



VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

ELEKTRONIKOS FAKULTETAS

KOMPIUTERIŲ INŽINERIJOS KATEDRA

Povilas Šiaudinis

**AUTOMOBILIŲ RAKTŲ SISTEMŲ TYRIMAS, PANAUDOJANT
PROGRAMĄ „SOFTWARE DEFINED RADIO“**
CARS KEYS SYSTEM RESEARCH USING „SOFTWARE DEFINED RADIO“

Baigiamasis magistro darbas

Kompiuterių inžinerijos studijų programa, valstybinis kodas 621H69001

Kompiuterių technologijų specializacija

Elektronikos inžinerijos studijų kryptis

Vilnius, 2014

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

ELEKTRONIKOS FAKULTETAS

KOMPIUTERIŲ INŽINERIJOS KATEDRA

TVIRTINU
Katedros vedėjas

(parašas)

Algirdas Baškys

(Vardas, pavardė)

(Data)

Povilas Šiaudinis

**AUTOMOBILIŲ RAKTŲ SISTEMŲ TYRIMAS, PANAUDOJANT
PROGRAMĄ „SOFTWARE DEFINED RADIO“**
CARS KEYS SYSTEM RESEARCH USING „SOFTWARE DEFINED RADIO“

Baigiamasis magistro darbas

Kompiuterių inžinerijos studijų programa, valstybinis kodas 621H69001

Kompiuterių technologijų specializacija

Elektronikos inžinerijos studijų kryptis

Vadovas

(Moksl. laipsnis, vardas, pavardė)

(Parašas)

(Data)

Lietuvių kalbos konsultantas

Dr. Vaida Buivydienė

(Moksl. laipsnis, vardas, pavardė)

(Parašas)

2014-06-

(Data)

Vilnius, 2014

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS
ELEKTRONIKOS FAKULTETAS
KOMPIUTERIŲ INŽINERIJOS KATEDRA

MAGISTRANTŪROS STUDIJŲ BAIGIAMOJO DARBO UŽDUOTIS

Elektronikos fakultetas
Kompiuterių inžinerijos katedra
Technikos mokslų sritis
Elektros ir elektronikos inžinerijos mokslo kryptis
Elektronikos inžinerijos studijų kryptis
Kompiuterių inžinerijos studijų programa
Kompiuterių technologijų specializacija

TVIRTINU

Kompiuterių inžinerijos katedros vedėjas
prof. Algirdas Baškys _____

2014 m. _____ sausio mėn. _____ d.

Studentui (ei) _____

Povilui Šiaudiniui

(vardas, pavardė)

Baigiamojo darbo tema: **Automobilių raktų sistemų tyrimas**

panaudojant programą „Software defined radio“

(lietuvių kalba)

Cars keys system research using “Software defined radio”

(anglų kalba)

Patvirtinta 201 _____ m. _____ mėn. _____ d. dekanų įsakymu Nr. _____

Baigiamojo darbo užbaigimo terminas 2014m. _____ mėn. _____ d.

Darbo tikslas: Ištirti automobilių naudojamas nuotolinio rakto sistemas panaudojant programuojamą radijo ryšį „SDR“. Išanalizuoti rakto perduodamus signalus.

BAIGIAMOJO DARBO UŽDUOTIS:

1. Išanalizuoti automobiliuose naudojamas raktų sistemas.
2. Išanalizuoti „SDR“ architektūrą, veikimo principą ir panaudojimą.
3. Atlikti įrangos, kuria būtų galima perimti signalus, siunčiamus į automobilį, analizę.
4. Ištirti perimtus signalus, nustatyti jų saugumo spragas.
5. Ištirti kaip priklauso perimtas signalas nuo atstumo.
6. Pateikti tyrimo rezultatus.

Baigiamojo darbo rengimo konsultantai: _____

(vardas, pavardė, mokslinis laipsnis ir vardas)

Vadovas: _____

(parašas)

(vardas, pavardė, mokslinis laipsnis ir vardas)

Užduotį gavau: _____

(studento parašas)

(data)

Vilniaus Gedimino technikos universitetas

Elektronikos fakultetas

Kompiuterių inžinerijos katedra

ISBN

ISSN

Egz. sk. 1

Data 2014

Kompiuterių inžinerijos studijų programos baigiamasis magistro darbas

Pavadinimas **Automobilių raktų sistemų tyrimas panaudojant programą „Software Defined Radio“**

Autorius **Povilas Šiaudinis**

Vadovas **Tadas Lipinskis**

Kalba

☒ X

lietuvių

☐

užsienio

Anotacija

Baigiamajame magistro darbe tiriama automobilių raktų perduodami signalai, jų saugumo spragos. Projektuojama įranga, skirta šiems signalams perimti ir analizuoti. Darbe apžvelgiamos naudojamos automobilių raktų sistemos. Išsiaiškinama kaip veikia programuojamas radijo ryšys. Sudaroma struktūrinė schema, skirta iš rakto į automobilį perduodamiems signalams perimti ir analizuoti. Sukonfigūruojama programinė įranga, sukuriamas signalų analizės algoritmas. Ištiriama 27-ių skirtingų automobilių priimami signalai ir Lietuvoje pagamintos automobilio signalizacijos veikimas. Nustatytos ištirtų signalų saugumo spragos, pasiūlyta, kaip galima padidinti perduodamų signalų saugumą. Darbą sudaro 6 dalys: įvadas ir užduoties analizė, automobilių raktų sistemos, „Software defined radio“ architektūra ir panaudojimas, siunčiamo signalo perėmimo įranga, automobilių atrakinimo signalų kodų tyrimas, išvados, literatūros ir informacinių šaltinių sąrašas, priedai.

Darbo apimtis – 50 p. teksto be priedų, 34 iliustr., 29 lent., 22 bibliografiniai šaltiniai.

Atskirai pridedami darbo priedai.

Prasminiai žodžiai: kodavimo algoritmas, nuotolinio rakto sistema, programuojamas radijo ryšys, TV imtuvas, mikroschema HCS200.

Vilniaus Gediminas technical university
Faculty of **Electronics**
Computer Engineering department

ISBN ISSN
Copies No. 1
Date 2014

Computers Engineering study programme master's thesis.

Title: **Cars keys system research using „Software Defined Radio“**

Author **Povilas Šiaudinis**

Executive Tadas Lipinskis

Thesis language

☐

Lithuanian

☒

Foreign (English)

Annotation

In the master thesis transmitted signals of car security systems and their security vulnerabilities are investigated. Equipment is designed to intercept and analyze these signals. An overview of the security systems used in car keys is given. Software and hardware of the programmable radio is explained. Equipment for taking over car security systems signals is designed using the programmable radio architecture. Flowchart for receiving car key transmitted signals is formed. A signal analysis algorithm is created. 27 different car key signals are analyzed. A sample car alarm system's, which is made in Lithuania, radio signals are analyzed. The vulnerabilities of signals are investigated and measures for improving the security of transmitted signals are proposed. The work consists of 6 parts : introduction, analysis of the system of car keys, „Software defined radio” architecture and uses, the transmitted signal scanning equipment, car unlocking signal transmitted codes investigation, a summary of results, references and sources of information, appendices.

Thesis consist of: 50 p. text without extras, 34 pictures, 29 tables, 22 bibliographical entries.

Appendixes included.

Keywords: coding algorithm, a remote keyless system, a programmable radio, TV receiver chip HCS200.

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

(Studijų programa, akademinė grupė)

Turinys

Žymenys ir santrumpos	9
Paveikslų ir lentelių sąrašas	10
1. Įvadas. Užduoties analizė	12
2. Automobilių raktų sistemos.....	13
2.1. Mechaniniai raktai ir imobilizatoriai	13
2.2. Nuotolinio rakto sistema.....	14
2.3. Pasyvios nuotolinio rakto sistemos	17
2.4. Ateities raktų sistemos.....	18
2.5. Skyriaus apibendrinimas.....	19
3. „Software defined radio“ architektūra ir panaudojimas	20
3.1. „SDR“ architektūra.....	20
3.2. „Software defined radio“ programinė įranga.....	26
3.3. „Software defined radio“ panaudojimas.....	29
3.4. Skyriaus apibendrinimas.....	31
4. Siunčiamo signalo perėmimo įranga	32
4.1. Struktūrinė schemos sudarymas	32
4.2. TV imtuvo parinkimas.....	33
4.3. Kompiuterio konfigūravimas.....	35
4.4. „HSDR“ programinės įrangos konfigūravimas	35
4.5. „Matlab“ algoritmo kūrimas.....	37
4.6. Perimto signalo kokybės nuo atstumo tyrimas	38
4.7. Skyriaus apibendrinimas.....	39
5. Automobilių atrakinimo signalų kodų tyrimas.....	40
5.1. Automobilių priimamų signalų kodų tyrimas.....	40
5.2. Ištirtų signalų saugumo spragos	51
5.3. Skyriaus apibendrinimas.....	52
6. Apibendrinimas. Išvados	53

Literatūros ir informacijos šaltinių sąrašas	55
Priedai	57
A Priedas. Signalų perėmimo ir analizės struktūrinė schema	57
B Priedas. Signalų analizės algoritmo programos kodas.....	58

Žymenys ir santrumpos

SCL (angl. <i>Secolink</i>)	Elektroninė identifikavimo kortelė
Start/Stop (angl. <i>Start-stop system</i>)	Variklio įjungimo/išjungimo sistema
SDR (angl. <i>Software Defined Radio</i>)	Programuojamas radijo ryšys
Anti carjack (angl. <i>Anti carjack</i>)	Apsauga nuo automobilio pavogimo
RFID (angl. <i>Radio-frequency identification</i>)	Radijo dažnio identifikavimo technologija
EEPROM (angl. <i>Electrically Erasable Programmable Read - Only Memory</i>)	Elektriškai trinama/įrašoma skaitymo atmintis
NLFSR (angl. <i>Non-Linear Feedback Shift Register</i>)	Perėjimo registras su netiesiniu atgaliniu ryšiu

Paveikslų ir lentelių sąrašas

2.1.1 pav. Mechaninis automobilio raktas	13
2.2.1 pav. Nuotolinio tipo raktai	14
2.2.2 pav. Automobilio ir nuotolinio rakto sistemos architektūra	15
2.2.3 pav. Kintančio rakto kodavimo schema	16
2.2.4 pav. „AES“ baitų sukeitimo lentelė	16
2.2.5 pav. „AES“ eilučių perstumdydas	17
2.2.6 pav. „AES“ stulpelių sumaišymas	17
2.3.1 pav. Pasyvaus nuotolinio rakto sistema	18
2.4.1 pav. Automobilio raktas su USB sąsaja	19
3.1.1 pav. Daugiakanalio imtuvo struktūra	22
3.1.2 pav. Vieno kanalo imtuvas	23
3.1.3 pav. Juostinio filtro elektrinė grandinė	23
3.1.4 pav. Vieno kanalo siųstuvas	25
3.2.1 pav. „HDSR“ programos darbinis langas	27
3.2.2 pav. „FM“ imtuvo „GNU radio“ programos blokinė schema	28
3.2.3 pav. „WebSDR“ programos darbinis langas	29
3.3.1 pav. „HDSR“ programos langas	30
3.3.2 pav. Signalų apdorojimo blokinė schema	30
3.3.3 pav. Demoduluotas signalas	31
4.1.1 pav. Signalų perėmimo ir analizės struktūrinė schema	32
4.2.1 pav. Signalų amplitudės pasiskirstymas nuo matuojamo dažnio nuokrypio	33
4.2.2 pav. TV imtuvas	34
4.2.3 pav. Automobilinės antenos strypas	34
4.4.1 pav. „HDSR“ programinės įrangos darbinis langas	36
4.4.2 pav. „Audacity“ programos langas	37
4.5.1 pav. „Matlab“ programos signalų analizės algoritmas	37
4.5.2 pav. Signalų prilyginimas loginiam „0“ ir „1“	38
4.6.1 pav. Signalų amplitudės pasiskirstymas nuo matuojamo atstumo.....	39
5.1.1 pav. Signalų kodo kitimo pasiskirstymas	47
5.1.2 pav. Signalų ilgio kitimo pasiskirstymas	47
5.1.3 pav. Signalų dažnių pasiskirstymas pagal automobilio markę	48
5.1.4 pav. Automobilio signalizacijos valdymo blokas	49
5.1.5 pav. Automobilio signalizacijos rakto spausdintinė plokštė	50

5.1.6 pav. „Keeloq“ algoritmo signalų struktūros	50
5.1.1 lentelė. „Opel vectra“ durų atrakinimo signalo struktūra	41
5.1.2 lentelė. „Skoda superb“ durų atrakinimo signalo struktūra	41
5.1.3 lentelė. „BMW 5 klasė“ durų atrakinimo signalo struktūra	41
5.1.4 lentelė. „Lexus“ durų atrakinimo signalo struktūra	41
5.1.5 lentelė. „Suzuki“ durų atrakinimo signalo struktūra	41
5.1.6 lentelė. „Toyota“ durų atrakinimo signalo struktūra	41
5.1.7 lentelė. „Alfa Romeo“ durų atrakinimo signalo struktūra	42
5.1.8 lentelė. „Audi“ durų atrakinimo signalo struktūra	42
5.1.9 lentelė. „Chrysler“ durų atrakinimo signalo struktūra	42
5.1.10 lentelė. „Citroen“ durų atrakinimo signalo struktūra	42
5.1.11 lentelė. „Fiat“ durų atrakinimo signalo struktūra	42
5.1.12 lentelė. „Ford“ durų atrakinimo signalo struktūra	42
5.1.13 lentelė. „Honda“ durų atrakinimo signalo struktūra	43
5.1.14 lentelė. „Hyundai“ durų atrakinimo signalo struktūra	43
5.1.15 lentelė. „Land Rover“ durų atrakinimo signalo struktūra	43
5.1.16 lentelė. „Mazda“ durų atrakinimo signalo struktūra	43
5.1.17 lentelė. „Mercedes“ durų atrakinimo signalo struktūra	43
5.1.18 lentelė. „Mitsubishi“ durų atrakinimo signalo struktūra	43
5.1.19 lentelė. „Nissan“ durų atrakinimo signalo struktūra	44
5.1.20 lentelė. „Pegeot“ durų atrakinimo signalo struktūra	44
5.1.21 lentelė. „Renault“ durų atrakinimo signalo struktūra	44
5.1.22 lentelė. „Rover“ durų atrakinimo signalo struktūra	44
5.1.23 lentelė. „Saab“ durų atrakinimo signalo struktūra	44
5.1.24 lentelė. „Seat“ durų atrakinimo signalo struktūra	44
5.1.25 lentelė. „Subaru“ durų atrakinimo signalo struktūra	45
5.1.26 lentelė. „Volkswagen“ durų atrakinimo signalo struktūra	45
5.1.27 lentelė. „Volvo“ durų atrakinimo signalo struktūra	45
5.1.28 lentelė. Rezultatų analizė	46
5.1.29 lentelė. Automobilinio užraktų sistemos gamintojai	48

1. Įvadas. Užduoties analizė

Šiuolaikiniai automobiliai naudoja keletą sujungtų sistemų, kurios padidina jų saugumą. Šios saugumo sistemos skirstomos į šias pagrindines grupes:

- durų ir vairo užraktai;
- užvedimo spynos;
- signalizacijos;
- variklio imobilizatoriai;
- apsaugos nuo atviros vagystės (angl. *anti-carjack*) sistemos.

Kai kurie automobilių imobilizatoriai turi integruotą „anti-carjack“ funkciją. Jeigu imobilizatorius per tam tikrą laiko tarpą po variklio degimo įjungimo neaptiks SCL kortelės, automobilio variklio darbas bus blokuojamas. Senesni automobiliai, pagaminti iki 2002 m. naudoja tik po vieną ar po dvi saugumo sistemos grupes. Automobiliai pagaminti po 2002 m. naudoja daugiau negu dvi saugumo sistemos grupes. Automobilio raktas suteikia naudotojui prieigą prie automobilio, taip apsaugodamas nuo nepageidaujamų naudotojų.

Pirmieji automobiliai atsirado 20-ojo amžiaus pradžioje. Juose nebuvo įrengta jokių spynų mechanizmų. Dabartinių automobilių durų užraktai gali būti valdomi keliais būdais: mechaniniu arba nuotoliniu valdymu. Pradžioje buvo naudojamas mechaninis durų užraktas, vėliau, dėl patogumo, buvo sukurta nuotolinio durų atrakinimo/užrakinimo sistema. Buvo tobulinama ir automobilio užvedimo sistema.

Tradiciniai mechaniniai raktai skirti užvesti automobilį sparčiai nyksta. Jie yra pakeičiami nuotoliniais raktais, kurie veikia be naudotojo įsikišimo. Tokios sistemos automatiškai atrakina automobilio duris, kai nuotolinis raktas atsiduria per tam tikrą atstumą nuo automobilio. Dauguma tokių automobilių neturi standartinės užvedimo spynelės. Vietoje jos įrengtas „Start/Stop“ mygtukas, kurio paskirtis įjungti arba išjungti automobilio variklį. Kadangi automobiliai yra naudojami masiškai visame pasaulyje, bet kokios problemos susijusios su jų saugumu turės didelį atgarsį visuomenėje. Siekiant užtikrinti automobilių saugumą, gamintojai neskelbia, kokias apsaugos technologijas naudoja automobilių pramonėje.

Baigiamojo magistro darbo užduotis - ištirti automobiliuose naudojamus nuotolinių raktų sistemų signalus, panaudojant programuojamą radijo ryšį (angl. *Software Defined Radio*). Nustatyti galimas jų saugumo spragas ir aptarti kaip būtų galima padidinti nuotolinių raktų saugumą. Pasirinkta ištirti 27 skirtingų automobilių nuotolinių raktų perduodamus signalus. Parenkama aparatinė įranga skirta perimti signalus, kurie yra siunčiami į automobilį. Pagal aparatinę įrangą parenkama programinė įranga skirta stebėti, perimti ir demoduliuoti perduodamus signalus. Sukuriama programa skirta perimtų signalų analizei.

2. Automobilių raktų sistemos

2.1. Mechaniniai raktai ir imobilizatoriai

Mechaninis raktas – įrenginys skirtas automobilio durims užrakinti ir atrakinti, bei varikliui užvesti. Norint atrakinti ar užvesti pirmuosius automobilius užtekdamo turėti mechaninį raktą (2.1.1 pav.). Pirmosios automobilio užvedimo spynos atsirado apie 1919 m. [1]. Išrastas raktas buvo skirtas blokuoti vairo mechanizmą ir išjungti elektros tiekimą į variklį. Neturint šio rakto, automobilio nebuvo galima užvesti. 1920 m. pabaigoje užvedimo spynelės buvo montuojamos į daugumą naujų automobilių. Didinant automobilių saugumą nuo vagysčių, tais pačiais metais buvo pradėta montuoti durų spynos automobiliuose [2]. Gamintojai dažniausiai naudoja dviejų tipų raktus: su išoriniais arba vidiniais grioveliais.



2.1.1 pav. Mechaninis automobilio raktas [3]

Iki 1998 m. imobilizatoriai buvo montuojami tik į prabangius automobilius. Nuo 1998 m. į visus naujai gaminamus automobilius Europos Sąjungoje pradėjo diegti imobilizatoriaus sistemas [4]. Tai sistema prieš automobilių nuvaramą, įgalinanti elektroniniu būdu užblokuoti vienu metu keletą sistemų pvz. kuro padavimo ir uždegimo sistemas. Imobilizatoriaus veikimo principas panašus kaip ir automobilio apsaugos signalizacijos, bet imobilizatoriai turi patikimesnes garantijas nuo intelektualaus įsilaužimo. Skirtingai nuo signalizacijų, kurios yra valdomos iš didesnio atstumo radijo bangomis, imobilizatoriai veikia labai mažu atstumu nuo rakto iki užvedimo spynos, todėl praktiškai neįmanoma nuskaityti darbinių dažnių su bet kokiais skaitytuvais. Ši sistema paremta radijo dažnio identifikavimo technologija. (angl. *RFID*). Šios atsakiklių sistemos yra pasyvios, ir nereikalauja jokio pastovaus maitinimo šaltinio. Sistema dažniausiai veikia 125 kHz dažniu, ir neturėdamos maitinimo šaltinio dirba labai nedideliu atstumu (nuo 1,5 cm iki 15 cm). Kai tik įkišamas raktas į automobilio degimo spyną ir pasukamas į „ON“ poziciją, raktas gauna elektromagnetinį signalą iš išorinio bloko antenos. Rakto apvijos aplink šerdį tą elektromagnetinį signalą paverčia į energiją, reikalingą atgaliniam

signalų išspinduliavimui. Atgalinis signalas susideda iš raidžių ir skaičių kombinacijos ir vadinamas identifikacijos kodu. Išorinis įrenginys t. y. antena perskaito tą signalą ir pasiunčia jį į imobilizatoriaus bloką. Imobilizatoriaus bloke gautas signalas palyginamas su teisingu signalo algoritmu, ir jeigu signalas sutampa – automobilis užsiveda. Jeigu signalas nesutampa – automobilis neužsiveda iki tol, kol bus gautas teisingas signalas.

Maždaug nuo 1993 m. automobilių gamintojai imobilizatoriuose pradėjo naudoti kintantį kodą. Kodas, įrašytas į atsakiklio atmintį, susideda iš 32 simbolių šešioliktainėje sistemoje (skaičiai nuo 0 iki 9 ir raidės nuo A iki F). Ši kombinacija yra slaptažodis ir leidžia imobilizatoriui atpažinti tikrąjį raktą. Ankstesniuose atsakiklių tipuose ši informacija nesikeisdavo, t. y. užvedant automobilį atsakiklis siųsdavo į imobilizatorių vis tą patą kodą. Tą kodą būdavo galima nukopijuoti turint rakto atsakiklio pavyzdį ir išjungti automobilio apsaugą. Gamintojai, norėdami ištaisyti šią spragą, sugalvojo kintantį kodą. Šį kodą sudaro dvi dalys. Pastoviosios dalies ir kintamosios dalies. Pastaroji, t. y. kintanti dalis, kinta pagal specialų algoritmą ir pavogti ar nukopijuoti tokią informaciją yra sunku [5].

2.2. Nuotolinio rakto sistema

Nuotolinio rakto sistemos (angl. *Remote keyless entry*) pradėtos naudoti nuo 1983 m. [6]. Tačiau tokios sistemos buvo diegiamos tik į labai prabangius automobilius. Dabar beveik visi automobiliai, pagaminti nuo 1998 m., turi nuotolinio rakto sistemas. Naudojami du gamybos tipai, gaminant nuotolinio rakto sistemas. Labiausiai paplitusi nuotolinio rakto mikroschema įmontuota kartu su raktu. Kitas gamybos būdas – nuotolinio rakto mikroschema montuojama atskirame, nuo mechaninio rakto, korpuse. Abu šie būdai pavaizduoti 2.2.1 paveiksle.



2.2.1 pav. Nuotolinio tipo raktai [5]

Nuotolinio užrakto sistemos suteikia galimybę automobilio savininkui atrakinti arba užrakinti automobilį fiziškai prie jo neprisiliečiant. Užtenka paspausti atitinkamą mygtuką, esantį ant rakto. Tokios sistemos dažniausiai turi papildomų funkcijų. Šios funkcijos yra tokios:

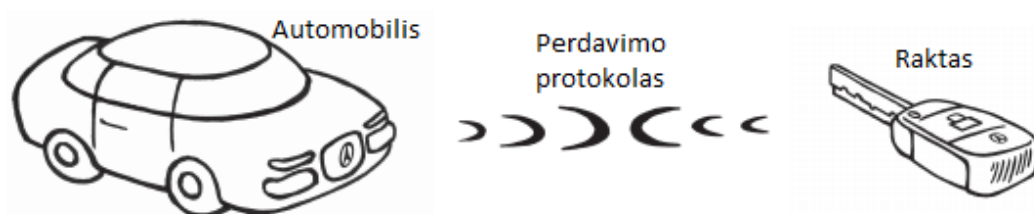
- bagažinės atidarymas;
- langų uždarymas arba atidarymas;

- stoglangio uždarymas ar atidarymas;
- automobilio signalizacijos įjungimas arba išjungimas;
- durų užrakto valdymas.

Pirmosios sistemos signalo perdavimui naudojo ne radijo bangas, o infraraudonuosius spindulius. Šiandien nuotolinio rakto sistemoms komunikuoti naudojami radijo dažniai. Šiaurės Amerikoje ir Japonijoje naudojama 315 MHz dažnių juosta. Europoje naudojama ~ 433,92 MHz dažnių juosta. Kokiu atstumu veikia nuotolinio rakto sistemos dažniausiai apibrėžia gamintojas. Pavyzdžiui „Ford“ įmonė Europoje naudoja 20 m. atstumą, Japonijoje 5 m. Kai kuriose šalyse perdavimo atstumas apribotas tos šalies įstatymų.

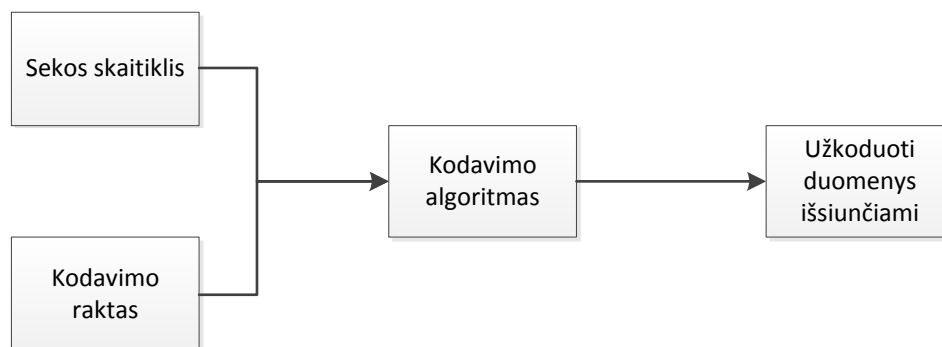
Automobilio ir nuotolinio rakto komunikacijos architektūra pavaizduota 2.2.2 paveiksle. Sistema susideda iš 3 pagrindinių komponentų:

- Raktas – viduje esanti mikroschema skirta siųsti signalus į automobilį;
- Perdavimo protokolas – ryšio tipas, kuriuo komunikuoja raktas ir automobilis. Dažniausiai naudojamos radijo bangos (315 MHz. arba 433 MHz.);
- Automobilis – viduje esanti mikroschema, skirta priimti signalus iš rakto ir juos autentifikuoti.



2.2.2 pav. Automobilio ir nuotolinio rakto sistemos architektūra [7]

Pagal 2.2.2 paveiksle pateiktą schemą, veikia nuotolinių raktų sistemos ir pasyvių raktų sistemos. Šiuo principu taip pat veikia imobilizatoriaus sistema, tačiau yra apribotas atstumas iki 15 cm. 2.2.3 paveiksle pavaizduota standartinė kintančio rakto kodavimo schema. Sekos skaitiklio duomenys su kodavimo raktu pirmiausia užkoduojami ir tik tada išsiunčiami. Kiekviena kartą išsiuntus duomenis sekos skaitiklio reikšmė yra padidinama. Gautus duomenis imtuvas (pvz. automobilis) iššifruoja, suranda sekos skaitiklio reikšmę. Jis šią reikšmę palygina su savo sekos skaitikliu. Jei skirtumas tarp siuntėjo sekos skaitiklio ir imtuvo sekos skaitiklio atitinką nustatytą intervalą, tada leidžiama vykdyti tam tikras operacijas.



2.2.3 pav. Kintančio rakto kodavimo schema [8]

Nuo 1950 m. ta pati technologija buvo naudojama garažo vartams atidaryti ir automobiliams atrakinti. Siųstuvas išsiųsdavo nekoduotą signalą į imtuvą. Naudojant tą patį pultelį buvo galima atidaryti tos pačios firmos, bet kurias garažo duris. Sparčiai populiarėjant šiai technologijai pradėjo augti saugumo reikalavimai. Šiuolaikinių nuotolinio rakto sistemos kūrėjai teigia, kad naudojamos kodavimo priemonės, siekiant užtikrinti saugumą. Dažniausiai gamintojai siekia neatskleisti naudojamus kodavimo algoritmus, tačiau yra žinoma, kad naudojami šie algoritmai: „AES“ (angl. *Advanced Encryption Standard*), „KeeLoq“, „Hitag2“, „Megamos“) [9], [10].

„AES“ yra simetrinis – blokinis šifras, kur bloko dydis yra 128 bitai. Rakto ilgiai gali būti 128, 192 arba 256 bitų, vadinami AES-128, AES-192, ir AES-256 atitinkamai. AES-128 naudoja 10 ciklų, AES-192 naudoja 12 ciklų, o AES-256 14 ciklų. „AES“ suskaldo duomenis į 16 baitų (128 bitų) blokus, ir traktuoja kiekvieną bloką kaip 4x4 matricą, su kuria atlieka pakeitimus. AES pagrindinės funkcijos:

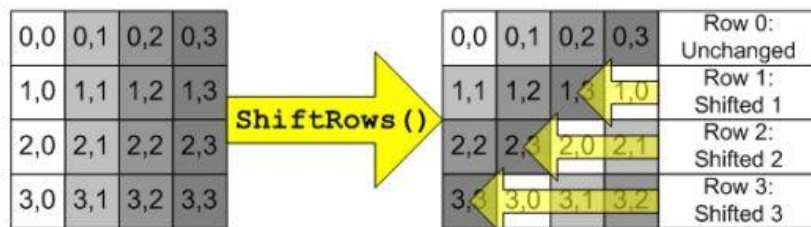
1. Baitų sumaišymas. Norint atlikti baitų sumaišymo (2.2.4 pav.) operaciją eilutės pavyzdžiui "ABC", reik paimti kiekvieno baito šešioliktąją vertę. ASCII "A" == hex 0x42, "B" == 0x43, o "C" == 0x44. Pirmasis (kairysis), skaitmuo atitinka lentelės stulpelius, o antrasis - eilutes. 0x42 tampa 0x2c; 0x43 tampa 0x1a, o 0x44 tampa 0x1b.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
-- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --																
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

2.2.4 pav. „AES“ baitų sukeitimo lentelė [11]

2. Eilučių perstumdymas

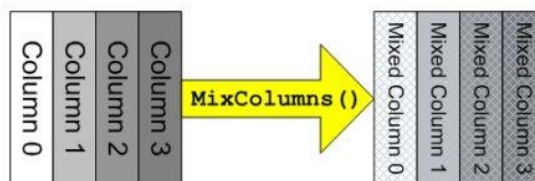
Antruoju veiksmu AES yra sumaišomos eilutės (2.2.5 pav.). Kiekvieno bloko nulinė eilutė nėra perstumiama, pirmoji eilutė perstumiama per vieną baitą, antroji - per du, trečioji - per tris baitus.



2.2.5 pav. „AES“ eilučių perstumdymas [11]

3. Stulpelių sumaišymas

Kiekvienas 4 baitų stulpelis yra traktuojamas kaip vienas 4 baitų ilgio numeris, ir yra pakeičiamas kitu numeriu.



2.2.6 pav. „AES“ stulpelių sumaišymas [11]

4. Užšifravimas

Tikrasis šifravimas vyksta šioje stadijoje, kai kiekvienas baitas yra išskirtinis arba užšifruojamas savo porakčiu. Poraktis yra kilęs iš rakto.

2.3. Pasyvios nuotolinio rakto sistemos

Plėtojant nuotolinio rakto sistemą buvo sukurta pasyvi nuotolinio rakto sistema (angl. *Passive keyless entry*). Pirmą kartą ši sistema buvo sukurta 1990 m. Jungtinėse Amerikos valstijose [12]. Ši sistema (2.3.1 pav.) suteikia galimybę automobilio savininkui atrakinti automobilį be fizinio įsikišimo. Tai reiškia, kad naudotojui nereikia paspausti mygtuko, esančio ant nuotolinio pultelio. Mašina yra atrakinama automatiškai, jeigu nuotolinis raktas atsiduria per tam tikrą atstumą nuo automobilio. 2005 m. priimtas visuotinis standartas, kad maksimalus pasyvaus rakto atstumas nuo automobilio neturėtų būti daugiau negu 10 cm. [13].



2.3.1 pav. Pasyvaus nuotolinio rakto sistema [14]

Skirtingi gamintojai naudoja skirtingas sistemas. Viena iš technologijų yra sukurta taip, kad net ir atsiradus raktui saugiu atstumu nuo automobilio, jis neatsirakina automatiškai. Ant durų rankenėlių yra įmontuoti jutikliai ir kai vartotojas paliečia rankenėlę, tada automobilis patikrina ar saugiu atstumu yra raktas. Jei raktas aptinkamas tada durelės atsirakina, jei raktas nerandamas tuomet durelės lieka užrakintos. Norint užrakinti automobilį, užtenka išnešti raktą iš saugios zonos. Saugi zona – tai gamintojo nustatytas atstumas, kuriame gali komunikuoti raktas su automobiliu.

Kaip ir nuotolinio rakto sistemos, taip ir pasyvaus rakto sistemos siunčia radijo signalus. Pultelyje yra įmontuota baterija ir mechaninis raktas. Mechaninis raktas gali būti panaudotas tuo atveju, jeigu baterija išsikrautų.

Neretai naudojant pasyvaus rakto sistemas, automobiliuose naikinamos standartinės užvedimo spynos. Šios spynos pakeičiamos mygtuku „Start/Stop“. Kai vairuotojas nori užvesti automobilį, jam reikia paspausti mygtuką „Start/Stop“. Nuspaudus šį mygtuką, automobilio kompiuteris ieško netoliese esančio rakto. Jeigu raktas randamas mašinoje (saugiu atstumu), tada išjungiamas imobilizatorius ir automobilis užvedamas.

2.4 Ateities raktų sistemos

Dauguma gamintojų bando, testuoja ir kitokio tipo komunikacijas tarp rakto ir automobilio. Tokie perdavimo protokolai gali būti „Bluetooth“, „Zigbee“. Tendencija yra integruoti kuo daugiau multimedijos funkcijų tarp automobilio ir rakto. Tai suteikia galimybę naudoti raktą kaip prieigą, prie tam tikrų automobilio funkcijų.

Automobilių gamintoja „Mercedes“ pristatė koncepcinį automobilį, kurio rakte integruota USB sąsaja. Pačiame automobilyje įmontuotas kietasis diskas. USB raktas (2.4.1 pav.) gali būti naudojamas įrašyti asmeninis nustatymus, duomenis.



2.4.1 pav. Automobilio raktas su USB sąsaja [6]

Bendrovė „Sony Ericsson“ bendradarbiaudama su automobilių gamintoja „Saab“ sukūrė koncepcinį automobilį „Saab 9-X BioHybrid“ su „Bluetooth“ sąsaja. Automobilio valdymui panaudotas mobilusis telefonas, valdymas vyksta „Bluetooth“ protokolu. Panaudojus specialią aplikaciją skirtą telefonui, buvo galima valdyti šias automobilio funkcijas:

- užrakinti automobilį;
- atidaryti bagažinės duris;
- valdyti galinių ir priekinių sėdynių nustatymus;
- įjungti ir išjungti priekinius automobilio žibintus;
- valdyti salono apšvietimą.

2.5 Skyriaus apibendrinimas

Šiame skyriuje apžvelgta automobiliuose naudojamos raktų sistemos. Išsiaiškinta imobilizatoriaus paskirtis, aptartas veikimo principas. Išanalizuota nuotolinių ir pasyvių raktų sistemų veikimas. Aptarta koncepcinės automobilių raktų sistemos, kurių pagrindinis tikslas į raktą įdiegti kuo daugiau multimedijos funkcijų. Apžvelgus įvairius literatūros šaltinius, kuriuose nagrinėjama nuotolinių ir pasyvių raktų sistemų veikimas ir saugumas nustatyta, kokie yra žinomi šifravimo algoritmai. Aptartas „AES“ kodavimo algoritmo veikimo principas.

Kadangi imobilizatoriaus sistemos naudoja 125 kHz dažnių diapazoną, o TV imtuvas tokio diapazono nepalaiko, tolimesniame darbe pasirinkta nagrinėti signalus, kuriuos naudoja nuotolinio rakto sistemos ir pasyvaus rakto sistemos. Šių sistemų perduodami dažniai yra 315 – 433 MHz diapazone, o maksimalus atstumas, kuriuo sklinda signalas yra iki 30 m. Tokiems signalams perimti naudosisime skaitmeninį USB TV imtuvą.

3. „Software defined radio“ architektūra ir panaudojimas

3.1. „SDR“ architektūra

SDR (angl. *Software defined radio*) – programinė įranga skirta radijo signalo apdorojimui, analizei ir signalų skaitmenizavimui. Ši programinė įranga suteikia galimybę pakeisti radijo ryšio fizinius komponentus (stiprintuvus, modulatorius, demodulatorius, filtrus) į skaitmeninio procesoriaus programinę įrangą. Pagrindinė „SDR“ sistema susideda iš kompiuterio ir garso plokštės. Vietoje garso plokštės gali būti naudojamas bet koks kitas įrenginys, kuris gali priimti analoginius signalus ir pakeisti juos skaitmeniniais (pvz. išorinis FM imtuvas). Vienas iš pagrindinių sistemos privalumų yra tas, kad signalų apdorojimui naudojamas bendrosios paskirties procesorius, o ne atskiri fiziniai įrenginiai. Taip suteikiama galimybė vienu įrenginiu apdoroti skirtingus radijo ryšio protokolus, atliekant pakeitimus tik programinio kodo lygmenyje. Programinėje įrangoje įdiegtas radijo ryšio funkcionalumas atveria ir nemažai kitų galimybių. Mobiliojo „SDR“ prietaiso ryšio nesutrikdytų ir dinamiškai kintantis bei nenuspėjamas mobiliojo ryšio tinklų veikimo pobūdis. Šiuo prietaisu būtų galima efektyviai naudoti radijo bangų galią bei jų spektrą, staigiai pereiti nuo vieno radijo ryšio standarto prie kito (tarkim, nuo GSM prie EDGE) [15]. Aparatinės įrangos gamyba tampa daug paprastesnė, nes „SDR“ technologija leidžia atsisakyti sudėtingų grandinių, juos pakeičiant programine įranga.

„SDR“ pradžia laikomi 1980 metų vidurys. Vienas iš pirmųjų „SDR“ projektų buvo „SpeakEasy“ – tai siųstuvai, paremtas „SDR“ technologija, kuri sukūrė „Hazeltine“ ir „Motorola“ kompanijos. „SpeakEasy“ siųstuvai buvo sukurti siekiant aprūpinti taktinius karinius objektus ryšiu nuo 2 MHz iki 2 GHz ir teikti sąveiką tarp skirtingų oro ryšio sąsajos standartų iš įvairių sričių. Nors daug žmonių prisidėjo prie šio projekto, tačiau pagrindiniu „SDR“ įkūrėju laikomas Joe Mitola.

Programinis radijo ryšio panaudojimas gali būti labai lankstus ir išvengta „riboto spektro“ naudojant šiuos metodus:

- Panaudojant (angl. *Spread spectrum*) ir ultra plačiajuosčio spektro technologijos metodus, galima keliems siųstuvams siųsti toje pačioje vietoje, tuo pačiu dažniu su labai mažais trukdžiais, paprastai su viena ar daugiau klaidų aptikimo ir korekcijos galimybėmis.
- Programinio radijo ryšio antenos prisitaiko prie „užraktas ant“ kryptinio signalo, todėl imtuvas gali tiksliau priimti jam reikalingą signalą ir atmesti pašalinius, daug stipresnius signalus

- Radijo pažinimo technika – kiekviena radijo priemonė naudojanti radijo spektrą perduodą šią informaciją kitoms radijo priemonėms, todėl siųstuvai gali išvengti tarpusavio trikdžių, pasirinkdami nenaudojamus dažnius.
- Dinamiškas siųstuvo galios reguliavimas, remiantis informacija gauta iš imtuvų. Leidžia sumažinti siųstuvo galia iki būtino minimumo, sumažinant trikdžius kitiems signalams.

Naudojantis įvairiomis moduliavimo schemomis, kurių nešliai pasirenkami iš 5 MHz - 2 GHz intervalo, siekiama, kad sistemos perkonfigūruojami siųstuvai-imtuvai galėtų tuo pat metu naudotis vaizdo, garso bei kita skaitmenine informacija.

„SDR“ terpėje veikiančios radijo ryšio priemonės (ne tik mobilieji telefonai) realiu laiku galėtų prisitaikyti prie greitai kintančių bevielio ryšio sistemos charakteristikų. Mobiliojo ryšio vartotojams ši savybė itin aktuali. Verta paminėti, kad radijo ryšio priemonė programiniu būdu gali būti papildyta naujomis funkcijomis. Pavyzdžiui, „SDR“ sistema galėtų valdyti radijo bangos galią, kad silpno signalo zonose būtų geresnis ryšys, arba galėtų įdiegti papildomą kodą, kad sumažėtų gretimų ryšio kanalų trukdžių. Ir atvirkščiai - retai naudojamas funkcijas ar nereikalingus kodus iš siųstuvų – imtuvų ji tokiu pat būdu pašalintų.

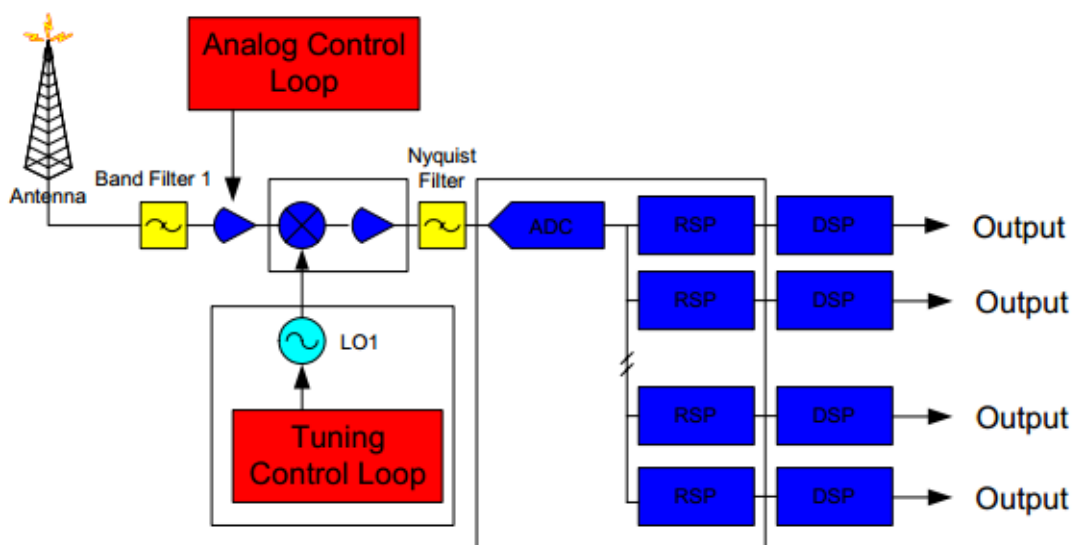
Tačiau šis funkcionalumas turi ir didelį trūkumą. Pasikeitus ryšio charakteristikoms, ryšys atsiranda kiek vėliau nei įprastai, nes siųstuvams prireikia papildomai laiko pasikeitusioms ryšio sąlygoms atpažinti ir į jas reaguoti. Toks vėlinimasis gali veikti garso ir vaizdo informacijos perdavimą.

Gėbėdamos sekti ryšio pralaidą, atpažinti pasikeitusias ryšio charakteristikas daugiajuostės „SDR“ sistemos gali išgauti naudos iš nenaudojamų dažnio kanalų ir šitaip tinklo operatoriams padėti veiksmingiau eksploatuoti ryšio tinklus. Pavyzdžiui, kuriuo nors metu nenaudojamas radijo ieškos (angl. *paging*) kanalas gali būti panaudotas kitokio pobūdžio informacijai siųsti.

Daugiakanaliai imtuvai

Aukštos kokybės SDR imtuvai paprastai naudoja superheterodininę architektūrą. Tokie imtuvai išlaiko didelį darbo našumą plačiame dažnio ruože, išlaikant didelį jautrumą ir selektyvumą. Priklausomai nuo programos, gali būti naudojami vienas ar keli imtuvo kanalai. Dažniausiai programos naudoja vieną radijo dažnio kanalą. Naudojant aukšto lygio programas pasirenkamas kelių kanalų režimas. Esant kelių kanalų režimui „SDR“ naudoja analogas – skaičius keitiklį (ASK) su pakankamu praleidžiamos juostos pločiu. Kadangi „SDR“ gali neturėti pakankamai informacijos apie priimamo signalo pralaidumą, reikia, kad imčių skaičius per sekundę būtų pakankamai didelis, kad apimtų visus numatomus pralaidumo juostos pločius.

Dabartinės ASK technologijos leidžia aukštus dinامينius pralaidumo juostos diapazonus iki 100 MHz. Naudojant tokio pralaidumo juostos plotį, galima apdoroti kelis kanalus. 3.1.1 paveiksle pavaizduota kelių kanalų imtuvo blokinė schema.

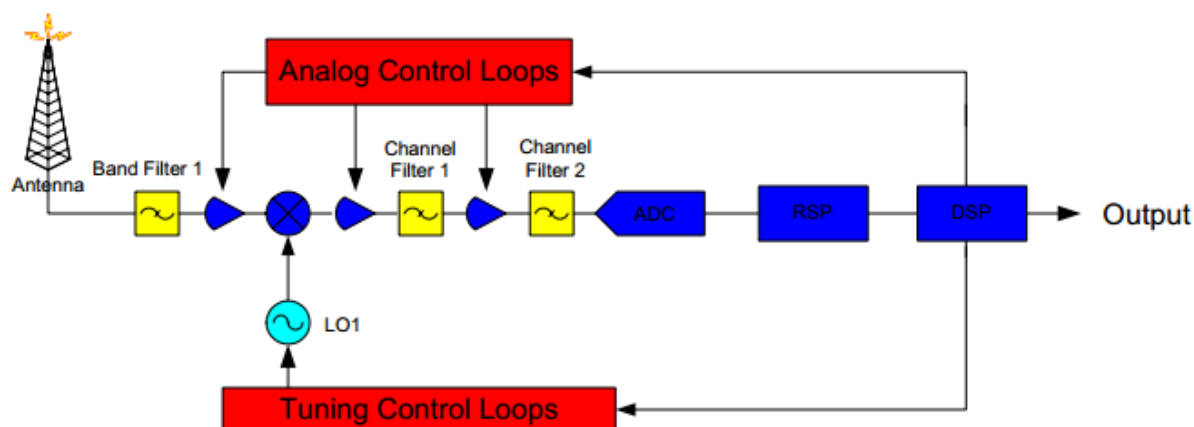


3.1.1 pav. Daugiakanalio imtuvo struktūra [17]

Tarkime, kad ASK imčių skaičius yra 61,44 mega ėmimai per sekundę, kurie suteikia Naikvisto pralaidumo juostos plotį – 30,72 MHz. Jeigu kiekvienas radijo dažnio kanalas yra 1,25 MHz pločio, tada potencialių kanalų skaičius yra apie 24,5. Dėl iškraipymų atsirandančių filtruose, naudojama trečdalis imčių skaičiaus dažnis, vietoj pusės Naikvisto dažnio. Todėl praleidžiamos juostos plotis yra 20,48 MHz, kas suteikia 16 kanalų po 1,25 MHz.

Vienkanaliai imtuvai

Ne visos „SDR“ aplikacijos reikalauja daugiau nei vieno kanalo. Nedidelio pajėgumo sistemoms užtenka vieno kanalo. Jeigu kanalas yra perprogramuojamas, galima nustatyti kanalo ploti nuo keletos kHz pločio iki 10 MHz. Kad pritaikytų šį juostos pločių diapazoną, imčių skaičiaus intensyvumas turi būti pakankamas aukščiausiam potencialiam juostos pločiui, šiuo atveju 10 MHz. Šiame pavyzdyje mėginių ėmimo intensyvumas yra 30,72 mega imtys per sekundę. Vieno kanalo imtuvas išlaiko tokias pačias savybes kai ir daugiakanalis imtuvas.

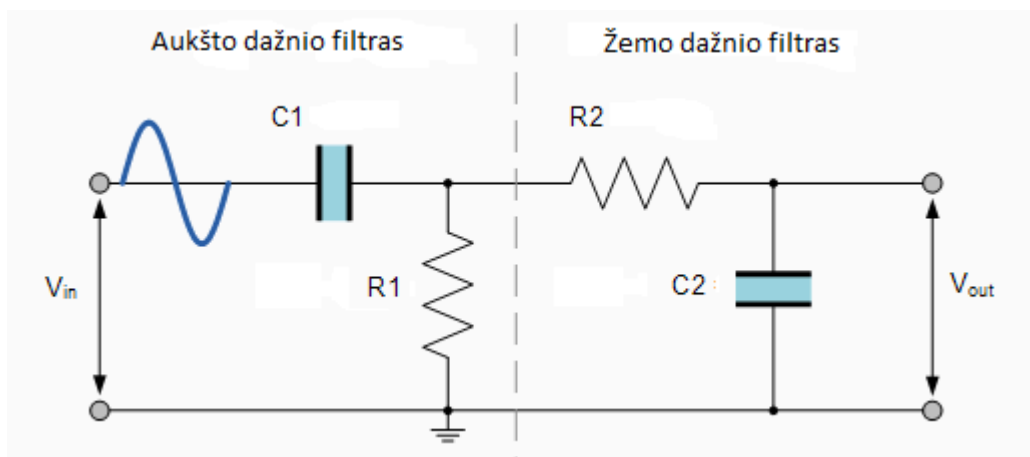


3.1.2 pav. Vieno kanalo imtuvas [17]

Remiantis 3.1.2 paveikslo blokine diagrama, matome, kad „SDR“ suteikia galimybę programuoti kiekvieną imtuvo elementą atskirai.

Antenos yra vienas iš silpniausių elementų „SDR“ sistemoje. Daugumoje sistemų, kur naudojamos vienos pralaidumo juostos plotis, problemų nėra. Kadangi dauguma antenų struktūrų turi tam tikrą pralaidumo juostos plotį, kuris nėra pakankamas norint atlikti operacijas su skirtingais dažniais, gali atsirasti problemų. Tada antenos turi būti suderintos, kad palaikytų operacinį dažnį, neprarandant jo našumo.

Sekanti dalis, imtuvo schemoje po antenos yra juostinis filtras. Šis elementas skirtas apriboti įeinamo signalo dažnio diapazoną, kad sumažintų intermoduliacijos iškreipimus. Juostinis filtras kuriamas kombinuojant aukšto ir žemo dažnio filtrus. Paprasčiausias juostinio filtro pavyzdys yra RC grandinė (3.1.3 pav.).



3.1.3 pav. Juostinio filtro elektrinė grandinė [17]

Daugumai imtuvų reikalingi žemo triukšmo stiprintuvai. Jų paskirtis sustiprinti labai silpnus signalus. Kadangi „SDR“ yra programuojama, tai galima žemo triukšmo stiprintuvą panaudoti labai plačiame dažnių diapazone.

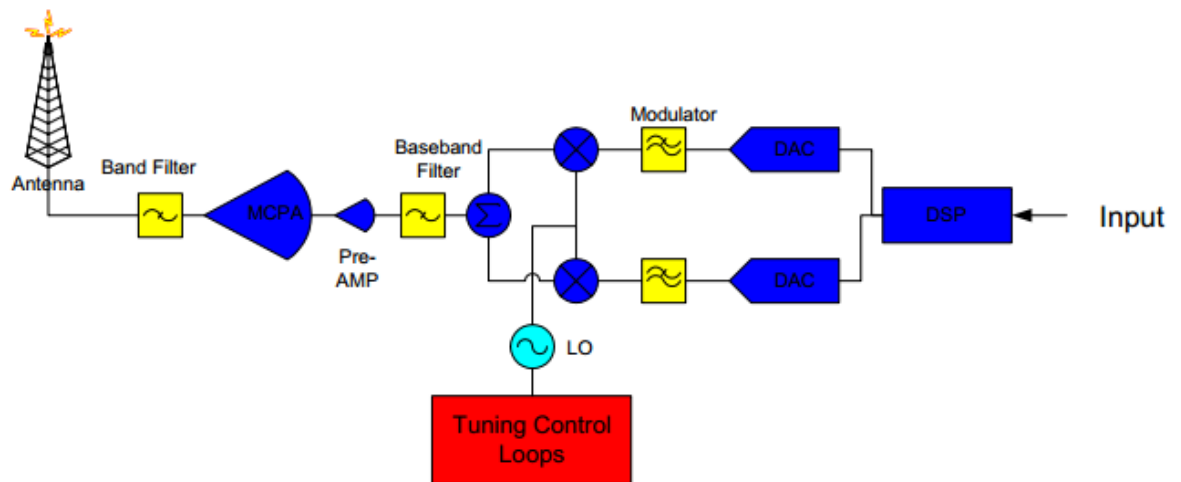
Maišytuvai naudojami perduoti radijo ryšio signalą, kurį būtų galima pritaikyti tarpiniam dažniui. Tarpinis dažnis – dažnis, kurio našlio dažnis yra perstumiamas kaip tarpinis žingsnis siuntimo arba gavime. Dauguma imtuvų naudoja du ar tris maišytuvus, kurie dažniausiai generuoja žemą signalą.

Labai svarbus „SDR“ elementas yra analoginis skaitmeninis keitiklis (ASK), nes nuo jo veikimo spartos priklauso, kurią grandinės vietą prie antenos reikia pasirinkti, norint analoginį signalą keisti skaitmeniniu. (Kuo mažesnė sparta, tuo ši vieta arčiau antenos). Apibrėžti keitiklio charakteristikas visuomet sunku, nes reikia nustatyti ir analoginių, ir skaitmeninių signalų parametrus. Apskritai turi būti apibrėžtos trys keitiklio charakteristikos: sparta (imčių skaičius per sekundę), skiriamoji geba imties metu (perduodamų bitų skaičius) ir tiesiškumas (parametras, nusakantis, ar tiksliai skaitmeninės išvesties kodas atitinka analoginės įvesties vertes).

Šiuo metu labiau apsimoka naudoti ne analoginės elektronikos komponentus, o programuojamus skaitmeninius prietaisus ir į juos integruoti radijo ryšio funkcijas. Tokias funkcijas įveiktų bendrosios paskirties spartieji skaitmeninių signalų procesoriai, atliekantys logines ir aritmetines operacijas, bet šiais laikais ekonomiškiau naudoti spartesnius ir lankstesnės konfigūracijos lustus: specialios paskirties integrinius grandynus (jų aritmetines funkcijas valdo koduotos loginės komandos) ir vartotojo programuojamas loginių elementų matricas (angl. *field programmable gate arrays* - FPGA), kurių programuojami sujungimai ir loginės funkcijos gali būti nustatytos jau įsigijus lustą. Kurdami ir tobulindami „SDR“ sistemą, projektuotojai sprendžia sudėtingą uždavinį - kaip racionaliau tarp esamų komponentų paskirstyti signalo apdorojimo funkcijas. Dažniausiai FPGA plokštėje sukonfigūruojamas signalo demodulatorius, reguliatorius, kanalo filtravimas, duomenų perdavimo spartos apribojimai. Galima naudotis ir kitas funkcijas, tokias kaip signalo galios valdymas ar signalo aproksimacija.

Specialios paskirties integrinės grandinės yra pigesnės, tam tikras užduotis atlieka greičiau nei kiti skaitmeniniai procesoriai, tačiau, esant didesniems integracijos laipsniams, mažėja jų programavimo galimybės. Reikia pridurti, kad įvairių standartų radijo ryšiui pasiekti dažnai reikia kelių specialios paskirties integrinių grandinių. Palyginimui galima paminėti, kad į vieną bendrosios paskirties skaitmeninių signalų procesorių ar FPGA būtų galima lengvai integruoti kelių standartų sąsajas.

Siųstuvas



3.1.4 pav. Vieno kanalo siųstuvas [17]

Skaitmeninis signalų procesorius gali būti naudojamas generuoti moduluotus praleidžiamos juostos pločio duomenis. Šie duomenys perduodami į skaitmeninį/analoginį keitiklį siekiant atlikti tiesioginį radijo dažnio moduliavimą arba į skaitmeninį procesorių atsakingą už perdavimą per atitinkamą tarpinį dažnį (IF). Priklausomai nuo programos, „DSP“ gali būti naudojamas skaitmeniniu būdu iškreipti signalą taip, kad vėliau dėl grandinėje atsirandančių iškraipymų, signalas grįžtų į pradinę būseną. Jeigu tarpinis dažnis IF yra naudojamas, tada „DSP“ sugeneruoti praleidžiamos juostos pločio duomenys turi būti suskaitmenizuoti su „FPGA“ arba maišytuvu, arba moduliatoriumi, pritaikant tarpiniam dažniui (IF).

Maišytuvas arba moduliatorius yra naudojamas dažnio konvertavimui į galutinį radijo dažnį. Norint naudoti tiesioginį radijo dažnio moduliavimą reikia naudoti radijo dažnio moduliatorių. Jei naudojamas tarpinis dažnis IF, tada maišytuvas perduoda galutinį radijo dažnio signalą. Kaip ir imtuvo vidinis generatorius, taip ir siųstuvo vidinis generatorius yra lengvai programuojamas, panaudojant fazės užrakinimo metodą.

3.2. „Software defined radio“ programinė įranga

„Software defined radio“ – programinė įranga skirta radijo signalo apdorojimui. Ji yra pritaikyta prie įvairių operacinių sistemų: Windows 2000/XP/Vista/7/8, Linux, MacOS X. Programa palaiko 32 ir 64 skilčių procesorių platformas. Testavimo aplinkoje yra sukurta „SDR“ programa Android 4.0+ operaciniai sistemai. Pagrindinės programos, kurios suteikia galimybę naudoti programuojamą radijo ryšį kaip radijo imtuvą: SDR Sharp, HDSDR, SDR-RADIO.COM V2, Linrad, GQRX, Studio1, ShinySDR, Sodira, SDR Touch, Wavesink Plus, cuSDR, PowerSDR, QtRadio, Multimode, Sdrangelove, Orbitron ir kt. [18]. Su kai kuriomis iš šių programų (Orbitron, OpenCPN) yra galimybė stebėti komercinių lėktuvų skrydžių planus, ar palydovo padėtį orbitoje.

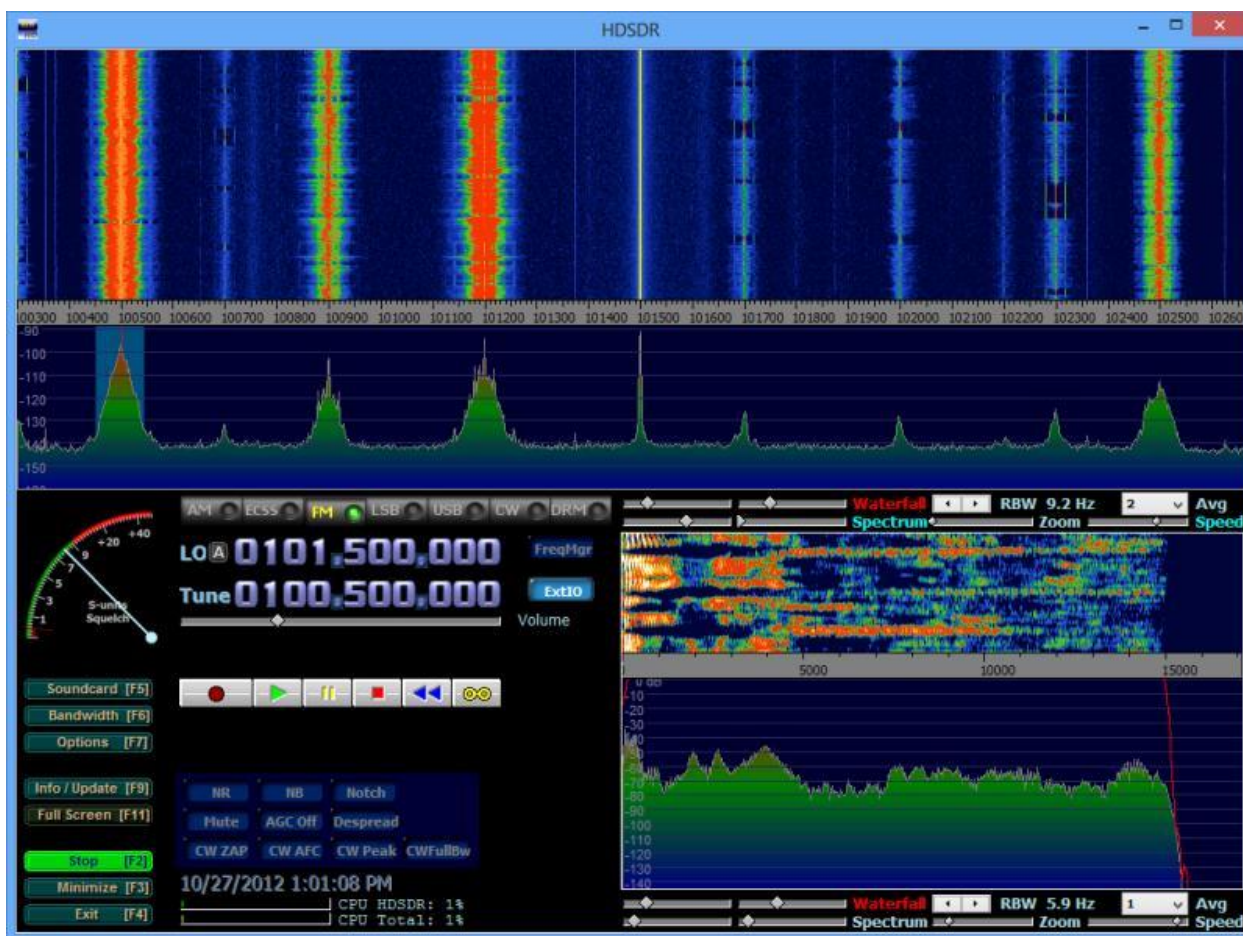
„HDSDR“ programinė įranga

„HDSDR“ – nemokama programinė įranga, skirta „Windows“ operacinėms sistemoms. Dažniausiai ši programa naudojama radijo klausymui, spektro analizavimui, mėgėjiško radijo klausymui (angl. *Ham radio*), trumpųjų bangų radijui. Programą sukūrė Alberto di Bene. Pagrindinės programos savybės yra šios:

- Atskiri spektro ir „tekančio krioklio“ ekranai, skirti stebėti įeinančius ir išeinančius signalus;
- naudojama ekrano raiška yra nuo 640x480 taškų. Maksimalus ekrano taškų skaičius neribojamas;
- lėtas spektro greitis leidžia nustatyti triukšmus ir stebėti trumpųjų bangų pokyčius;
- „AM“, „ECSS“, „FM“, „CW“ signalų demoduliacija;
- siuntimo režimas naudojant „SSB“, „AM“, „FM“, „CW“ modelius;
- reguliuojamas juostinio dažnio filtras;
- programa turi iki 10 reguliuojamų filtrų;
- įrašymas ir atkūrimas iš RF, IF, AF WAV formato failų su įrašymo planavimo galimybe;
- palaiko įvairia aparatinę įrangą su išorinio įrenginio bibliotekos sąsaja;
- programos nustatymai gali būti įrašyti į failą, o po to įkelti iš naujo. Taip galima susikurti keletą skirtingų imtuvų.

„HDSDR“ programos darbinis langas pavaizduotas 3.2.1 paveiksle. Iš paveikslo matome, kad nustatyta dažnio moduliacija (FM). Darbinis dažnis nustatytas ties 101,5 MHz dažnių juosta. Šiuo dažniu Vilniuje transliuojamas radijas. Iš „tekančio krioklio“ matome, kad netoliese esančiais dažniais transliuojamos kitos radijo stotys (100,5 MHz, 100,9 MHz, 101,2 MHz, 102,5 MHz). Kuo „tekančiame krioklyje“ signalas raudonesnis, tuo jis yra stipresnis. Programa leidžia

įrašyti stebimą signalą į failą atliekant amplitudinę arba tarpinio dažnio demoduliaciją. Įrangos matuojamas aplinkos triukšmas yra -140 dB.



3.2.1 pav. „HDSDR“ programos darbinis langas

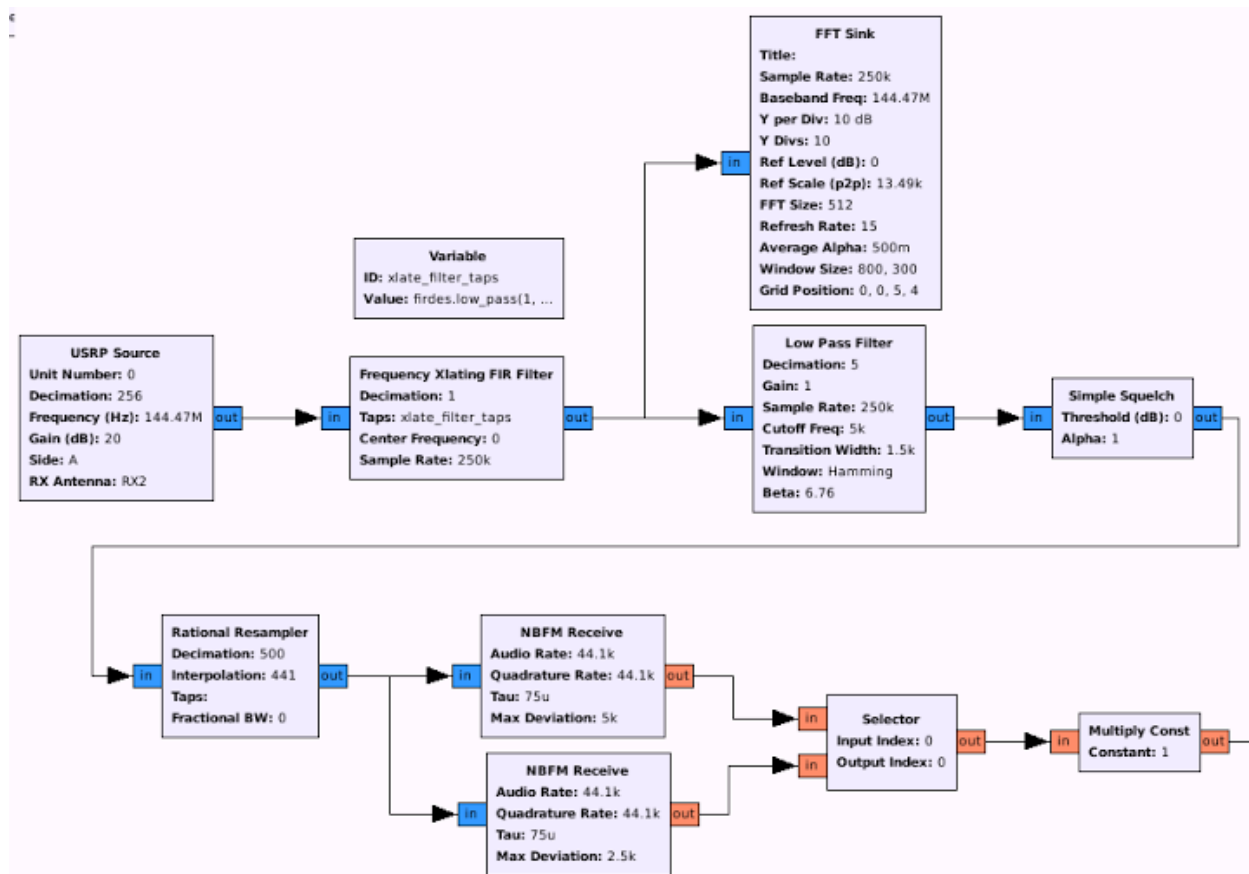
„GNU radio“ programinė įranga

„GNU radio“ yra nemokamas, atviro kodo programinės įrangos kūrimo įrankis, kuris apjungia programavimą į blokų kūrimą, programiniame radijo ryšyje. Programa leidžia suderinti išorinę radijo ryšio aparatinę įrangą su programuojamu radijo ryšiu. Ši programa plačiai naudojama radijo mėgėjų, mokslininkų, komercinių įmonių, siekiant plėtoti belaidžio ryšio komunikacijas ir pasaulinio ryšio sistemas.

„GNU radio“ pradinė aplikacija parašyta „Python“ programavimo kalba, tuo pat metu signalo apdorojimo procesas vykdomas C++ programavimo kalba, panaudojant procesorius su slankiojančio kabelio funkcijomis. Tokiu būdu projektuotojas gali realiu laiku naudoti didelio našumo radijo ryšio sistemas. Programa gali būti naudojama be jokios išorinės aparatinės įrangos. Aplikacija turi keletą iš anksto parašytų blokų, kurie gali būti naudojami kaip signalo generatoriai, skaityti ir rašyti informaciją skirtingais formatais. Daug pavyzdžių yra sukurtų su nebrangia aparatine įranga, tačiau ją tinkamai sukonfigūravus galima gauti aukšto lygio radijo

ryšio sistemą. Su programa galima naudoti šiuos išorinius įrenginius: garso plokštę, universalius programuojamo radijo ryšio įrenginius (angl. *USRP*), specialiuosius „Perseus“ imtuvus.

Kiekviename kompiuteryje yra integruota garso plokštė. Paprasčiausios tokios plokštės turi du kanalus, 16 bitų skiriamąją gebą ir 44,1 kHz diskretizacijos dažnį. Jeigu šių charakteristikų nepakanka, galima naudoti atskiras, didelio našumo garso plokštes. Jos dažniausiai turi daugiau nei 12 kanalų, yra 24 skilčių raiškos. Tokios plokštės jungiamos per PCI arba USB sąsajas. Vėliau buvo sukurti universalūs programuojami radijo ryšio įrenginiai (angl. *USRP*). Šiems įrenginiams priklauso atskiros pagrindinės plokštės su „USB“ arba „Gigabit Ethernet“ sąsajomis, priėmimo ir perdavimo dažnis siekė nuo 0 iki 5,8 GHz. USRP įrenginiai tapo labai našūs, buvo patogų jiems kurti programinę įrangą. Šie įrenginiai naudoja bendrą universalią programinės įrangos tvarkyklę. Kiekvienas įrenginys, kurį palaiko operacinė sistema, gali naudoti „GNU radio“ programinę įrangą. Galima parašyti atskiras tvarkykles kiekvienam įrenginiui kuriant atskirus blokus.

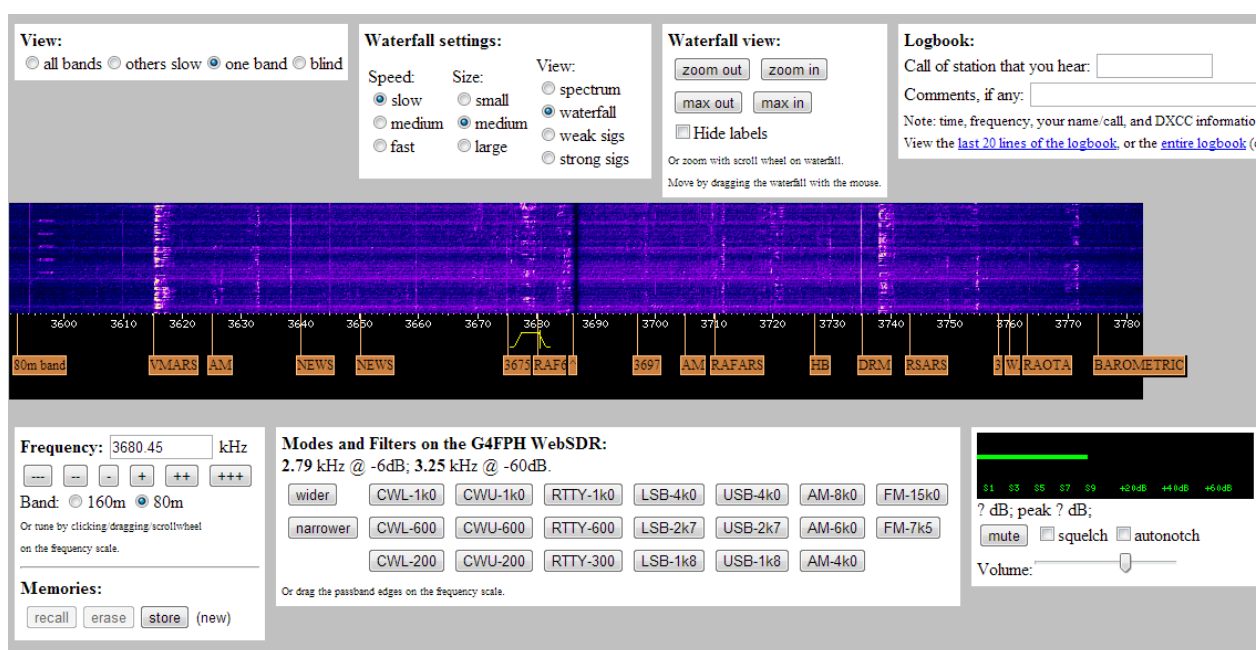


3.2.2 pav. „FM“ imtuvo „GNU radio“ programos blokinė schema [19]

3.2.2 paveiksle pavaizduotas paprastas „FM“ imtuvas, sukurtas su „GNU radio“ programine įranga. Schema sukurta panaudojant atskirus struktūrinius blokus. Schemoje panaudoti NBFM tipo demodulatoriai, leidžiantys keisti nuokrypio dažnį tarp 2,5 kHz ir 5 kHz.

„WebSDR“ programinė įranga

„Web SDR“ – programinio radijo ryšio imtuvai prijungti prie interneto, leidžiantys naudotojams vienu metu prisijungti prie imtuvo, keisti jo parametrus, klausantis tam tikro dažnio. Programinio radijo ryšio technologija leidžia klausytis nepriklausomų, skirtingų signalų. Yra galimybė užduoti klausimą ar palikti komentarą svetainės kūrėjui. 2014-05-22 buvo 80 aktyvių serverių ir 236 aktyvių vartotojų. 3.2.3 paveiksle pavaizduota kaip naudojant „WebSDR“ programinę įrangą galima prisijungti prie vidurio Anglijos imtuvo. Imtuvas priimamų dažnių diapazonas nuo 3,591 MHz iki 3,783 MHz. Prisijungus prie šio imtuvo galime keisti jo darbinis parametrus.



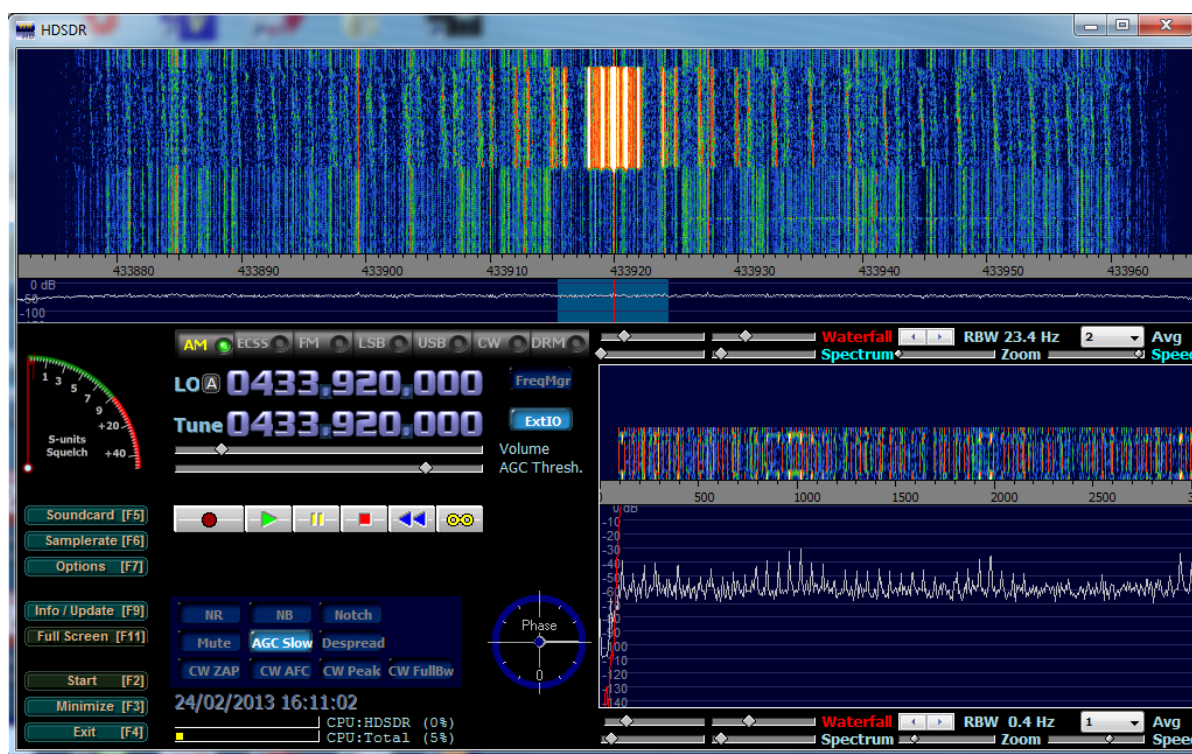
3.2.3 pav. „WebSDR“ programos darbinis langas [20]

3.3. „Software defined radio“ panaudojimas

Programinis radijo ryšys gali būti panaudojamas karinėje pramonėje, komerciniais ar asmeniniais tikslais. SDR gali būti panaudojamas kiekvieno žmogaus butyje. Pirmajame pavyzdyje pateikiama, kaip galima pasigaminti bevielio durų skambučio siųstuvą. Kai siųstuvą išsiunčia signalą, tada suskamba durų skambutis.

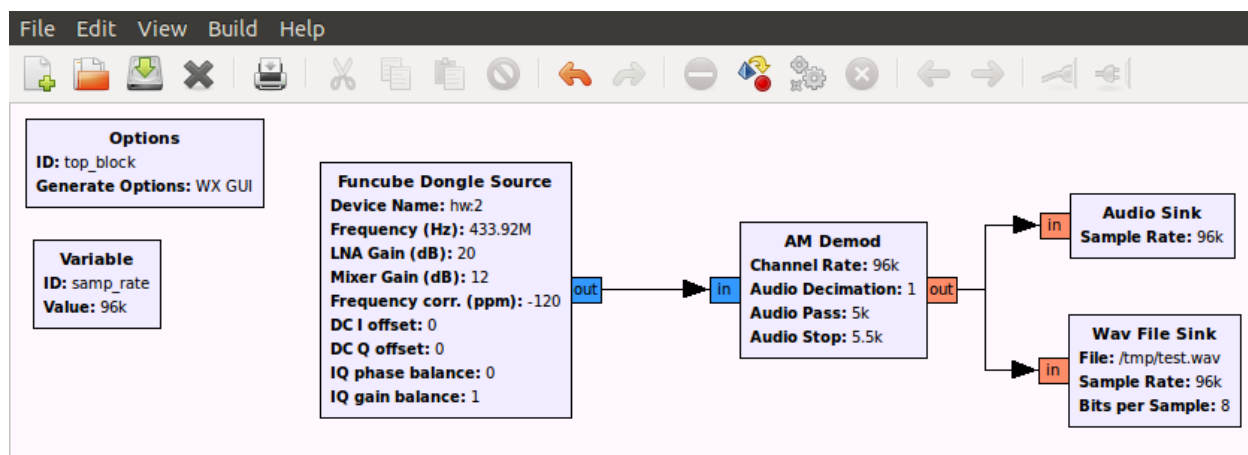
Pirmiausiai reikia nustatyti kokiam dažnių diapazone veikia bevielis durų skambutis. Šiuo atveju, pagal gamintojo specifikaciją, bevielis durų skambutis naudoja 433,92 MHz diapazoną. Prie kompiuterio turi būti prijungtas imtuvas, kuris galėtų priimti 433,92 MHz diapazono bangas. Panaudotas „FunCube dongle“ imtuvas, kuriam nereikalingi papildomos programinės įrangos tvarkyklės. Jos yra įdiegtos operacinėje sistemoje (Windows, Linux, MacOSX). Imtuvas suderinamas su 32 ir 64 skilčių operacinėmis sistemomis. Imtuvo darbo

diapazonas yra nuo 150 kHz iki 1,9 GHz. Kad įsitikintume, kad durų skambutis naudoja tikrai nurodytą dažnį, pasileidžiame programinę įrangą „HSDR“ (3.3.1 pav.)



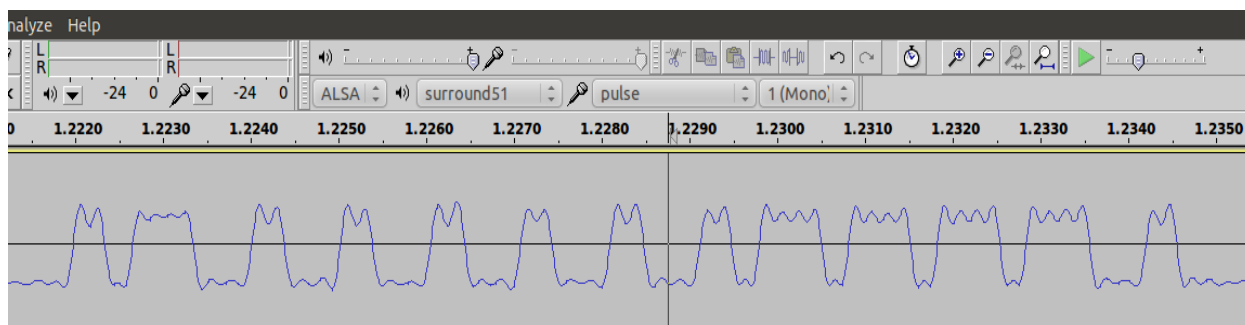
3.3.1 pav. „HSDR“ programos langas [21]

Kadangi bevielis durų skambutis naudoja amplitudinę moduliaciją, reikia nustatyti programos darbo režimą į „AM“. Pagal durų skambučio gamintojo specifikaciją nustatomas 433,92 MHz programos darbinis diapazonas. Paspaudus programos mygtuką „Start“ pradeda skenuoti 433,88 MHz – 433,96 MHz dažnių juosta. Tuo pat metu pasiuntus signalą į durų skambutį, „HSDR“ programa užfiksuoja, kad jos parinktame dažnių ruožo skenavime yra siunčiamas signalas. Tai parodo atsiradusios oranžinės/raudonos linijos, atsiradusios spektro analizatoriuje. Pagal atsiradusias linijas galima nustatyti tikslų signalo dažnį. Žinant tikslų dažnį sudaroma blokinė schema (3.3.2 pav.), skirta signalo apdorojimui.



3.3.2 pav. Signalų apdorojimo blokinė schema [21]

Pagal 3.3.2 paveikslo schemą, matome, kad pirmiausia nustatomas tikslus signalo šaltinio dažnis (433,92 MHz). Toliau signalas praeina pro amplitudinį demoduliatorių ir signalas įrašomas į failą pavadinimu „test“. Demoduliuotą signalą atidarome su bet kokia garso redagavimo programa. (3.3.3 pav.)



3.3.3 pav. Demoduliuotas signalas [21]

Gautą signalą reikia paversti į dvejetainį kodą. 4.4.3 paveiksle demoduliuoto signalo trumpas impulsas atitinka loginį 0, o ilgas impulsas loginį 1. Gauname signalo dvejetainį skaičių: 0100000011110. Gautą skaičių reikia paversti į šešioliktinę skaičiavimo sistemą, gauname – 81E. Gautą kodą reikia įrašyti į siųstuvą ir išsiųsti signalą. Kaip siųstuvą naudojamas „RFCat“ įrenginys. Jis programuojamas per USB sąsają. Šis įtaisas įrašytą skaitmeninį kodą paverčia į radijo dažnius, atliekant amplitudinę moduliaciją. Tinkamai suprogramavus įrenginį ir įrašius gautą kodą, galima siųsti signalą į durų skambutį ir jis suskambės.

3.4. Skyriaus apibendrinimas

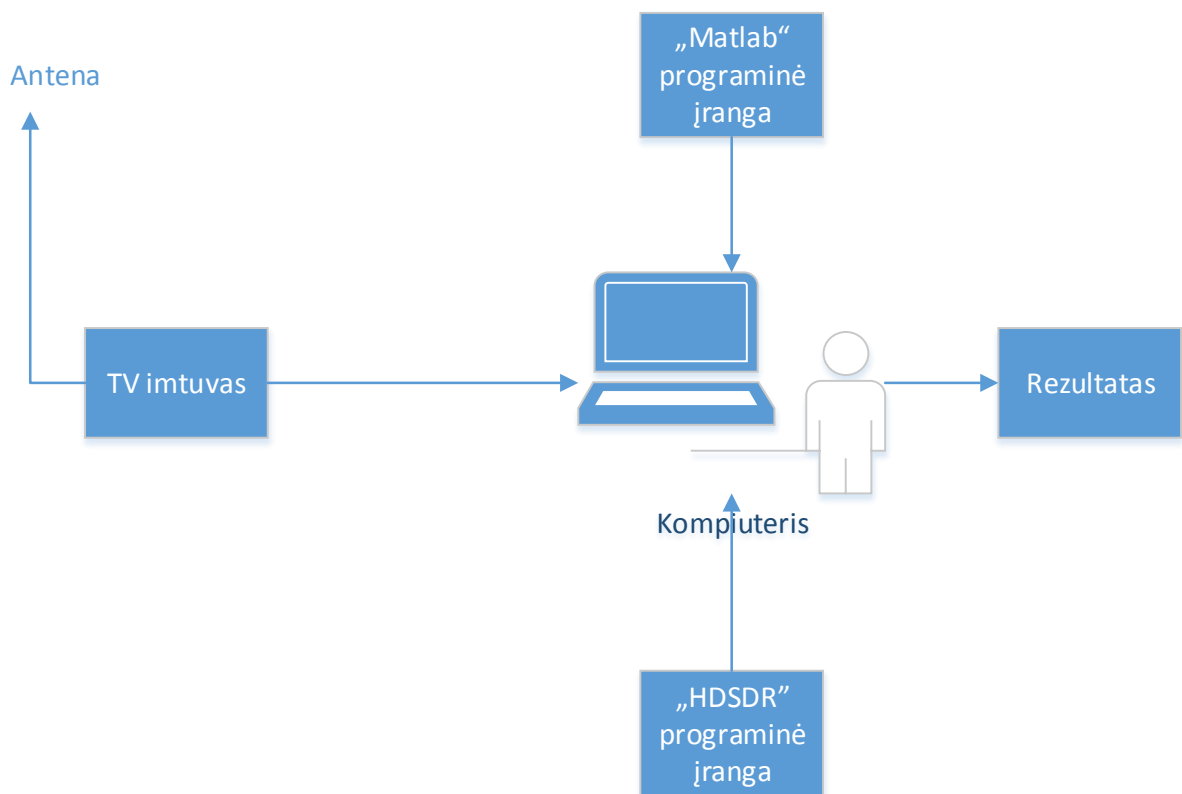
Šiame skyriuje išanalizuota programuojamo radijo ryšio architektūra (angl. *SDR*). Aptarta vienkanalių ir daugiakanalių imtuvų/siųstuvų struktūros. Išsiaiškinta, kokią programinę įrangą gali naudoti „SDR“. Aptartas populiariausių programų panaudojimas. Išsamiai išanalizuotas pavyzdys, kaip galima, pasinaudojant programuojamu radijo ryšiu, perimti ir analizuoti signalus, siunčiamus į bevielį durų skambutį.

Nustatyta, kad „SDR“ gali būti naudojamas analizuojant radijo bangų spektrą, televizoriaus žiūrėjimui, lėktuvų skrydžių maršrutų stebėjimui ir kt. Tolimesniam tyrimui Windows operacinės sistemos aplinkoje pasirinkta naudoti „HDSR“ programinę įrangą, nes ši programa turi galimybę iš karto atlikti signalo amplitudinę demoduliaciją. „GNU radio“ programinė įrangą pasirinkta naudoti Linux operacinės sistemos aplinkoje, nes ši programa turi didžiausią struktūrinių blokų biblioteką, todėl jos programavimo galimybės yra universaliausios.

4. Siunčiamo signalo perėmimo įranga

4.1. Struktūrinė schemos sudarymas

Signalų priėmimo įtaiso struktūrinė schema sudaroma žinant visas funkcijas, kurias turi atlikti projektuojama sistema. Užduotyje parašyta ištirti ir perimti nuotolinio rakto siunčiamus signalus į automobilį. Sudarant struktūrinę schemą reikia įvertinti darbo užduotyje nurodytus reikalavimus. Pagal sudarytą struktūrinę schemą parenkame aparatinę ir programinę įrangą, įvertinami minimalūs sistemos parametrai.



4.1.1 pav. Signalo perėmimo ir analizės struktūrinė schema

Sudaryta struktūrinė schema pavaizduota 4.1.1 paveiksle. Schemą sudaro šie komponentai:

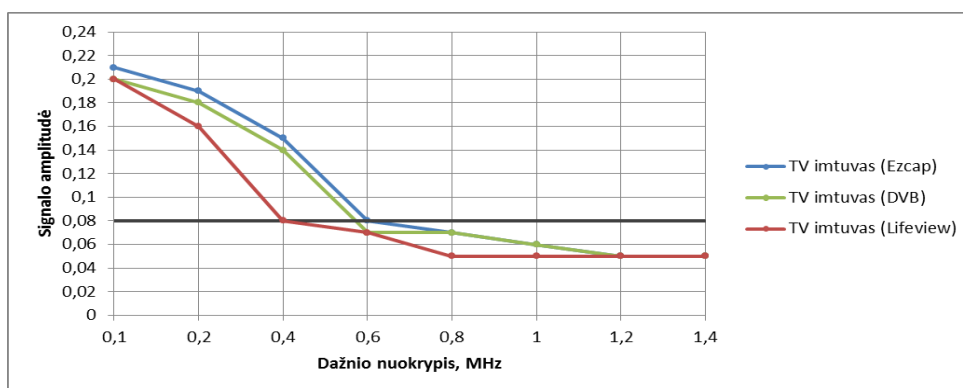
- Antena;
- TV imtuvas;
- Kompiuteris;
- „HSDR“ programinė įranga;
- „Matlab“ programinė įranga.

Pagal numatytas funkcijas buvo sudaryta įtaiso struktūrinė schema. Struktūrinės schemos paskirtis: TV imtuvas sujungtas su kompiuteriu. TV imtuvas skirtas priimti signalus iš pasirinktos dažnių juostos. Naudotojas kompiuteryje, naudodamas „HSDR“ programinę įrangą

gali pasirinkti norima skanuoti dažnių ruožą. Skanuojant pasirinktą dažnių ruožą, stebime ar tame ruože vyksta kokie nors signalų perdavimai. Vykstant signalo perdavimui pasirenkame įrašymo funkciją ir užfiksuotas signalas įrašomas į kompiuterio kietąjį diską ir atliekama signalo amplitudinė demoduliacija. Po to įrašytas signalas yra apdorojamas su „Matlab“ programine įranga, panaudojant specialiai sukurtus signalo apdorojimo algoritmus. Apdorojus signalą gauname rezultatą, kurį galime analizuoti, lyginti jį su kitais signalais ar atlikti signalo transformacijas.

4.2. TV imtuvo parinkimas

Norint naudoti TV imtuvą su programuojamu radijo ryšiu, TV imtuvas turi turėti vieną iš šių valdymo mikroschemų: Elonics E4000, Rafael Micro R820T, Rafael Micro R828D, Fitipower FC0013, Fitipower FC0012, FCI FC2580. TV imtuvas turi turėti USB sąsają, prijungimui prie kompiuterio. Buvo atliekami bandymai su trimis TV imtuvais, siekiant išsiaiškinti kurio techninės charakteristikos labiausiai atitinka mūsų pasirinktus tyrimus. TV imtuvas (Ezcap) naudoja Elonics E4000 valdymo mikroschemą, TV imtuvas (DVB) – Rafael Micro R820T valdymo mikroschemą, TV imtuvas (Lifeview) – FCI FC2580 valdymo mikroschemą.



4.2.1 pav. Signalų amplitudės pasiskirstymas nuo matuojamo dažnio nuokrypio

Iš 4.2.1 paveikslo matome, kad naudojant „Ezcap“ firmos TV imtuvą, signalo santykinė amplitudė yra 0,08 esant 0,6 MHz dažnio nuokrypiui. Tai suteikia galimybę nagrinėti signalą, nežinant kokių tikslų dažnių jis yra perduodamas. Pasirinkus šį TV imtuvą, galime nagrinėti perduodamą signalą su 0,6 MHz dažnio paklaida. Naudojant kitokius TV imtuvus dažnio paklaida yra mažesnė (0,4 MHz. arba 0,59 MHz.).

Panaudotas „EZCAP“ firmos TV imtuvas (4.2.2 pav.) su RTL2832U mikroschema. Įrenginys jungiamas prie kompiuterio per USB 2.0 sąsają. Šio imtuvo paskirtis žiūrėti skaitmeninę televiziją kompiuteryje. Palaiko MPEG2, H.264 (MPEG4) formato kodavimus.

Palaikoma (Windows Vista/7 ir linux) operacinėse sistemose su 32 bitų arba 64 bitų procesoriaus architektūra. Minimalus kompiuterio reikalavimai turi būti tokie:

- Procesoriaus architektūra ne senesnė kaip Pentium IV su 1,7 GHz greičiu;
- ne mažiau negu 512 MB operatyvinės atminties (RAM) arba vaizdo plokštė su ne mažiau kaip 32 MB atminties;
- USB 2.0 sąsaja.



4.2.2 pav. TV imtuvas

Standartinė antena pridedama prie TV imtuvo yra 0,1 m. ilgio. Apskaičiuokime kokiam dažniui esant antena geriausiai priima signalus. Kadangi antenos ilgis sudaro ketvirtį bangos ilgio, gauname kad bangos ilgis $\lambda=0,4$. Iš formulės (1) formulės gauname, kad 0,1 m. ilgio

$$\lambda = \frac{v}{f} \quad (1)$$

antena geriausiai priima signalus perduodamus tokiu dažnių diapazonu:

$$f = \frac{v}{\lambda} = \frac{300000000}{0,4} = 750 \text{ MHz}$$

Mums reikia, kad antena geriausiai veiktų 433 MHz. dažnių diapazone. Apskaičiuokime koks bangos ilgis turėtų būti tokiai antenai:

$$\lambda = \frac{v}{f} = \frac{300000000}{433000000} = 0,69 \text{ m}$$

Kadangi antenos ilgis yra ketvirtis bangos ilgio, gautą bangos ilgį padaliname iš 4 ir gauname, kad mūsų antenos ilgis turėtų būti 0,17 m. Todėl pasirinkta naudoti 0,17 m. ilgio automobilinę anteną, kuri pavaizduota 4.2.3 paveiksle.



4.2.3 pav. Automobilinės antenos strypas

4.3. Kompiuterio konfigūravimas

Kompiuteris buvo naudojamas asmeninis, turintis tokius parametrus:

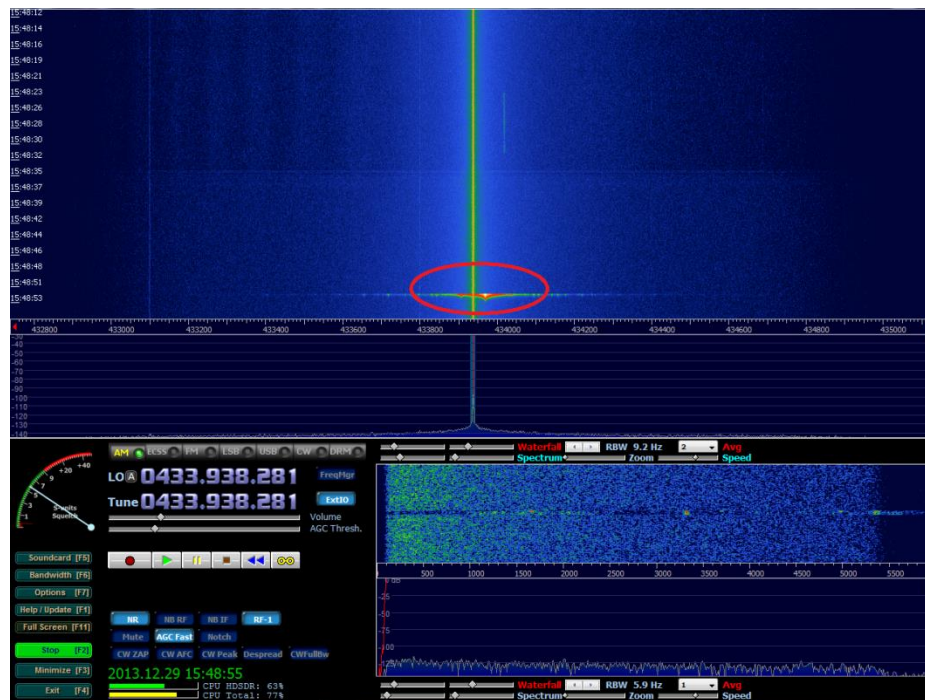
- Intel Core 2 Duo E6420 tipo procesorius su 2,13 GHz greičiu;
- 4 GB operatyvinės atminties;
- Vaizdo plokštė RADEON X1950Pro su 512 RAM atmintimi;
- 500 GB talpos kietasis diskas;
- 64 bitų operacinė sistema Windows 7;
- USB 2.0 sąsaja.

Matome, kad parinkto kompiuterio parametrai pilnai atitinka TV imtuvo keliamus reikalavimus, todėl duomenys iš TV imtuvo į kompiuterį turėtų būti perduodami sklandžiai, be klaidų.

Toliau reikalinga programinė įranga, kuri galėtų stebėti pasirinktą dažnių ruožą, atlikti amplitudinę demoduliaciją ir įrašyti rezultatą į kompiuterį „wav“ tipo formatu. Pasirinkta naudoti „HSDR“ programinę įrangą. Norint sėkmingai paleisti „HSDR“ programinę įrangą su pasirinktu TV imtuvu (4.2.1 pav.) pirmiausia reikia pašalinti originalius „Realtek“ tvarkykles iš sistemos ir įdiegti „Zadig“ tvarkykles. Tada reikia įkelti papildomą biblioteką (ExtIO_RTL.dll) į programos direktoriją. Atlikus šiuos veiksmus „HSDR“ programinė įranga atpažįsta išorinį TV imtuvą ir juo galima naudotis kaip radijo dažnio skaneriu. Tada įrašome „Matlab“ programinį paketą (panaudota R2009a versija), kad būtų galima kurti signalo apdorojimo algoritmus.

4.4. „HSDR“ programinės įrangos konfigūravimas

„HSDR“ programinės įrangos darbinis langas pavaizduotas 4.4.1 paveiksle. Kadangi automobilių raktų signalai siunčiami atliekant amplitudinę moduliaciją pasirenkame AM darbinį režimą. Žinodami, kad tarp rakto ir automobilio signalai perduodami maždaug 433,9 MHz dažnių juostoje, pasirenkame šį dažnį, kaip stebėjimo atskaitos tašką. Dažnio ruožo skanavimas vyksta realiu laiku. „Tekančio krioklio“ darbiniame lange, apibrėžtame apskritime matome, kad tam tikru laiko momentu (15:48:52) įvyko duomenų perdavimas, tarp rakto ir automobilio, 433,99 MHz dažniu. Šiam signalui buvo atlikta amplitudinė demoduliacija ir gauti duomenys įrašyti į kompiuterio kietąjį diską tolimesnei analizei.

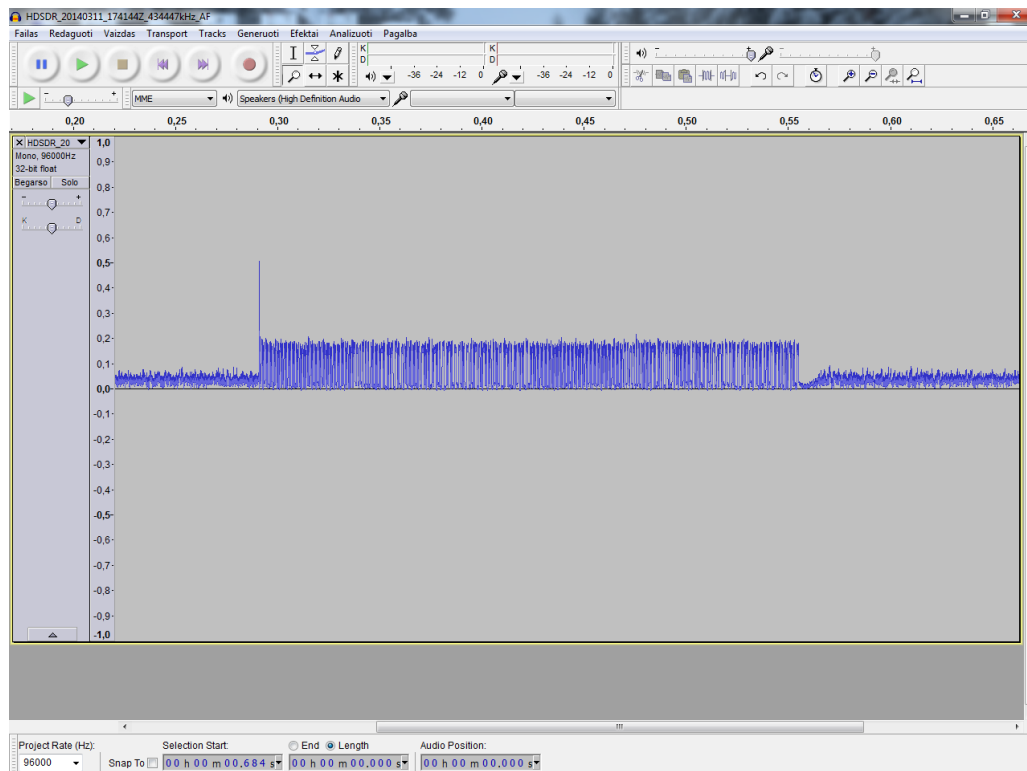


4.4.1 pav. „HDSR“ programinės įrangos darbinis langas

Toliau įrašo apkarpymui ir analizuojamo signalo išskyrimui naudojama „Audacity“ programa. „Audacity“ - nemokama atviro kodo garsų redagavimo ir įrašinėjimo programa. Programa veikia su Linux, Windows ir kt. operacinėmis sistemomis. Pagrindinės funkcijos, kurias gali atlikti „Audacity“ programinė įranga:

- Įrašinėti garsą realiu laiku;
- konvertuoti kasečių įrašus į skaitmeninius įrašus ar kompaktinius diskus;
- redaguoti Ogg Vorbis, MP3, WAV, AIFF failus;
- iškirpti, kopijuoti, įklijuoti, ištrinti, suskaidyti ar miksuoti garsus kartu;
- pakeisti įrašinėjimo greitį ar tono aukštį.

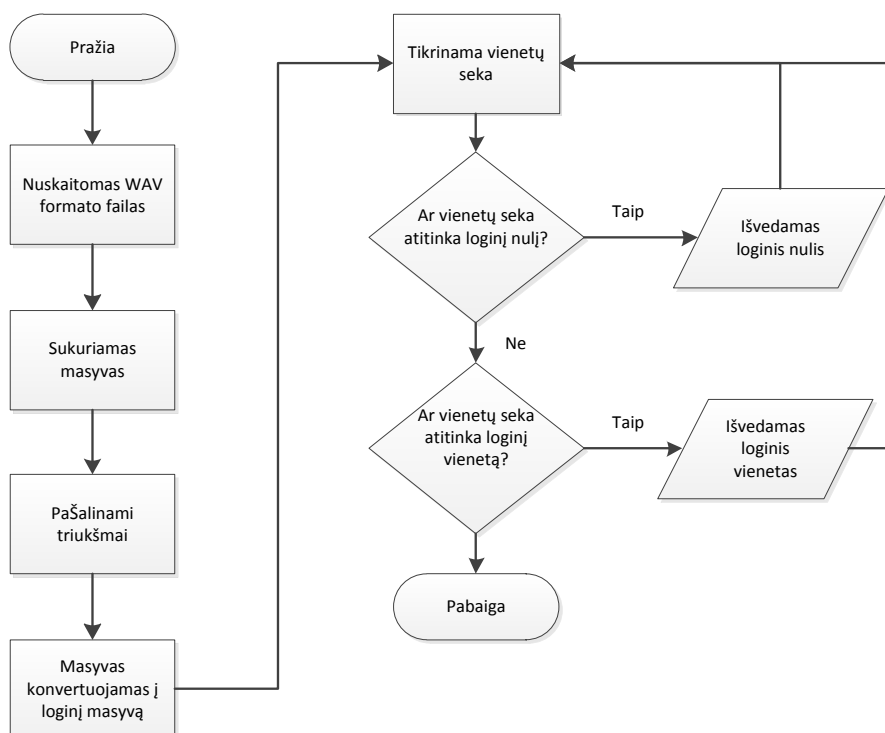
Pasinaudojus šia programa, bus redaguojamas WAV tipo failas. 5.4.2 paveiksle matome įrašą padarytą su „HDSR“ programine įranga. Iš paveikslo aiškiai matome, kad mūsų nagrinėjamas signalas smarkiai išsiskiria iš bendro aplinkos triukšmo. Kadangi įrašas gali būti labai ilgas, reikia rasti mus dominančią signalą. Šį signalą iškerpame ir įrašome į atskirą failą. Tais suteiks galimybę greičiau analizuoti pasirinktą signalą. Naudojant trumpesnį ilgio signalą, bus atliekamas greitesnis jo apdorojimas su „Matlab“ programinės įrangos algoritmu.



4.4.2 pav. „Audacity“ programos langas

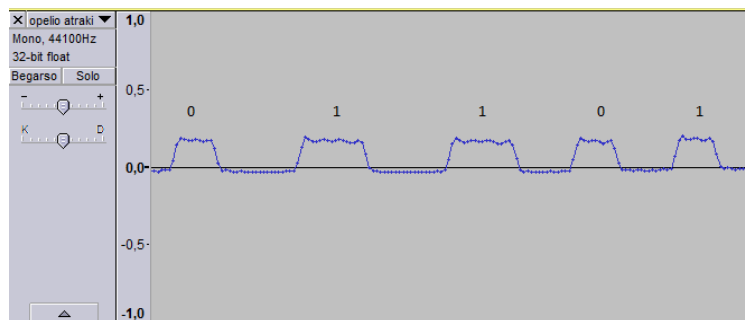
4.5. „Matlab“ algoritmo kūrimas

Siekiant išanalizuoti signalą, kuris perduodamas tarp rakto ir automobilio, buvo sukurtas „Matlab“ programinės įrangos algoritmas. Tikslas – gauti nuskanuoto signalo reikšmę dvejetainėje skaičiavimo sistemoje.



4.5.1 pav. „Matlab“ programos signalo analizės algoritmas

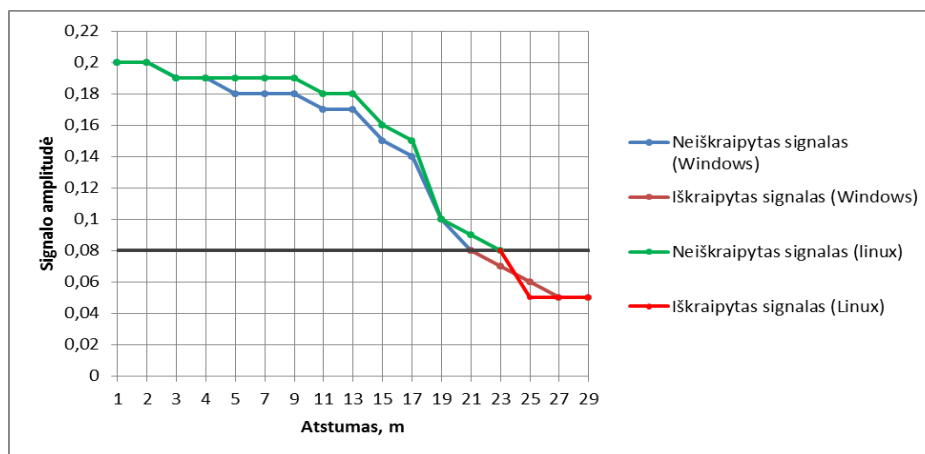
4.5.1 paveiksle pavaizduotas sukurtas „Matlab“ programinės įrangos algoritmas skirtas analizuoti signalą, kuris naudojamas automobilio atrakinimui. Pirmiausiai programa nuskaityto signalą, kuris yra įrašytas WAV formatu. Šiam signalui jau atlikta amplitudinė demoduliacija su programa „HSDR“. Iš nuskaityto signalo yra sukuriamas masyvas. Masyvo dydis tiesiogiai priklauso nuo signalo dydžio. Toliau yra pašalinami triukšmai. Tam tikslui išrenkamos reikšmės iš masyvo kurios yra didesnės už 0,15. Analizuojant kitus signalus ši reikšmė gali skirtis, todėl reikia analizuoti kiekvieno signalo struktūrą atskirai. Visos reikšmės esančios mažesnės už 0,15 prilyginsime triukšmams ir jų nenagrinėsime. Reikšmės didesnės už 0,15 prilyginsime perduodamo signalo reikšmėms. Iš šių reikšmių suformuojame loginį masyvą. Pagal 4.5.2 paveikslą laikysime, kad ilgas perduodamas signalas atitinka loginį „1“, o trumpas – loginį „0“. Iš to gaunasi, kad jeigu iš eilės einančių vienetų seka yra trumpa, vadinasi perduodamas loginis „0“, o jeigu iš eilės einančių vienetų seka ilga – vadinasi loginis „1“. Todėl ir buvo sukurtas loginis masyvas. Toliau programa tikrina ar vienetų seka atitinka loginį „0“, tai reiškia, kad yra tikrinama nuo 1 iki 13 iš eilės einančių vienetų. Jeigu tokių vienetų yra, tada į rezultatą išvedamas nulis ir ieškoma toliau. Jeigu iš eilės einančių vienetų yra daugiau negu 13, tada į rezultatą išvedamas loginis vienetas. Baigus tikrinti visą masyvą programa baigia darbą. Rezultate gauname signalo kodą dvejetainė skaičiavimo sistema. Kadangi skirtingi šifravimo algoritmai naudoja skirtingą impulso pločio moduliaciją (pvz. ilgo pločio impulso signalas prilyginimas loginiam „0“, trumpo impulso signalas loginiam „1“), algoritmas pritaikytas keisti impulso pločio moduliacijos nustatymus. Signalų analizės algoritmo programos kodas pateiktas pirmame priede.



4.5.2 pav. Signalų prilyginimas loginiam „0“ ir „1“

4.6. Perimto signalo kokybės nuo atstumo tyrimas

Atliktas tyrimas siekiant nustatyti kokių maksimalių atstumų su turima sukomplektuota įranga galima perimti ir analizuoti signalą, siunčiamą iš raktų į automobilį. Tyrimas atliktas naudojant skirtingas operacines sistemas (Windows ir Linux).



4.6.1 pav. Signalų amplitudės pasiskirstymas nuo matuojamo atstumo

Iš 4.6.1 paveiksle pavaizduotas signalų amplitudės pasiskirstymas nuo matuojamo atstumo. Jeigu signalų amplitudės vertė yra didesnė negu 0,08, tada signalas yra nuskaitomas pagal sukurtą algoritmą (4.5.1 pav.). Jeigu signalų amplitudė mažesnė 0,08, tada signalas yra nenuskaitomas. Esant atstumui iki 4 m signalų nuskaitymo kokybė yra vienoda su abejomis operacinėmis sistemomis. Naudojant Linux operacinę sistemą, signalų nuskaitymo atstumas yra iki 23 m., o naudojant Windows operacinę sistemą – iki 21 m. Skirtumas yra 2 m., taip yra todėl, kad skirtingose operacinėse sistemose naudojamos skirtingos įrenginio tvarkyklės. Matavimai buvo atlikti naudojant 8 skirtingus automobilių signalizacijos raktus. Paveiksle pavaizduota visų aštuonių bandymų atstumų vidurkis. Bandymo metu pavyko perimti signalus iki 30 m. atstumu, tačiau signalas perimtas iš 22 m. – 30 m. yra iškraipytas, jį sunku analizuoti. Signalų kokybė taip pat priklauso nuo rakto galios, nuo baterijos įkrovimo lygio. Kuo baterija naujesnė, tuo perduodamas signalas stipresnis.

4.7. Skyriaus apibendrinimas

Ketvirtame skyriuje sudaryta struktūrinė schema, pagal kurią bus perimami signalai siunčiami iš rakto į automobilį. Aptartas struktūrinės schemos veikimas. Parenkamas „EZCAP“ firmos USB TV imtuvas, kuris bus naudojamas tolimesniuose tyrimuose. Šis TV imtuvas pasirinktas, nes esant didžiausiam dažnio nuokrypiui (0,06 MHz) sugeba nuskaityti signalą, kurio normalizuota amplitudė didesnė nei 0,08. Apskaičiuojamas antenos ilgis, tinkantis 433 MHz. dažnio juostos diapazonui. Pateikiama programos „HSDR“ konfigūravimo parametrai. Sukuriamas signalų analizės algoritmas, veikiantis „Matlab“ programinėje įrangoje. Pateikiamas detalus algoritmo veikimas. Atliekant tyrimus nustatoma, kad su turima įrangą galime perimti signalą siunčiamą iš už 21 – 23 m. Šis atstumas yra pakankamas, norint analizuoti perduodamus signalus nedidelėje automobilių aikštelėje. Turint aparatinę įrangą ir sukonfigūravus programinę įrangą, galima pradėti bandyti perimti signalus ir juos analizuoti.

5. Automobilių atrakinimo signalų kodų tyrimas

5.1. Automobilių priimamų signalų kodų tyrimas

Siekiant ištirti automobilių atrakinimo signalus, bus tiriamos populiariausios Lietuvoje automobilių markės. Iš viso bus ištirti 27 skirtingų automobilių gamintojų modeliai (Alfa Romeo, Audi, BMW, Chrysler, Citroen, Fiat, Ford, Honda, Hyundai, Land Rover, Lexus, Mazda, Mercedes, Mitsubishi, Nissan, Opel, Peugeot, Renault, Rover, Saab, Seat, Subaru, Suzuki, Toyota, Volkswagen, Volvo, Škoda). Tirama bus kiekvieno gamintojo po vieną automobilį. Bandymai buvo atliekami raktui nuo signalo perėmimo įrangos esant įvairiems atstumams. Atstumai kito nuo 3 metrų iki 20 metrų.

Įsigijus aparatinę įrangą ir sukonfigūravus programinę įrangą galime pabandyti perimti rakto siunčiamą signalą į automobilį. Norint ištestuoti visos sistemos veikimą, pirmiausiai buvo pasirinkta testuoti „Opel“ markės automobilį. Šis automobilis yra „Opel vectra“, pagamintas 1998 m. Šiame automobilyje naudojama nuotolinio rakto sistema. Atliekant bandymus, nustatyta, kad norint išsiaiškinti signalo pilną struktūrą užtenką atlikti bandymą 3 kartus. Todėl bandymai su kitais automobiliais bus atliekami po 3 kartus. Įrašius signalą ir atlikus matematinius skaičiavimus pagal „Matlab“ algoritmą, apdoroto signalo rezultatai pateikti 5.1 lentelėje. Iš šios rezultatų lentelės galime daryti išvadą, kad signalas yra pastovaus ilgio. Matome, kad signalas yra iš dalies kintantis, iš pradžių eina nekintanti signalo dalis, vėliau kintanti. Nekintantis signalas pažymėtas žalia spalva, o kintantis signalas bespalvis. Iš programos „Audacity“ galima nustatyti signalo ilgį sekundėmis. Visais trim bandymais signalo ilgis buvo pastovus, t. y. 0,19 sekundės. Kintama signalo dalis susieta su skaitikliu, pagal 2.2.3 paveikslą. Kodavimo algoritmo gamintojas neatskleidžia.

Nustačius, kad aparatinė ir programinė įranga veikia gerai, toliau buvo atliktas automobilio durų atrakinimo signalų tyrimas su kitais automobiliais. Gautos signalų struktūros dvejetainė sistema pateiktos 5.1.1-5.1.27 lentelėse.

5.1.1 lentelė. „Opel vectra“ durų atrakinimo signalo struktūra

Bandymo Nr.	Opel vectra 1998 m. durų atrakinimo signalo struktūra																										
1	00000100	0...0*	00000001	10101100	11110110	10100110	11111110	00111110	10001101	01001000	11000000	01101011	00111101	10101001	10111111	10001111	10100011	01010010	00110000	00011010	11001111	01101010	01101111	11100011	11101000	11010100	10001100
2	00000100	0...0*	00000001	10101100	11110110	10100110	11110111	01101000	00011000	01000010	01010000	01101011	00111101	10101001	10111101	11011010	00000110	00010000	10010100	00011010	11001111	01101010	01101111	01110110	10000001	10000100	00100101
3	00000100	0...0*	00000001	10101100	11110110	10100110	11110111	01101000	00011100	00010010	11100000	01101011	00111101	10101001	10111101	11011010	00000111	00000100	10111000	00011010	11001111	01101010	01101111	01110110	10000001	11000001	00101110

*- 6 skiltys po aštuonis „0“

5.1.2 lentelė. „Skoda superb“ durų atrakinimo signalo struktūra

Bandymo Nr.	Skoda superb 2007 m. durų atrakinimo signalo struktūra																															
1	0...0*	00100000	00100100	11001000	00001100	10000000	10000001	00010010	01011000	00110100	00001000	00000100	10001000	00000000	00000000	00000000	00000000	00000000	00010010	00000000	11010000	00100000	10010010	10110000	11010000	01000000	01001001					
2	0...0*	00000100	11110000	00000100	10010100	00000110	10011000	00000100	00101000	01010000	10010000	0...0*	00111100	00000001	00101011	00000001	10100110	00000001	00001010	00010100	00100100	00111100	0...0*	00001111	00000000	01001001	01000000	01101001	10000000	01000010	10000101	00001001
3	0...0*	01000100	00000100	00000001	11100000	00001000	10110111	00000000	01101100	10100010	01000001	01001001	0...0*	00000001	11100000	00001000	10110111	00000000	01101100	10100010	01000001	01001001	0...0*	00000011	11000000	00010001	01101110	00000000	11011001	00100010	01000001	01001001

*- 5 skiltys po aštuonis „0“

5.1.3 lentelė. „BMW 5 klasė“ durų atrakinimo signalo struktūra

Bandymo Nr.	BMW 520d 2002 m. durų atrakinimo signalo struktūra																														
1	00010001	01001000	01001100	11110000	01011101	10010000	01000101	00100001	00110011	11000001	01110110	01000001	00010100	10000100	11001111	00000101	11011001	00000100	01010010	00010011	00111100	00010111	01100100	00010001	01001000	01001100	11110000	01011101	10010000		
2	00010001	00001010	00110010	01100111	00001110	10000010	00010000	00001010	00110010	01100111	00001110	10000010	00010000	00001010	00110010	01100111	00001110	10000010	00010000	00001010	00110010	01100111	00001110	10000010	00010000	00001010	00110010	01100111	00001110	10000010	
3	00010001	01100001	10110001	00110010	01011101	11001000	10000011	00001101	10001001	10010010	11101110	01000100	00011000	01101100	01001100	10010111	01110010	00100000	11000011	01100010	01100100	10111011	10010001	00000110	00011011	00010011	00100101	11011100	1	10000010	

5.1.4 lentelė. „Lexus“ durų atrakinimo signalo struktūra

Bandymo Nr.	Lexus GS250 2008 m. durų atrakinimo signalo struktūra																							
1	0...0*	0...0*	0...0**	00100000	00000100	00000100	10100000	01000100	00101100	00011000	01000000	00001001	0...0*	0...0*	0...0***	00000010	00010000	00000010	01001000	00100000	01001000	00001100	00011000	00001001
2	0...0*	0...0*	0...0**	00100000	00010011	00001010	00000000	00000000	10101001	00101101	01000000	00000100	0...0*	0...0*	0...0***	00000110	00000000	10011000	01010000	00100100	10101010	00101011	01010000	00010000
3	0...0*	0...0*	0...0**	00110000	00001010	00100000	00001010	00000100	01001100	10101000	01100100	00100000	0...0*	0...0*	0...0***	0000111	0001000	0101101	00001000	00000000	00001000	01010100	00100001	00001001

*- 6 skiltys po aštuonis „0“

** - 4 skiltys po aštuonis „0“

***- 3 skiltys po aštuonis „0“

5.1.5 lentelė. „Suzuki“ durų atrakinimo signalo struktūra

Bandymo Nr.	Suzuki 4x4 2010 m. durų atrakinimo signalo struktūra																						
1	00001000	10000000	00000000	00100000	00101000	01100001	00000100	00000001	00000001	01000000	00100100	00000100	00000000	01100100	00001010	00101000	00000110	11000010	00101100	01010000	00001011	00010010	01000101
	00100010	00100100	00010100	10100101	10100100	10110000	11001001	00001010	11110101	01101100	11101010	01011001	00010100	00000010	10000001	11011010	01000010	00100010	01001101	01100100	01100111	00111110	00011110
	10100000	10001111	11010111	01000110	10011111	00100010	00000000	01010000	10011010	00000100	00100001	00010000	00100110	10010101	00000100	11011001	11011000	00111011	01111111	11110111	01101000	11011110	11011110
2	00001000	00100000	00010100	00100010	10100011	00101000	00001100	01000000	00001000	10010010	11000001	00000010	10000010	11001000	00000000	00010000	01010110	10001010	00111100	01010000	00000001	00010011	01000001
	10000110	00100000	00000100	01001010	01000101	00111010	01110000	10001111	10010010	10110010	10010110	11111101	11100110	00100000	00000101	10001001	10100100	01011011	11000011	01010000	00000110	00100101	01011111
	01000011	01111000	10110001	00111101	01000110	10000110	01001101	10000111	00010100	00000010	00010101	00101001	10110000	00001010	10000000	00010000	00101010	00000111	01011000	00100010	01111100	01100010	00000000

5.1.6 lentelė. „Toyota“ durų atrakinimo signalo struktūra

Bandymo Nr.	Toyota corola 2002 m. durų atrakinimo signalo struktūra						
1	0...0*	10111010	00000010	00111011	00101110	10001011	10010111
2	0...0*	10111010	10011101	10011010	00101110	10001011	10101010
3	0...0*	10111010	00010010	00101011	00101110	10001011	10100110

*- 4 skiltys po aštuonis „0“

5.1.7 lentelė. „Alfa Romeo“ durų atrakinimo signalo struktūra

Bandymo Nr.	Alfa Romeo 2002 m. durų atrakinimo signalo struktūra																									
1	10010000	0...0*	00100100	00010011	01000110	00010001	10100011	00001100	00011000	10110101	10100101	10110111	00010010	01010001	11110010	11101111	11101010	10000010	11010001	10001100	00000000	00001001				
2	10010000	0...0*	00010011	00100101	00001100	10110000	10100000	11000101	00110011	10110010	10100011	11100000	00001100	11100001	11110000	00100010	00101110	10100010	10010101	00010101	00000001	11000100	10010100	00010100	11110101	10100110
3	10010000	0...0*	10100011	01011000	00001110	10101111	11110101	11110101	10100011	10100000	11100100	01100000	11001111	10110011	11111000	00101010	00000010	00000010	10010101	11010100	10000001	11001110	00010001	11010101	10110101	00000010

*- 6 skiltys po aštuonis „0“

5.1.8 lentelė. „Audi“ durų atrakinimo signalo struktūra

Bandymo Nr.	Audi A4 2000 m. durų atrakinimo signalo struktūra																						
1	00010000	0...0*	00000100	01110010	11000110	01010011	00100010	00001100	00011100	10110000	0...0*	01110100	00010010	01000001	10010010	00001110	01101010	10001110	00010001	10001111	00000100	00000001	11000000
2	00010000	0...0*	10010011	00100101	01001100	10111000	10101000	11000111	10110011	11110010	0...0*	11100010	01001100	11100001	10110000	00100011	00101110	11100010	11010101	01010101	00010001	00000100	10010101
3	00010000	0...0*	10100011	01111000	10001110	10101101	10110101	11100101	10100000	10000000	0...0*	01100100	11001111	10110011	11101000	00001010	01100000	00000000	00010001	01010100	10100001	00001110	00011101

*- 6 skiltys po aštuonis „0“

5.1.9 lentelė. „Chrysler“ durų atrakinimo signalo struktūra

Bandymo Nr.	Chrysler pacifica 2003 m. durų atrakinimo signalo struktūra																		
1	00000001	00100000	0...0*	11000000	00001000	10000011	10010001	00000010	01000000	00110000	00001001	00000100	10001100	00000000	01000000	00011000	00000100	00001100	
2	00000001	0...0*	11111000	00000000	00010100	01000110	10010000	00100100	00101001	00010000	10010001	0...0*	00110100	00100001	00100101	00001001	10100110	00000111	00100000
3	00000001	11000000	0...0*	00100001	11000010	00101000	10100010	00100000	01101000	00100010	00001001	01000001	0...0*	00010001	11100000	00001000	10110111	00000011	

*- 6 skiltys po aštuonis „0“

5.1.10 lentelė. „Citroen“ durų atrakinimo signalo struktūra

Bandymo Nr.	Citroen C4 2001 m. durų atrakinimo signalo struktūra																					
1	00000001	0...0*	00100100	00000100	00100100	00010110	11011111	00011000	00011101	00000000	00110000	01110100	00011100	01000011	10001010	00010100	00000001	00111110	00100100	00100000	00111000	
2	00000001	0...0*	00100100	00000100	00100100	01000111	00010011	00010100	00000100	00000100	10100000	01110100	00011100	01000011	10001010	00010100	00000001	00111110	01101000	00101100	00101011	
3	00000001	0...0*	00100100	00000100	00100100	11010101	00010111	00001100	00010000	00001100	10111100	01110100	00011100	01000011	10001010	00010100	00000001	00111110	11101000	00101011	00101001	

*- 6 skiltys po aštuonis „0“

5.1.11 lentelė. „Fiat“ durų atrakinimo signalo struktūra

Bandymo Nr.	Fiat Punto II 2003 m. durų atrakinimo signalo struktūra								
1	00000100	0...0*	01101010	01101010	10011010	00011000	00000011	10010101	00011001
2	00000100	0...0*	01101010	01011101	10011010	00011000	10100001	10010101	00011001
3	00000100	0...0*	01101010	00001100	10011010	00011000	00100010	10010101	00011001

*- 3 skiltys po aštuonis „0“

5.1.12 lentelė. „Ford“ durų atrakinimo signalo struktūra

Bandymo Nr.	Ford Mondeo 1994 m. durų atrakinimo signalo struktūra																		
1	00000001	0...0*	01101000	00001100	11011100	00011000	01111110	01101010	10011010	00001100	01100000	00000000	10110101	01100111	11100010	10000100	00101101	00000011	00110100
2	00000001	0...0*	01101000	00001100	11011100	00011000	01111110	01101010	10011010	00001100	01100000	00000000	10110101	01100111	11100010	10000100	00101101	00000011	00110100
3	00000001	0...0*	01101000	00001100	11011100	00011000	01111110	01101010	10011010	00001100	01100000	00000000	10110101	01100111	11100010	10000100	00101101	00000011	00110100

*- 5 skiltys po aštuonis „0“

5.1.13 lentelė. „Honda“ durų atrakinimo signalo struktūra

Bandymo Nr.	Honda accord 2000 m. durų atrakinimo signalo struktūra																		
1	0...0*	00010011	00000011	10010011	00000011	00010001	00010010	00010000	00011111	00010011	00011111	00000000	01010000	00110011	00010001	00000011	00010001	00110011	11010011
2	0...0*	00000010	00000001	11100111	00100011	00011100	00011010	00011010	00011101	00111011	00000111	00100000	01011000	00111111	01110001	00011011	00000001	00100011	11011111
3	0...0*	00100000	00110000	00110000	00000001	01010000	00001000	00001100	00001100	00111000	00111111	00000100	00001111	00110000	00000001	00010000	00101000	00110000	00001111

*- 4 skiltys po aštuonis „0“

5.1.14 lentelė. „Hyundai“ durų atrakinimo signalo struktūra

Bandymo Nr.	Hyundai Lantra 1996 m. durų atrakinimo signalo struktūra															
1	00000100	00010011	01010110	00010001	10101011	00001100	00011000	10110101	10100101	10110111	00000010	01010001	11110010	11111111	11001010	10010010
2	00010011	00100101	00010011	10110000	10101000	11000101	00110001	10110010	10100111	11100100	00001100	11100101	11100000	00100010	00101110	10101010
3	00010011	01011000	01001110	10101111	11110101	11110101	10100111	10100000	11101100	01100001	11001111	10110011	11011000	00101000	00000010	00100010

5.1.15 lentelė. „Land Rover“ durų atrakinimo signalo struktūra

Bandymo Nr.	Land Rover Freelander 1999 m. durų atrakinimo signalo struktūra																			
1	0...0*	0...0**	00100100	00100000	00000100	00000100	10100000	01000100	00101100	00001000	01000000	00001001	0...0*	0...0**	00100000	00000010	00010100	00100010	01001000	
2	0...0*	0...0**	00100010	00100010	00000011	00001010	00000000	00010000	10101001	00101101	01000100	00000100	0...0*	0...0**	00001001	00000110	00010000	10011000	01010000	
3	0...0*	0...0**	00100001	00110000	00001010	00100000	00001010	00010100	01001100	10100000	01100100	00100000	0...0*	0...0**	00100110	0000111	0001000	0101101	01101000	

*- 6 skiltys po aštuonis „0“

** - 5 skiltys po aštuonis „0“

5.1.16 lentelė. „Mazda“ durų atrakinimo signalo struktūra

Bandymo Nr.	Mazda 323F 2003 m. durų atrakinimo signalo struktūra																			
1	00001000	10000000	00000011	00100001	00101000	01100001	00000100	00000011	01000001	01010000	10000000	00000000	00100000	00101000	01100001	00000100	00000001	00100001	01000000	
2	00001000	10000000	00001000	00101000	00101000	01100001	00000100	00000001	00000011	01000100	10000000	00000000	00100000	00101000	01100001	00000100	00000001	00000001	01010000	
3	00001000	10000000	00000000	00100000	00101000	01100001	00000100	00100001	00000001	01000001	10000000	00000000	00100000	00101000	01100001	00000100	00000001	00110001	01001000	

5.1.17 lentelė. „Mercedes“ durų atrakinimo signalo struktūra

Bandymo Nr.	Mercedes C200 2001 m. durų atrakinimo signalo struktūra																					
1	00100001	00100011	0..0*	01100100	01001001	00010000	10000100	11001110	00000101	11010001	00000100	01000010	00010011	00110100	00100011	00110010	11000000	01100110	01000101	01000010	00000011	
2	00100001	00100011	0..0*	00001110	10000010	00010000	00001010	00110010	01100111	00001110	10000010	00010000	01001010	00100010	00001010	00110011	01000111	00001110	10000000			
3	00100001	00100011	0..0*	11101110	01000100	00011000	01101100	01000100	10010111	01110010	00100000	11000011	01100010	01100100	00001101	10001001	10010010	10101110	01000100	11000011	01100000	01100110

*- 4 skiltys po aštuonis „0“

5.1.18 lentelė. „Mitsubishi“ durų atrakinimo signalo struktūra

Bandymo Nr.	Mitsubishi Carisma 1997 m. durų atrakinimo signalo struktūra														
1	00010010	10100010	10000110	11101101	11100010	01100001	00000001	10001001	10100100	01011010	00000011	00000101	00100101	00000101	
2	00010010	10100010	10000110	11101101	11000110	00100100	00000001	10001001	10100100	00010011	11001011	00000101	00100101	00000101	
3	00010010	10100010	10000110	11101101	11100100	00100000	00000001	10001001	10100100	01011001	11001111	00000101	00100101	00000101	

5.1.19 lentelė. „Nissan“ durų atrakinimo signalo struktūra

Bandymo Nr.	Nissan Almera 2002 m. durų atrakinimo signalo struktūra														
1	00000100	00000100	00010110	11011111	00011001	00011101	00010000	00110000	00110100	00010100	01000011	10001010	00010100	00001001	
2	00000100	00000100	01001111	10010011	00010100	01000100	00000100	10100100	00110100	00010100	01000011	10001010	00010100	00001001	
3	00000100	00000100	11010101	00010111	00101100	00010010	00001100	10111100	00110100	00010100	01000011	10001010	00010100	00001001	

5.1.20 lentelė. „Pegeot“ durų atrakinimo signalo struktūra

Bandymo Nr.	Pegeot 406 2003 m. durų atrakinimo signalo struktūra																			
1	00000110	10010001	00000010	01011000	00100100	00001000	00000100	10001000	00000000	00000000	00100000	00000000	00100000	00010010	00000000	11010000	00100000	10000010	10110000	
2	00000110	10011000	00000100	00101010	01000000	10010000	0...0*	00111100	01000001	00100101	00000001	10110110	00000001	00101010	00010100	00100100	00111100	0...0*	00001101	
3	00000110	10100111	00010011	01101100	10100010	01000000	01001001	0...0*	00000001	11100000	00001000	10100111	00100000	01101100	10100010	01000001	01001001	0...0*	01100011	

*- 4 skiltys po aštuonis „0“

5.1.21 lentelė. „Renault“ durų atrakinimo signalo struktūra

Bandymo Nr.	Renault Laguna 1999 m. durų atrakinimo signalo struktūra															
1	10001011	0...0*	01010001	00000001	00010011	10001010	00111100	01010000	00111100	01010001	00001001	00010011	00110100	01010000	00100001	00010111
2	10001011	0...0*	01010000	00010110	00100101	01011111	11000010	01010010	11100011	01010001	00000110	00100101	11000011	01010000	00000110	00100001
3	10001011	0...0*	00100010	01110100	01101010	00010111	01111000	00100010	01111000	00100011	01111100	01101010	01010000	00100010	01111100	01100010

*- 5 skiltys po aštuonis „0“

5.1.22 lentelė. „Rover“ durų atrakinimo signalo struktūra

Bandymo Nr.	Rover 620 1997 m. durų atrakinimo signalo struktūra											
1	00000110	0...0*	01101011	01101010	00011010	00011100	00000011	10000101	00010001	00001100	0...0*	01000100
2	00000110	0...0*	01101000	01011101	10111110	00011000	10000001	10010101	00011001	00100000	0...0*	00000001
3	00000110	0...0*	01101010	00001000	10011010	00011000	00100010	00000101	00011001	00000100	0...0*	00100100

*- 4 skiltys po aštuonis „0“

5.1.23 lentelė. „Saab“ durų atrakinimo signalo struktūra

Bandymo Nr.	Saab 93 2004 m. durų atrakinimo signalo struktūra																							
1	0...0*	01000000	11001000	00001101	11000000	10000001	00011010	01010000	00110101	00001000	00000100	10001000	00000000	00000000	00000000	00000000	00010010	00000000	00000010	01100000	00100001	00101000		
2	0...0*	11100000	00010100	10000100	01000110	10010000	00010100	00111000	01010100	10010000	0...0*	00111100	00000001	00100101	00000001	10100110	00001001	00001010	00010100	00001000	00011000			
3	0...0*	10111001	10000011	11100001	00001001	10110011	01000000	01100100	10101010	01000001	01001001	0...0*	00000001	11100000	00001000	10110110	00000000	01101100	10100010	00000110	00000000	11100011	00001001	

*- 4 skiltys po aštuonis „0“

5.1.24 lentelė. „Seat“ durų atrakinimo signalo struktūra

Bandymo Nr.	Seat Ibiza 2002 m. durų atrakinimo signalo struktūra																			
1	00000110	00010010	00000010	01000000	00101000	01001000	00001101	00011000	00001111	00000011	00010000	00100010	01001001	00100100	01001100	00000010	00110000	00000010	01101000	
2	00000110	00010010	10001000	01010001	00111100	10001010	00101011	01110000	00010000	00000110	00000000	10011000	01110000	00111100	11101010	00010110	00000001	10111000	01110000	
3	00000110	00010010	01001101	00001000	00100000	00001001	01000100	00100011	01001001	01001101	00001000	01111001	00001000	00100000	00001001	00001110	00101000	01101101	00101000	

5.1.25 lentelė. „Subaru“ durų atrakinimo signalo struktūra

Bandymo Nr.	Subaru Outback 2005 m. durų atrakinimo signalo struktūra																									
1	00001001	0...0*	11000000	01110110	01100001	00110100	10001100	11001101	00000111	11011101	00100100	01110010	00010001	00110100	00010111	01110100	00110001	01000000	01001000	11110010	01011101	00100001	00110011	11000101		
2	00001001	0...0*	01100111	00011110	10010010	00110000	01001010	00100010	01100011	01001110	11000010	00011000	00001110	00110110	01100101	00001110	10001010	00010000	00001010	00110010	01100111	00111010	00110010	01100111	00001010	11101010
3	00001001	0...0*	10010011	01101110	01000110	00011001	01101110	01000100	10010011	01010010	00110000	10000011	01100011	01100101	10111011	11010001	01000110	00011001	00000011	00100101	11011100	00001101	10001001	11010010	00001111	

*- 5 skiltys po aštuonis „0“

5.1.26 lentelė. „Volkswagen“ durų atrakinimo signalo struktūra

Bandymo Nr.	Volkswagen golf IV 2002 m. durų atrakinimo signalo struktūra																			
1	00010000	0...0*	00100100	01100010	11010110	01010011	01100010	01001100	01011100	10110000	0...0*	01110100	00010010	01001001	10010010	00001010	00101010	10001100	00010101	
2	00010000	0...0*	11010001	00101101	01101100	10110000	10101000	11110111	10110011	11110110	0...0*	11100010	01001100	11100001	10111000	00101011	00001110	11100010	11111101	
3	00010000	0...0*	11100011	01110000	10011110	10101101	10010101	11100101	10100000	10000000	0...0*	01100100	11001101	10110011	11101000	00101000	01101000	00001000	01010011	

*- 6 skiltys po aštuonis „0“

5.1.27 lentelė. „Volvo“ durų atrakinimo signalo struktūra

Bandymo Nr.	Volvo S40 2002 m. durų atrakinimo signalo struktūra											
1	0...0*	11111010	00001010	00111011	00001010	10001011	10010111	0...0*	10111010	00000010	00111011	00101110
2	0...0*	11111010	10011101	10011010	00001010	10001011	10101010	0...0*	10111010	10011101	10011010	00101110
3	0...0*	11111010	00110010	00101011	00001010	10001011	10100110	0...0*	10111010	00010010	00101011	00101110

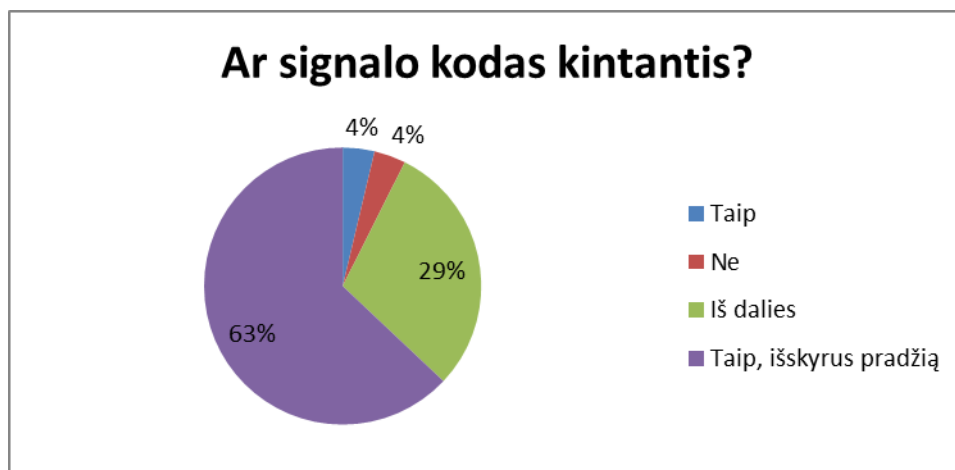
*- 5 skiltys po aštuonis „0“

5.1.28 lentelė. Rezultatų analizė

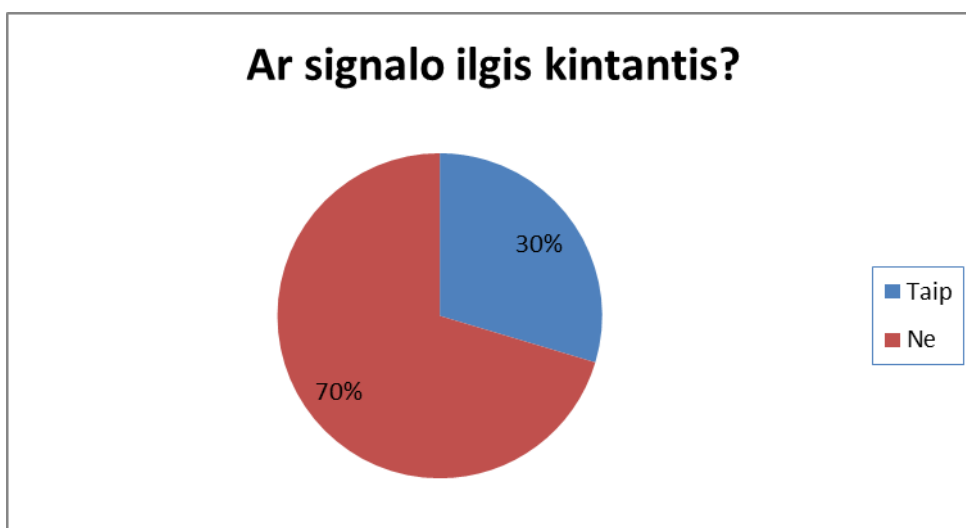
Nr.	Automobilio markė	Signalų ilgis, s	Ar kintamas signalo ilgis?	Ar kintantis signalo kodas?
1	Opel vectra 1998 m.	0.19	Ne	Iš dalies
2	Skoda superb 2007 m.	0.26-0.4	Taip	Taip, išskyrus pradžią
3	BMW 520d 2002 m.	0.3-0.34	Taip	Taip, išskyrus pradžią
4	Lexus GS250 2008 m.	0.43	Ne	Taip, išskyrus pradžią
5	Suzuki 4x4 2010 m.	0.43	Ne	Taip, išskyrus pradžią
6	Toyota corola 2002 m.	0.15	Ne	Iš dalies
7	Alfa Romeo 145 2002 m.	0.48-0.5	Taip	Taip, išskyrus pradžią
8	Audi A4 2000 m.	0.4	Ne	Taip, išskyrus pradžią
9	Chrysler pasifica 2003 m.	0.4-0.44	Taip	Taip, išskyrus pradžią
10	Citroen C4 2001 m.	0.3	Ne	Iš dalies
11	Fiat Punto II 2003 m.	0.17	Ne	Iš dalies
12	Ford Mondeo 1994 m.	0.39	Ne	Ne
13	Honda accord 2000 m.	0.17	Ne	Taip, išskyrus pradžią
14	Hyundai Lantra 1996 m.	0.2	Ne	Taip
15	Land Rover Freelander 1999 m.	0.45	Ne	Taip, išskyrus pradžią
16	Lexus GS250 2008 m.	0.22	Ne	Iš dalies
17	Mazda 323F 2003 m.	0.38-0.42	Taip	Taip, išskyrus pradžią
18	Mercedes C200 2001 m.	0.3	Ne	Iš dalies
19	Mitsubishi Carisma 1997 m.	0.32	Ne	Iš dalies
20	Peugeot 406 2003 m.	0.27-0.42	Taip	Taip, išskyrus pradžią
21	Renault Laguna 1999 m.	0.18	Ne	Taip, išskyrus pradžią
22	Rover 620 1997 m.	0.24	Ne	Taip, išskyrus pradžią
23	Saab 93 2004 m.	0.3-0.5	Taip	Taip, išskyrus pradžią
24	Seat Ibiza 2002 m.	0.29	Ne	Taip, išskyrus pradžią
25	Subaru Outback 2005 m.	0.3-0.34	Taip	Taip, išskyrus pradžią
26	Volkswagen Golf IV 2002 m.	0.4	Ne	Taip, išskyrus pradžią
27	Volvo S40 2002 m.	0.18	Ne	Iš dalies

Iš 5.1.28 lentelės gautų rezultatų matome, kad skirtingų automobilių gamintojai, naudoja skirtingo ilgio durų atrakinimo signalus. Matome, kad siunčiami signalai laiko atžvilgiu skiriasi. Siuntimo signalo laikas kinta nuo 0,17 s iki 0,5 s. Iš 27 - ties tirtų automobilių 8 naudoja kintamo ilgio signalą, kiti pastovaus ilgio signalą. Iš 5.1.12 lentelės matome, kad vienas iš ištirtų automobilių, durų užraktui naudojo nekintamą signalo kodą. Atlikus tris bandymus, nustatyta, kad visais atvejais naudojamos toks pats signalo kodas. Šis signalo kodas yra pastovus, signalo ilgis nekinta. Tai 1994 m. laidos automobilis „Ford Mondeo“. Išsiaiškinta, kad šis automobilis naudoja ne gamyklinę signalizaciją.

17 Automobiliai naudoja kaskart kintantį kodą išskyrus jo pradžią, likę 8 naudoja iš dalies kintantį kodą. Tai reiškia, kad dalis signalo yra pastovus, kita dalis kintanti. Procentinis kintamo signalo ilgio ir kintamo signalo kodo pasiskirstymas pateiktas 5.1.1 ir 5.1.2 paveiksluose.



5.1.1 pav. Signalo kodo kitimo pasiskirstymas



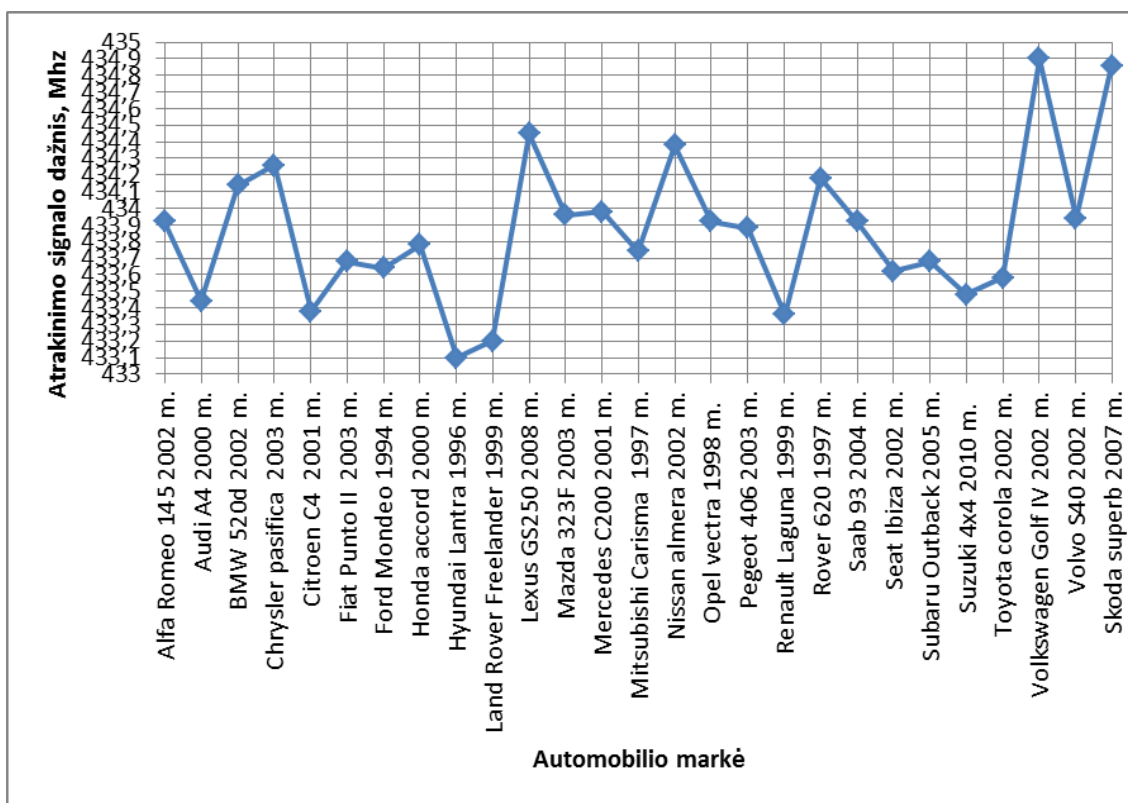
5.1.2 pav. Signalo ilgio kitimo pasiskirstymas

5.1.2 paveiksle matome, kad iš visų tirtų automobilių 29 % naudoja iš dalies kintantį kodą. 63 % naudoja kintantį signalą, išskyrus signalo pradžią. Po 4 % automobilių naudoja visiškai nekintamą ir visiškai kintamą signalo kodą. Galime daryti prielaidą, kad vienoda signalo kodo pradžia reikalinga automobiliui žinoti ar siunčiamas signalas yra skirtas jam ar ne. 5.1.2 paveiksle matome, kad 70 % tirtų automobilių naudoja kintamo ilgio signalą, 30 % nekintamo ilgio signalą.

5.1.29 lentelėje pateikiama automobilio durų atrakinimo signalo dažniai. Iš jau testuotų automobilių nustatyta, kad signalo dažniai yra įvairūs ir kinta nuo 433,1 MHz iki 434,9 MHz. Lentelėje pateikiama automobilio užrakto sistemos gamintojai, kuriuos naudoja tiriami automobilių gamintojai. Kai kurie automobilių gamintojai nenurodo firmų, kurie jiems tiekia apsaugos signalizacijos sistemas. 5.1.3 paveiksle pavaizduota kokį tikslų dažnį naudoja konkretus automobilis. Tikslus dažnis reikalingas, nes maksimalus nuokrypis nuo darbinio dažnio gali būti iki 0,6 MHz. Jei dažnio nuokrypis didesnis, su turima įranga, signalas tampa nebeuskaitymas.

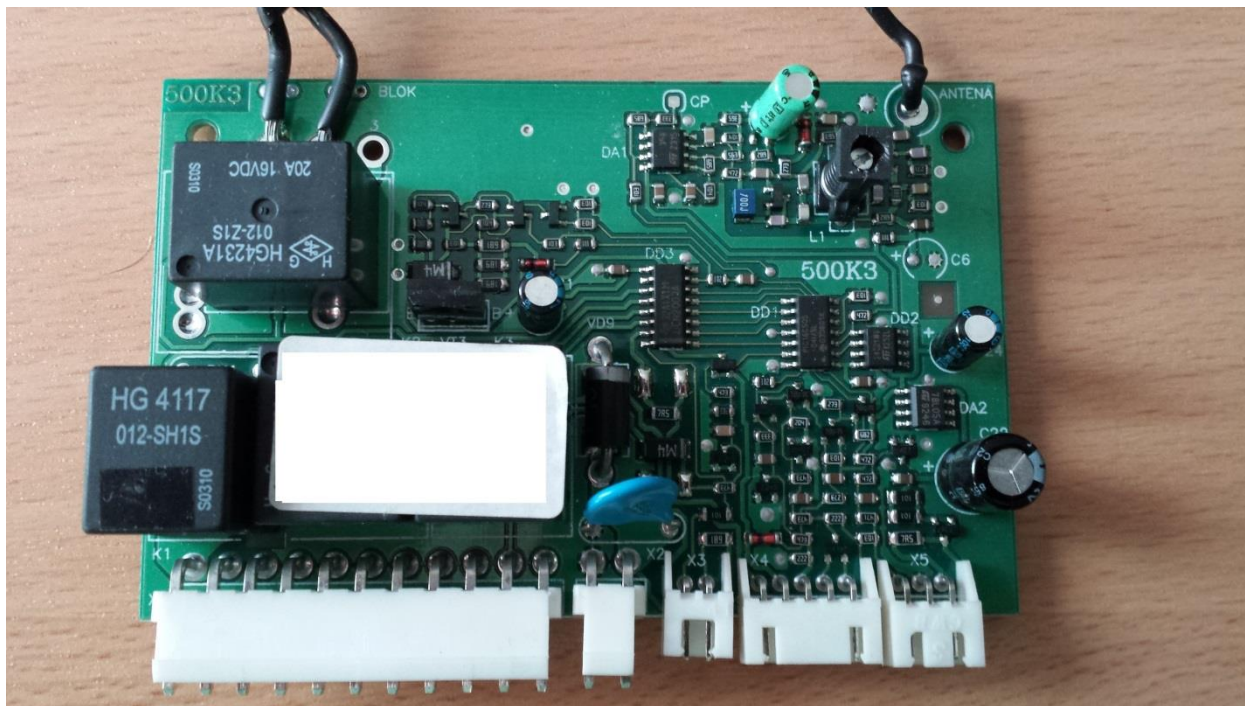
5.1.29 lentelė. Automobilinio užraktų sistemos gamintojai

Automobilio modelis	Signalų dažnis	Rakto mikroschemos gamintojas
Alfa Romeo 145 2002 m.	433,92 MHz	-
Audi A4 2000 m.	433,44 MHz	Hella
BMW 520d 2002 m.	434,14 MHz	-
Chrysler pasifica 2003 m.	434,26 MHz	-
Citroen C4 2001 m.	433,38 MHz	Delphi
Fiat Punto II 2003 m.	433,68 MHz	TRW
Ford Mondeo 1994 m.	433,64 MHz	Siemens
Honda accord 2000 m.	433,78 MHz	Valeo
Hyundai Lantra 1996 m.	433,10 MHz	-
Land Rover Freelander 1999 m.	433,20 MHz	-
Lexus GS250 2008 m.	434,45 MHz	-
Mazda 323F 2003 m.	433,96 MHz	Siemens
Mercedes C200 2001 m.	433,98 MHz	-
Mitsubishi Carisma 1997 m.	433,74 MHz	-
Nissan almera 2002 m.	434,38 MHz	-
Opel vectra 1998 m.	433,92 MHz	Delphi
Peugeot 406 2003 m.	433,88 MHz	Delphi
Renault Laguna 1999 m.	433,36 MHz	JCI
Rover 620 1997 m.	434,18 MHz	-
Saab 93 2004 m.	433,92 MHz	-
Seat Ibiza 2002 m.	433,62 MHz	Hella
Subaru Outback 2005 m.	433,68 MHz	-
Suzuki 4x4 2010 m.	433,48 MHz	-
Toyota corola 2002 m.	433,58 MHz	Tokai Rika
Volkswagen Golf IV 2002 m.	434,90 MHz	Hella
Volvo S40 2002 m.	433,94 MHz	Siemens-VDO
Skoda superb 2007 m.	434,86 MHz	-



5.1.3 pav. Signalų dažnių pasiskirstymas pagal automobilio markę

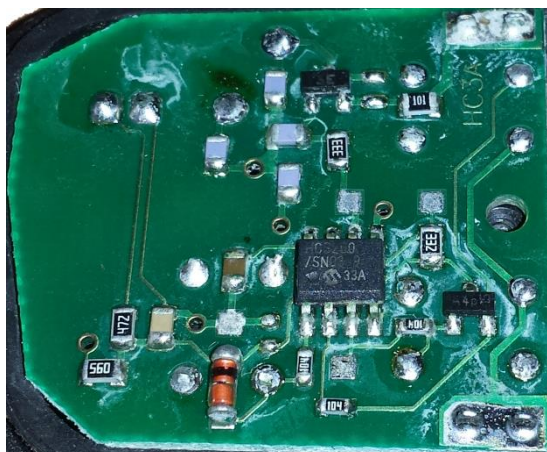
Toliau buvo atliekamas tyrimas su Lietuvoje pagaminta automobilių signalizacija. Tikslas yra apžvelgti pagrindinius spausdintinės plokštės elementus ir ištirti perduodamų signalų struktūras.



5.1.4 pav. Automobilio signalizacijos valdymo blokas

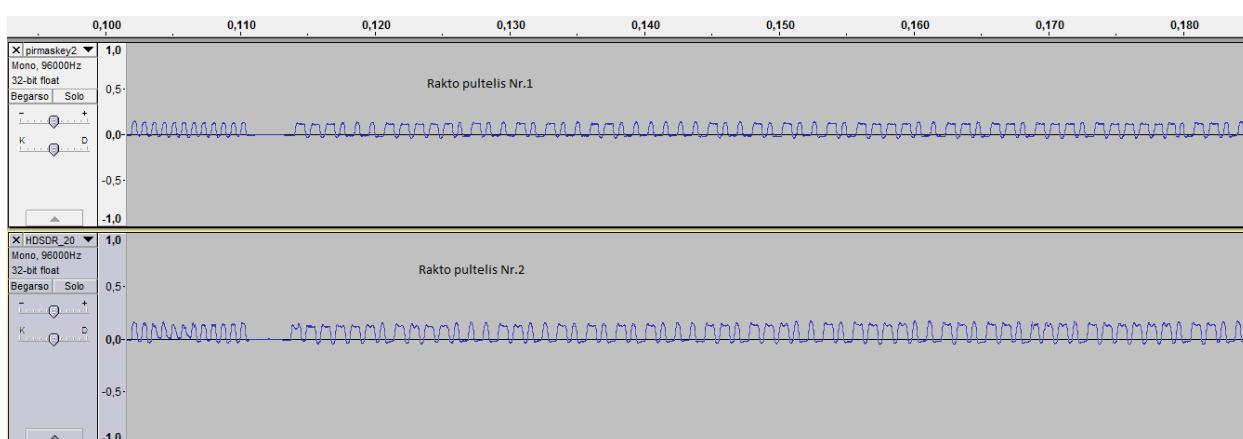
5.1.4 paveiksle pavaizduota automobilio signalizacijos valdymo bloko surinkta spausdintinė plokštė. Į valdymo bloką per X2 jungtį paduodama +12 V nuolatinė maitinimo įtampa. Mikroschema DD1 skirta priimti ir apdoroti iš raktų siunčiamus signalus. Išanalizavus gautą signalą mikroschema DD1 atitinkamai siunčia signalus į kitus schemos elementus, pvz. rėlių valdymo mikroschemą DD3. Ši mikroschema valdoma TTL loginiais lygiais. Jos atitinkamo kanalo įjungimui į jėgumus reikia paduoti loginio „1“ signalą. Tada jos atitinkamame išėjime gaunamas žemo lygio (0 V) signalas. Esant uždarytam atitinkamam šios mikroschemos kanalui, jos išėjimuose yra +12 V įtampa, paduodama iš maitinimo šaltinio per X2 mikroschemos išvadą. Esant reikalui į šios mikroschemos išvadą gali būti paduota iki +50 V įtampa. Visų išėjimo išvadų maksimali leistina srovė yra 500 mA. To pilnai užtenka valdyti reles. Relių paskirtis valdyti automobilio centrinio užrakto variklius. Mikroschema DD2 – EEPROM atminties modulis, skirtas informacijos saugojimui. Mikroschema DA2 skirta įtampos stabilizavimui grandinėje. Siekiant sustiprinti antenos užfiksuotą signalą naudojama mikroschema DA1. Apžvelgus pagrindinius plokštės elementus, galime daryti išvadą, kad raktų perduodami signalai į valdymo bloką nėra užšifruoti papildoma mikroschema. Visa signalo analizė ir dešifravimas atliekamas programiniame lygmenyje, mikroschemoje DD1. Ši

mikroschema yra PIC šeimos mikrovaldiklis. Relės K1 – K4 skirtos įjungti arba išjungti išorines apkrovas (pvz. durų atrakinimo varikliai ir t. t.)



5.1.5 pav. Automobilio signalizacijos rakto spausdintinė plokštė

5.1.5 paveiksle pavaizduota nagrinėjamos signalizacijos rakto surinkta spausdintinė plokštė. Pagrindinė plokštės mikroschema yra HCS200 [16]. Ši mikroschema dažniausiai naudojama nuotolinio rakto sistemose. Mikroschema gali turėti iki trijų įvesties mygtukų. Signalų šifravimui mikroschema naudoja „Keeloq“ algoritmą. Šis blokinis šifras paremtas perėjimo registru su netiesiniu atgaliniu ryšiu (angl. *NLFSR*). „Keeloq“ algoritmas naudoja 32 bitų ilgio duomenų blokus ir 64 bitų ilgio raktai. Jame naudojama du perėjimo registrai: vienas iš jų yra 64 bitų be grįžtamo ryšio funkcijos (tam, kad sugeneruoti pagrindinį raktą), kitas 32 bitų ilgio perkėlimo registras su netiesine grįžtamojo ryšio funkcija NLF iki penkių pasikeitimų (skirtas šifravimui). Siunčiamas signalas koduojamas mikroschemoje HCS200. Prieš signalui patenkant į anteną, jam atliekama amplitudinė moduliacija.



5.1.6 pav. „Keeloq“ algoritmo signalų struktūros

5.1.6 paveiksle pavaizduota automobilio atrakinimo signalų struktūros, naudojant atskirus automobilio rakto pultelius. Matome, kad signalo struktūra yra pastovi, signalo ilgis nekinta. Iš pradžių signalo kodas yra nekintantis, po to eina kintanti signalo kodo dalis, užšifruotas

„Keeloq“ kodavimo algoritmu. Išsiaiškinus kaip atrodo signalas užšifruotas su „Keeloq“ algoritmu, galime daryti išvadą, kad 63 % iš visų tirtų automobilių naudoją būtent šį šifravimo algoritmą.

5.2. Ištirtų signalų saugumo spragos

Ištirus 27 automobilių raktų atrakinimo signalus pastebėta, kad 63 % automobilių naudoja kintančio kodo sistemą su „Keeloq“ šifravimo algoritmu. Šis algoritmas nėra saugus, nes 2007 m. mokslininkai iš Belgijos, Leveno universiteto bendradarbiaudami su kolegomis iš Izraelio [22], atrado saugumo spragas šiame algoritme. Turint signalą siunčiamą tarp rakto ir automobilio, pasinaudojus matematiniais skaičiavimais, galima surasti unikalų siunčiamą raktą. Tačiau šio algoritmo iššifravimas gali užtrukti nuo 3 valandų iki kelių dienų. Šifravimo greitis priklauso nuo to, kaip greitai pavyks atspėti teisingą kodą. Visoms įmanomoms kombinacijoms atspėti gali prireikti 2 dienų. Vienas iš tirtų automobilių naudojo nekintantį kodą. Kadangi kodas yra nekintantis, jį perimus, galima nesunkiai persiųsti iš naujo ir atrakinti automobilį. 6.14 lentelėje perimti signalai visus kartus buvo kintami. Nors tai yra negamyklinė signalizacija, tačiau pakankamai saugi, nes iš signalų struktūros sunku pasakyti kokį šifravimo algoritmą naudoja. 29 % ištirtų automobilių naudoja iš dalies kintantį kodą. Kadangi tokiuose signaluose didžioji kodo dalis yra nekintanti, kintančią dalį galima atspėti iš eilės spėjant dalį kintančio kodo. Pavyzdžiui 5.1.11 lentelėje pateiktas iš dalies kintantis kodas. Matome, kad kintamo signalo dalis yra dvi skiltys po aštuonis bitus. Taigi šiame signale kinta 16 bitų. Viena bite gali būti viena iš dviejų loginių būsenų (0 arba 1). Atlikus matematinius skaičiavimus gauname, kad iš viso gali būti 65536 (2^{16}) skirtingi signalai. Jeigu į sekundę spėtume po 2 signalus, tai teisingam signalui atspėti ilgiausiai užtruktume 9 valandas.

Yra galimybė perimti signalus siunčiamus į automobilį ir juos persiųsti iš naujo, nepriklausomai nuo naudojamo kodavimo algoritmo. Vienu metu reikia siųsti triukšmo signalą į automobilį ir perimti iš rakto į automobilį siunčiamą signalą. Tokiu atveju automobilis nesupranta, kad siunčiamas signalas buvo skirtas jam ir Jūs turite perimtą originalų signalą. Tačiau šį signalą galite panaudoti tik vieną kartą. Jeigu po perimto signalo automobilio savininkas dar bent kartą užrakins ar atrakins savo automobilį, perimtas raktas nebeteks prasmės, jis bus neaktyvus.

Ištirus perimtus signalus, skirtus atrakinti automobilį, galime daryti šias išvadas norint padidinti signalizacijų saugumą:

- Naudoti tik pilnai kintamo kodo signalus;
- naudoti daugiau negu vieną impulso ploto moduliacijos variantą, siunčiant signalus iš rakto į automobilį. Taip bus sunkiau išsiaiškinti signalo struktūrą;

- nežymėti pagrindinių valdymo mikroschemų pavadinimu, kad būtų sunkiau išsiaiškinti kokie kodavimo algoritmai naudojami;
- mažinti nuotolinio rakto veikimo atstumą. Sukels papildomų nepatogumų naudotojui, tačiau piktavaliui bus daug sunkiau perimti signalus, jam reikėtų būti labai arti naudotojo;
- naudoti kintamo ilgio signalus;
- neleisti automobiliui iš eilės priimti tris ar daugiau neteisingų signalų. Taip automobilis būtų apsaugotas nuo teisingo kodo atspėjimo, bandant visus įmanomus teisingo kodo variantus.

5.3. Skyriaus apibendrinimas

5.1.1 – 5.1.27 lentelėse pateikiamos perimtų signalų struktūros. Iš viso ištirtos 27 - ios skirtingos automobilių markės. Nustatyti tikslūs radijo dažniai, kuriais perduodami kiekvieno automobilio atrakinimo signalai. Išanalizuota Lietuvoje pagaminta signalizacija, jos komponentai, veikimo principas. Aptartos ištirtų signalų saugumo spragos.

Nustatyta, kad Lietuvoje pagaminta signalizacija naudoja kintamo kodo signalą, užšifruotą „Keeloq“ algoritmu. Išanalizavus šios signalizacijos perduodamų signalų struktūras, pastebėta, kad 63 % tirtų automobilių turi tokią pačią signalo struktūrą. Galime daryti prielaidą, kad šie automobiliai taip pat naudoja „Keeloq“ šifravimo algoritmą. Iš gautų rezultatų taip pat matome, kad 29 % automobilių naudoja iš dalies kintantį kodą. Nustatyta, kad iš dalies kintančio kodo nulaužimas tiesiogiai proporcingas kintamų bitų skaičiui signale. Kuo daugiau kintamų bitų signale, tuo ilgiau užtrunka iššifruoti signalą. Iš aptartų signalo saugumo spragų galime daryti prielaidą, kad visi tirti automobiliai nėra saugūs, tačiau norint perimti ir persiųsti atrakinimo signalą gali užtrukti tam tikrą laiką. Laiko intervalas priklauso nuo labai daug veiksnių: perduodamo signalo ilgio, struktūros, šifravimo algoritmo, ar po perimto signalo dar buvo siunčiami signalai į automobilį ar ne.

6. Apibendrinimas. Išvados

- 1) Atlikta automobilių raktų sistemų apžvalga, išsiaiškintos jų pagrindinės savybės, techninės charakteristikos, skirtumai. Pasirinkta tirti nuotolinio rakto ir pasyvaus rakto siunčiamus signalus. Išsiaiškinta, kad tokio tipo raktai naudoja 315 MHz arba 433 MHz radijo dažnius.
- 2) Išsiaiškinta, kas yra „Software defined radio“. Apžvelgta šios programos ir aparatinės įrangos vystymosi istorija. Išanalizuota programuojamo radijo ryšio architektūra, elektrinės schemos, veikimo principas. Apžvelgtas „SDR“ naudojama programinė įranga. Nustatyta, kad programuojamas radijo ryšys naudojamas nuo mėgėjiško radijo klausymo iki palydovo orbitos stebėjimo. „Windows“ operacinėje sistemoje pasirinkta naudoti „HDSDR“ programinę įrangą, nes ji suteikia galimybę perimti signalus ir atlikti jiems amplitudinę demoduliaciją. „Linux“ operacinės sistemos aplinkoje naudojama „GNU radio“ programinė įranga, kuri suteikia galimybę programuoti iš struktūrinių blokų, keičiant tų blokų parametrus. Ši programa turi didžiausią struktūrinių blokų biblioteką, skirtą Linux operacinėms sistemoms.
- 3) Sudaryta struktūrinė schema, skirta perimti signalus siunčiamus tarp rakto ir automobilio. Pagal struktūrinę schemą įsigyta aparatinė įranga ir sukonfigūruota programinė įranga. Sukurtas „Matlab“ programos algoritmas skirtas perimtų signalų analizei. Aptartas šio algoritmo veikimas. Tai suteikia galimybę perimti signalus 433 MHz dažnių diapazonu, atlikti perimtiems signalams amplitudinę demoduliaciją ir įrašyti signalą į kietąjį diską. Su signalo analizės algoritmu galima signalą konvertuoti į dvejetainę sistemą ir jį analizuoti. Algoritmas sukurtas taip, kad būtų galima analizuoti įvairaus tipo signalus, atsižvelgiant į signalo naudojamą impulso pločio moduliaciją.
- 4) Atliktas tyrimas su 27-iais gamintojų automobiliais. Nustatyta, kad įvairių automobilių signalų perdavimo ilgiai kinta nuo 0,15 s. iki 0,5 s. Pastebėta, kad 19 % tirtų automobilių visais trimis bandymais naudojo vis skirtingo ilgio signalus. Išanalizavus visus perimtus signalus, pastebėta, kad signalai gali būti keturių tipų: nekintantys signalai, iš dalies kintantys signalai, kintantys signalai ir kai nekinta tik signalo pradžia. Nustatytas tikslus dažnių diapazonas (nuo 433,1 MHz. iki 434,9 MHz.), kuriais perduodami automobilių atrakinimo signalai.
- 5) Ištirta, kad su turima įranga galima perimti signalą išsiųstą iš už 21 – 23 metrų. Tokio atstumo pakanka, norint analizuoti perduodamus signalus, nedidelėje automobilių stovėjimo aikštelėje.
- 6) Ištirta Lietuvoje pagaminta signalizacija. Aptarta valdymo bloko ir signalizacijos rakto spausdintinės plokštės sudėtis, jos veikimo principas. Ištyrus perduodamų signalų struktūrą

ir naudojamą aparatinę įrangą, nustatyta, kad ši signalizacijos sistema naudoja „Keeloq“ šifravimo algoritmą. Palyginus „Keeloq“ algoritmu užšifruoto signalo struktūrą su perimtu signalų struktūromis padaryta prielaida, kad 63 % tirtų automobilių naudoja „Keeloq“ šifravimo algoritmą.

- 7) Aptartos signalų, kuriuos pavyko perimti, saugumo spragos. Padaryta prielaida, kad visų tirtų automobilių atrakinimo signalai nėra saugūs, tačiau skiriasi jų nulaužimo laikas. Iširta, kad didžiausias pažeidžiamumas yra tuose sistemose, kurios naudoja nekintamo ilgio ir nekintamo kodo signalus. Tokius signalus nesunku perimti ir persiųsti iš naujo į automobilį. Apskaičiuota, kad iš dalies kintančio signalo kodo atspėjimo laikas proporcingas kintamų bitų skaičiui signale. Vienas kintamas bitas teisingo signalo kodo atspėjimo laiką prailgina dvigubai. Atsižvelgiant į aptiktas saugumo spragas, pasiūlyta, kaip būtų galima padidinti perduodamų signalų saugumą (pvz. naudoti kintamo ilgio signalus, skirtingas impulso pločio moduliacijas). Taip būtų sunkiau analizuoti perimamus signalus, išsiaiškinti kokios tų signalų struktūros. Automobilis būtų apsaugotas nuo kryptinių teisingo kodo paieškos atakų. Tai leistų sumažinti įsilaužimo į automobilius skaičių.

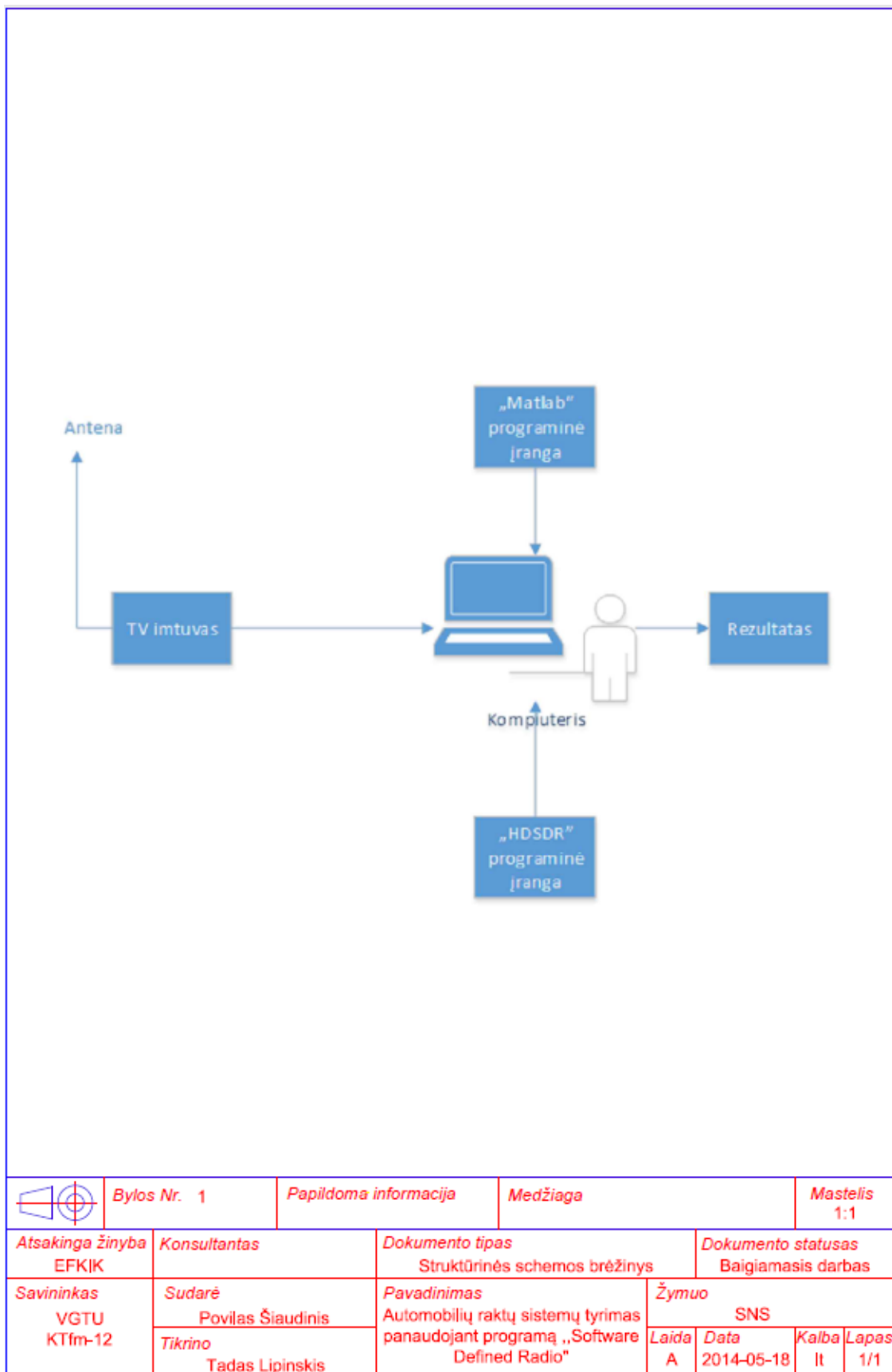
Literatūros ir informacijos šaltinių sąrašas

1. *Auto-Lock* [interaktyvus]. United States patent office [žiūrėta 2014 m. Gegužės 21 d.]. Prieiga per internetą: <<https://www.google.lt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CEAQFjAA&url=http%3A%2F%2Fpatentimages.storage.googleapis.com%2Fpdfs%2FUS1329391.pdf&ei=mnJ8U8DQC6yWyQPUv4HQA&usg=AFQjCNGpyzrVgt9AJ2yaJWyckpwWE4OTxg&bvm=bv.67229260,d.bGQ>>
2. Phillips, Bill. *The complete book of Locks and locksmithing*. 2005. 27 p.
3. *Hyundai Transponder Key* [interaktyvus]. Beijing Autokey Transponder Tec Co., Ltd [žiūrėta 2013 m. Birželio 19 d.]. Prieiga per internetą: <http://www.aliexpress.com/store/product/Hyundai-Transponder-Key-HYN12-46/500700_428853641.html>
4. *The engine immobilizer: A non – Starter for Car Thieves* [interaktyvus]. Social Science Research Network [žiūrėta 2014 m. Gegužės 21 d.]. Prieiga per internetą: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2202165>
5. Raktų su imobilizieriais gamyba [interaktyvus]. Raktinė [žiūrėta 2014 m. Sausio 19 d.]. Prieiga per internetą: <<http://www.raktine.lt/imobilizers.htm>>
6. *What is an Automotive Keyless Entry Remote System* [interaktyvus]. Arcticlebase [žiūrėta 2014 m. Gegužės 21 d.]. Prieiga per internetą: <<http://www.articlesbase.com/cars-articles/what-is-an-automotive-keyless-entry-remote-system-456455.html>>
7. *Remote keyless entry (RKE) systems* [interaktyvus]. Car security: remote keyless \entry and go" [žiūrėta 2013 m. Birželio 19 d.]. Prieiga per internetą: <<http://www.delaat.net/rp/2008-2009/p42/report.pdf>>
8. *Analysis of Attacks Against the Security of Keyless-Entry Systems for Vehicles and Suggestions for Improved Designs* [interaktyvus]. IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY [žiūrėta 2014 m. Balandžio 30 d.]. Prieiga per internetą: <http://www.calcsnop.com/images/Analysis_Keyless-entry.pdf>
9. *Hitag2* [interaktyvus]. Institute for Computing and Information Sciences KU Leuven ESAT/COSIC and IBBT Radboud University Nijmegen, The Netherlands. [žiūrėta 2014 m. Gegužės 21 d.]. Prieiga per internetą: <<http://www.scribd.com/doc/103710681/Hitag2>>
10. *Criminals find the key to car immobilisers* [interaktyvus]. NewScientist. [žiūrėta 2014 m. Gegužės 21 d.]. Prieiga per internetą: <http://www.newscientist.com/article/mg20827894.500-criminals-find-the-key-to-car-immobilisers.html#.U3yDK_mSyOM>
11. *Advanced encryption standard* [interaktyvus]. Tinklų saugumas [žiūrėta 2013 m. Birželio 19 d.]. Prieiga per internetą: <<http://www.tinklusaugumas.lt/cgi-bin/moin.py/Advanced%20Encryption%20Standard>>
12. *Passive keyless entry system* [interaktyvus]. Patents. [žiūrėta 2014 m. Gegužės 21 d.]. Prieiga per internetą: <<http://www.google.com/patents/US4942393>>
13. *How smart is your car key?* [interaktyvus]. The Car Expert. [žiūrėta 2014 m. Gegužės 21 d.]. Prieiga per internetą: <<http://www.thecarexpert.co.uk/how-smart-is-your-car-key/>>

14. *Victor PKE Car Alarm System* [interaktyvus]. Auto Safety Products [žiūrėta 2013 m. Birželio 19 d.]. Prieiga per internetą: < <http://www.cn-victor.com.cn/car-alarms-systems-c-18/victor-pke-car-alarm-system-p-176.html>>
15. *Visų ryšio standartų mobilusis telefonas* [interaktyvus]. Ryšių technika [žiūrėta 2013 m. Birželio 19 d.]. Prieiga per internetą: < <http://rtn.elektronika.lt/rtn/0203/visuryσιο.html> >
16. *Keeloq code hopping encoder* [interaktyvus]. Microchip [žiūrėta 2014 m. Balandžio 29 d.]. Prieiga per internetą: < <http://ww1.microchip.com/downloads/en/DeviceDoc/40138c.pdf>>
17. *Software defined radio* [interaktyvus]. Hand Book of RF & wireless [žiūrėta 2013 m. Birželio 19 d.]. Prieiga per internetą: < <http://www.converter-radio.com/SDR.pdf>>
18. *The big list of RTL-SDR supported software* [interaktyvus]. RTL-SDR.COM. [žiūrėta 2014 m. Gegužės 21 d.]. Prieiga per internetą:< <http://www.rtl-sdr.com/big-list-rtl-sdr-supported-software/>>
19. *Hardware* [interaktyvus]. GNU radio [žiūrėta 2013 m. Birželio 19 d.]. Prieiga per internetą: < <http://gnuradio.org/redmine/projects/gnuradio/wiki> >
20. *WebSDR receiver* [interaktyvus]. WebSDR [žiūrėta 2013 m. Birželio 24 d.]. Prieiga per internetą: < <http://www.160m.net/>>
21. *You can ring my bell* [interaktyvus]. Door bell [žiūrėta 2013 m. Birželio 19 d.]. Prieiga per internetą: < <http://adamsblog.aperturlabs.com/2013/03/you-can-ring-my-bell-adventures-in-sub.html> >
22. *Cryptanalysis of KeeLoq code-hopping using a Single FPGA* [interaktyvus]. Computer and Network Security Lab School of Electrical Engineering. [žiūrėta 2014 m. Gegužės 21 d.]. Prieiga per internetą:< <http://eprint.iacr.org/2011/242.pdf>>

Priedai

A Priedas. Signalo perėmimo ir analizės struktūrinė schema



B Priedas. Signalų analizės algoritmo programos kodas

```
filePattern = fullfile('suzuki 4x4 2.wav');           //Prenkamas masyvas
wavFiles = dir(filePattern);
for k = 1:length(wavFiles)                             //Nustatomas masyvo dydis
    baseFileName = wavFiles(k).name;
    fullFileName = fullfile(baseFileName);
    fprintf(1, 'Now reading %s\n', fullFileName);
    [Masyvas, Fs] = wavread(fullFileName);             // Sukuriamas masyvas
    x = [Masyvas];
        x >= 0.08 ;                                     //Išrenkamos visos vertės didesnės už 0,08
y=double(ans);                                         // Sukuriamas loginis masyvas
z=num2str(y);
z1=z(:)'                                              // Rezultatas kopijuojamas į r
r = ' ';
n=45;                                                 // Maksimalus vienetų skaičius loginiam „1“
ii=repmat({'1'},1,n+1);
ii(1:19)={'0'};                                       //Maksimalus vienetų skaičius loginiam „0“
out=char(ii(cellfun(@numel,regexp(r,'1+', 'match'))))' // Rezultatas
end
```