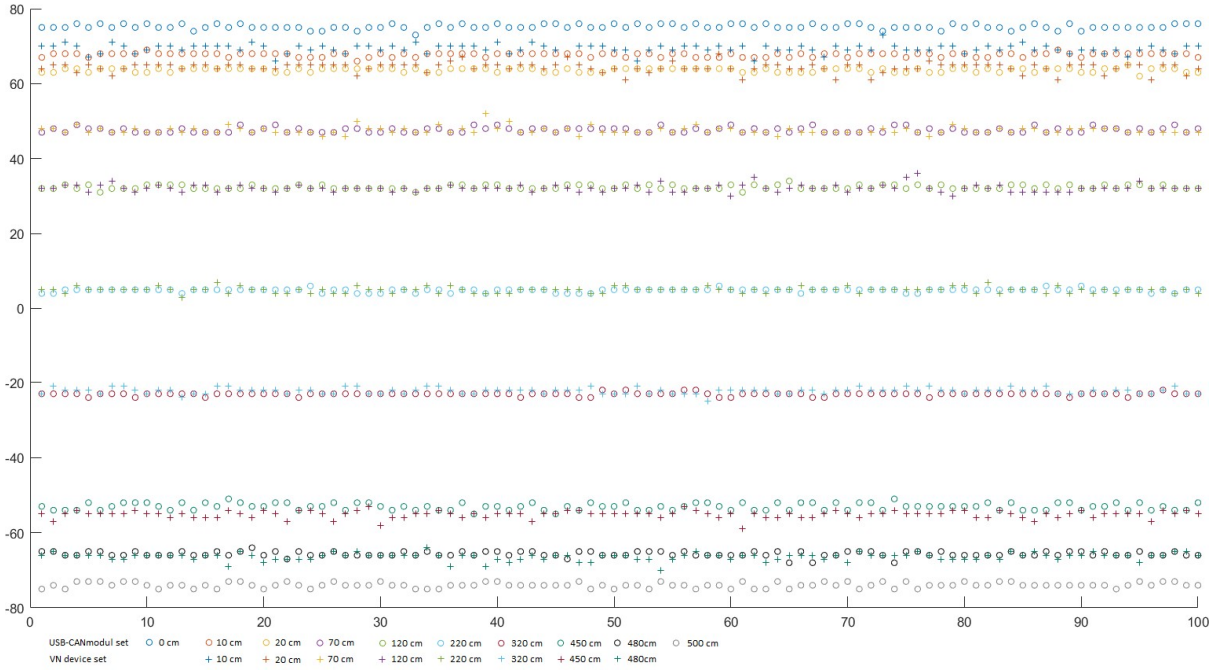

Figura 6. Rezultate esperimentale pentru localizarea nodurilor transmițătoare pe două seturi de date diferite

Figura 6 ilustrează rezultatele experimentale obținute pentru validarea metdologiei pe modelul experimental construit folosind două seturi de dispositive ca transmițători: un set format din 10 dispozitive USB-CANmodul și un al doilea format din 8 dispositive VN. Rezultatele demonstrază faptul că metoda propusă poate indentifica nodurile transmițătoare cu o precizie de 100% dacă distanțele minime relative între noduri sunt mai mari de 15cm. Eroarea de localizare crește pentru nodurile poziționate la distanțe mai mici de alte noduri. Spre exemplu pentru două noduri poziționate la distanță de 10cm unul față de celălalt localizarea este corectă în aproximativ 80% din cazuri.

Lucrarea care prezintă pe larg metodologia aplicată și rezultatele experimentale se află în curs de redactare urmând să fie adăugate noi rezultate exerimentale înainte de trasmiterea lucrării pentru evaluare la un jurnal din categoria Q1 sau Q2.

3 Concluzii

Rezultatele științifice obținute în această etapă a proiectului s-au concentrat pe identificarea de soluții pentru probleme de securitate existente în două protocoale utilizate în industrie: FlexRay și CAN.

În ceea ce privește protocolul FlexRay, a fost propus și validat experimental un mecanism pentru stabilirea de chei pe baza caracteristicilor nivelului fizic. Articolul cu rezultatele obținute se află în evaluare pentru publicarea în jurnal [3]. O a doua propunere a fost pentru un

mecanism de autentificare a comunicării, rezultatele obținute fiind prezentate la o conferință în domeniul securității [5].

Pentru protocolul CAN s-a analizat problema indentificării intruziunilor în rețea folosind două abordări, una bazată pe machine learning și informațiile disponibie la nivelul aplicației [6] și o a doua ce folosește caracteristici fizice ale liniei de transmisie.

În continuare cercetarea în cadrul proiectului se va concentra pe evaluarea performanțelor pentru mecanisme de securitate.

4 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] Pal-Stefan Murvay and Bogdan Groza, *Efficient Physical Layer Key Agreement for FlexRay Networks*, în curs de evaluare, IEEE Transactions on Vehicular Technology.

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

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