Raport Ştiinţific Nr. 1

Proiect PN-III-P1-1.1-TE-2016-1317

Interacţiuni private şi sigure între vehicule şi dispozitive electronice inteligente

PRESENCE

(anul 2018)

Echipa

Prof. Habil.Dr. Ing. Bogdan Groza
S.l.Dr. Ing. Pal-Ştefan Murvay
As.Dr. Ing. Horaţiu Eugen Gurban
Drd. Ing. Tudor-Sebastian Andreica
Drd. Ing. Camil Jichici

Universitatea Politehnica Timisoara

Decembrie 2018

Raport Ştiinţific Nr. 1

Proiect PN-III-P1-1.1-TE-2016-1317

Interacţiuni private şi sigure între vehicule şi dispozitive electronice inteligente

PRESENCE

Prezentul raport adresează activitatea ştiinţifică a proiectului **Proiect PN-III-P1-1.1-TE-2016-1317, Interacţiuni private şi sigure între vehicule şi dispozitive electronice inteligente (PRESENCE)** aferentă anului 2018. Stadiul curent de implementare al proiectului este menţinut la zi pe site-ul proiectului http://www.aut.upt.ro/~bgroza/projects/presence/index.html şi poate fi consultat pentru detalii suplimentare la acest raport (de ex. date tehnice care există în publicaţiile asociate).

În conformitate cu contractul de finanţare, în anul 2018 am demarat Etapa 1 – designul, analiza şi implementarea protocoalelor de securitate în interacţiuni între vehicule şi dispozitive mobile inteligente, etapă ce a avuta la bază următoarele 3 activităţi:

- ***A1. Designul, analiza şi implementarea protocoalelor de securitate (prima iteraţie)***
- ***A2. Tehnologii pentru creşterea securităţii folosind carduri NFC***
- ***A3. Asocieri bazate pe date din ecosistem folosind date de la accelerometre***

Proiectul a demarat doar în luna mai a acestui an şi am reuşit să redactăm în primele luni ale proiectului 2 lucrări ce au fost deja publicate şi susţinute în cadrul unor conferinţe de cercetare [1], [2]. Sunt în paralel demarate şi în curs de redactare încă 2 lucrări ce vor fi destinate unor jurnale ISI urmând să fie înaintate la începutul anului următor. Lista de lucrări ştiinţifice este menţinută la zi pe site-ul proiectului http://www.aut.upt.ro/~bgroza/projects/presence/publications.html

Detaliem în cele ce urmează rezulatele şi activităţile de cercetare aferente acestei etape.

A1. Designul, analiza şi implementarea protocoalelor de securitate (prima iteraţie)

O problemă cu care ne-am confruntat înainte de a începe designul efectiv al protocoalelor de securitate a fost stabilirea funcţionalităţilor la care telefoanele moderne trebuie sa răspundă respectiv a canalelor de comunicare ce pot fi folosite pentru crearea unor conexiuni telefon-maşină.

Chiar dacă proiectul nostru vizează strict controlul accesului la maşini, nu putea fi neglijate şi era necesară documentarea cu privire la alte funcţionalităţi. Poate că deloc surprinzător, am reuşit să identificăm în lucrări de cercetare recente un număr foarte mare de funcţionalităţi ce au fost delegate telefoanelor mobile inteligente în relaţia cu autovehiculele, un sumar se găseşte în Tabelul I.

Legat de interfeţele de comunicare, în tabelul II sunt prezentate şi comparate principalele tehnologii wireless de transmisie de date utilizate în autovehiculele moderne, şi care sunt disponibile în mare parte şi pe telefoane mobile inteligente. Din motive evidente legate de consumul de putere, interfeţele preferate par a fi NFC şi Bluetooth pe care vom axa implementarea protocolului de securitate.

Tabelul I. Funcţionalităţi delegate telefoanelor mobile inteligente în conjuncţie cu autovehiculele moderne

Categorie	Funcționalități
Funcţionalităţi de securitate	• Utilizarea datelor biometrice pentru identificarea utilizatorului în scopul obținerii drepturilor de acces și pentru personalizare, e.g., configurare oglinzi, scaun, volan, mod condus • Interconectarea dispozitivelor utilizând informații specifice mediului: accelerații, sunet, etc. • Identificarea șoferului pe baza stilului de condus utilizând informații de la accelerometru • Stabilire dacă dispozitivul se află în mașină • Identificare șofer/pasageri, număr persoane în autovehicul, folosind diverse datele de la senzori, e.g., sunet • RSSI fingerprinting, recunoaștere/localizare dispozitiv bazat pe RSSI(*received signal strength indicator*)
Management autovehiculelor	• Diagnoza autovehiculului la distanță pentru identificarea problemelor tehnice sau pentru accesarea datelor înregistrate de tahograf • Închirierea mașinilor • Partajarea drepturilor de acces, partajarea unui subset de drepturi de acces, e.g., uși, motor, infotainment etc. • Urmărirea flotei, afișare vehicule flotă pe hartă
	• Identificarea și afișarea pe smartphone a culorii semaforului, avertizarea șoferului • Avertizarea șoferului în cazul în care există bicicliști sau pietoni în proximitatea

Sisteme avansate de asistență șoferi (ADAS-*Advanced Driver Assistance Systems)*	autovehiculului • Detectarea și avertizarea șoferului în cazul în care există animale pe carosabil • Avertizarea șoferului în cazul în care există secțiuni de carosabil cu gheață/ polei sau zone nesemnalizate cu gropi • Avertizare accidente rutiere sau avertizarea în cazul în care într-o zonă există un risc ridicat de producere a accidentelor • Avertizare pericol coliziune • Identificarea locurilor de parcare libere • Plată parcare prin intermediul unei aplicații • Avertizarea șoferului în cazul congestionării traficului pe ruta selectată • Îndrumarea șoferului pentru reducerea consumului de combustibil, e.g., schimbarea treptelor de viteză • Localizarea locului unde a fost parcat autovehiculul • Avertizarea șoferului în cazul în care există în apropiere autovehicule în misiune (salvare, poliție sau pompieri), informarea șoferului - direcția din care se apropie vehiculul

Tabelul II. Sumar al caracteristicilor pentru interfeţe de comunicare wireless disponibile în maşini contemporane şi/sau telefoane mobile inteligente

Comunicație	NFC	Bluetooth	Bluetooth low energy	WiFi	LTE
Consum energie	foarte scăzut	scăzut	foarte scăzut	ridicat	ridicat
Distanță	<20 cm	<10m	50m interior, 150m exterior	50m interior, 250m exterior (echipament standard)	100m-1km
Frecvență	13.56 MHz	2.400–2.4835 GHz bandă ISM	2.400–2.4835 GHz bandă ISM	2.4 & 5Ghz	multiple domenii de frecvență alocate
Lățime de bandă	106 kbit/s, 212 kbit/s sau 424 kbit/s	700 kb/s	1 Mb/s	>500Mbps (802.11 ac)	100Mb/s downlink 50Mb/s uplink

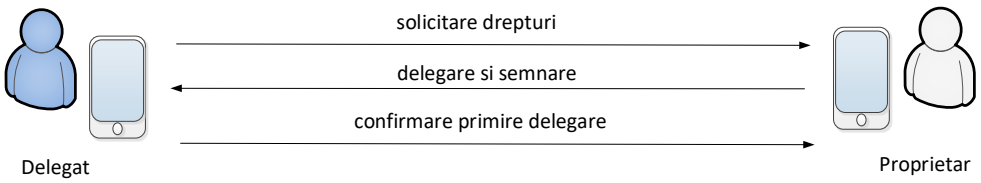

Figura 1. Secvența delegare drepturi de acces

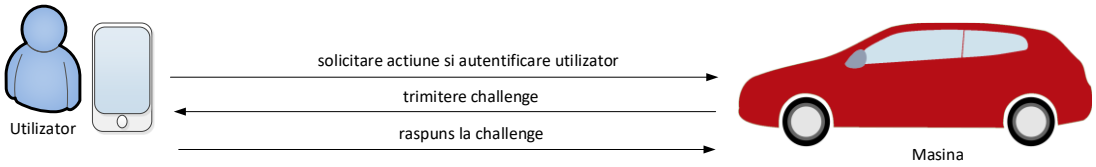

Figura 2. Secvența solicitare acțiune și autentificare

Odată clarificate funcţionalităţile şi interfeţele de comunicare am trecut la construcţia protocolului de autentificare şi control al accesului. Datele complete sunt încă nepublicate pentru care designul complet va fi discutat doar în următorul raport din motive de confidenţialitate. La nivel principial există un protocol de delegare a drepturilor de acces care se derulează de la utilizator la utilizator (sugerat în Figura 1) şi un protocol de acces la maşină care este la bază un protocol de tip challenge response (sugerat în Figura 2). Toate aceste protocoale se vor baza pe funcţii cripografice simetrice şi asimetrice de ultimă generaţie, parte din ele fiind deja evaluate în prima lucrare publicată în cadrul proiectului [1].

A2. Tehnologii pentru creşterea securităţii folosind carduri NFC

Analiza tehnologiei NFC și a dispozitivelor care au capabilitatea de a folosi această tehnologie a fost un pas necesar stabilirii interfeţei de comunicare pentru dezvoltarea protocolului de securitate. NFC (Near Field Communication) are la bază identificarea prin frecvență radio (RFID) cu posibilitatea de comunicare la o distanță mai mică de 20 cm. Acest lucru conduce la un avantaj datorat consumului redus de energie dar şi pentru securitate deoarece interceptarea mesajelor de către adversari de la distanţe mai mari devine problematică.

Un dipozitiv capabil să folosească tehnologia NFC poate funcționa în unul dintre următoarele trei moduri: NFC card emulation, NFC reader/writer şi NFC peer-to-peer. În primul dintre cele trei moduri, dispozitivele inteligente pot să emuleze carduri inteligente și în acest fel acestea pot fi folosite pentru

anumite tranzacții, ca de exemplu plata unui serviciu. Al doilea mod, permite dispozitivelor compatibile NFC să citească sau să scrie informații. Cel de al treilea și ultimul mod, poate fi folosit pentru comunicația între două dispozitive inteligente, de exemplu două tablete, într-o manieră ad-hoc. În general, etichetele NFC nu posedă baterii, ci sunt alimentate de către dispozitivele de scriere sau citire printr-un câmp electromagentic.

În cadrul proiectului am ales să folosim și să analizăm cardul NXP MIFARE DESFire EV1[1]. Cardul este produs de MIFARE, care este o marcă deținută de NXP Semiconductors, și se adresează în special următoarelor tipuri de aplicații: transport public inteligent, gestionarea accesului, programe de loialitate și micropayment. Cardul folosit în proiectul nostru are o memorie de stocare non-volatilă de 2 kilo-octeți și oferă câteva funcționalități de securitate [3]. din care enumerăm: autentificare mutuală în trei pași, hardware dedicat pentru DES (Data Encryption Algorithm) și AES (Advanced Encryption Standard) cu chei de criptare: 56-bit DES, 112-bit 3DES, 168-bit 3DES și AES 128 biți, 1 cheie master și până la 14 chei per aplicație. Cardul suportă următoarele moduri de comunicație: transfer de date simplu, transfer de date cu checksum criptografic (Message Authentication Code) și transfer de date criptat.

Produsul este conceput să suporte mai multe tipuri de aplicații pe un singur card și are memoria organizată în aplicații și fișiere. Aplicațiile pot fi văzute/interpretate de către utilizatori ca niște directoare Windows, în interiorul cărora se pot crea fișiere unde se stocheaza efectiv datele. Cheile se pot folosi pentru autentificare în aplicații și pentru accesul de tip scriere sau citire a datelor. Tipul de sistem criptografic folosit în fiecare aplicație trebuie specificat de către utilizator la crearea aplicației.

Pentru a utiliza cardul MIFARE DESFire EV1, producătorul a pus la dispoziție utilizatorilor un SDK (Software Development Kit) numit TapLinx SDK[2]. Acest SDK l-am integrat în Android Studio și astfel am reușit să implementăm propriile noastre aplicații Android cu ajutorul cărora putem să manipulăm cardul folosind tehnologia NFC.

În continuare am decis să folosim pentru comunicarea cu cardurile placa de dezvolatre DLP-7970ABP. Această placă este un modul de evaluare, produs de Texas Instrument, pentru transceiverul RFID/NFC TRF7970A. Pentru a controla DLP-7970ABP am folosit kitul de dezvoltare MSP430G2 Launchpad de la Texas Instruments. Cele doua dispozitive, MSP430G2 și DLP-7970ABP, au fost conectate să comunice prin interfața SPI (Serial Peripheral Interface). Bazându-ne pe informațiile din [4] am reușit să programăm MSP430G2 și DLP-7970ABP și să configurăm cardul MIFARE DESFire EV1 astfel încât să reușim să efectuăm o autentificare challenge-response în trei pași, bazată pe AES-128 biți, conform cu specificaţiile de manual ale produsului.

[1] https://www.mifare.net/wp-content/uploads/2018/05/MIFARE-DESFire-EV1-Product-Flyer-Web.pdf
[2] https://www.mifare.net/en/products/tools/taplinx/

Tehnologie (NFC) este folosită de noi în cadrul protocolului de autentificare pentru controlul accesului la autovehicule. Protocolul este subiect al unei lucrări ce va trimisă în curând către un jurnal ISI, iar din motive de confidenţialitate a rezultatelor cercetării până la publicare, nu putem include detalii în acest raport, urmând ca detaliile să fie incluse în raportul pe anul următor. Dispozitivele cu capabilităţi NFC folosite sunt prezentate în Figura 3.

Figura 3. Dispozitivele cu capabilităţi NFC folosite: telefon mobil, card NFC şi kit embedded de dezvoltare

A3. Asocieri bazate pe date din ecosistem folosind date de la accelerometre

Vehiculele moderne înglobează tot mai multe componente electronice cum ar fi: unități electronice de control, senzori, actuatoare, traductoare etc. Acestea aduc după sine o gamă tot mai variată de comunicații și interacțiuni între pasager și vehicul realizate prin magistrale cablate (CAN, LIN, Flex-Ray), precum și interfețe fără fir (Bluetooth, Wi-fi), dar și între dispozitive electronice inteligente (smart-phones, ceasuri, tablete etc.) şi ecosistemul vehicular dat fiind faptul că oferă un mediu propice pentru a extrage date care îl pot caracteriza. Aceste date pot fi reprezentate de vibrații, sunete, lumină care pe lângă faptul că pot oferi informații despre vehicul, ne pot indica și caracteristici ale șoferului (stil de condus) și chiar ale drumului (drum cu „gropi”), lucru care este confirmat și de numeroase lucrări care tratează următoarele funcționalități cu rol în creșterea siguranței și confortul pasagerului.

- Recunoașterea modului de transport (mașină, tren, autobuz, tramvai) [5]
- Determinarea poziției pasagerului în vehicul [6]

- Aflarea informațiilor despre presiunea din roți [7]
- Monitorizarea performanței suspensiilor vehiculului [8]
- Determinarea comportamentului care caracterizează șoferul [9]

Odată cu evoluția dispozitivelor inteligente, informațiile din mediul vehicular pot fi colectate cu ajutorul senzorilor prezenți în acestea. Studiul de caz din primul an de proiect este axat pe accelerometru care ne oferă informații despre accelerațiile pe cele 3 axe x, y, z. Există însă şi alţi senzori de interes: senzorul de lumină care ne oferă informații despre gradul de luminozitate al mediului ambiental, senzorul de sunet, etc.

Astfel, rezultatele noastre constau în:

- studiul alegerii unui de mediu de colectare a datelor (un traseu scurt care să conțină cât mai multe evenimente cum ar fi: limitatoare de viteză, sensuri giratorii, curbe etc.),
- colectarea acestora,
- construirea de grafice pe baza datelor obținute,
- identificarea evenimentelor pe baza graficelor,
- extragerea unor caracteristici din datele obținute în domeniul timp și frecvență.

După cum se poate vedea în Figura 4 colectarea datelor s-a realizat cu ajutorul a două tipuri de dispozitive și anume suport de fixare a telefonului cu braț şi ventuză pe care l-am fixat pe parbriz și suport de fixare a telefonului de tip anti-alunecare pe care l-am fixat pe bord.

Fig 4. Suporții folosiți pentru colectarea datelor

Dat fiind faptul că, tipul de accelerometru diferă de la un smart-phone la altul, lucru care se poate observa și din datele obținute, am folosit mai multe telefoane pentru a colecta date. Un exemplu de grafic pe un traseu dintr-o parcare bazat pe datele obținute cu un telefon Samsung A3, într-o masină Honda este prezentat în figura 5. De asemenea în figură sunt marcate și cele două evenimente care reprezintă trecerea

peste cele două limitatoare de viteză prezente în traseu. Figura 6 evidențiază cele două evenimente în detaliu.

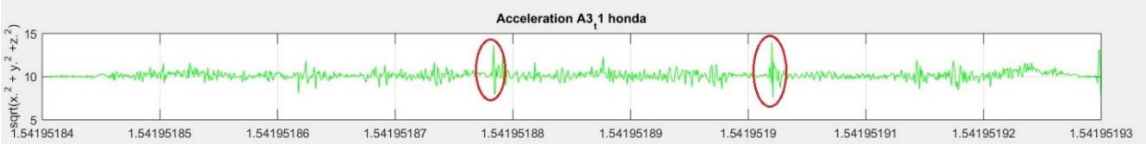

Fig 5. Grafic al datelor de la accelerometru pe un traseu realizat într-o parcare și identificarea evenimentelor din acesta

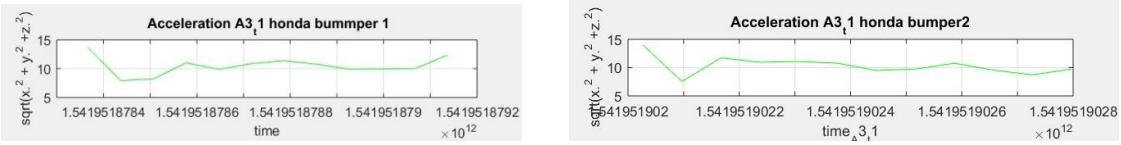

Fig 6. Evenimentele generate de limitatoarele de viteza în detaliu

Odată ce vom analiza datele folosind mai mulți algoritmi de extracție a caracteristicilor și combinarea acestora vom putea completa acest raport mai detaliat. Momentan am demarat lucrul cu algoritmi de inteligenţă artificială pentru clasificarea datelor, algoritmi pe care i-am folosit şi în cadrul celei de a doua lucrări publicate în proiect [2].

Concluzii

Rezultatele din primul an de desfăşurare al proiectului au fost axate pe definirea paşilor din protocolul de securitate, studiul funcționalităților şi al interfețelor de comunicare, a tehnologiei NFC ce va fi utilizată ca interfaţă de comunicare respectiv extragerea datelor din mediu, date care pot fi folosite la asocierea telefon-maşină.

La partea experimentală am reuşit momentan să folosim cu succes cardurile NFC MIFARE DESFire EV1 care vor sta la baza implementării protocolului de securitate pentru accesul la maşină. De asemenea vor fi probabil utilizate şi alte interfeţe precum Bluetooth şi WiFi datorită razei de acoperire mai bune şi a flexibilităţii mai mari la trimiterea pachetelor. Au fost realizate cu succes şi activităţile de colectare a datelor din mediu folosind senzorii de tip accelerometru. Aceste date ne vor permite asocierea dispozitivelor mobile sau chiar identificarea maşinii şi a şoferului ce devin funcţionalităţi de mare relevanţă în interacţiunea telefon-maşină.

În conformitate cu contractul, în primul an de proiect am reuşit să publicăm două lucrări în conferinţe de specialitate [1], [2] respectiv am demarat redactarea a două lucrări destinate jurnalelor. În anul ce urmează vom trimite lucrări către jurnale ISI bazate pe datele experimentale obţinute în acest an, estimăm trimiterea a 2-3 lucrări către jurnale încă din primele luni ale anului 2019. Desigur că vom continua şi cu participări la conferinţe aşa cum am precizat în planul de realizare.

Referinţe

[1] Tudor Andreica, Bogdan Groza, Stefan Murvay, Intrusion detection in Controller Area Networks with Time-covert Cryptographic Authentication, 1st International Workshop on Safety, securiTy, and pRivacy In automotiVe systEms (STRIVE 2018, SAFECOMP 2018 Workshops), Vasteras, Sweeden.

[2] Camil Jichici, Bogdan Groza, Stefan Murvay, Examining the Use of Neural Networks for Intrusion Detection in Controller Area Networks, 11th International Conference on Innovative Security Solutions for Information Technology and Communications, SecITC 2018, Bucharest, Romania, 2018.

[3] NXP, MIFARE DESFire EV1 contactless multi-application IC, Product short data sheet, 2015

[4] Ralph Jacobi, Josh Wyatt, MIFARE DESFire EV1 AES Authentication With TRF7970A, Application Report, 2014

[5] Feng, Tao, and Harry JP Timmermans. "Transportation mode recognition using GPS and accelerometer data." Transportation Research Part C: Emerging Technologies 37 (2013): 118-130.

[6] He, Z., Cao, J., Liu, X., & Tang, S. (2014). Who sits where? Infrastructure-free in-vehicle cooperative positioning via smartphones. Sensors, 14(7), 11605-11628.

[7] Siegel, Joshua, et al. "Smartphone-based vehicular tire pressure and condition monitoring." Proceedings of SAI Intelligent Systems Conference. Springer, Cham, 2016.

[8] Yin, Shen, and Zenghui Huang. "Performance monitoring for vehicle suspension system via fuzzy positivistic C-means clustering based on accelerometer measurements." IEEE/ASME Transactions On Mechatronics 20.5 (2015): 2613-2620.

[9] Singh, Pushpendra, Nikita Juneja, and Shruti Kapoor. "Using mobile phone sensors to detect driving behavior." Proceedings of the 3rd ACM Symposium on Computing for Development. ACM, 2013.