Raport Ştiinţific

Proiect PN-II-RU-TE-2014-4-1501

Securitate criptografică pentru sisteme embedded şi reţele folosite în vehicule

Autori

Conf. Habil. Dr. Ing. Bogdan Groza, Ş.l. Dr. Ing. Pal-Ştefan Murvay,
As. Dr. Ing. Horaţiu Eugen Gurban, Ing. Alexandru Ioan Matei, Ing. Tudor Sebastian Andreica

Universitatea Politehnica Timisoara

Decembrie 2016

Raport Ştiinţific

Proiect PN-II-RU-TE-2014-4-1501

Prezentul raport adresează activitatea ştiinţifică a proiectului PN-II-RU-TE-2014-4-1501, Cryptographic Security for Automotive Embedded Systems and Networks (cSEAMAN) aferentă perioadei 2015-2016. În cele ce urmează prezentăm sintetic rezultatele obţinute, detalii tehnice se găsesc în publicaţiile asociate şi pe pagina web a proiectului.

În conformitate cu propunerea de proiect, în această perioadă, noi am abordat următoarele obiective ştiinţifice:

- *Implementarea funcțiilor criptografice pe dispozitive embedded de clasă automotive (O1)*
- *Proiectare protocoalelor de criptografice pentru rețele cablate din vehicule (O2)*
- *Proiectarea protocoalelor criptografice pentru rețele wireless din vehicule (O3)*

Rezultatele ştiinţifice obţinute în jurul acestor obiective au fost prezentate în lucrări din cadrul unor conferinţe de specialitate şi jurnale din domeniu. Din cele 5 lucrări de conferinţă 4 au fost acceptate şi una este în curs de evaluare, acestea sunt:

- Bogdan Groza, Stefan Murvay, Tudor Andreica, *Designing wireless automotive keys with rights sharing capabilities on the Texas Instruments MSP430 microcontroller*, în curs de evaluare, 2016.

- Bogdan Groza, Stefan Murvay, Tudor Andreica, *Evaluating SRAM as Source for Fingerprints and Randomness on Automotive Grade Controllers*, 13th International Conference on Security and Cryptography (SECRYPT 2016), full paper, 2016.

- Bogdan Groza, Horatiu Gurban, Stefan Murvay, *Designing security for in-vehicle networks: a Body Control Module (BCM) centered viewpoint*, The 2nd International Workshop on Safety and Security of Intelligent Vehicles (SSIV 2016, affiliated to DSN 2016), full paper, 2016.

- Stefan Murvay, Alexandru Matei, Cristina Solomon, Bogdan Groza, *Development of an AUTOSAR Compliant Cryptographic Library on State-of-the-Art Automotive Grade Controllers*, The 11th International Conference on Availability, Reliability and Security (ARES), full paper, 2016.

- Marcela Roxana Farcasescu, *Trust management for vehicular cloud computing*, The 6th International Conference on Cloud Computing and Services Science, Doctoral Consortium (position paper), 2016.

Rezultate din lucrările [1-4] sunt ilustrate în acest raport. Nu în ultimul rând, două rapoarte ştiinţifice (proiecte de diplomă-dizertaţie) au fost susţinute de studenţii cercetători [5-6]. De asemenea există 3 articole înaintate sau în curs de înaintare către jurnale ISI. Finalul raportului referenţiază articolele deja publicate, din motive de confidenţialitate articolele înaintate către jurnale nu sunt citate în acest raport dar sunt disponibile în platforma de raportare şi vor fi disponibile pe site-ul proiectului imediat după decizia editorială. În Octombrie 2015 am prezentat în cardul unei conferinţe internaţionale 1 lucrare ştiinţifică [7] având ca subiect performanţa protocoalelor de securitate pentru magistrale din vehicule (lucrarea nu citează grantul ca sursă de finanţare fiind transmisă cu scurt timp înainte de demararea proiectului, dar prezentarea lucrării în cadrul conferinţei a avut loc pe durata proiectului). În aprilie 2016, directorul de proiect şi-a susţinut teza de abilitare, teză ce se încadrează ca subiect în tema prezentului proiect [8].

În cele ce urmează continuăm cu o descriere a contribuţiilor şi preocupărilor în jurul obiectivelor ştiinţifice din planul de realizare propus, aşa cum în mare parte se regăsesc în articolele ştiinţifice rezultate din proiect.

O1. Implementarea funcțiilor criptografice pe dispozitive embedded de clasă automotive

În cadrul acestui obiectiv în conformitate cu propunerea de proiect am abordat evaluarea capabilităţilor computaţionale ale platformelor embedded de clasă automotive şi analiza securităţii unor primitive criptografice existente în implementări embedded. În ceea ce priveşte evaluarea performanţelor au fost folosite 12 platforme embedded dintre care SP37, S12XDT512, S16ZVH64, MSP430F2274, MPC5606B, TC1782 și TC1797 sunt disponibile în laboratoarele noastre (fiind achiziţionate din proiect sau fiin prezente ca infrastructură de cercetare anterioară).

Ca ţintă de implementare în zona funcţiilor de criptare simetrice am fixat următoarele, aşa cum au fost prezentate în raportul ştiinţific intermediar ca fiind de interes:

- AES ca fiind standardul current în domeniul codurilor bloc şi imposibil de ignorat,
- KATAN32 pentru că este un cod bloc light-weight larg utilizat,

- PRESENT un al cod bloc light-weight, larg utilizat, mai recent decât KATAN32,
- SPECK şi SIMON două coduri bloc ligh-weight propuse de NSA, mult mai eficiente computaţional decât cele anterioare,

Am exclus din aceastea SIMON deoarece acesta a fost construit pentru implementări hardware iar noi adresăm în proiect implementări software. Nu trebuie însă să uităm că ţinta principal în sisteme automotive nu este confidenţitatea informaţiei (realizată prin criptări simetrice) ci autenticitatea adică posibilitatea că într-adevăr informaţia provine de la o anume sursă. Fără autenticitate poarta în faţa unor atacuri prin injecţie de mesaje rămâne deschisă. Din fericire oricare din codurile bloc, inclusive cele mai sus menţionate, poate fi utilizat în construcţii de tip CBC-MAC sau CMAC pentru a asigura autenticitate. Dar, în mod traditional autenticitatea este asigurată prin coduri MAC care e construiesc peste funcţii hash. Pentru aceasta considerăm de interes şi următoarele funcţii hash pentru a fi implementate pe dispozitivele embedded ce le avem ca ţintă:

- MD5 deşi nu poate fi considerat sigur datorită numeroaselor atacuri prin coliziune, reprezintă un baseline pentru cerinţele computaţionale,
- SHA1 şi succesorul său SHA2 care este vechiul standard în funcţii,
- SHA3 care este noul standard ales prin competiţie publică, construit pe candidatul Keccak,
- BLAKE este unul dintre finaliştii SHA3, acesta este cel mai puţin intensive computational, aproape de MD5 la cerinţe, dar mai sigur (cel putin pe moment).

Analiza securităţii a constat în analiza rezistenţei la atacuri side-channel a unei biblioteci existente de clasa embedded, i.e., Mbed TLS, axându-ne pe criptosistemul RSA. De asemenea am fost preocupaţi de analiza securităţii generatoarelor de randomness folosind ca sursă starea memoriei de tip SRAM după reset (subliniem că marea parte a platformelor embedded de clasă automotive, din restricţii de cost, nu deţin generatoare de numere aleatoare, în timp ce starea memoriei SRAM după reset reprezintă sursa de bază pentru extragerea entropiei şi amprentarea device-urilor aşa cum cele mai recente lucrări în domeniu demonstrează).

A.1.1. Biblioteci de functii criptografice pentru platforme folosite in sisteme embedded

La baza protocoalelor criptografice de comunicare stau primitivele criptografice. Pentru a implementa și utiliza astfel de protocoale este necesară implementarea acestor primitive. În aces scop am realizat o bibliotecă de primitive criptografice pe care să se bazeze implementările ulterioare ale protocoalelor de comunicare. Biblioteca, realizată conform celei mai recente specificații de AUTOSAR (AUTomotive Open System ARchitecture), oferă suport pentru următoarele funcții hash și coduri bloc:

MD5, SHA1, SHA256, SHA3-256, AES, Katan, Speck și Present. Implementările au fost realizate pornind de la implementările de referință, de exemplu, RFC1321 pentru MD5, RFC 3174 pentru SHA1, BLAKE2s pentru BLAKE2, KATAN bitsliced pentru Katan și altele adaptate pentru a le face generice și utilizabile pe orice platformă.

Pentru a evalua performanțele microcontrollerelor utilizate în domeniul automotive am selectat o serie de dispozitive care, prin diversitatea caracteristicilor lor, constituie un eșantion semnificativ și cuprinzător. Cele 12 dispozitive alese și caracteristicile lor sunt enumerate în Tabelul 1.

Device	Core	Flash size	RAM size	Frequency	Manufacturer
S08AC128	S08	128KB	8KB	40MHz	NXP(Freescale)
SP37	8051	6B	256B	12MHz	Infineon
S16XDT512	S12(X)	512KB	20KB	80MHz	NXP(Freescale)
S16ZVH64	S12Z	64KB	4KB	64MHz	NXP(Freescale)
RL78/D1A	RL78	512KB	24KB	32MHz	Renesas
MSP430F2274	MSP430	32KB	1KB	16MHz	Texas Instruments
MPC5606B	e200	1MB	80KB	64MHz	NXP(Freescale)
iMX6	Cortex-A9	96KB	128KB	800MHz	NXP(Freescale)
TC1782	TriCore 1.3.1	2.5MB	176KB	180MHz	Infineon
TC1797	TriCore 1.3.1	4MB	176KB	180MHz	Infineon
RH850/F1L	RH850 G3K	2MB	192KB	80MHz	Renesas
RH850/E1x-FCC1	RH850 M3K	4MB	352KB	320MHz	Renesas

Tabel 1 Platformele alese pentru teste conform cu [4]

Pe fiecare din aceste platforme au fost executate primitivele criptografice cu diverşi parametri de intrare, pentru fiecare rulare măsurându-se timpii de execuție. Tabelul 2 ilustrează rezultatele obținute şi publicate de noi în lucrarea [4].

Platform	Input size (bytes)	Cryptographic primitive (block size and key length)								
		MD5 128	SHA1 160	SHA2 256	SHA3 256	Blake2 256	AES 128-128	Katan 32-80	Present 64-128	Speck 128-128
S08	8	34177.88	60201.75	135030.38	1952959.50	81942.25	7481.75	356709.00	94472.63	64011.63
	64	8367.11	15421.53	33319.19	253866.42	10255.02	2688.56	58850.25	85394.72	20599.17
	576	4573.71	8796.18	18295.47	128830.82	9784.00	2377.86	39572.49	84241.97	17213.73
	1536	4277.35	8278.58	17121.74	114808.04	9748.71	2353.54	37437.09	84151.91	16949.87
	4096	4166.21	8084.48	16681.59	110612.63	9735.48	2344.72	37265.64	84118.14	16518.22
	long msgs	4099.53	7968.02	16417.50	106819.63	9727.54	2349.27	37162.77	84097.88	16126.53
S12	8	5052.38	14418.13	31543.63	445194.00	13409.00	3821.13	56714.88	33277.13	9054.75
	64	1205.66	3679.77	7756.36	58188.17	1683.81	1495.81	10254.45	31001.03	2943.23
	576	645.36	2092.81	4247.22	28985.94	1584.79	1373.15	7745.72	30712.00	2463.86
	1536	601.59	1968.65	3973.07	25769.49	1577.28	1363.56	7464.92	30754.53	2426.41
	4096	585.18	1922.15	3870.26	28391.24	1574.46	1359.97	7446.62	30680.96	2412.36
	long msgs	575.33	1894.25	3808.58	31121.57	1572.77	1357.81	7432.13	30675.88	2403.94
S12Z	8	2076.00	8016.00	12864.00	428000.00	9424.00	9824.00	109760.00	44720.00	5936.00
	64	385.50	2070.00	2940.00	54900.00	1204.00	4075.00	16260.00	40050.00	1656.00
	576	156.89	1195.56	1522.22	27888.89	934.44	3827.78	9600.00	39500.00	1288.89
	1536	138.75	1127.08	1412.50	24791.67	914.58	3808.33	8854.17	39416.67	1260.42
	4096	132.03	1101.56	1370.31	23875.00	906.25	3796.88	8812.50	39453.13	1250.00
	long msgs	127.97	1087.50	1345.31	23031.25	901.56	3787.50	8781.25	39468.75	1243.75
RL78 D1A	8	849.75	12274.00	4613.50	461547.87	2876.75	2909.62	40351.12	19021.87	1307.62
	64	182.23	3075.38	1099.17	60454.98	362.22	1063.52	7464.80	17963.34	395.55
	576	87.93	1714.38	587.06	29950.12	284.22	947.78	5985.94	17828.93	323.95
	1536	80.56	1608.05	547.05	26609.24	278.27	938.74	5828.97	17818.43	318.36
	4096	77.80	1568.18	532.05	25595.80	276.04	935.35	5811.54	17814.49	316.26
	long msgs	76.15	1544.26	523.06	24700.48	274.70	933.31	5801.09	17812.13	315.00
TC1782	8	281.25	1102.50	1327.50	117225.00	1399.50	1287.00	10687.50	7863.75	632.25
	64	41.23	271.69	290.81	14821.88	168.75	502.31	1614.38	7228.13	168.47
	576	16.47	151.88	149.84	8015.63	129.69	465.00	962.50	7109.38	128.13
	1536	14.58	142.50	138.75	7183.59	126.80	461.13	888.28	7101.56	124.92
	4096	13.84	139.09	134.91	6952.15	125.68	459.67	883.30	7110.35	123.71
	long msgs	13.43	137.20	132.36	6723.63	124.80	458.79	880.66	7110.35	123.13
TC1797	8	282.60	1113.75	1332.00	117225.00	1401.75	1284.75	10676.25	7751.25	627.75
	64	41.23	271.69	291.38	14821.88	169.31	501.75	1611.56	7059.38	167.91
	576	16.50	151.88	150.63	8015.63	129.84	464.38	962.50	6984.38	127.97
	1536	14.55	142.50	139.69	7183.59	126.80	461.13	888.28	6972.66	124.69
	4096	13.84	138.87	135.57	6952.15	125.68	459.67	883.30	6978.52	123.66
	long msgs	13.41	136.76	133.15	6723.63	124.98	458.79	880.66	6978.52	123.05
MSP430	8	854.13	7284.13	7381.50	N/A	4525.00	3310.25	43154.63	20993.88	3154.63
	64	177.27	1825.91	1779.19	N/A	567.38	1054.02	9180.23	19613.02	993.30
	576	82.92	1020.67	958.44	N/A	467.96	875.49	6706.38	19309.26	824.68
	1536	75.55	957.76	894.32	N/A	460.36	861.64	6426.41	19288.99	811.27
	4096	72.78	934.17	870.27	N/A	457.51	856.39	6408.12	19277.00	806.07
	long msgs	71.13	920.02	855.84	N/A	455.80	853.21	6397.15	19270.41	802.95
MPC5606B	8	403.00	2280.00	2408.00	158800.00	1772.00	2976.00	43154.63	16960.00	844.00
	64	74.13	578.75	563.75	19125.00	224.00	1277.50	4405.00	15850.00	231.75
	576	29.72	329.44	297.78	10041.67	176.11	1215.28	2605.56	15777.78	178.06
	1536	26.25	309.90	277.08	8979.17	172.50	1210.42	2395.83	15750.00	173.96
	4096	24.96	302.73	269.14	8671.88	171.09	1210.94	2390.63	15742.19	172.46
	long msgs	24.18	298.44	264.45	8390.63	170.31	1209.38	2386.72	15742.19	171.48
iMX6	8	1038.51	4582.12	3861.89	276594.12	5228.98	16213.63	124730.10	113939.10	2804.67
	64	201.24	1107.10	883.64	35730.34	660.64	6084.42	81259.20	110448.11	766.11
	576	81.90	605.34	451.47	18310.13	507.73	5488.07	78579.88	110119.63	583.15
	1536	72.88	565.34	417.84	16308.63	493.68	5441.57	78133.33	110055.31	569.43
	4096	69.38	673.24	405.45	15738.47	488.39	5421.07	78013.76	109997.74	563.99
	long msgs	67.27	718.38	397.84	15196.68	485.57	5407.57	77871.30	109989.03	560.22
RH850 G3K	8	295.48	1858.60	1429.36	129263.00	1576.72	2306.24	16128.72	13551.48	559.48
	64	48.78	469.75	321.59	16505.17	201.09	962.78	2507.11	12593.59	159.78
	576	16.34	266.11	163.54	8673.26	145.95	906.92	1531.55	12471.95	127.97
	1536	13.80	250.20	151.19	7757.24	141.71	902.56	1419.99	12462.45	125.49
	4096	12.85	244.24	146.56	7489.74	140.13	900.91	1413.50	12458.89	124.56
	long msgs	12.28	240.66	143.78	7238.03	139.17	899.91	1409.61	12456.75	124.00
RH850 G3M	8	240.24	1134.48	857.60	101158.48	1205.24	1556.72	11818.84	9340.84	400.84
	64	37.72	284.75	187.72	12867.73	150.95	630.70	1732.48	8522.08	114.58
	576	13.71	163.00	95.90	6824.79	122.26	591.69	1025.05	8419.67	93.10
	1536	11.83	153.49	88.74	6110.75	120.04	588.64	943.02	8411.67	91.44
	4096	11.13	149.92	86.05	5903.47	119.23	587.50	939.02	8408.67	90.81
	long msgs	10.70	147.78	84.44	5706.54	118.73	586.81	936.63	8406.88	90.44

Tabel 2 Performante computaționale (cicli/byte) ale platformelor alese, conform cu [4]

Am evaluat de asemenea și consumul de memorie realizat pe fiecare platformă pentru utilizarea fiecărei primitive criptografice din librăria implementată. Conform datelor din Tabelul 3 consumul de

memorie pentru fiecare primitivă (ilustrat atât ca spațiu necesar în memoria Flash pe fiecare platformă cât și ca procent ocupat din totalul memoriei disponibile) este în mare parte din cazuri acceptabil. În unele cazuri mai mult de 10% din memoria Flash este ocupată doar de codul primitivei criptografice, iar în alte cazuri consumul de memorie se situeaza în intervalul 5-10% situație acceptabilă dacă gradul de complexitate a aplicației de pe device este moderat.

Platform	Code size																	
	MD5		SHA1		SHA2 256		SHA3 256		Blake2		AES 128-128		Katan 32-80		Present 64-128		Speck 128-128	
	bytes	%	bytes	%	bytes	%	bytes	%	bytes	%	bytes	%	bytes	%	bytes	%	bytes	%
S08	14120	11.03	1227	0.96	2675	2.09	7005	5.47	5275	4.12	2119	1.66	3185	2.49	4113	3.21	4918	3.84
S12	5528	1.08	1042	0.20	2251	0.44	4021	0.79	3455	0.67	1692	0.33	2741	0.54	2186	0.43	2596	0.51
S12Z	5374	8.40	902	1.41	2081	3.25	4922	7.69	4828	7.54	2688	4.20	2761	4.31	4252	6.64	3659	5.72
MSP430	6394	19.98	1338	4.18	2610	8.16	5384	16.83	4046	12.64	1810	5.66	2628	8.21	1776	5.55	1376	4.30
RL78 D1A	8606	1.68	1137	0.22	2304	0.45	5436	1.06	3606	0.70	2611	0.51	3005	0.59	2247	0.44	1309	0.26
TC1782	2856	0.11	730	0.03	1360	0.05	3924	0.16	2634	0.11	1682	0.07	2004	0.08	3080	0.12	1396	0.06
TC1797	2856	0.07	730	0.02	1360	0.03	3924	0.10	2634	0.07	1682	0.04	2004	0.05	3080	0.08	1396	0.03
MPC5606B	3998	0.40	880	0.09	1730	0.17	5916	0.59	3244	0.32	2258	0.23	2518	0.25	3720	0.37	3324	0.33
iMX6	7688	8.01	1516	1.58	2820	2.94	11296	11.77	4628	4.82	5428	5.65	3552	3.70	7756	8.08	5040	5.25
RH850 G3K	2216	0.11	734	0.04	1194	0.06	4464	0.22	2082	0.10	2528	0.13	2182	0.11	2842	0.14	746	0.04
RH850 G3M	2216	0.06	734	0.02	1194	0.03	4464	0.11	2082	0.05	2528	0.06	2182	0.05	2842	0.07	746	0.02

Tabel 3 Consum de memorie pentru primitivele implementate, conform cu [4]

Din cauza constrângerilor de spațiu pe platforma SP37 s-au putut implementa doar Present și Speck motiv pentru care acest dispozitiv nu apare in tabelele anterioare fiind tratat separat.

În urma analizei datelor experimentale a reieșit faptul că mare parte din dispozitivele automotive utilizate în automobilele moderne pot suporta implementarea unor mecanisme de securitate, constrângerile venind, după cum era de așteptat, din partea dispozitivelor limitate ca memorie și viteză de calcul.

A.1.2.1. Analiza securității primitivelor criptografice pe platforme embedded automotive

Criptanaliza presupune exploatarea slăbiciunilor teoretice ale algoritmilor, dar aceste proprietăți sunt de cele mai multe ori bine studiate şi algoritmi nu ajung în implementări practice dacă sunt vulnerabili. În contrast cu aceasta, analiza side-channel țintește implementarea fizică a criptosistemului, sunt specifice sistemelor embedded, şi se bazează pe caracteristici fizice ale rulării: timp ce calcul, consum de putere, etc. Atacurile side-channel necesită cunoașterea comportamentului intern al sistemului pe care se face analiza dar şi modul de implementare al algorimtului (acesta este în general public, iar în caz contrar poate fi aflat prin reverse-engineering).

Sistemul pe care s-au făcut măsurătorile este STM32F7 discovery, produs de către firma STMicro, care are la bază microcontrolerul STM32F746NG care are ca aplicații: sisteme de control, echipament medical, aplicații mobile, Internet of Things și multe altele. Acest microcontroler nu dispune de mecanisme de accelerare criptografică, studiul având ca țintă implementarea sistemului de criptare asimetrică RSA

inclusă în cunoscuta bibliotecă livrată de ARM sub denumirea Mbed TLS (versiunea 2.2.1). Tipul de atac studiat a fost bazat pe măsurarea duratei transformărilor criptografice.

Primul scenariu de atac a fost exploatarea posibilităţii de a distinge între 2 chei diferite de semnare (key indistinguishability). Aceasta presupune că pentru oricare două perechi de chei, cheie publică – cheie privată, cu exponenţi de decriptare E1 și E2, cu condiția ca E1 să fie diferite de E2, se urmărește ca durata globală a operațiunii de semnare cu cele două perechi de chei să fie de asemenea diferită pentru oricâte repetări sau indiferent de mesaj. Pentru a testa acest scenariu am generat două chei cu dimensiunea de 2048 de biți și am urmărit durata a 1000 de operațiuni de semnare cu RSA folosind un periferic de tip timer setat la o rezoluție de 1 microsecunda. Pentru două chei aleatoare am obținut timpii din Figura 1 care arată că este posibil a face distincția între cele 2 chei.

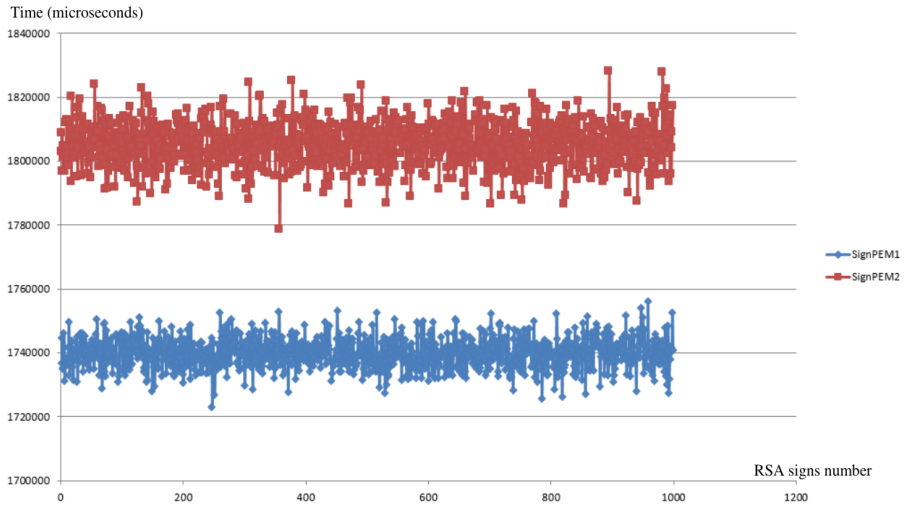

Figura 1. Timpii de semnare cu RSA pentru cele două perechi de chei diferite (E1 și E2) conform cu [6]

Atacul anterior nu este un atac cu consecinţe grave. Pentru care am urmărit un al doilea scenariu care recuperearea completă a chei secrete (exponentul privat) pe baza timpului de decriptare (la sistemul RSA exponentul de decriptare este acelasi cu exponentul de semnare, deci adresăm aceeaşi parte a cheii cu scenariul anterior). Am considerat o cheie privata de bază și o serie de chei private care împart începând de la 1 până la 255 din 256 de octeți cu cheia de bază (cheia considerată are 2048 de biţi). Măsurând timpii de decriptare se dorește ca modulul diferenței de timp dintre cheia de bază și cheia cu octeți comuni să aibă o dependență corelată cu numărul octeți comuni. Pentru acest al doilea scenariu, se poate observa din Figura 2, că deși cheia cu 255 de octeți comuni este foarte apropiată de cheia de bază nu avem o corelaţie între timp și numărul de octeți comuni cu cheia de bază.

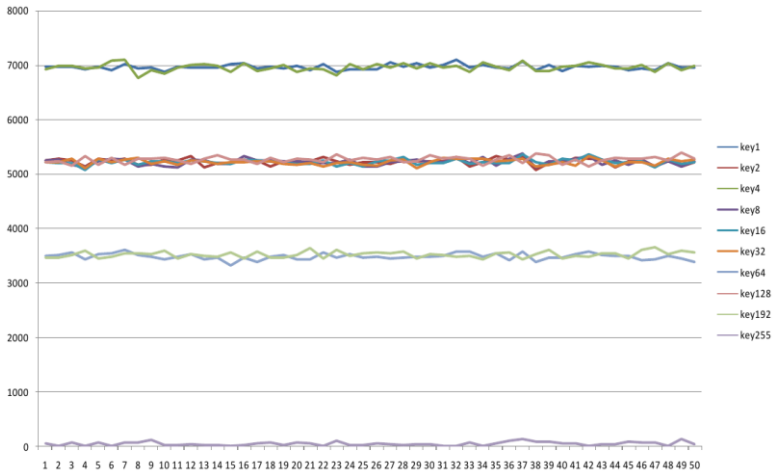

Figura 2. Modulul diferenței dintre timpul de decriptare cu cheia de bază şi timpul de decriptare cu cheile candidat care împart octeți cu cheia de bază conform cu [6]

Concluzia studiului este că sistemul incorporat STM32F746NG împreună cu biblioteca de funcții criptografice Mbed TLS 2.2.1 oferă securitate satisfăcătoare la atacurile side-channel bazate pe analiza timpului pentru criptosistemul RSA. Am reuşit doar să demonstrăm că putem face distincţia între două chei dar nu putem recupera cheia de decriptare. Varianta extinsă a acestor rezultate este în lucrare de dizertaţie [6] a studentului încadrat în proiect ca asistent de cercetare.

O preocupare de maximă importanţă în cadrul acestui obiectiv a fost obţinerea de numere aleatoare pe platforme embedded. Justificare pentru această preocupare este cât se poate de simplă: fără randomness nu avem chei secrete suficient de sigur şi deci implementarea mecanismelor de securitate nu este posibilă. În lucrarea [2] am evaluat calitatea SRAM-ului ca sursă de generare de entropie şi amprentare fizică a device-urilor. Subliniem că în contextul în care nu există o abordare unitară în implementarea generatoarelor de numere aleatoare pe sistemele de clasă embedded, respectiv în contextul în care acestea sunt absente pe marea parte a platformelor embedded, strea după reset a memoriei SRAM reprezintă sursa cea mai de încredere. În Figura 3 am sugerat câteva zone şi direcţii de aplicare ce sunt explicitate în lucrarea [2]: generarea de numere aleatoare, amprentarea ECU-urilor, generarea cheilor unice pe un dispozitiv embedded.

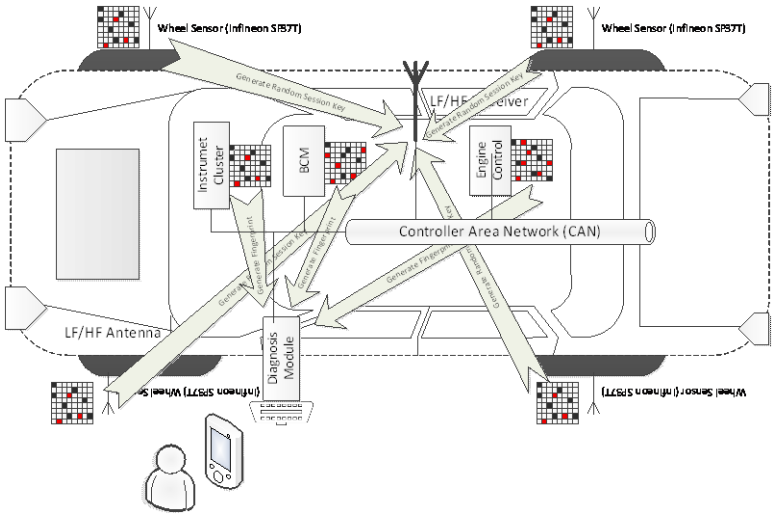

Figura 3. Aplicaţii posibile folosind starea memoriei SRAM: generarea de numere aleatoare, amprentarea ECU-urilor, generarea cheilor unice pe un dispozitiv embedded discutate în [2]

Analiza prezentată în [2] a avut ca target 9 platforme embedded specifice domeniului automotive: SP37, MC9S12C128, MC9S12DT256, MC9S12XDP512, MSP430F2274, RL78/F14, Renesas, TC1782, TC1797. Metricile folosite în evaluare au constat în distanţa Hamming intra şi inter dispozitiv, probabilitatea de guessing a unei locaţii şi entropia minimă ce decurge din aceasta, respectiv distanţa Hamming a valorilor extreme şi a celulelor alăturate.

Pe baza analizei efectuate am concluzionat că marea parte a memorilor SRAM furnizează suficientă entropie, approx. 0.5 bit/byte, rezultat conform cu alte rezultate menţionate în literatura de specialitate. O excepţie, unde entropia a fost apropiată de 0, au fost memorile de pe controllerul Infineon TC1782 unde suspectăm că memoria de tip ECC este cauza lipsei de de entropie şi controllerul MSP430 unde suspectăm că interferenţe cu debuggerul au dus la o pierdere semnificativă de entropie. În Figura 4 prezentăm o mapare de memorie sugestivă pentru acestea. Detalii se găsesc în lucrarea [2].

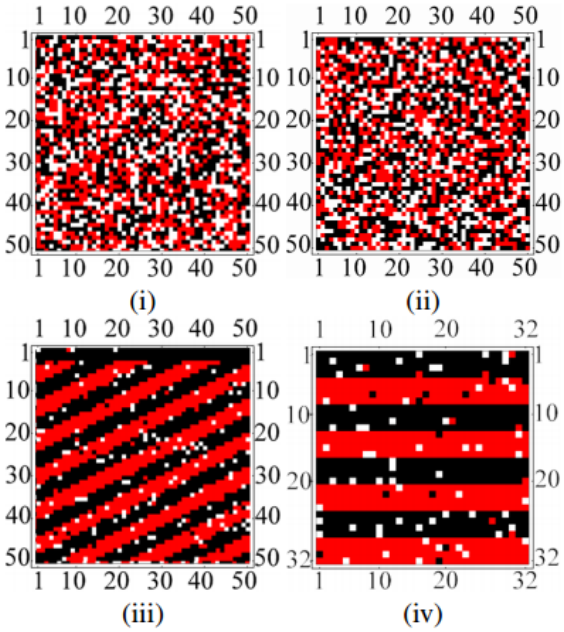

Figura 4. Distribuţia aleatoare a biţilor în memoria MC9S12XDP512 (i) şi TC1797 (ii) respectiv non-aleatoare în memoria TC1782 (iii) şi MSP430F2274 (iv) (semnificaţia culoarilor: alb bit fluctuant 0-1, negru bit dominant 0, alb bit domninant 1) conform cu lucrarea [2]

O2. Proiectare protocoalelor de criptografice pentru rețele cablate din vehicule

Vehiculele moderne includ un număr tot mai mare de subsisteme și funcționalități implementate utilizând zeci de ECU-uri. Aceste subsistemele pot fi grupate în următoarele categorii (Figura 5): i) subsisteme pentru habitaclu (**body**) - responsabile pentru diverse funcționalități legate de acces securizat, geamuri, uși, oglinzi retrovizoare, interfața de diagnosticare, încălzire ventilație și aer condiționat (HVAC), etc. ii) subsisteme pentru șasiu (**chassis**) - responsabile de subsistemul de frânare, controlul stabilității, a direcției, funcționalități legate de siguranță în conducerea vehiculului, subsistemele de asistență a șoferului (ADAS) etc. iii) subsisteme pentru propulsie și transmisie (**powertrain and transmission**), între acestea regasindu-se și subsistemele responsabile cu aprindere, controlul tracțiunii precum și cele folosite pentru a îmbunătăți economia de combustibil, reduce emisiile de CO_2, etc. iv) subsisteme telematice, de navigație și informare (**infotainment and telematics**). Aceste subsisteme sunt responsabile pentru o experiență de utilizare cât mai plăcută, furnizând conținut multimedia, oferind conectivitate cu dispozitive portabile, de exemplu, telefon mobil, tablete, etc. De asemenea, faciliteaza diagnosticarea vehiculului de la distanță, prin intermediul tehnologiilor de telecomunicații mobile, de exemplu, 4G.

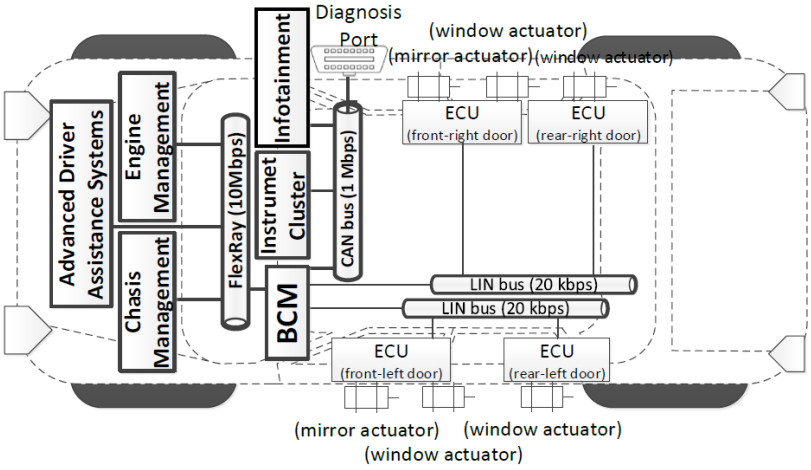

Figura 5. Model de arhitectură de rețea generică reprezentativă pentru autovehiculele moderne conform cu [3]

Intuiția ar sugera că atacurile legate de șasiu, propulsie și transmisie au un impact mai mare, însă aceste sisteme sunt mai usor de izolat spre deosebire de subsistemele pentru habitaclu. Cel mai important ECU în cazul acestei rețele este modulul BCM (Body Control Module). Raționamentul din spatele alegerii acestui modul pentru studiul nostru, are la bază cel puțin trei factori cheie: i) un număr mare de componente care sunt conectate direct la BCM au fost ținta unor atacuri (imobilizator electronic, senzori de presiune în pneuri - TPMS, interfețe de diagnoza, etc), ii) prin proiectarea, componentele caroseriei sunt în general expuse și este rezonabil a presupune că adversarii vor avea în mod frecvent acces la modulele periferice controlate de BCM, iii) BCM controlează subsistemele atractive atât din punct de vedere economic (de exemplu, accesul la mașină), sau dintr-o perspectivă a siguranței (de exemplu, centuri de siguranță, faruri, etc).

În primul rând noi am realizat o analiză a riscurilor bazându-ne pe atacurile raportate în literatura de specialitate. Riscul a fost evaluat pe baza a două componente: impactul amenințării și dificultatea în realizarea atacului. Impactul este obținut prin ponderarea a patru termeni care analizează: siguranța ocupanților vehiculului precum și a celorlalți participanți la trafic, costul asociat prejudiciului, confidențialitate precum și aspecte operaționale pentru a evalua modificarea comportamentului autovehiculului. Detalii se găsesc în lucrarea [3].

Dificultatea realizării unui atac este obținut prin ponderarea a cinci termeni care analizează: timpul necesar pentru a identifica o vulnerabilitate, nivelul de cunoștințe necesare pentru a realiza atacul, necesitatea obținerii de informații confidențiale, nivelul constrângerile de timp precum și costul echipamentelor.

În Tabelul 4 prezentăm un set restrâns de de atacuri, indicele de impact și dificultate precum și riscul asociat fiecarui tip de atac, tabelul complet conținând toate atacurile studiate se regasește în [3].

Sistem ţintă	Atac	Acces	Impact					Dificultate							
			I_{Sf}	I_{Fin}	I_{Prv}	I_{Op}	$\mathbb{I}$	D_T	D_{Ex}	D_{In}	D_W	D_{Eqp}	$\mathbb{D}$	$\mathbb{R}$
Geamuri acţionate electric	Deschidere ferestre (simulare CANoe) [11]	CAN	3	0	2	2	**36**	0	2	1	0	2	**14**	**2.57**
	DoS - pentru fiecare comandă transmite mesaj de comandă cu acţiune opusă [12]	CAN	3	0	2	2	**36**	1	2	1	0	2	**15**	**2.40**
	Dezactivare relee geamuri [17]	OBD	3	0	2	2	**36**	0	2	1	0	2	**14**	**2.57**
Ştergatoare parbriz	Activare ştergătoarele în mod continuu [17]	OBD	0	0	0	2	**4**	0	2	1	0	2	**14**	**0.29**
	Activare pompa lichid de parbriz în mod continuu [17]	OBD	0	0	0	2	**4**	0	2	1	0	2	**14**	**0.29**
	Dezactivare ştergătoarele & activare pompa lichid de parbriz în mod continuu [17]	OBD	3	0	0	4	**32**	0	2	1	0	2	**14**	**2.29**
Lumini exterior	Oprirea tuturor luminilor (frână şi auxiliare)[17]	OBD	3	0	4	4	**48**	0	2	1	0	2	**14**	**3.43**
	Oprirea luminilor auxiliare [17]	OBD	3	0	4	4	**48**	0	2	1	0	2	**14**	**3.43**
	Dezactivare faruri dacă controlul automat al farurilor e activat [17]	OBD	3	0	4	4	**48**	0	2	1	0	2	**14**	**3.43**
	Aprindere/stingere faruri dacă controlul automat al farurilor e activat [21]	OBD Diag	3	0	4	4	**48**	0	2	1	0	2	**14**	**3.43**
Lumini interior	Control lumini habitaclu [17]	OBD	3	0	4	2	**44**	0	2	1	0	2	**14**	**3.14**
Hayon	Deschidere hayon [17]	OBD	0	0	2	2	**12**	0	2	1	0	2	**14**	**0.86**
Uşi	Deblocare uşă (în mers) [17]	OBD	3	0	0	2	**28**	0	2	1	0	2	**14**	**2.00**
	Blocare/deblocare uşi [17]	OBD	3	0	2	2	**36**	0	2	1	0	2	**14**	**2.57**
	Activare releu uşă în mod continuu [17]	OBD	3	0	2	2	**36**	0	2	1	0	2	**14**	**2.57**
	Blocare/deblocare uşi în mers [21]	OBD Diag	3	0	0	2	**28**	0	2	1	0	2	**14**	**2.00**
Claxon	Activare permanentă [17]	OBD	0	0	0	2	**4**	0	2	1	0	2	**14**	**0.29**
	Modificare frecvenţă [17]	OBD	0	0	0	2	**4**	0	2	1	0	2	**14**	**0.29**
	Pornire/oprire claxon [21]	OBD Diag	0	0	0	2	**4**	0	2	1	0	2	**14**	**0.29**

Tabel 4 Risc calculat pentru o serie de atacuri conform cu [3]

În urma analizării acestor atacuri am concluzionat că cel mai mare risc este dat de atacurile care dezactivează anumite subsisteme ale mașinii, în special atunci când acest lucru se face de la distanță. Prin urmare, pledăm pentru utilizarea următoarelor trei tipuri de contramăsuri, modelul de securitate propus fiind prezentat în Figura 6:

A. Funcționalități standard de firewall. În cazul în care arhitectura existentă conține funcționalități care pot afecta altele componente, accesul la acestea ar trebui acordat numai prin intermediul unor mecanisme adecvate de autorizare și autentificare.

B. Protocoalele utilizate de către toate ECU-urile care implementează funcționalităţi critice pentru siguranță trebuie să fie protejate prin protocoale criptografice de autentificare.

C. Redundanța, separarea fizică și tamperproofing trebuie să fie luate în considerare în cazul în care nu este posibil să se utilizeze firewall-uri sau mecanisme de autentificare. În acest caz se încadrează senzorii și actuatoarele precum și ECU-urile conectate la magistrale LIN.

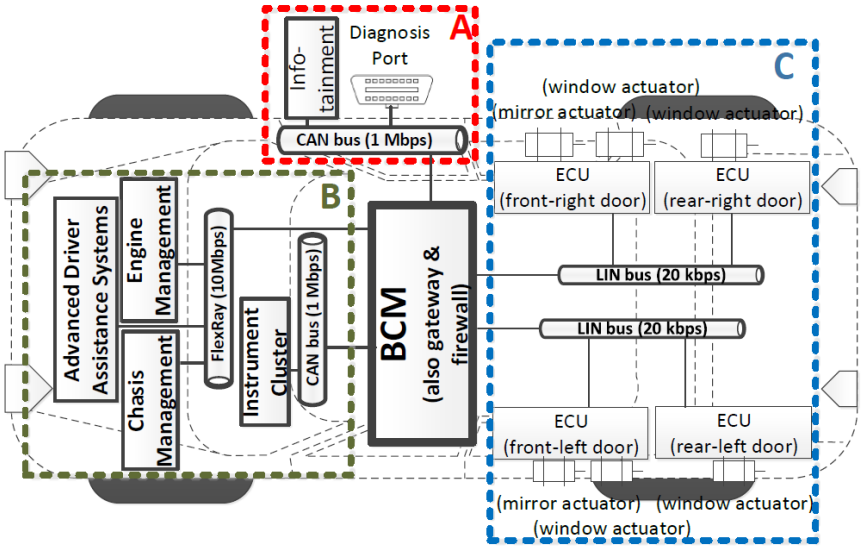

Figura 6. Modelul de securitate propus conform cu [3]

A.2.1. Realizarea de simulari ale unor protocoale de securitate criptografica in sisteme embedded folosind instrumente dedicate, e.g., CANoe

Pentru simularea unei rețele intra-vehiculare reale am ales ca studiu de caz vehiculele comerciale. Acestea folosesc pentru comunicare protocolul SAE J1939, protocol situat le nivelul aplicației având ca nivel fizic protocolul CAN. Ca mediu de lucru pentru simulare am folosit CANoe pornind de la simularea demonstrativă a subsistemului de propulsie bazată pe protocolul J1939. Simularea reprezintă o rețea CAN, ilustrată și în Figura 7, cu 6 noduri, fiecare dedicat unei funcționalități importante: controlul motorului, al transmisiei și al sistemului de frânare, monitorizarea presiunii în pneuri, instrumentul de bord și nodul gateway.

Pornind de la această simulare, am analizat în primă fază limitările protocolului J1939 care pot facilita realizarea unor atacuri asupra rețelei folosind nivelul aplicație. Am identificat astfel o serie de atacuri de tip DoS (Denial of Services) și DDoS (Distributed DoS): blocarea alocării de adrese pentru anumite noduri, creșterea încărcării pe bus prin cereri frecvente de adresă, întreruperea protocolului de transport și excluderea din seturi de lucru.

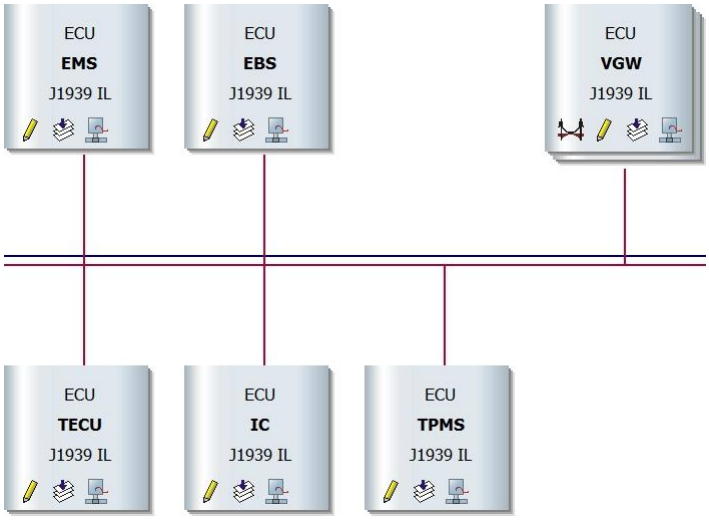

Figura 7. Topologia rețelei simulate

Pentru a introduce securitate în comunicarea într-un astfel de sistem am propus utilizarea unui mecanism de autentificare bazat pe o infrastructură cu cheie publică. Procesul presupune 4 etape:

- producătorul principal implementează module responsabile cu securitatea
- producătorul principal distribuie certificate către producătorii subcontractați
- aceste certificate sunt integrate și atribuite în mod unic fiecărui modul electronic produs
- în cadrul vehiculului are lor comunicarea autentificată cu inițializare bazată pe infrastructura cu cheie publică

Am extins simularea pentru a evalua influența introducerii unui astfel de mecanism asupra comunicării pe bus. Având în vedere intențiile curente ale industriei de actualiza specificația protocolului J1939 pentru a suporta comunicarea folosind CAN-FD ca suport fizic, am implementat frame-urile de autentificare ca frame-uri specifice CAN-FD. Astfel pentru fiecare frame de date transmis pe bus, se transmite și un frame de autentificare ce conține ID-ul mesajului autentificat, tag-ul de autentificare, ștampila de timp și un counter.

Statisticile obținute în urma rulării simulării arată că încărcarea busului crește de la ~20% la 38.3% în urma introducerii mecanismului de autentificare pentru tot traficul, în condițiile în care se migreaza spre utilizarea CAN-FD. Pentru utilizarea standardului CAN și pentru transmisia informației de autentificare încărcarea pe bus ar crește mai aproape de limita de 100% făcând posibilă pierderea sau întârzierea unor mesaje.

Rezultatele extinse sunt subiect al unei lucrări înaintate către un jurnal ISI ce va fi facută disponibilă pe site-ul proiectului imediat după decizia editorială.

A.2.2. Implementarea unui protocol de comunicare pe un sistem embedded in scopul obtinerii unor rezultate experimentale

În cadrul acestei activităţi ne-am concentrat în particular pe implementare de module componente ale unui gateway cu funcții de detecție a intruziunii (IDS – Intrusion Detection System). Sistemul conține următoarele componente (Fig. 8, 9): *i)* PC, folosit pentru simularea unor sisteme embedded dintr-un autovehicul, *ii)* sistem embedded cu interfațare CAN Low speed și CAN High speed, care implementează funcții de gateway și sistem de detecție a intruziunii, *ii)* tablou de bord (Instrument Cluster) PSA produs și pus la dispoziție de firma Yazaki.

Pentru realizarea unei simulari cât mai realiste a fost utilizată o bază de date conținând mesaje CAN specifice modelului de autovehicul în a cărui echipare există acest tablou de bord. Transmisia mesajelor CAN a fost realizată utilizând software-ul Vector CANalyzer precum și modulele hardware Vector CANcardXL și CANcab251 mag. Pentru transmiterea mesajelor pe CAN a fost utilizat modulul IG (interactiv generator) din CANalyzer, valorile semnalelor fiind modificate pentru a fi în conformitate cu specificațiile primite de la producătorul tabloului de bord.

Modulul IDS & Gateway a fost implementat pe o placă de dezvoltare NXP LFEBS12UB echipată cu un microcontroller MC9S12DG128. Aceasta placă de devoltare conține două tranceivere de CAN TJA1040T dar datorita faptului ca s-a dorit interconectarea unei magistrale CAN High speed cu o magistrală CAN Low speed a fost utilizat și un tranceiver NXP TJA1055T/C care a fost lipit pe partea de prototipare a unei plăci de dezvoltare.

Mesajele transmise pe Low speed CAN sunt retransmise pe High speed CAN și invers. Au fost implementate și funcții de firewall, mesajele CAN considerate valide pentru magistrala Low/High speed CAN sunt retransmise pe magistrala High/Low speed CAN. Deasemenea este verificată periodicitatea mesajelor CAN, în cazul în care mesajele periodice trimise pe cele doua magistrale nu respectă periodicitatea descrisă în specificații aceste mesaje nu vor fi retransmise.

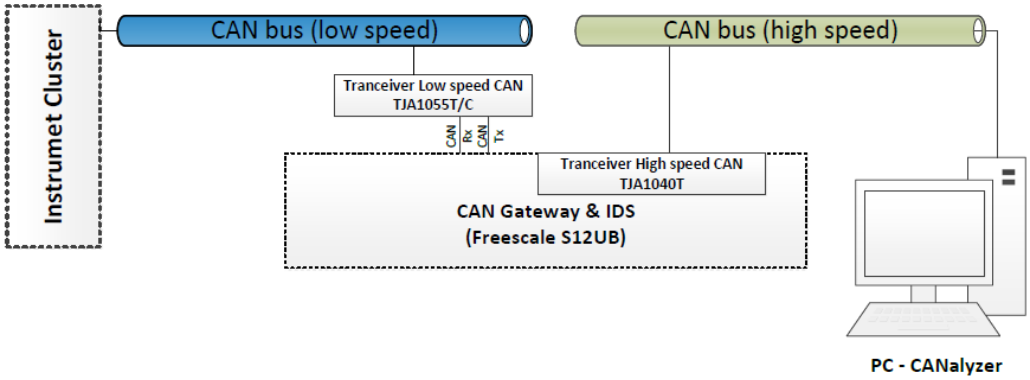

Figura 8. Arhitectura sistemului embedded

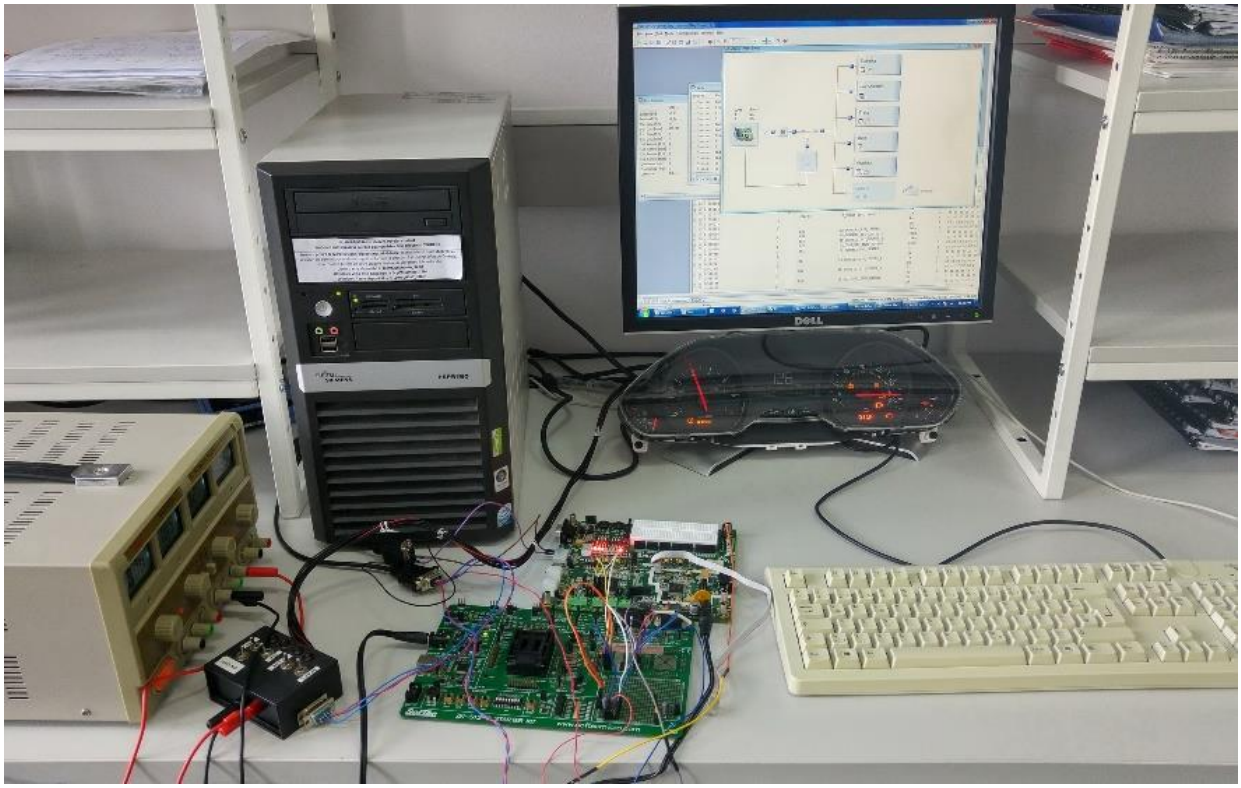

Figura 9. Stand experimental utilizat în cadrul proiectului

O3. Proiectarea protocoalelor criptografice pentru reţele wireless din vehicule

A.3.1. Implementarea de protocoale criptografice pentru retele wireles

În cadrul acestui obiectiv ne-am axat actitivităţiile pe microprocesorul MSP430 de la Texas Instrument. Pentru implementarea protocoalelor criptografice pentru chei de acces wireless pe platforma MSP430 s-a folosit instrumentul de dezvoltare eZ430-RF2500. Acest instrument conţine un microcontroller MSP430F2274 şi un transceiver radio-frecvenţă CC2500 2.4-GHz.

Protocolul care a fost implementat pe doua plăci MSP430 a plecat de la ideea posibilităţii înlocuirii cheii clasice de maşină cu un telefon inteligent care să aibe ataşat un dispozitiv pentru emiterea comenzilor către maşină. Schimbul de mesaje între cele două plăci au scopul de a asocia două dispozitive folosind o cheie master. Protocolul impune ca cele două părţi sa conţină o cheie master comună, care este folosită periodic pentru a genera şi a împărtăşi chei de sesiune. O cheie de sesiune poate fi folosită un anumit interval de timp sau de un anumit număr de ori iar apoi trebuie schimbată. Proceseul de asociere a două dispozitive

se executa în trei paşi. Primul pas constă din trimiterea unui mesaj a dispozitivului care doreşte să iniţieze asocierea. Acest mesaj conţine ID-ul dispozitivului şi o valoare aleatorie, criptate folosind cheia master. Destinatarul primului mesaj, decriptează informaţia primită, stochează valoare aleatorie şi ID-ul dispozitivului emitent şi răspunde cu un nou mesaj. Acest mesaj este format din ID-ul şi valoare aleatorie primite de la primul dispozitiv şi o nouă valoarea aleatorie. Folosind cheia master, primul dispozitiv decriptează mesajul şi pregăteşte ultimul mesaj. Acesta conţine aceeaşi informaţie ca mesajul precedent, dar diferenţa este că două dintre componentele mesajului sunt criptate cu noua cheie de sesiune iar cea de a treia componenta nu este criptata. Dispozitivul destinatar foloseşte datele trimise anterior pentru a descoperi noua cheie de sesiune. Urmatoarele mesaje, care conţin informaţii de comandă, sunt criptate şi decriptate cu cheia de sesiune.

Protocolul şi mesajele folosite sunt descrise în Figura 10. Parte din rezultate sunt prezentate în lucrare de diplomă [5] a studentului asistent cercetare iar rezultate ştiinţifice în jurul acestei teme se găsesc publicate în lucrarea [1].

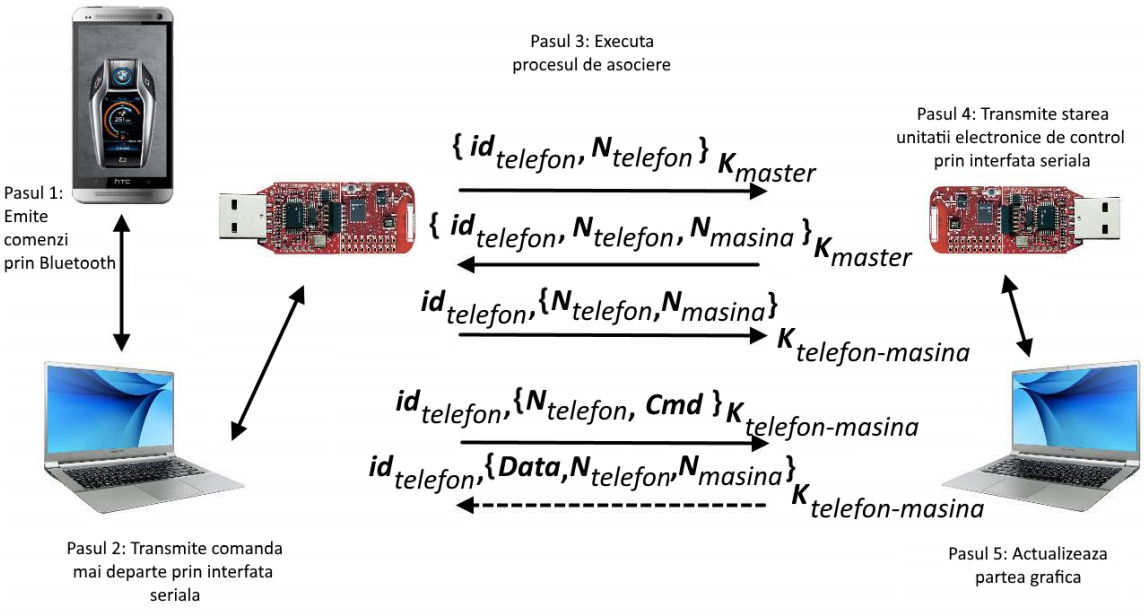

Figura 10. Topologia rețelei simulate, conform cu [5]

4. Concluzii

Rezultatele noastre ştiinţifice demonstrează fezabilitatea implementărilor criptografice pe platforme embedded de clasă automotive cu scopul folosirii în reţele wireless sau cablate. Aşa cum lucrări recente demonstrează securitatea criptografică pentru sisteme automotives este o zonă critică care necesită preocupări de cercetare din ce în ce mai intense. De asemenea, prin lucrările publicate am adus rezultate noi în implementarea funcţiilor criptografice pe sisteme embedded (obiectivul O1), designul protocoalelor pentru reţele cablate (obiectivul O2) şi designul protocoalelor criptografice pentru reţele wireless (obiectivul O3). La finalul celei de a doua etape echipa a cumulat 6 articole trimise către conferinţe (5 fiind deja acceptate, prezentate şi publicate iar 1 în curs de evaluare) şi 3 articole trimise sau în curs de trimitere către jurnale. Considerăm că suntem la zi cu planul ştiinţific de realizare al proiectului şi în etapa finală vom închia cu succes toate obiectivele propuse completând lista de publicaţii ştiinţifice asociate proiectului.

Referinţe

[1] Bogdan Groza, Stefan Murvay, Tudor Andreica, Designing wireless automotive keys with rights sharing capabilities on the Texas Instruments MSP430 microcontroller, under submission, 2016.

[2] Bogdan Groza, Stefan Murvay, Tudor Andreica, Evaluating SRAM as Source for Fingerprints and Randomness on Automotive Grade Controllers, 13th International Conference on Security and Cryptography (SECRYPT 2016), full paper, 2016.

[3] Bogdan Groza, Horatiu Gurban, Stefan Murvay, Designing security for in-vehicle networks: a Body Control Module (BCM) centered viewpoint, The 2nd International Workshop on Safety and Security of Intelligent Vehicles (SSIV 2016, affiliated to DSN 2016), full paper, 2016.

[4] Stefan Murvay, Alexandru Matei, Cristina Solomon, Bogdan Groza, Development of an AUTOSAR Compliant Cryptographic Library on State-of-the-Art Automotive Grade Controllers, The 11th International Conference on Availability, Reliability and Security (ARES), full paper, 2016.

[5] Tudor Andreica, Bachelor Thesis, *Secure RF Automotive Keys based on randomness and patterns extracted from SRAM*, Universitatea Politehnica Timişoara, Advisor: Bogdan Groza, June, 2016.

[6] Alexandru Matei, MsC Thesis, *Development of an AUTOSAR compliant cryptographic toolkit and timing analysis for an RSA implementation on automotive/industrial grade controllers*, Universitatea Politehnica Timişoara, Advisor: Bogdan Groza, June, 2016.

[7] Vasile, Paula, Bogdan Groza, and Stefan Murvay. *Performance analysis of broadcast authentication protocols on CAN-FD and FlexRay*. Proceedings of the WESS'15: Workshop on Embedded Systems Security. ACM, 2015.

[8] Bogdan Groza, Teza abilitare: *Cryptographic Security for Automotive Embedded Devices and Networks*, Universitatea Politehnica Timişoara, 2016.