KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

Karolis Mauragas

DAIKTŲ INTERNETO INFORMACINĖS SISTEMOS SAUGUMO PAGERINIMO TYRIMAS

Baigiamasis magistro projektas

Vadovas
prof. dr. R. Plėštys

KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

DAIKTŲ INTERNETO INFORMACINĖS SISTEMOS SAUGUMO PAGERINIMO TYRIMAS

Baigiamasis magistro projektas
Informacinių sistemų inžinerijos studijų programa (kodas 621E15001)

Vadovas
prof. dr. R. Plėštys
2016-05-23

Recenzentas
prof. dr. I. Lagzdinytė-Budnikė
2016-05-23

Projektą atliko
Karolis Mauragas
2016-05-23

KAUNAS, 2016

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS

(Fakultetas)

Karolis Mauragas

(Studento vardas, pavardė)

Informacinių sistemų inžinerijos studijų programa, 621E15001

(Studijų programos pavadinimas, kodas)

Baigiamojo projekto „Pavadinimas“

AKADEMINIO SĄŽININGUMO DEKLARACIJA

20 ___ m. _____ ____ d.

Kaunas

Patvirtinu, kad mano, **Karolio Maurago**, baigiamasis projektas tema „Daiktų interneto informacinės sistemos saugumo pagerinimo tyrimas“ yra parašytas visiškai savarankiškai ir visi pateikti duomenys ar tyrimų rezultatai yra teisingi ir gauti sąžiningai. Šiame darbe nei viena dalis nėra plagijuota nuo jokių spausdintinių ar internetinių šaltinių, visos kitų šaltinių tiesioginės ir netiesioginės citatos nurodytos literatūros nuorodose. Įstatymų nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs.

Aš suprantu, kad išaiškėjus nesąžiningumo faktui, man bus taikomos nuobaudos, remiantis Kauno technologijos universitete galiojančia tvarka.

(vardą ir pavardę įrašyti ranka)	*(parašas)*

Mauragas, Karolis. DAIKTŲ INTERNETO INFORMACINĖS SISTEMOS SAUGUMO PAGERINIMO TYRIMAS. Magistro baigiamasis projektas / vadovas Prof. dr. Rimantas Plėštys; Kauno technologijos universitetas, Informatikos fakultetas.

Mokslo kryptis ir sritis: Informatikos inžinerija, technologijos mokslai

Reikšminiai žodžiai: *informacinės sistemos saugumas*; *daiktų internetas; išmanusis įrenginys.*

Kaunas, 2016. 68 p.

SANTRAUKA

Darbo tikslas - pagerinti sukurtos daiktų interneto informacinės sistemos saugumą, aptinkant įsilaužėlių atakas ir pritaikant apsaugos priemones.

Daiktų interneto viena iš pagrindinių sudedamųjų dalių yra informacinė sistema, kuri apdoroja sukauptus duomenis. Viena iš iškylančių problemų kuriant tokias sistemas yra duomenų perdavimo ir saugojimo saugumas. Daiktų interneto informacinė sistema turi užtikrinti tris pagrindines saugumo funkcijas, tokias kaip: duomenų konfidencialumą, vientisumą ir prieinamumą.

Realizuotoje daiktų interneto informacinėje sistemoje pagerinu išmaniojo įrenginio autorizavimo metodą bei pritaikau perduodamų ir talpinamų duomenų šifravimo algoritmą. Taip pat realizuoju įrenginio blokavimo ir atakų aptikimo metodus.

Realizuoti metodai gali būti pritaikomi visiems, tirtą belaidį duomenų perdavimo protokolą palaikantiems įrenginiams, nepakeičiant standarto specifikacijų. Tai užtikrina sistemos suderinamumą su visais šią technologiją palaikančiais įrenginiais.

Mauragas, Karolis. RESEARCH ON SECURITY IMPROVEMENT OF INFORMATION SYSTEM OF INTERNET OF THINGS: Master‘s thesis in Information Systems Engineering / supervisor Prof. dr. Rimantas Plėštys. The Faculty of Informatics, Kaunas University of Technology.

Research area and field: Informatics Engineering, Technology Science

Key words: *information system security*; *internet of things; smart device.*

Kaunas, 2016. 68 p.

SUMMARY

The goal of this work is to improve the internet of things information system security by detecting hacker attacks and applying security measures.

One of the key components of internet of things is an information system, which processes the collected data. Data transmission and storage security is one of the problems facing the development of such systems. Information system of internet of things must guarantee the three key security features: data confidentiality, integrity and availability.

In established internet of things information system it was improved smart device authentication method and applied cryptographic algorithm for the transferred and stored data. It was also implemented device blocking and attack detection methods.

Researched methods can be applied to all devices which support tested wireless data transmission protocol, without changing standard specification. This ensures that the system will be compatible with all of this technology enabled devices.

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

TERMINŲ IR SANTRUMPŲ ŽODYNAS

AES - Pažangus šifravimo standartas (angl. *Advanced Encryption Standard*)

ATT - Atributų protokolas (angl. *Attribute Protocol*)

BSD - Nemokama programinės įrangos licencija (angl. *Berkeley Software Distribution*)

CRC - Ciklinė pertekliaus kontrolė (angl. *Cyclic Redundancy Check*)

DES - Duomenų šifravimo standartas (angl. *Data Encryption Standard*)

FCS - Kadrų tikrinimo eilė (angl. *Frame check sequence*)

GAP - Bendrasis prieigos profilis (angl. *Generic Access Profile*)

GATT - Bendrasis atributų profilis (angl. *Generic Attribute Profile*)

GFSK - Gauso dažnio manipuliacija (angl. *Gaussian frequency shift keying*)

GNU GPL - Atvirojo kodo viešoji licencija (angl. *GNU General Public License*)

HIDS - Kompiuterio įsibrovimo aptikimo sistemos (angl. *Host based Intrusion Detection Systems*)

IEEE - Elektros ir elektronikos inžinierių institutas (angl. *Institute of Electrical and Electronic Engineers*)

IoT - Daiktų internetas (angl. *Internet of Things*)

IP - Interneto protokolas (angl. *Internet Protocol*)

ITU - Tarptautinė telekomunikacijų sąjunga (angl. *International Telecommunication Union*)

MAC - Unikalus tinklo sąsajos adresas (angl. *Media Access Control Address*)

MD5 - Kriptografinė maišos funkcija (angl. *Message Digest 5 Algorithm*)

MITM - Duomenų pasiklausymo ataka (angl. *Man In The Middle attack*)

NFC - Artimojo lauko komunikacijos duomenų perdavimo technologija (angl. *Near Field Communication*)

NIDS - Tinklų įsibrovimo aptikimo sistemos (angl. *Network based Intrusion Detection Systems*)

OSI - Ryšio protokolų, naudojamų kompiuteriniuose tinkluose, aprašymas (angl. *Open Systems Interconnection*)

PAN - Asmeninis tinklas (angl. *Personal Area Network*)

PDU - Protokolo duomenų vienetas (angl. *Protocol Data Unit*)

RFID - Radijo dažnio atpažinimo įrenginys (angl. *Radio Frequency Identification*)

RSA - Viešojo rakto šifravimo metodas

RSSI - Gauto signalo stiprumo indikatorius (angl. *Received signal strength indication*)

SD - Išorinė duomenų talpykla (angl. *Storage Device*)

SHA - Saugus maišos algoritmas (angl. *Secure Hash Algorithm*)

SSH - Kriptografinis saugaus tinklo protokolas (angl. *Secure Shell*)

TCP - Duomenų perdavimo kontrolės protokolas (angl. *Transmission Control Protocol*)

USB - Universali duomenų perdavimo jungtis (angl. *Universal Serial Bus*)

UUID - Visuotinai unikalus identifikatorius (angl. *Universally Unique Identifier*)

VPN - Virtualus privatus tinklas (angl. *Virtual Private Network*)

WPAN - Belaidis asmeninis tinklas (angl. *Wireless Personal Area Network*)

WSN - Belaidis jutiklių tinklas (angl. *Wireless Sensor Network*)

ĮVADAS

Darbo problematika ir aktualumas

Daiktų interneto viena iš pagrindinių sudedamųjų dalių yra informacinė sistema, kuri apdoroja sukauptus duomenis. Viena iš iškylančių problemų kuriant tokias sistemas yra duomenų perdavimo ir saugojimo saugumas. Išmaniųjų įrenginių informacinė sistema turi vykdyti tris pagrindines saugumo funkcijas:

1. Duomenų konfidencialumą - užtikrina, kad kiekvienas duomenų perdavimo etapas bus neprieinamas neautorizuotiems asmenims. Ši kategorija užtikrina konfidencialų duomenų perdavimą nuo jų sukūrimo iki pristatymo vartotojui.
2. Duomenų vientisumą - yra užkirstas kelias neautorizuotai duomenų modifikacijai, užtikrinamas duomenų perdavimo tikslumas ir patikimumas.
3. Duomenų prieinamumą - užtikrina laiku patikimą prieinamumą autorizuotiems asmenims prie informacinės sistemos resursų.

Saugumo pažeidimai vykdomi atakuojant informacinės sistemos elementus norint išvesti visą daiktų internetą iš normalaus darbo režimo. Atakos vykdomos tiek į pačius daiktus, tiek į valdymo įrenginius.

Darbo tikslas ir uždaviniai

Darbo tikslas - pagerinti sukurtos daiktų interneto informacinės sistemos saugumą, aptinkant įsilaužėlių atakas ir pritaikant apsaugos priemones. Norint sukurti saugią daiktų interneto informacinę sistemą būtina atlikti šiuos uždavinius:

1. Išanalizuoti daiktų interneto informacinių sistemų įsilaužėlių aptikimo metodus ir įrankius bei saugumo sprendimus.
2. Suformuluoti reikalavimus kuriamai daiktų interneto informacinei sistemai.
3. Pasirinkti informacinės sistemos tyrimui skirtus aparatūrinius ir programinius komponentus.
4. Suprojektuoti daiktų interneto informacinę sistemą su pasirinktais komponentais.
5. Pasiūlyti papildomus įsilaužėlių aptikimo metodus ir įdiegti papildomas saugumo priemones.
6. Atlikti sukurtos daiktų interneto informacinės sistemos saugumo analizę.

Darbo rezultatai ir jų svarba

Darbo rezultatas yra pagerintas daiktų interneto informacinės sistemos saugumas nuo atakų. Šis sprendimas užtikrina informacinės sistemos konfidencialumą, vientisumą ir prieinamumą.

Darbo struktūra

Magistrinis darbas sudarytas iš šešių skyrių:

1. Probleminės srities analizė - analizuojami esami daiktų interneto informacinių sistemų įsilaužimo aptikimo metodai ir įrankiai bei saugumo sprendimai.
2. Reikalavimų specifikacija - pateikiami kuriamos informacinės sistemos reikalavimai.
3. Eksperimentinės realizacijos projektas - pateikiamas ir aprašomas eksperimentinės realizacijos projektas, siūlomų saugos metodų specifikacija, sukurtos architektūros modelis.
4. Realizacija - pritaikomi nauji saugumo sprendimai sukurtai informacinei sistemai.
5. Sukurtos informacinės sistemos testavimas - atliekamas sistemos eksperimentinis saugumo metodų tyrimas.
6. Rezultatų apibendrinimas ir išvados - pateikiami gauti tyrimo rezultatai ir išvados.

1. PROBLEMINĖS SRITIES ANALIZĖ

Probleminės srities analizės skyriuje analizuojama daiktų interneto informacinės sistemos ir esami jų saugumo metodai, įrankiai ir standartai.

1.1. Analizės tikslas

Analizės tikslas - ištirti ir palyginti daiktų interneto informacinių sistemų esamų saugumo sprendimų metodus, įrankius ir standartus.

1.2. Tyrimo objektas, sritis ir problema

Tyrimo sritis yra daiktų interneto informacinės sistemos įsilaužimų aptikimas. Įsilaužimo aptikimas sistemoje užtikrinamas įvairiais metodais bei įrankiais.

Tyrimo objektas yra daiktų interneto informacinės sistemos. **Tyrimo problema** - daiktų interneto informacinės sistemos geresnis saugumo užtikrinimas. Sistema nusakoma, kaip elementų aibė, kuri apibrėžia sąveikaujančius sistemos elektroninius komponentus, kurie skirti informacijos gavimui, apdorojimui ir pateikimui vartotojui.

Keičiantis duomenimis tarp belaidžių įrenginių, iškyla problema užtikrinti duomenų saugumą. Kuriama sistema turi užtikrinti geresnį sistemos konfidencialumą, vientisumą ir prieinamumą. Ši problema sprendžiama patobulinant duomenų apsikeitimo metodus tarp išmaniųjų ir valdymo įrenginio bei diegiant naujus atakų aptikimo metodus.

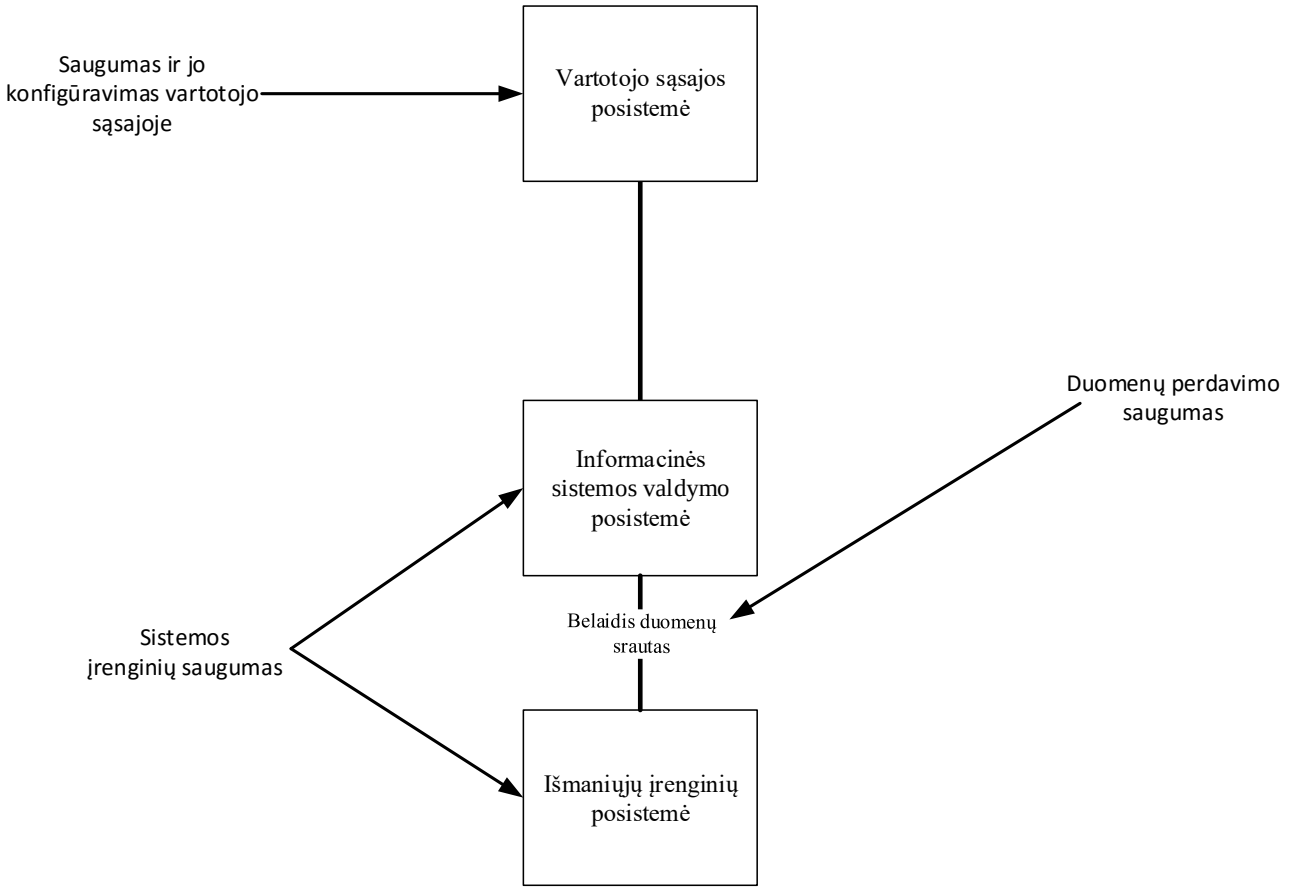
1.3. Tyrimo objekto saugumo analizė

Remiantis tarptautine telekomunikacijų sąjunga, daiktų internetas yra fizinių objektų tinklas su įmontuota elektronika, programine įranga, jutikliais bei tinkliniu ryšiu, kas įgalina šiuos objektus rinkti ir keistis informacija [1]. Tyrime daiktų interneto objektai vadinami išmaniaisiais įrenginiais. Išmanusis įrenginys yra elektroninis prietaisas kuris gali nuotoliniu būdu prisijungti, komunikuoti ir dalintis informacija su vartotoju ar kitu išmaniuoju įrenginiu [2].

Įsilaužimų aptikimas vykdomas daiktų interneto informacinėje sistemoje. Ši sistema susideda iš trijų dalių: duomenų sukūrimo, jų apdorojimo bei jų pateikimo. Kuriamoje sistemoje, duomenų sukūrimas vyksta išmaniajame įrenginyje, apdorojimas - valdymo sistemoje, o pateikimas - vartotojo sąsajoje. Įvertinus duomenų perdavimo srautą, kuriamos sistemos objektas pateikiamas diagramoje 1.1 pav. Kuriamos sistemos sudedamosios dalys:

a. vartotojo sąsajos posistemė - informacinė vartotojo sąsaja skirta apdorotos informacijos pateikimui vartotojui;
b. informacinės sistemos valdymo posistemė - centrinė valdymo sistema skirta informacijos apdorojimui, saugojimui ir pateikimui vartotojo sąsajai;

c. išmaniųjų įrenginių posistemė - įrenginiai skirti surinkti informaciją apie tam tikrus vykstančius aplinkos procesus;
d. belaidis duomenų perdavimas - belaidė duomenų perdavimo terpė tarp išmaniojo įrenginio ir informacinės sistemos valdymo sistemos.



1.1 pav. Tiriamos informacinės sistemos diagrama

Turi būti užtikrinamas saugus duomenų apsikeitimas tarp trijų tiriamo objekto posistemių: išmaniųjų įrenginių, informacinės sistemos valdymo ir vartotojo sąsajos. Sistemos sauga apima duomenų perdavimą, įrenginius ir vartotojo sąsają.

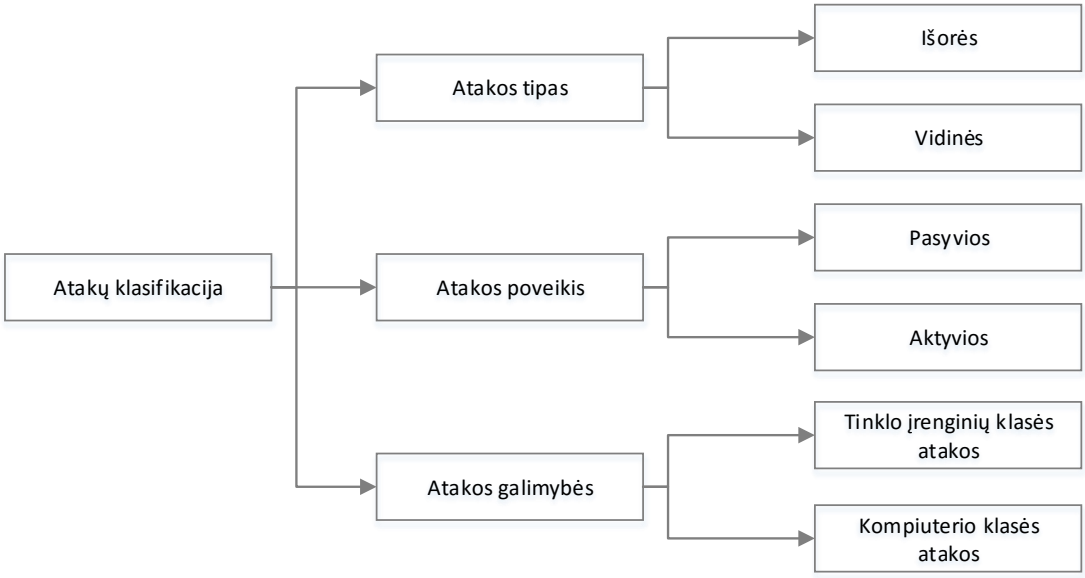
Išmanusis įrenginys yra elektroninis prietaisas kuris yra sujungtas su kitais įrenginiais. Išmaniųjų įrenginių aibė kartu su valdymo įrenginiu sudaro informacinę sistemą. Šios informacinės sistemos architektūrą galima suskirstyti į tris pagrindines dalis: suvokimo, tinklo ir taikymo lygmenis [3]. Visi šie lygmenys turi skirtingas informacijos pateikimo ir apdorojimo technologijas bei metodus.

Suvokimo lygmenyje (angl. *Perception layer*) sistemos tikslas yra pasiekti, ir apdoroti duomenis, gaunamus iš fizinės aplinkos. Tinklo lygmenyje sistemos tikslas yra duomenų perdavimas tarp įrenginių. Taikymo lygmenyje duomenys yra apdorojami ir pateikiami vartotojui. Išmanių įrenginių sistemos lygmenų santrauka ir specifikacijos pateiktos 1.1 lent. [3].

1.1 lentelė. Daiktų interneto lygmenų santrauka ir specifikacijos

Daiktų interneto lygmenys	**Komponentai**	**Lygmens veikla**	**Saugumo problemos**	**Saugumo parametrai**	**Saugumo priemonės**
Suvokimo lygmuo	Jutikliai	Duomenų rinkimas	Jutiklių tinklo saugumas	Autentifikavimas; konfidencialumas	Sertifikatai ir prieigos kontrolė; autentifikavimo metodai
Tinklo lygmuo	Belaidis ir laidinis tinklas; valdymo įrenginys	Duomenų perdavimas	Duomenų perdavimo saugumas	Vientisumas; prieinamumas; konfidencialumas	Duomenų šifravimas šuoliais
Taikymo lygmuo	Išmanusis įrenginys; valdymo įrenginys	Duomenų analizė; valdymo sprendimų priėmimas	Informacijos apdorojimo saugumas	Privatumas	Šifravimas

Belaidis išmaniųjų įrenginių tinklas yra labai pažeidžiamas dėl duomenų transliavimo perdavimo terpėje. Be to, tinklo mazgai dažnai laikomi mažai fiziškai apsaugotoje ar pavojingoje aplinkoje. Įsilaužėlis naudodamasis įvairiomis saugumo spragomis gali perimti ar pakeisti visos informacinės sistemos elgseną. Esanti problema yra sprendžiama aptinkant įsilaužėlių atakas ir taikant apsaugos priemones. Atakų klasifikacija belaidžiuose tinkluose pateikta 1.2 pav. [4].



1.2 pav. Atakų klasifikacija belaidžiuose tinkluose

Atakos klasifikacijos:

a. išorės atakos - vykdomos iš išorinio tinklo;
b. vidinės atakos - vykdomos vietiniame tinkle;
c. pasyvios atakos - vykdomos pasyviai analizuojant gautą informaciją;
d. aktyvios atakos - vykdomos analizuojant informaciją realiu laiku, atliekant įsilaušimus;
e. tinklo mazgo klasės atakos - vykdomos prieš tinklo mazgus;

f. kompiuterio klasės atakos - vykdomos prieš valdymo įrenginius.

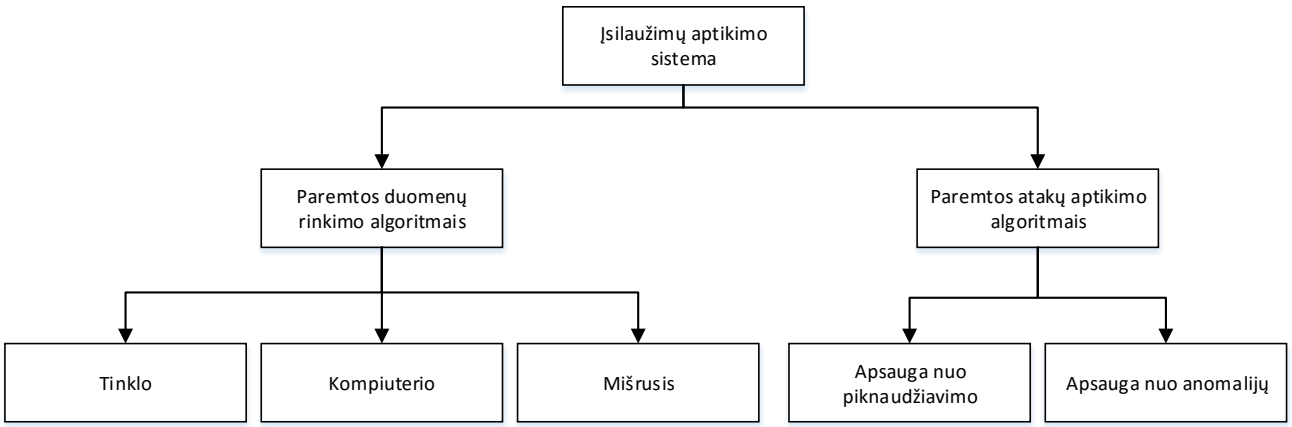
Norint užtikrinti saugumą prieš visų tipų atakas ir išpildyti visas saugumo charakteristikas, kuriami nauji informacinės sistemos atakų aptikimo metodai. Saugesnis tinklinis komunikavimas užtikrinamas šifruojant duomenis ir apsaugant nuo modifikavimo ir perėmimo juos perduodant. Įsilaužimų aptikimas formuoja įspėjimus vartotojui, į kuriuos reaguojant galima apsisaugoti. Problemos sprendimas formuluojamas atsižvelgiant į galimas atakas belaidžiuose jutiklių tinkluose, kurios pateiktos 1.2 lent. [5], [6].

1.2 lentelė. Galimos atakos belaidžiuose jutiklių tinkluose

Eil. Nr.	**Atakos pavadinimas**	**Veikimas**
1	Įrenginių ir tinklo aptikimas (angl. *Probing and Network Discovery*)	Aptinkami veikiantys tinklo įrenginiai. Atliekamas skenuojant elektromagnetines bangas erdvėje. Tai dažniausiai yra pirmas dalykas atliekamas įsibrovėlio.
2	Sistemos duomenų rinkimas (angl. *Surveillance*)	Aptikus egzistuojantį tinklą yra renkami perduodami duomenys paketų pavidalu.
3	Atkirtimas nuo paslaugos (angl. *denial of service attack*)	Šios atakos metu įsibrovėlio tikslas - trukdyti normaliai sistemos veiklai.
4	Įrenginio klastojimas (angl. *Impersonation*)	Šios atakos metu yra klastojami sistemos įrenginiai, naudojant surinktą informaciją apie juos.
5	Suklastoto valdymo įrenginio įterpimas į sistemą (angl. *Man in the middle and Rouge AP*)	Šios atakos metu yra bandoma įsiterpti tarp komunikuojančių įrenginių, modifikuojant perduodamą informaciją.

1.3.1. Išmaniųjų įrenginių informacinių sistemų įsilaužimų aptikimo metodų analizė

Daiktų interneto informacinių sistemų saugumo problema sprendžiama diegiant įsilaužimų aptikimų sistemas (angl. *Intrusion Detection Systems*) ir taikant duomenų apsaugos priemones. Šios priemonės leidžia informacinėms sistemoms apsisaugoti nuo įsilaužėlių atakų. Tai atliekama tikrinant duomenų srautą tarp komunikuojančių įrenginių ir taikant įsilaužimo aptikimo algoritmus [7]. Įsilaužimų aptikimo sistemų klasifikacija pateikta 1.3 pav. [8].



1.3 pav. Įsilaužimų aptikimo sistemų klasifikacija

Įsilaužimų aptikimo sistemų, paremtų pagal duomenų rinkimo algoritmus, klasifikacijos dalys:

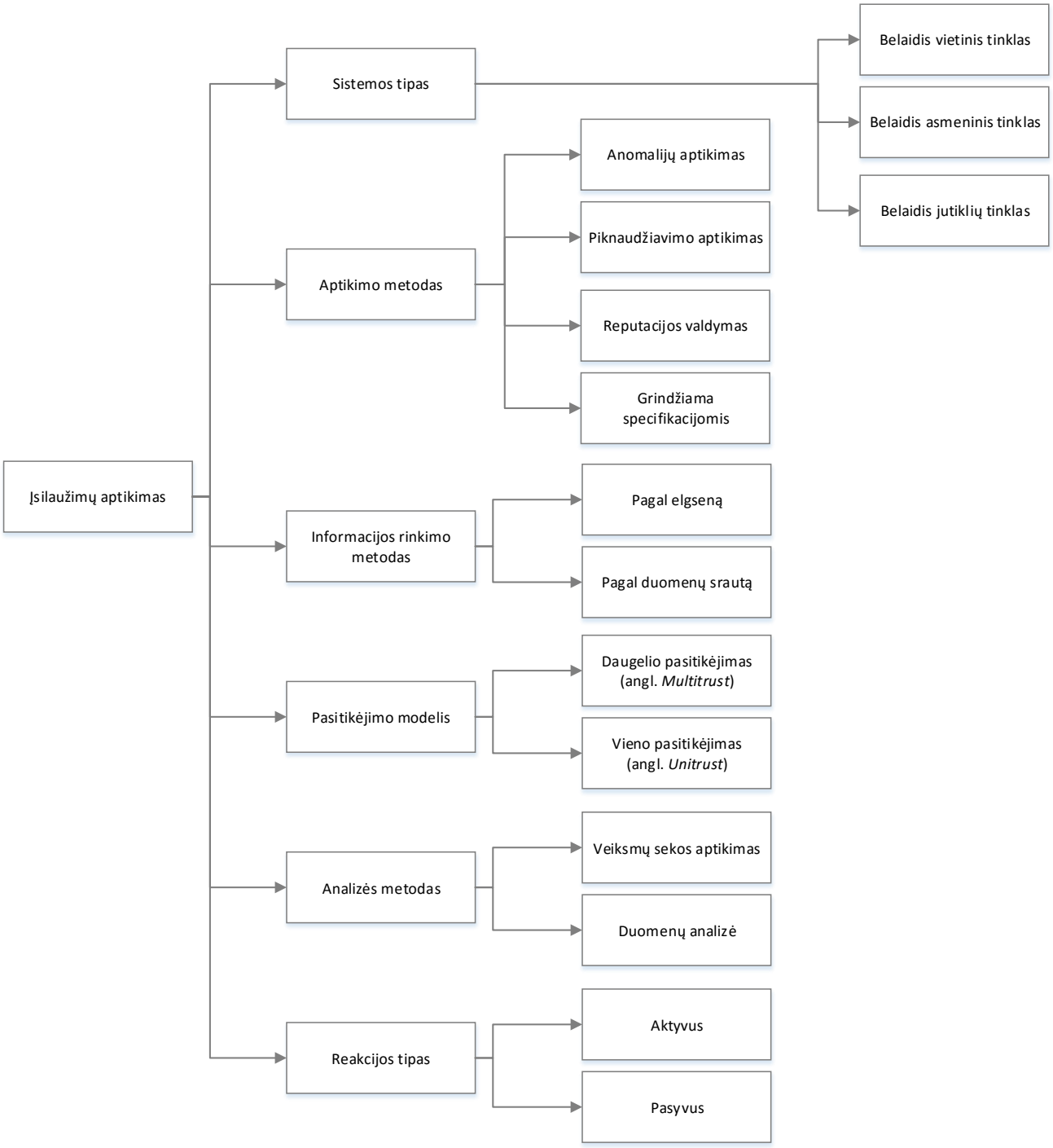
a. tinklo - įsilaužimo aptikimo sistemos, veikiančios sistemos tinkle, skirtos tikrinti kiekvieną duomenų paketą [9];

b. kompiuterio - sistemos, veikiančios valdymo kompiuteryje;
c. mišrusis - sistemos, kurios gali veikti kaip tinklo įrenginio ar kompiuterio įsilaužimo aptikimo sistema.

Piktnaudžiavimo aptikimas (angl. *Misuse Detection*). Šis metodas skirtas aptikti netinkamą sistemos naudojimasi [9] analizuojant įvairias veiksmų sekas (angl. *Signature*) [7]. Sistema registruoja visas sistemos veiklas ir, aptikus įtartiną veiksmų seką, sukuriamas perspėjimas. Pagrindinis iššūkis yra tinkamai sudaryti sistemos veiksmų sekas, kurios neprieštarautų normaliai sistemos veiklai. Šis metodas yra neveiksmingas, jei yra vykdoma nežinoma ataka [9].

Anomalijų aptikimas. Skirtingai nuo piktnaudžiavimo aptikimo, anomalijų aptikimo metodas skirtas nustatyti nežinomą atakos pobūdį, analizuojant neįprastus sistemos įrenginių ar vartotojų veiksmus [9]. Šie veiksmai gali būti leistini, bet neįprasti normaliai sistemos veiklai ir gali būti priskiriami atakai.

Įsilaužimų aptikimo metodų klasifikacija belaidžiams tinklams pateikta 1.4 pav. [10].



1.4 pav. Įsilaužimų aptikimo sistemų metodų klasifikacija belaidžiams tinklams

Įsilaužimo aptikimo sistemos naudoja tokius faktorius [7]:

a. atakuojamos sistemos tipo nustatymą - šis kriterijus apibūdina numatomą įsilaužimų aptikimo sistemos aplinką;
b. aptikimo taikymo būdą - šis kriterijus išskiria įsilaužimo aptikimo sistemas pagal jų įsilaužimų aptikimo metodą;
c. informacijos rinkimo metodą - šis kriterijus išskiria pagal elgsena aptinkančias įsilaužimų aptikimo sistemas, analizuojančias duomenų srautą;

d. pasitikėjimo modelį - šis kriterijus atskiria sistemas, kurios pačios surenka ir analizuoja duomenis, nuo sistemų, kurios gauna informaciją iš nuotolinių įsilaužimo aptikimo sistemų;
e. duomenų analizės būdus - šis kriterijus apibūdina kaip įsibrovimų aptikimo sistema ieško įsibrovėlio atakų;
f. reakcijos tipą - šis kriterijus išskiria pasyvius ir aktyvius sistemos reakcijos tipus.

Įsilaužimų aptikimo sistemos informacinėse sistemose diegiamos nes norima užtikrinti tinklo kontrolę ir aptikti įtartiną veiklą. Šios sistemos diegiamos tinklo ar valdymo įrenginiuose. Šių sistemų tipai priklauso nuo naudojamos įrenginio operacinės sistemos. Atvirojo kodo įsilaužimų aptikimo sistemų palyginimas pateiktas 1.3 lent. [7].

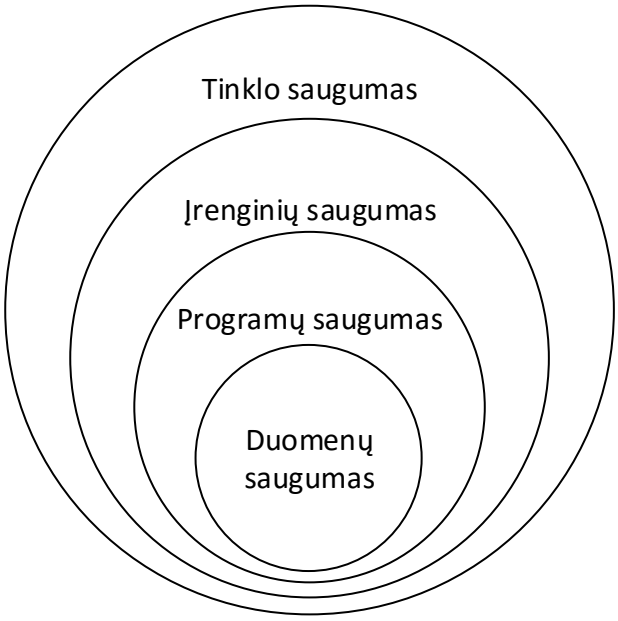
1.3 lentelė. Įsilaužimų aptikimo sistemų palyginimas

	Snort	**Bro**	**OSSEC**	**AIDE**	**Samhain**
Kategorija	NIDS	NIDS	HIDS	HIDS	HIDS
Naudojama licencija	GNU GPL v.2	BSD	GNU GPL v.2	GNU GPL	GNU GPL
Įsilaužimo prevencijos funkcija	Taip	Ne	Taip	Ne	Ne
Privatumo parašo (angl. *Pretty Good Privacy*) palaikymas	Taip	Taip	Taip	Taip	Taip
Neautorizuotos sistemos valdymo (angl. *Rootkit*) aptikimas	-	-	Taip	Taip	Taip
Duomenų vientisumo tikrinimas	-	-	Taip	Taip	Taip
Anomalijų aptikimas	Taip	Taip	-	-	-
Piktnaudžiavimo aptikimas	Ne	Taip	-	-	-
Apsauga nuo zondo atakos (angl. *Probe attack*)	Taip	Taip	-	-	-
Apsauga nuo buferio perpildymo (angl. *Buffer overflow*)	Taip	Taip	-	-	-
Apsauga nuo SQL injekcijų (angl. *SQL injection*)	Taip	Taip	-	-	-
Apsauga nuo naršyklės programų atakų (angl. *WEB application attack*)	Taip	Taip	-	-	-
Apsauga nuo atkirtimo nuo paslaugos atakos (angl. *DoS attack*)	Taip	Taip	-	-	-
Palaikomos operacinės sistemos	„Unix“; „Windows“	„Unix“	„Unix“; „Windows“	„Unix“	„Unix“; „Windows“
Šaltiniai	[11], [12], [13]	[11], [14], [13]	[15], [13]	[13]	[13]

Įsilaužimų aptikimo sistemos (1.3 lent.) skiriasi atakų aptikimo metodais, priklausomai ar sistema yra skirta veikti tinklo ar įrenginio lygmenyje. Tinklo lygmens įsilaužimų sistemos yra funkcionalesnės, nes jos analizuoja kiekvieną perduodamą duomenų paketą.

1.3.2. Daiktų interneto informacinių sistemų apsaugos metodų analizė

Daiktų interneto informacinių sistemų apsaugos metodai priklauso nuo sistemos saugos sluoksnių. Kartu visi sluoksniai sudaro bendrą sistemos saugumą. Tiriamos informacinės sistemos saugumą galima suskirstyti į 4 sluoksnius: duomenų, programų, įrenginio ir tinklo (1.5 pav.) [16].



1.5 pav. Informacinės sistemos saugumo sluoksniai

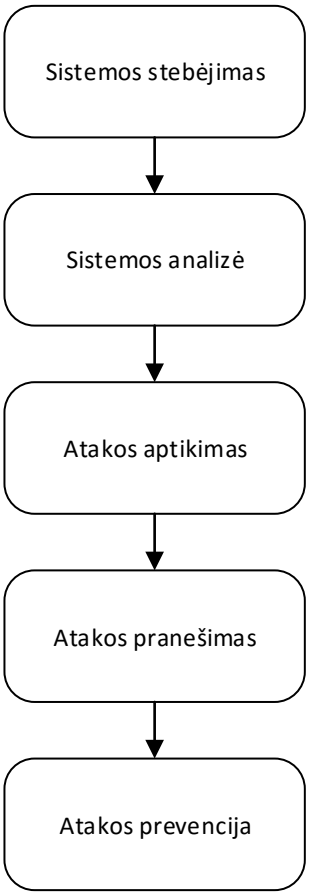
Sistemos pažeidžiamumas priklauso nuo informacinės sistemos saugos sluoksnio. Tinklo saugumo sluoksnis (1.5 pav.) yra labiausiai pažeidžiamas, o duomenų saugumas yra labiausiai apsaugotas. Norint pasiekti duomenis, reikia pirmiausiai įveikti pirmus tris sluoksnius. Kiekviename iš jų yra taikomi skirtingi saugumo metodai. Informacinės sistemos saugumo modelio (1.5 pav.) sluoksniai ir taikomi saugos metodai aprašyti 1.4 lent. [16].

1.4 lentelė. Informacinės sistemos saugos modelio sluoksniai

Eil. Nr.	**Saugumo sluoksnis**	**Apsaugos metodai**
1	Duomenų saugumas	Prieigos kontrolė; duomenų praradimo prevencija (angl. *Data loss prevention*); duomenų šifravimas; maišos algoritmai.
2	Programų saugumas	Internetinių programų ugniasienė (angl. *Web application firewall*); programinės įrangos kūrimo ciklo saugumas (angl. *Security in the software development life cycle*).
3	Įrenginių saugumas	Pataisų valdymas (angl. *Patch management*); pagrindinio kompiuterio įsibrovimų aptikimo sistema (angl. *Host based intrusion detection system*); antivirusinė programa.
4	Tinklo saugumas	Ugniasienė; įsibrovimų aptikimo sistema.

Duomenų saugumas (1.5 pav.) užtikrina duomenų konfidencialumą juos talpinant ir perduodant. Programų saugumas aprašo sistemos įrenginiuose diegiamų programų unikalumą bei veikimo stabilumą. Įrenginių saugumas apibūdina daiktų interneto objektų saugumą, užtikrinant jų neprieinamumą, konfidencialumą ir stabilumą. Tinklo saugumas užtikrina perduodamų duomenų kontrolę.

Įsilaužimų prevencijos sistemos (angl. *Intrusion prevention systems*) yra įsilaužimų aptikimo sistemų plėtinys, kurio tikslas yra blokuoti aptiktą ataką. Šių sistemų metodai priklauso nuo aptiktos atakos tipo. Atakos aptikimo ir prevencijos procesai vyksta etapais, pavaizduotais 1.6 pav. [17].



1.6 pav. Įsilaužimų aptikimo ir prevencijos sistemos procesai

Įsilaužimų aptikimo sistemos veikia stebėdamos ir analizuodamos informacinės sistemos veiklą (1.6 pav.). Aptikus ataką, sistema formuoja pranešimus į kuriuos reaguodami tam tikri komponentai imasi atakos prevencijos. Prevencijos metodai skiriasi nuo atakos pobūdžio.

Norint apsaugoti daiktų interneto informacinę sistema nuo atakų, reikia taikyti įvairius saugumo metodus. Atakų apsaugos ir prevencijos metodai priklauso nuo apsaugos priemonių. Daiktų interneto informacinėse sistemose taikomos apsaugos priemonės nuo atakų [18]:

a. virtualusis privatusis tinklas;
b. duomenų šifravimas;
c. autentifikavimas ar autorizavimas;
d. vartotojo sąsajos saugumo metodai;
e. privatumo užtikrinimo metodai;
f. duomenų bazės saugumo metodai;
g. valdymo įrenginio saugumo metodai;
h. saugumo konfigūracija;
i. programinės ir aparatinės įrangos saugumo metodai;

j. fizinės apsaugos metodai.

Virtualusis privatusis tinklas. Norint užtikrinti saugų prisijungimą prie nutolusių įrenginių yra sudaromas virtualusis privatusis tinklas. Tai tinklas, kuriame sujungimas tarp dviejų komponentų sudaromas panaudojant viešą internetą, bet perduodami paketai yra šifruojami. Sudaromas loginis perdavimo „tunelis“, per kurį galime perduoti šifruotą duomenų srautą, nesijaudinant, kad kas perims šiuos duomenis. Siuntėjas prieš išsiųsdamas duomenis kiekvieną perduodamą paketą užkoduoja tam tikrais algoritmais. Norint duomenis iššifruoti, gavėjas turi būti tam specialiai paruoštas. Virtualiojo privačiojo tinklo trūkumas yra sumažėjusi perduodamų duomenų sparta.

Duomenų šifravimas yra pagrindinis duomenų apsaugos būdas, kuris užkerta kelią duomenų atskleidimui pašaliniams asmenims. Šis metodas užtikrina duomenų privatumą. Šifravimui dažniausiai naudojami kriptografijos metodai. Šifravimas atliekamas panaudojant unikalų raktą, analogiškai kaip sudarant virtualų privatų tinklą. Duomenų šifravimas atliekamas įvairiais sertifikuotais algoritmais [19]. Yra išskiriami trys kriptografijos tipai [19]:

a. simetrinis (slapto rakto);
b. asimetrinis (viešojo rakto);
c. mišrusis (simetrinio ir asimetrinio metodo kombinacija).

Simetriniai kriptografijos metodai naudoja slaptąjį apsikeitimo raktą. Šie metodas yra gan sudėtingi, nes kyla daug keblumų raktų apsikeitimo procese. Šių metodų algoritmų yra gana daug, pavyzdžiui DES, AES ir t.t.

Asimetriniai kriptografijos metodai naudoja du raktus, vienas duomenims užšifruoti, kitas iššifruoti. Kiekvienos bendraujančios šalys turi po du raktus, viešą ir uždarąjį. Pagrindinis trūkumas, kad šis šifravimas palyginti su simetriniu yra lėtesnis ir reikalauja daugiau sistemos resursų. Vienas iš plačiausiai naudojamų asimetrinio šifravimo algoritmų yra RSA [20].

Dėl simetrinio ir asimetrinio metodų privalumų ir trūkumų yra kartais naudojami mišrieji metodai. Tai daroma dėl ribotų sistemos resursų, nes asimetrinio algoritmo naudojimas gali sąlygoti trumpesnę įrenginio gyvavimo trukmę, kai prietaisas yra priklausomas nuo nepakankamos maitinimo šaltinio talpos. Simetrinio kodo apsikeitimas yra vykdomas naudojant asimetrinį algoritmą ir po to yra vykdomas duomenų apsikeitimas naudojant simetrinį kriptografijos metodą.

Maišos funkcijos (angl. *Hash function*) algoritmai yra naudojami informacijos vientisumo tikrinimui ar slaptažodžių saugojimui. Norint patikrinti ar pateikta informacija nebuvo modifikuota, įprastai yra naudojami MD5 ir SHA [20] maišos funkcijos algoritmai.

Norint saugiai prisijungti prie nutolusios sistemos įprastai yra naudojami SSH ar SSL protokolai [21]. Naudojant SSH protokolą yra užtikrinamas kliento vardo ir slaptažodžio šifravimas 128 bitų raktu [22].

SSL protokolas yra skirtas šifravimo būdu apsaugoti perduodamą informaciją tarp dviejų sistemų [23]. Šis protokolas naudoja mišrųjį kriptografijos metodą, kuris suderinamas su TCP/IP protokolų rinkiniu.

Jei daiktų interneto informacinėje sistemoje nėra įdiegtas duomenų šifravimas, vietiniu arba išoriniu tinklu perduodama informacija gali būti perskaitoma pašalinių asmenų. Dauguma šio tipo saugumo spragų galima nesunkiai aptikti stebint duomenų perdavimą ar ieškant skaitomų duomenų. Norint užtikrinti saugų duomenų perdavimą reikia užtikrinti perduodamų duomenų žinutės naudingosios dalies duomenų šifravimą standartizuotais šifravimo algoritmais ir užtikrinti, kad yra naudojamas ryšio užmezgimo algoritmas ir, jei yra galimybė, naudoti gautų duomenų vientisumo tikrinimo algoritmus.

Autentifikavimas ar autorizavimas. Nesaugus vartotojo autentifikavimas dėl netinkamo vartotojo vardo ir slaptažodžio tikrinimo algoritmų. Norint apsisaugoti nuo šių saugumo spragų, reikia užtikrinti, kad pradinės produkto sąrankos metu, būtų atliktas numatyto slaptažodžio keitimas ir po 3-5 neteisingų bandymų prisijungti, vartotojas ar įrenginys turi būti blokuojamas. Taip pat reikia užtikrinti, kad vartotojo paskyros slaptažodis yra sudarytas iš ne mažiau kaip 8 simbolių ir būtų panaudotos raidės (mažosios ir didžiosios), skaičiai ir bent vienas specialus simbolis. Sistemos informacijos valdymui turi būti suteikiamos skirtingos vartotojo teisės kiekvienam sistemos vartotojui ir užtikrinama, kad vartotojo vardas ir slaptažodis yra patikimai saugomi atitinkamoje duomenų bazėje. Atliekant jautrias sistemai funkcijas, būtina reikalauti papildomo vartotojo autentifikavimo. Turi būti užtikrinamas tinkamas duomenų bazei apsaugoti autentifikavimo metodas. Kiekvieno vartotojo, įrenginio ar programos identifikacijos numeriai turi būti surišti tarpusavyje ir saugomi autentifikavimo duomenų bazėje. Turi būti užtikrinama, kad autentifikavimo sesijos raktas, išduodamas vartotojui prisijungus prie sistemos, būtų visada naujas, bei būtų užtikrinama, kad vartotojo, programų ir įrenginių identifikacijos numeriai būtų universalūs bei unikalūs.

Vartotojo sąsajos saugumo metodai. Saugumo spragos yra aptinkamos atlikus sistemos testavimą ir simuliuojant vartotojo veiklą. Norint apsisaugoti nuo šių saugumo spragų, reikia išpildyti tam tikrus saugumo reikalavimus. Įvykus vartotojo paskyros blokavimui, užtikrinamas saugus vartotojo atkūrimo mechanizmas, nesuteikiant užpuolikui informacijos apie esamą vartotojo paskyrą bei užtikrinama, kad neegzistuoja pažeidžiamumas, kaip pašalinio programinio kodo įskiepiai, neautorizuotų komandų perdavimas. Taip pat turi būti užtikrinama, kad vartotojo duomenys nebus atskleisti tiek vidiniame, tik išoriniame tinkle.

Privatumo užtikrinimo metodai. Skirtingi vidiniai ir išoriniai asmenys turi skirtingą priėjimą prie tam tikrų sistemos dalių, tokių kaip jutikliai, mobiliosios programos ar duomenų saugojimo bazės. Vartotojui aktyvavus informacinę sistemą yra surenkami įvairūs duomenys, kurie yra talpinami duomenų bazėse. Šių saugyklų administratoriai neturi galėti savavališkai perskaityti duomenis ir juos

panaudoti piktaviškiems tikslams. Norint padidinti duomenų privatumą, reikia atskiruose tinklo įrenginiuose saugoti tik jiems funkcionuoti reikalingus vartotojo duomenis ir turi būti išlaikytas surinktų duomenų anonimiškumas. Duomenų bazėje saugomi, tinklo įrenginiuose ir jų komponentuose esantys duomenys turi būti šifruojami. Reikia užtikrinti, kad tik autorizuoti tinklo vartotojai gali naudotis tik tam tikrais sistemos resursais ir yra naudojamas duomenų saugojimo galiojimo laikas. Taip pat reikia užtikrinti, kad vartotojui bus pranešta, jei sistemos perduodami duomenys yra įtartini ar duomenų daugiau nei įprasta ir yra naudojamos skirtingos duomenų rolės, kai vartotojas norėdamas peržiūrėti sistemos informaciją yra paprašomas autorizuoti savo teises.

Duomenų bazės saugumo metodai. Duomenų bazės sąsaja gali sukelti duomenų vagystę ar pilną informacinės sistemos valdymo sutrikimą. Nesaugią duomenų talpyklos sąsają galima aptikti identifikuojant ar yra naudojamas saugaus sujungimo protokolas. Taip pat ar yra naudojamas saugus slaptažodžio atstatymo algoritmas. Norint užtikrinti saugią duomenų bazės sąsają, reikia duomenų bazės diegimo metu užtikrinti, kad sistemos naudotojas pakeistų pradinį vartotojo vardą ir slaptažodį ir nenaudotų tokių frazių kaip „Neteisingai įvestas vartotojo vardas“ arba „Neteisingai įvestas slaptažodis“, kurios galėtų informuoti apie teisingai įvestą vartotojo vardą. Jei įmanoma, įdiegti dviejų faktorių vartotojo autentifikavimą [24], kai yra naudojamas vartotojo asmeninis įrenginys papildomam saugumui užtikrinti. Taip pat identifikuoti ir blokuoti neįprastus sistemos reikalavimus ar pageidavimus.

Valdymo įrenginio saugumo metodai. Saugumo spraga yra tada, kai yra fizinis prieinamumas prie informacinės sistemos valdymo įrangos. Jei yra naudojama atvira įrenginio sąsaja, gali būti perimtas sistemos valdymas, pavogti ar modifikuoti įvairūs saugomi duomenys. Norint identifikuoti saugumo spragas reikia atlikti programos testavimą, kurio metu identifikuojamos tinklo jungtys, naudojami saugumo algoritmai ir slaptažodžio atkūrimo metodai. Norint pagerinti valdymo įrangos saugumą, reikia užtikrinti, kad prisijungimo duomenys nebūtų matomi vartotojo sąsajoje, naudoti apsaugą, nuo programinio kodo atkūrimo [25], naudoti suklastotos programinės įrangos atpažinimo metodus, šifruoti įrenginio atmintinės duomenis ir užtikrinti, kad programinė įranga būtų įrašyta tik į galiojantį įrenginį.

Saugumo konfigūracija. Nepakankamos saugumo konfigūracijos galimybės atsiranda, kai vartotojas turi ribotas ar išvis neturi galimybės pakeisti saugumo nustatymus. Norint užtikrinti pakankamas konfigūravimo galimybes, reikia išskirti administratoriaus ir įprasto vartotojo teises, užtikrinti visų duomenų šifravimą, suteikti vartotojui papildomas saugumo konfigūracijos galimybes, priverstinį saugaus slaptažodžio kūrimą, įdiegti automatinius pranešimus apie sistemos saugumo pažeidimui.

Programinė ar aparatinė įranga. Įsilaužėlis, turintis fizinį priėjimą prie įrenginio, jo tinklo ar atnaujinimų duomenų bazės, gali pasinaudoti nesaugia programine ar aparatine įranga ir atlikti atakas.

Įsilaužėlis gali pasinaudoti neužšifruotais atnaujinimo failais, kurie yra perduodami neužšifruotu tinklu ir juos pakeisti savu - kenkėjišku programiniu kodu. Tuo pačiu negalėjimas atnaujinti prietaiso programinės įrangos, gali sukelti tam tikrų saugumo spragų. Ši saugumo spraga aptinkama skenuojant sistemos perduodamus duomenis bei atliekant atnaujinimo imitaciją. Norint panaikinti šias saugumo spragas, reikia užtikrinti, kad bus šifruojamas kiekvienas atnaujinimo failas žinomu kriptografiniu metodu, atnaujinimo failai bus perduodami koduota duomenų perdavimo terpe bei užtikrinama, kad atnaujinimo failas neatskleidžia svarbios vartotojo informacijos. Taip pat užtikrinti, kad prieš išsiunčiant ir pritaikant sistemos atnaujinamus, jie būtų patikrinti bei verifikuoti ir, jei įmanoma, įdiegti saugios įkrovos režimą.

Fizinė apsauga. Įsibrovėlis, turėdamas fizinį priėjimą prie aparatinės sistemos įrangos, gali perskaityti įrenginių duomenis, naudodamasis USB ar SD kortelių sąsajomis, kurios įprastai skirtos sistemos konfigūracijai ar priežiūrai. Taip pat, pašalinis asmuo gali perprogramuoti ar kitaip pakenkti informacinę sistemą. Pakankamas fizinis saugumas reikalauja, kad duomenų saugyklos būtų integruotos įrenginyje, šifruojami atmintinės duomenys, užtikrinti, kad nebūtų galimybės pasinaudoti išoriniu prievadu, kaip piktavališku priėjimu prie įrenginio resursų, bei užtikrinti, kad įrenginys nebūtų lengvai išardomas, o taip pat užtikrinti, kad įtaisais turėtu griežtai apibrėžtas administravimo galimybes.

1.4. Siekiami darbo sprendimai

Šiame darbe siekiamas sprendimas - saugumo pagerinimas daiktų interneto informacinėje sistemoje. Pasirenkama daiktų interneto informacinė sistema ir ištiriamas jos saugumas, bei pritaikomi tinkami atakų prevencijos metodai, įdiegiamos apsaugos priemonės ir atliekamas eksperimentinis sistemos saugumo metodų testavimas.

Prisijungimas prie sistemos išmaniųjų įrenginių sudaromas naudojantis prisijungimo slaptažodį sudarytą iš tam tikro ilgio skaitmenų, kai vartotojas įveda išmaniojo įrenginio ekrane rodomą slaptažodį, taip pat gali būti naudojamos tam tikros specialios slaptažodžio perdavimo technologijos, kaip NFC. Galima išskirti tris prisijungimo būdus [26]:

a. tiesiog veikia (angl. *Just Works*) - sujungimas tarp įrenginių sudaromas nenaudojant slapto rakto;
b. rakto generavimas (angl. *Passkey Display*) - rakto apsikeitimui naudojami vaizdo ekranai;
c. dažnių juostos sujungimas (angl. *Out Of Band Pairing*) - naudojama papildoma rakto apsikeitimo aparatinė įranga.

Kuriama sistema turi naudoti autoriaus sukurtą prisijungimo metodą. Siūlomo prisijungimo metodo palyginimas su kitais analogiškais metodais [26] pateiktas 1.5 lent.

1.5 lentelė. Prisijungimo metodų palygimas

Metodas / **Savybė**	**Tiesiog veikia (angl. *Just Works*)**	**Rakto generavimas (angl. *Passkey Display*)**	**Dažnių juostos sujungimas (angl. *Out Of Band Pairing*).**	**Siūlomas naujas metodas**
Rakto apsikeitimui reikalingas išorinis ekranas	Ne	Tai	Ne	Ne
Reikalinga papildoma radijo bangų perdavimo technologija	Ne	Ne	Taip	Ne
Nuolatinio slaptažodžio suteikimas	Ne	Ne	Ne	Taip
Papildomas duomenų šifravimas vartotojo nurodytu raktu	Ne	Ne	Ne	Taip
Apsauga nuo pasyvios duomenų pasiklausymo atakos	Ne	Ne	Ne	Taip
Išmaniojo įrenginio blokavimas po neteisingai įvesto slaptažodžio	Ne	Ne	Ne	Taip

Autoriaus siūlomas metodas pagerina išmaniojo įrenginio konfidencialumą, kai prie jo yra prisijungiama naudojant slaptą raktą ir šiuo raktu šifruojami perduodami duomenys. Apsauga nuo duomenų pasiklausymo atakos užtikrina, kad nebus galima pasinaudoti atrakintu išmaniuoju įrenginiu.

1.5. Analizės išvados

1. Išanalizavus išmaniųjų įrenginių informacines sistemas ir jų įsilaužimų aptikimo sprendimus nustatyta, kad išmaniųjų įrenginių informacinių sistemų įsibrovimų aptikimo priemonės turi būti diegiamos kartu su įsilaužimų prevencijos sistemomis.
2. Atlikus atakų aptikimo sistemų analizę, buvo nustatyta, kad tiriamos informacinės sistemos atakų aptikimo metodai turi veikti išmaniuosiuose įrenginiuose ir valdymo kompiuteryje, norint aptikti įvairių tipų atakas.
3. Išanalizavus informacinės sistemos saugumo sluoksnius, buvo nustatyta, kad sistemos saugumą reikia užtikrinti tinklo, įrenginių, programų ir duomenų lygiuose.
4. Išanalizavus daiktų interneto informacinėse sistemose taikomas apsaugos priemones nuo atakų, buvo nustatyta, kad norint pagerinti sistemos saugumą, reikia įdiegti duomenų šifravimą visuose sistemos įrenginiuose, išmaniojo įrenginio autentifikavimą bei saugumo konfigūravimą valdymo įrenginyje.

2. DAIKTŲ INTERNETO INFORMACINĖS SISTEMOS REIKALAVIMŲ SPECIFIKACIJA

Daiktų interneto informacinės sistemos reikalavimų specifikacijos skyriuje pateikiamas kuriamos informacinės sistemos reikalavimų aprašas.

2.1. Reikalavimų specifikacija

Reikalavimų specifikacija apibrėžia vartotojo poreikius sistemai. Reikalavimams identifikuoti naudojama įvairi informacija apie sistemos dalykinę sritį, vartotojo poreikiai ir sistemos kontekstas. Funkciniai reikalavimai pateikiami natūralia kalba ir lentelių pavidalu, kurie nusako pakankamą sistemos funkcionalumą sistemos kūrėjui.

2.1.1. Apribojimai reikalavimams

Apribojimai reikalavimams - tai reikalavimų specifikaciją apribojantys reiškiniai ir charakteristikos. Kuriamos sistemos reikalavimų apribojimai:

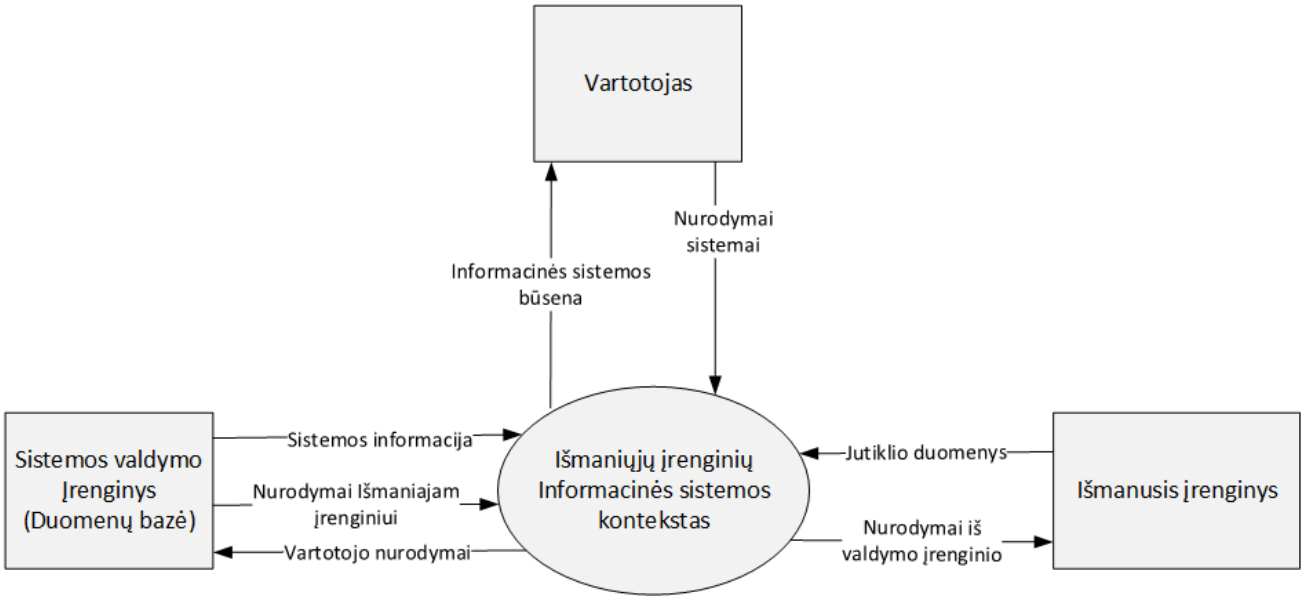
1. Kuriama informacinė sistema susidaryta iš išmaniojo įrenginio ir sistemos valdymo kompiuterio diegimo aplinkų.
2. Naudojamas centrinis valdymo kompiuteris, kuris atlieka duomenų bazės paskirtį, surinktiems jutiklių duomenims talpinti.
3. Vartotojas turi turėti galimybę stebėti jutiklių duomenis vartotojo sąsajoje.
4. Išmanusis įrenginys neturi ekrano ir klaviatūros.

2.1.2. Veiklos kontekstas

Konteksto diagrama naudojama apibrėžti nagrinėjamai veiklai. Ši diagrama apima sistemos dalykinę sritį ir leidžia labiau suprasti darbo veiklą. Diagramoje atvaizduojami duomenų srautai tarp komunikuojančių sistemos dalių, nurodant informacijos kryptį bei atvaizduojami vartotojai ir gretimos, komunikuojančios sistemos. Tokiu būdu yra nusakomos išorinių sistemos dalių atsakomybės.

Sudaromas sistemos veiklos padalijimas lentelės pavidalu. Joje surašomi veiklos pavadinimai ir jos reakcijos, įėjimai ir išėjimai. Šie įvykiai yra tam tikros sistemos dalies atliekami veiksmai. Padalijant veiklą galima identifikuoti reikalavimus, kuriais remiantis galima atlikti sistemos projektavimą.

Kuriamos išmaniųjų įrenginių informacinės sistemos konteksto diagrama pateikta 2.1 pav.



2.1 pav. Kuriamos informacinės sistemos konteksto diagrama

Veiklos įvykių sąrašas pateiktas 2.1 lent.

2.1 lentelė. Veiklos įvykių sąrašas

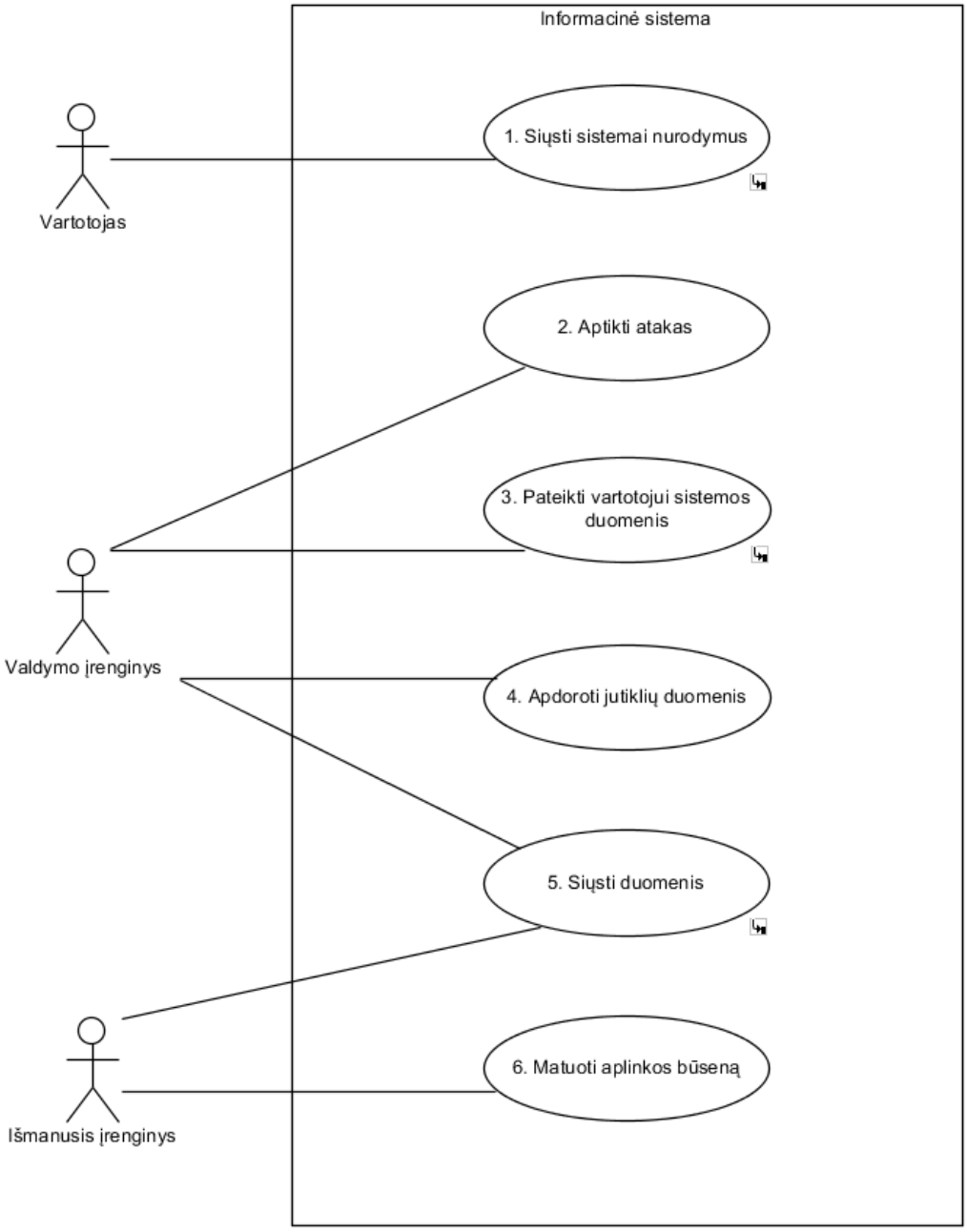
Eil. Nr.	Įėjimo/išėjimo informacijos srautas	Įvykio pavadinimas
1	Informacinės sistemos būsena (išėjimas)	Informacija vartotojui apie esamą sistemos būseną.
2	Nurodymai sistemai (įėjimas)	Vartotojas siunčia nurodymus sistemos valdymo įrenginiui, kuris atitinkamai reaguoja. Nurodymai gali būti kaip jutiklio įjungimas ar išjungimas ir pan.
3	Jutiklio duomenys (įėjimas)	Konkretaus išmaniojo įrenginio jutiklių duomenys.
4	Nurodymai iš valdymo įrenginio (įėjimas)	Tam tikri nurodymai skirti įrenginio funkcionalumui keisti.
5	Vartotojo nurodymai (išėjimas)	Valdymo įrenginys gauna tam tikrus nurodymus iš vartotojo.
6	Nurodymai išmaniajam įrenginiui (išėjimas)	Tam tikri vartotojo nurodymai skirti tam tikram išmaniajam įrenginiui.
7	Sistemos informacija (įėjimas)	Valdymo įrenginys sukaupia visų išmaniųjų įrenginių jutiklių duomenis ir juos siunčia pateikdamas vartotojui grafinėje vartotojo sąsajoje GUI.

Veiklos įvykių sąraše (2.1 lent.) pateikti informacijos srautai apibūdina kuriamos informacinės sistemos duomenų mainus tarp vartotojo, valdymo ir išmaniojo įrenginio. Identifikavus įėjimo ir išėjimo kryptis, galime spręsti apie šių aktorių atliekamas veiksmų sekas informacinėje sistemoje.

2.1.3. Sistemos panaudojimo atvejų modelis

Panaudojimo atvejų diagrama nusako sistemos ribas tarp vartotojo ir sistemos. Įvertinant kiekvieną veiklos įvykį (2.1 lent.) ir sistemos pobūdį galima sudaryti panaudojimo atvejų diagramą.

Panaudojimo atvejų modelis pateiktas 2.2 pav.



2.2 pav. Tiriamos išmaniųjų įrenginių informacinės sistemos panaudos atvejų diagrama

Tiriamos išmaniųjų įrenginių informacinės sistemos panaudos atvejų diagrama apima vartotojo, valdymo įrenginio ir išmaniųjų įrenginių aktorius (2.2 pav.). Vartotojas apima pirmąjį „Siųsti sistemai nurodymus“ panaudos atvejį, kuris nusako vartotojo indėlį į kuriamą informacinę sistemą. Valdymo įrenginys apima 2, 3, 4 ir 5 panaudos atvejus. Jis atsakingas už visos sistemos atakų aptikimą, duomenų apdorojimą bei pranešimus vartotojui. Išmanusis įrenginys apima 5 ir 6 panaudojimo atvejus, kurie nusako jo vaidmenį duomenų gavime ir jų perdavime valdymo įrenginiui.

2.1.4. Funkciniai reikalavimai informacinei sistemai

Funkciniai reikalavimai nurodo kuriamos sistemos funkcionalumą ir aprašo duomenų manipuliaciją. Vartotojas formuluoja reikalavimus sistemos veiklos logikai, numatant būsimos sistemos veiksmus. Vartotojas nusako sistemos veiksmus taip, kad būtų aišku ką sistema turėtų atlikti.

Informacinės sistemos kūrėjas, atsižvelgdamas į vartotojo pateiktus sistemos funkcinius reikalavimus, turi žinoti kaip sistema turi funkcionuoti.

Funkciniai reikalavimai nusakomi panaudojimo atvejų diagrama. Funkciniai ir nefunkciniai reikalavimai registruojami naudojant „Volere“ šablono kortelių pavidalą [27], jų specifikacija vykdoma trimis parametrais: numeriu, tipu ir panaudojimo atveju. Reikalavimų kortelės sudarytos iš punktų [27]:

a. reikalavimo numeris - reikalavimo kortelės eilės numeris;

b. panaudojimo atvejis - panaudojimo atvejo numeris. Naudojamas konkretaus panaudojimo atvejo numeris, kuris susiejamas su funkciniu reikalavimu;

c. aprašymas - tai reikalavimo paskirties apibrėžimas kuriame atskleidžiami vartotojo pageidavimai;

d. pagrindimas - nusako reikalavimo reikalingumą, svarbumą ir jo įtaką visai sistemai ir jos tikslams. Parodo specifikuojamo reikalavimo prasmę;

e. šaltinis - su kuriamos informacinės sistemos objektu susijęs asmuo;

f. tinkamumo kriterijus - tai yra tikimo kriterijus, nusakantis kvalifikuotus tikslus, kurie turi tenkinti sistemą;

g. priklausomybės - reikalavimas kuris daro įtaką kuriamam reikalavimui arba nurodo kuriamo reikalavimo priklausomybę nuo kito ar kitų reikalavimų;

h. konfliktai - tai yra kelių reikalavimų prieštaravimas vienas kitam. Konfliktai gali atsitikti dėl įvairių realios sistemos kūrimo etapų;

i. papildoma medžiaga - tai yra nuoroda, į tiesiogiai susijusią, su kuriamu reikalavimu informaciją, kuri daro įtaką esamam reikalavimui;

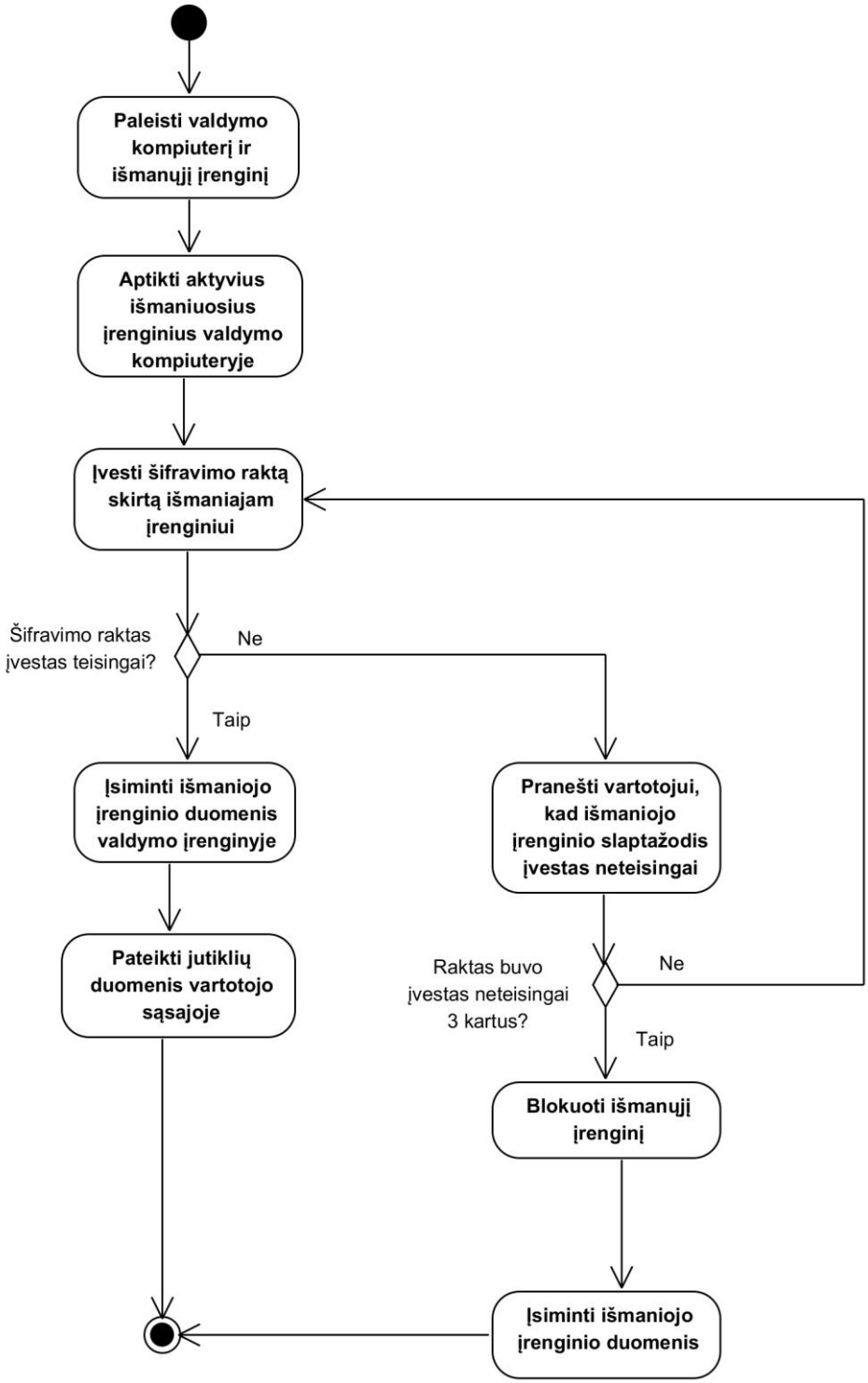
j. istorija - reikalavimo registracijos, pataisymo ar pakeitimo data. Taip pat gali būti registruoti asmenys atsakingi už reikalavimo redagavimą.

Kuriamos informacinės sistemos funkciniai reikalavimai pateikiami nuo 2.2 iki 2.7 lent.

2.2 lentelė. Funkcinis reikalavimas „Siųsti sistemai nurodymus“ panaudojimo atvejui

Reikalavimas #:	1	**Panaudojimo atvejis #:**	1
Aprašymas:	Vartotojas turi turėti galimybę siųsti nurodymus sistemai		
Pagrindimas:	Vartotojui turi būti suteikta galimybė valdyti sistemos parametrus		
Šaltinis:	Vartotojas		
Tinkamumo kriterijus:	Nėra		
Priklausomybės:	Nėra	**Konfliktai:**	Nėra
Papildoma medžiaga:	Nėra		
Istorija:	Užregistruotas 2016-03-05		

Veiklos diagrama „Siųsti sistemai nurodymus“ panaudojimo atvejui pateikta 2.3 pav.



2.3 pav. Veiklos diagrama „Siųsti sistemai nurodymus“ panaudojimo atvejui

2.3 lentelė. Funkcinis reikalavimas „Aptikti atakas“ panaudojimo atvejui

Reikalavimas #:	2 **Panaudojimo atvejis #:** 2
Aprašymas:	Valdymo įrenginys gali aptikti atakas įvykdytas prieš informacinę sistemą
Pagrindimas:	Vartotojas turi būti informuotas apie bandymą įvykdyti ataką
Šaltinis:	Sistemos projektuotojas
Tinkamumo kriterijus:	Išmanusis įrenginys blokuojamas po neteisėto bandymo pasinaudoti
Priklausomybės:	Nėra **Konfliktai:** Nėra
Papildoma medžiaga:	Nėra
Istorija:	Užregistruotas 2016-03-05

2.4 lentelė. Funkcinis reikalavimas „Pateikti vartotojui sistemos duomenis“ panaudojimo atvejui

Reikalavimas #:	3	**Panaudojimo atvejis #:** 3
Aprašymas:	Valdymo įrenginys pateikia duomenis vartotojui grafinėje sąsajoje	
Pagrindimas:	Sistemos valdymo įrenginys (kompiuteris) surenka duomenis iš tinklo mazgų (išmaniųjų įrenginių) ir pateikia duomenis vartotojui grafinėje sąsajoje	
Šaltinis:	Sistemos projektuotojas	
Tinkamumo kriterijus:	Perduodami duomenys turi būti šifruojami	
Priklausomybės:	Nėra	**Konfliktai:** Nėra
Papildoma medžiaga:	Nėra	
Istorija:	Užregistruotas 2016-03-05	

Veiklos diagrama „Pateikti vartotojui sistemos duomenis“ panaudojimo atvejui pateikta (2.4 pav.).

2.4 pav. Veiklos diagrama „Pateikti vartotojui sistemos duomenis“ panaudojimo atvejui

2.5 lentelė. Funkcinis reikalavimas „Apdoroti jutiklių duomenis“ panaudojimo atvejui

Reikalavimas #:	4	**Panaudojimo atvejis #:** 4
Aprašymas:	Valdymo įrenginys šifruoja gautus jutiklių duomenis ir talpina juos duomenų bazėje	
Pagrindimas:	Duomenys turi būti apsaugoti nuo neteisėto panaudojimo	
Šaltinis:	Sistemos projektuotojas	
Tinkamumo kriterijus:	Šifravimui naudojamas AES algoritmas	
Priklausomybės:	Nėra	**Konfliktai:** Nėra
Papildoma medžiaga:	Nėra	
Istorija:	Užregistruotas 2016-03-05	

2.6 lentelė. Funkcinis reikalavimas „Siųsti duomenis“ panaudojimo atvejui

Reikalavimas #:	5	**Panaudojimo atvejis #:** 5
Aprašymas:	Išmanusis įrenginys gauna matavimų duomenis iš jutiklių ir juos perduoda valdymo įrenginiui.	
Pagrindimas:	Jutiklių duomenys yra būtini sistemos funkcionavimui.	
Šaltinis:	Sistemos projektuotojas	
Tinkamumo kriterijus:	Nėra	
Priklausomybės:	Nėra	**Konfliktai:** Nėra
Papildoma medžiaga:	Nėra	
Istorija:	Užregistruotas 2016-03-05	

2.7 lentelė. Funkcinis reikalavimas „Matuoti aplinkos būseną“ panaudojimo atvejui

Reikalavimas #:	6	**Panaudojimo atvejis #:** 6
Aprašymas:	Išmanusis įrenginys matuoja aplinkos būsenos parametrus	
Pagrindimas:	Išmaniojo įrenginio testavimui reikalinga pateikti realaus veikimo pavyzdį	
Šaltinis:	Sistemos projektuotojas	
Tinkamumo kriterijus:	Jutiklio rodmenis gali automatiškai keistis kas viena sekundė	
Priklausomybės:	Nėra	**Konfliktai:** Nėra
Papildoma medžiaga:	Nėra	
Istorija:	Užregistruotas 2016-03-05	

2.1.5. Nefunkciniai reikalavimai

Nefunkciniai reikalavimai pateikia sistemos kriterijus, kurie sprendžia jos operacijas. Pateikiamas nefunkcinis reikalavimas veikimo sąlygoms 2.8 lent.

2.8 lentelė. Nefunkcinis reikalavimas veikimo sąlygoms

Reikalavimas #:	6	**Panaudojimo atvejis #: 1-6**
Aprašymas:	Išmanieji įrenginiai turi būti mobilūs	
Pagrindimas:	Išmaniųjų įrenginių pritaikymas įvairiems panaudojimo atvejams.	
Šaltinis:	Vartotojas	
Tinkamumo kriterijus:	Išmanusis įrenginys turi sverti ne daugiau kaip 0,2 kg.	
Priklausomybės:	Nėra	**Konfliktai:** Nėra
Papildoma medžiaga:	Nėra	
Istorija:	Užregistruotas 2016-03-05	

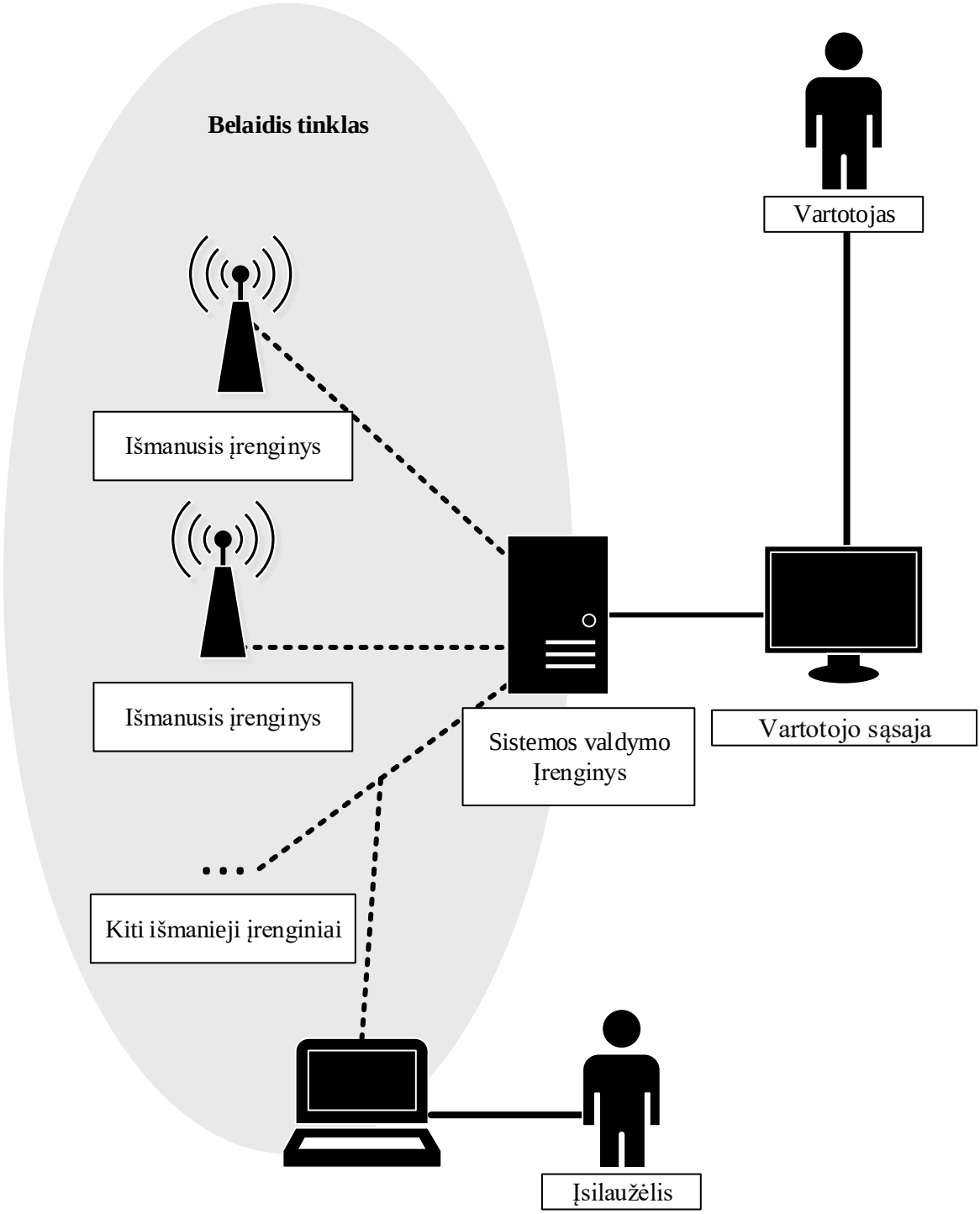
2.2. Reikalavimų apibendrinimas

Atlikus reikalavimų specifikaciją, buvo apibrėžta informacinės sistemos struktūra. Kuriama sistema turi atitikti vartotojo keliamus reikalavimus, kurie apibūdina reikalaujamą informacinę sistemą. Sistema naudoja belaidžio perdavimo technologijas, tad duomenų saugumas turi būti užtikrinamas ne tik vartotojo sąsajoje.

Norint išpildyti esamus sistemos reikalavimus, reikalinga sukurti išmaniųjų įrenginių informacinės sistemos prototipą. Norint užtikrinti sistemos saugumą, reikia atlikti prototipo saugumo tyrimą nuo išorės atakų. Atlikus sukurtos sistemos saugumo analizę yra pasiūlomi ir diegiami nauji saugumo sprendimai. Įdiegus naujus saugumo sprendimus yra atliekamas saugumo metodų testavimas.

3. DAIKTŲ INTERNETO INFORMACINĖS SISTEMOS PROJEKTAVIMAS

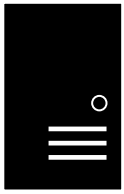
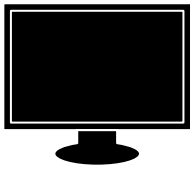
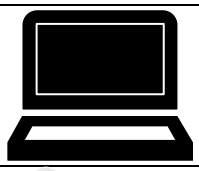
Projektuojama informacinė sistema susideda iš išmaniųjų įrenginių ir vieno valdymo įrenginio. Siekiamo sprendimo architektūros modelis pateiktas 3.1 pav.



3.1 pav. Siekiamo sprendimo architektūros modelis

Siekiamo sprendimo architektūros modelis susideda iš aštuonių komponentų, kurie atvaizduoja kuriamos sistemos vartotoją, įsilaužėlį, įrangą ir duomenų mainus. Komponentų sąrašas su paaiškinimais pateiktas 3.1 lent.

3.1 lentelė. Daiktų interneto informacinės sistemos komponentų sąrašas

Eil. Nr.	Komponento simbolis	Komponento pavadinimas	Komponento paaiškinimas
1		Išmanusis įrenginys	Išmanusis įrenginys skirtas įvairiems duomenims gauti iš jutiklių ir perduoti valdymo įrenginiui.
2		Sistemos valdymo įrenginys	Valdymo įrenginys skirtas išmaniųjų įrenginių duomenims surinkti, apdoroti, saugoti ir pateikti vartotojui.
3		Vartotojo sąsaja	Vartotojo sąsaja skirta pateikti jutiklių duomenis ar sistemos valdymo galimybę interaktyvioje vartotojo sąsajoje.
4		Įsilaužėlio kompiuteris	Įsilaužėlio kompiuteris skirtas atlikti atakas prieš projektuojamą informacinę sistemą.
5		Belaidis tinklas	Belaidis išmaniųjų įrenginių tinklas skirtas komunikacijai su valdymo įrenginiu.
6		Vartotojas arba įsilaužėlis	Išmaniųjų įrenginių informacinės sistemos vartotojas.
7		Belaidis duomenų srautas	Jutiklių duomenų srautas skirtas valdymo įrenginiui.
8		Sąveika su naudojamu įrenginiu	Vartotojo tiesioginis kontaktas su interaktyvia terpe, kurioje pateikta vartotojo grafinė sąsaja.

Norint pagerinti kuriamos informacinės sistemos saugumą yra pasiūlomi nauji sprendimai. Šie sprendimai apima išmaniojo ir valdymo įrenginio bei duomenų perdavimo saugumą. Siūlomi saugumo sprendimai pateikti 3.2 lent.

3.2 lentelė. Siūlomi informacinės sistemos saugumo sprendimai

Eil. Nr.	Sprendimas	Rezultatas
1	Išmaniojo ir valdymo įrenginių autentifikavimas naudojant šifravimo raktą.	Įrenginio konfidencialumas.
2	Atakos prevencijos ir informavimo metodai.	Apsauga nuo neteisėto įrenginio panaudojimo ir saugos pažeidimų pranešimai.

3	Iš išmaniojo įrenginio siunčiamų duomenų šifravimas.	Siunčiamų duomenų konfidencialumas.
4	Gautų duomenų šifravimas ir talpinimas valdymo įrenginio duomenų bazėje.	Talpinamų duomenų konfidencialumas ir privatumas.

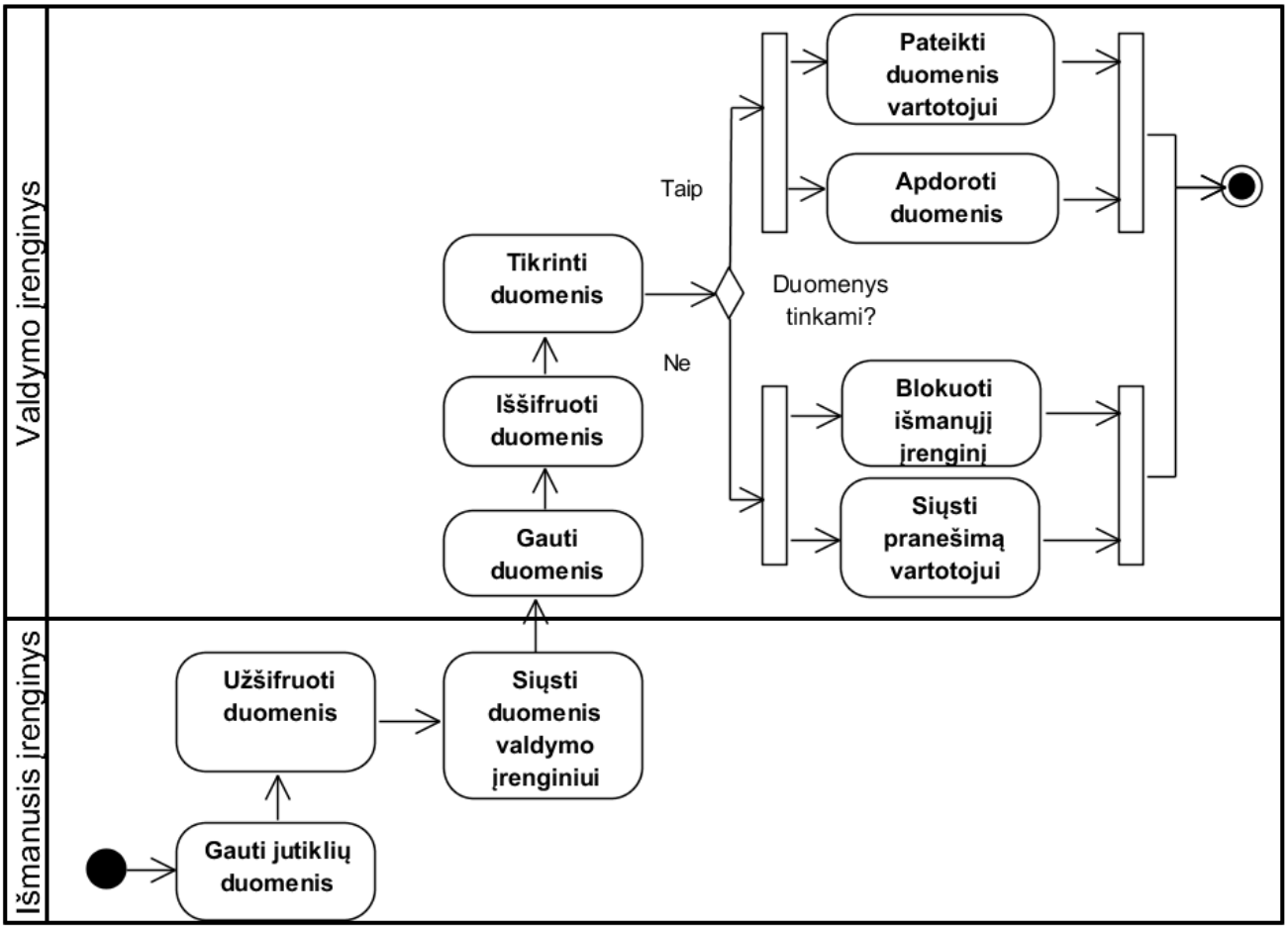
Siūlomi sprendimai (3.2 lent.) įgyvendinami programuojant išmaniojo įrenginio ir valdymo kompiuterio programinę įrangą.

3.1. Valdymo kompiuterio ir išmaniojo įrenginio saugumo metodų projektavimas

Valdymo kompiuterio ir išmaniojo įrenginio saugumo metodų projektavimo skyriuje projektuojami nauji saugumo sprendimai skirti kuriamai informacinei sistemai.

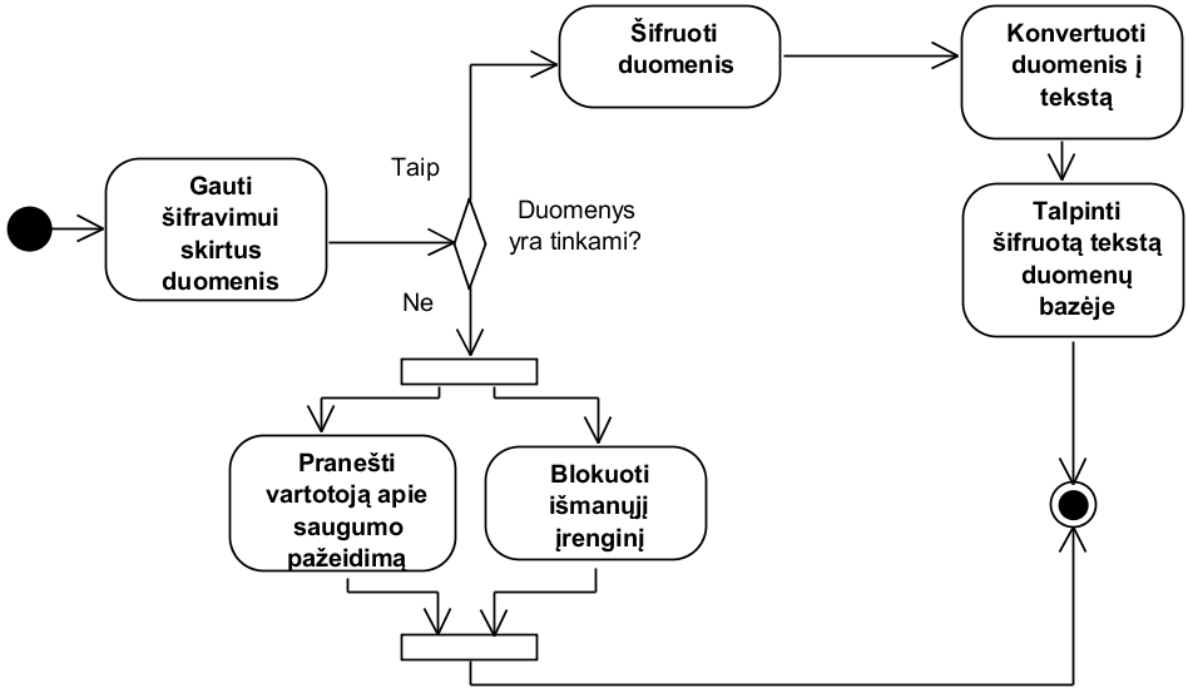
3.1.1. Valdymo kompiuterio duomenų šifravimo metodas

Valdymo įrenginys kuriamoje informacinėje sistemoje skirtas išmaniųjų įrenginių valdymui, gautų duomenų apdorojimui ir talpinimui duomenų failuose. Kuriamoje sistemoje galima pasirinkti bet kurį palaikomą šifravimo algoritmą. Duomenų apsikeitimo veiklos diagrama pateikta 3.2 pav.



3.2 pav. Duomenų apsikeitimo veiklos diagrama

Duomenys apdorojami juos patikrinant ar jie yra tinkami, šifruojant ir talpinant duomenų bazėje. Duomenų šifravimo funkcijos veiklos diagrama pateikta 3.3 pav.



3.3 pav. Duomenų šifravimo funkcijos veiklos diagrama

Veiklos diagramoje (3.3 pav.) pateiktas gautų duomenų iš išmaniojo įrenginio šifravimo metodas. Duomenys šifruojami ir talpinami duomenų failuose. Norint duomenis vėl panaudoti, juos reikia iššifruoti.

3.1.2. Prisijungimo prie išmaniojo įrenginio metodas

Projektuojamoje sistemoje išmanusis įrenginys neturi ekrano ar klaviatūros, o sujungimas su valdymo įrenginiu sudaromas be jokių saugumo sprendimų. Tad iškyla grėsmė, kad išmaniuoju įrenginiu bus galima pasinaudoti neautorizuotiems asmenims.

Norint pagerinti šio įrenginio saugumą yra kuriamas naujas išmaniojo įrenginio identifikavimo metodas (1.5 lent.). Tam tikslui naudoju šifravimo algoritmą, kuris yra pritaikomas tiriamam išmaniajam įrenginiui. Išmaniojo įrenginio vidinėje atmintyje yra saugomas numatytasis šifravimo raktas, kuris naudojamas duomenims šifruoti ir įrenginiui identifikuoti.

Įrenginio instaliacijos metu pakeičiamas numatytasis raktas. Vidinėje atmintyje talpinamas raktas, kuris užšifruotas tuo pačiu šifravimo raktu.

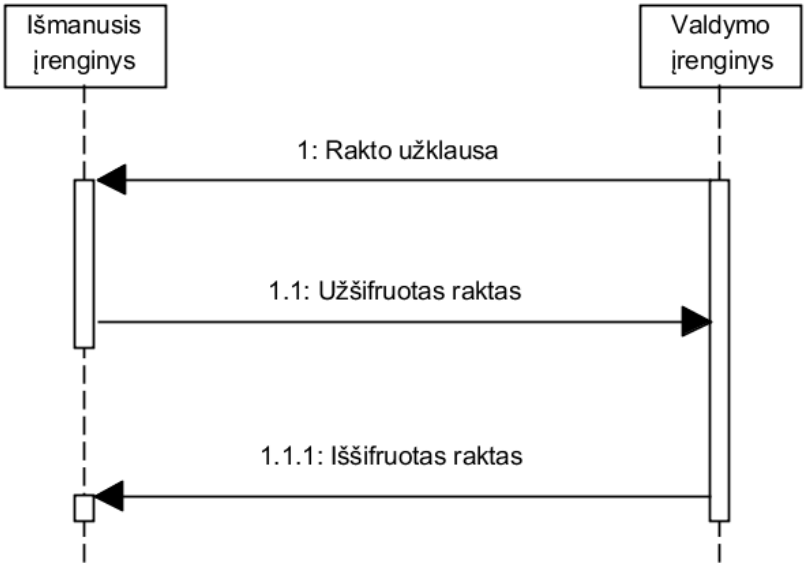
Identifikuojamas naujas įrenginys ir numatytasis raktas atliekant šiuos punktus:

a. valdymo įrenginys siunčia išmaniajam įrenginiui užklausą, kad atsiųstų užšifruotą raktą;
b. išmanusis įrenginys siunčia užšifruotą raktą valdymo įrenginiui;
c. valdymo įrenginys iššifruoja gautą raktą naudodamasis turimą raktą;
d. jei atsiųstas ir iššifruotas raktai sutampa, valdymo įrenginys siunčia šifravimo raktą išmaniajam įrenginiui;
e. išmanusis įrenginys iššifruoja raktą su atsiųstu iš valdymo įrenginio, jei raktai sutampa, atrakinamos visos įrenginio paslaugos;

f. visi perduodami duomenys šifruojami esamu šifravimo raktu;

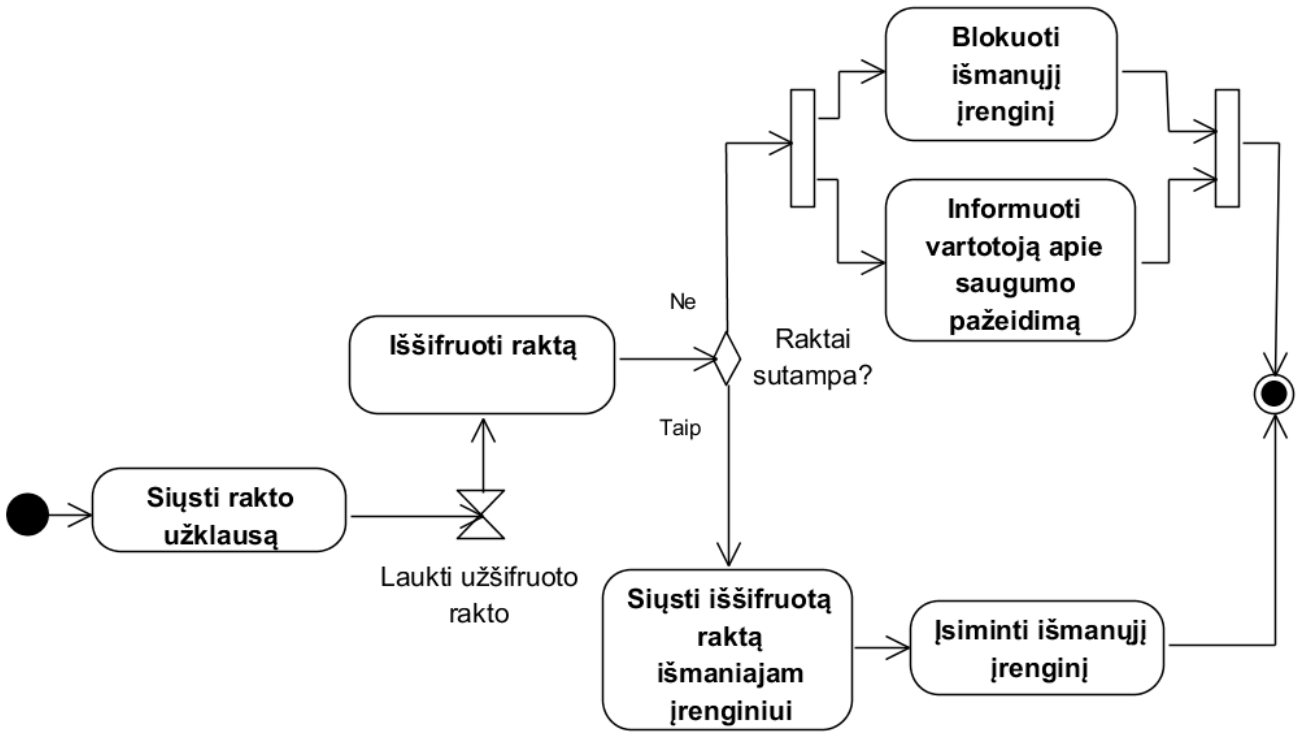
g. valdymo įrenginyje išsaugoma visa informacija apie išmanųjį įrenginį ir jo unikalų raktą.

Sekų diagrama tarp išmaniojo ir valdymo įrenginio pateikta 3.4 pav.



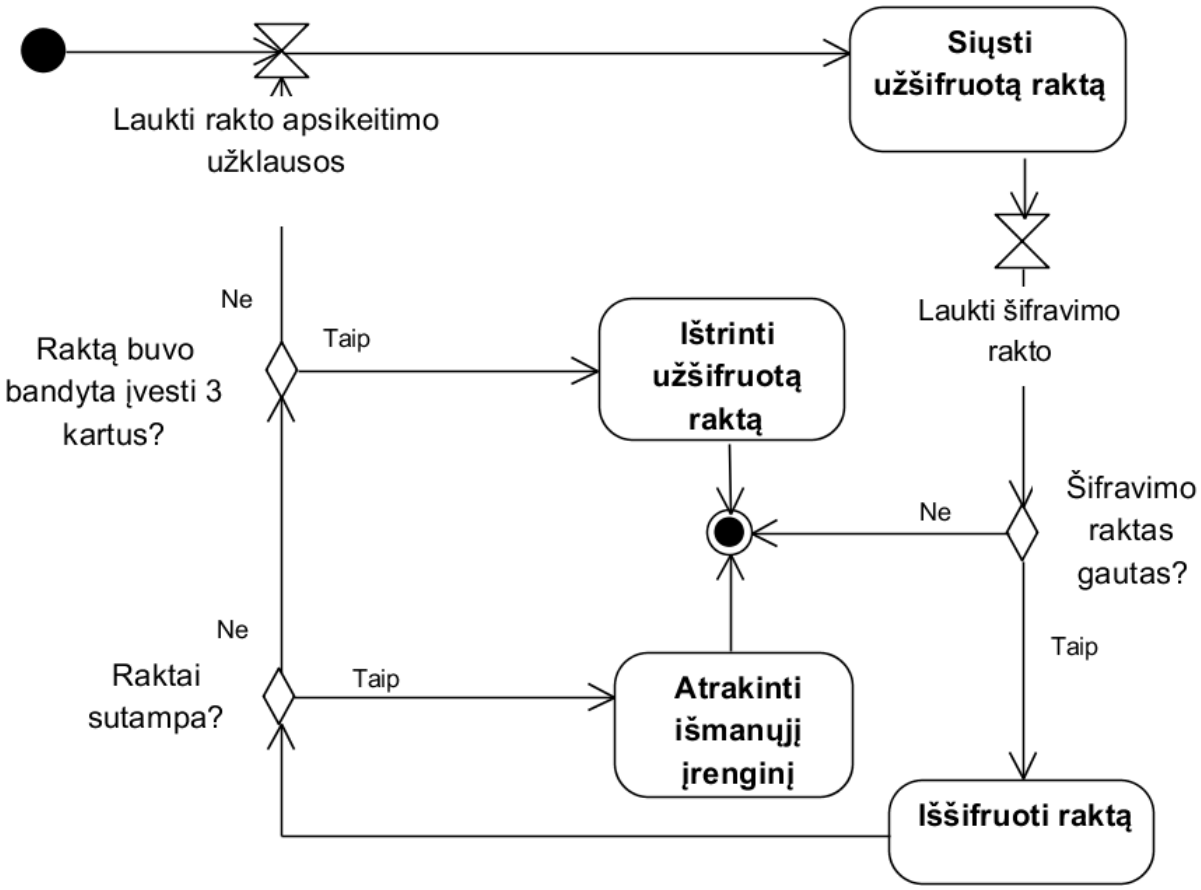
3.4 pav. Prisijungimo metodo sekų diagrama

Sekų diagramoje (3.4 pav.) yra pavaizduotas sėkmingas valdymo ir išmaniojo įrenginio identifikavimas. Šis metodas užtikrina išmanųjį įrenginį, kad jis prisijungė prie tinkamo valdymo įrenginio, nes jis žino slaptą raktą. Išmanusis įrenginys sužino tikrąjį raktą tik pabandęs jį iššifruoti duotu raktu. Jei iššifruoti raktai sutampa, įrenginys yra atrakinamas. Valdymo įrenginio veiklos diagrama pateikta 3.5 pav.



3.5 pav. Valdymo įrenginio prisijungimo metodo veiklos diagrama

Veiklos diagramoje (3.5 pav.) yra pavaizduota valdymo įrenginio veikla išmaniojo įrenginio identifikavimo procese. Išmaniojo įrenginio rakto apsikeitimo metodo veiklos diagrama pateikta 3.6 pav.



3.6 pav. Išmaniojo įrenginio prisijungimo metodo veiklos diagrama

Veiklos diagramoje (3.6 pav.) yra pavaizduota išmaniojo įrenginio veikla valdymo įrenginio identifikavimo procese. Šis metodas užtikrina įrenginio autorizaciją tarp komunikuojančių įrenginių. Taip pat po trijų, neteisingų bandymų įvesti raktą, išmanusis įrenginys ištrina savo ilgalaikėje atmintyje esantį raktą. Tokiu būdu yra nutraukiamas bet koks prisijungimas prie išmaniojo įrenginio, o prietaisas tampa nebepanaudojamas.

4. DAIKTŲ INTERNETO INFORMACINĖS SISTEMOS REALIZACIJA

Daiktų interneto informacinės sistemos realizacijos skyriuje pateikiu kuriamos daiktų interneto informacinės sistemos saugumo metodų realizaciją. Atlieku pasirinktos informacinės sistemos komponentų saugumo tyrimą.

4.1. Informacinės sistemos tyrimui skirti aparatūriniai ir programiniai komponentai

Tiriami aparatūriniai komponentai yra išmanusis įrenginys ir valdymo kompiuteris. Tyrimui naudojami aparatiniai ir programiniai komponentai pateikti 4.1 lent.

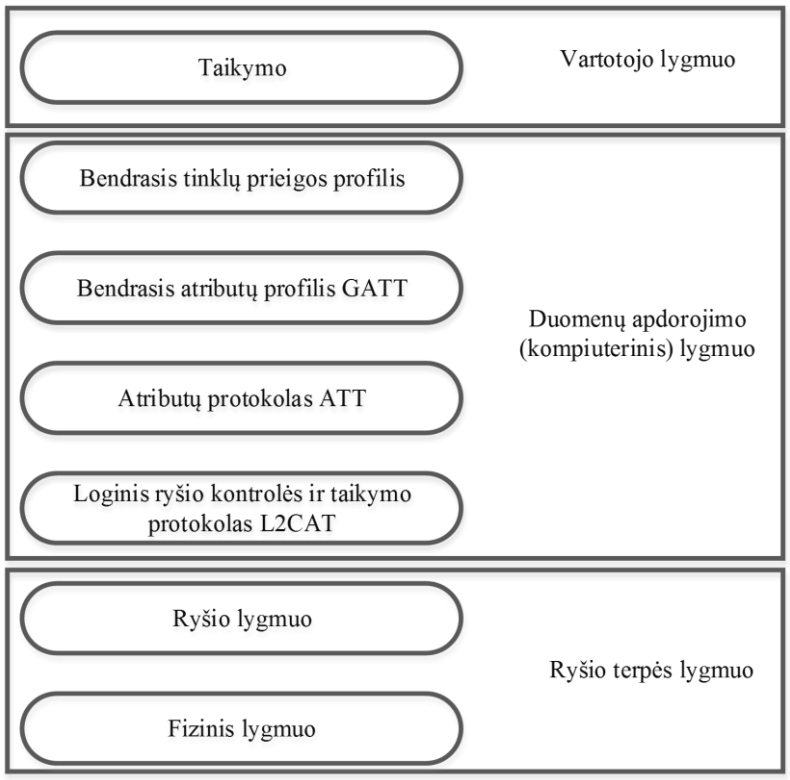
4.1 lentelė. Tiriami informacinės sistemos komponentai

Eil. Nr.	Komponento pavadinimas	Komponentas
1	Išmanusis įrenginys	„Sensortag CC2650“ [28].
2	Išmaniojo įrenginio programiniai projektai	„ProjectZeroApp_CC2650STK“ – įrenginio atrakinimo ir užrakinimo metodų realizacijai [29]. „SensorTag“ – jutiklių duomenų šifravimui skirto metodo realizacijai [30].
3	Valdymo įrenginys	„Raspberry Pi 2 Model B V1.1“ [31].
4	Šifravimo algoritmas	Pažangus šifravimo standartas AES [32]. Šis algoritmas naudojamas su 128 bitų raktu.
5	Belaidis duomenų perdavimo protokolas	„Bluetooth smart“ [33].

Tiriamas belaidis duomenų perdavimo protokolas (4.1 lent.) yra naudojamas komunikacijai tarp išmaniojo ir valdymo įrenginių. Duomenų šifravimas atliekamas naudojant AES algoritmą, kuris naudoja 128 bitų ilgio raktą. Šis raktas sudaromas iš 16 šešioliktainių skaičių, kurių kiekvieno duomenų ilgis yra 8 bitai.

4.2. Saugumas „Bluetooth“ duomenų perdavime

Klasikinis „Bluetooth“ įrenginys negali komunikuoti su „Bluetooth smart“ prietaisais, dėl fizinio ir ryšio OSI modelio lygmenų skirtumų. Bet yra naudojami tie patys L2CAP ir ATT protokolai. „Bluetooth smart” technologija yra įdiegta ketvirtoje „Bluetooth” versijoje. „Bluetooth“ protokolų stekas pateiktas 4.1 pav. [34].



4.1 pav. Duomenų perdavimo protokolo stekas

Fizinis lygmuo. Duomenų perdavimas vyksta naudojant GFSK moduliaciją 2,4 GHz dažnyje. Paskirsčius dažnių spektrą į 40 skirtingų kanalų yra naudojamas šuolių (angl. *Hopping*) algoritmas. Kiekvienas iš jų yra 1 MHz pločio ir paskirstytas 2 MHz tarpais tarp kanalų [35]. Esant komunikacijai tarp įrenginių, yra nuolatos keičiami kanalai, pagal tam tikrą šuolių algoritmą. Iš 40 kanalų, 37 yra skirti duomenims perduoti, o likę trys pranešimams. Dviem komunikuojantiems įrenginiams, yra naudojamas vienas kanalas, vienam paketui perduoti. Baigiat perdavimą yra pereinama prie sekančio kanalo.

Ryšio lygmuo. Perduodami paketai yra sudaromi iš keturių dalių, preambulės, kreipties adreso, protokolo duomenų vieneto ir ciklinės pertekliaus kontrolės. Paketo struktūra pateikta 4.2 pav. [26].

Mažiausias reikšminis bitas
LSB

Didžiausias reikšminis bitas
MSB

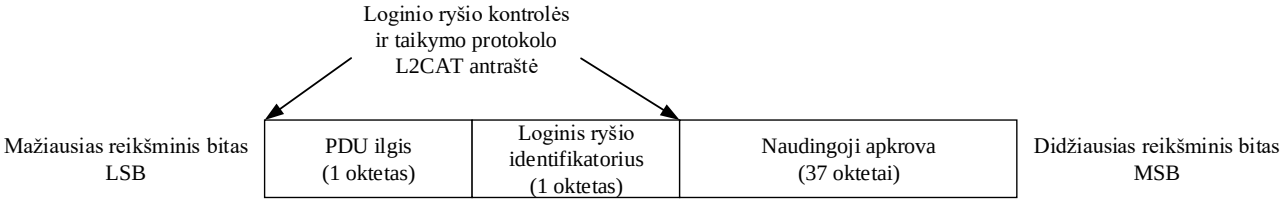
Preambulė (1 oktetas)	Kreipties adresas (4 oktetai)	Protokolo duomenų vienetas PDU (2 - 39 oktetai)	Ciklinė pertekliaus kontrolė CRC (3 oktetai)

4.2 pav. Duomenų perdavimo protokolo paketo struktūra

Preambulė skirta gavėjui, kuris pagal gautus duomenis atlieka paketų sinchronizaciją. Kreipties adresas skirtas paketų maršrutizacijai ir įrenginių atpažinimui. Minimalus PDU dydis yra 2 oktetai, nes į tai įeina loginis ryšio identifikatorius ir PDU ilgis. Ciklinė pertekliaus kontrolė skirta bitų patikrai, ar nebuvo iškraipyti duomenys perdavimo metu.

Loginis ryšio kontrolės ir taikymo protokolas. L2CAT antraštė sudaryta iš 2 oktetų, nes į ją įeina loginis ryšio identifikatorius ir PDU ilgis. Loginis ryšio identifikatorius skirtas kontrolinių ir

duomenų paketų atskyrimui, o PDU ilgis charakterizuoja jo ilgį. Identifikatorius gali turėti tik vieną, atributo protokolo reikšmę. Loginis ryšio kontrolės ir taikymo protokolas pateiktas 4.3 pav.



4.3 pav. Loginis ryšio kontrolės ir taikymo protokolas

Atributų protokolas ir bendrasis atributų profilis. GATT yra protokolas skirtas duomenų skaitymui rašymui ar skaitymui iš įrenginio. Tai atliekama tam tikromis paslaugomis (angl. *Services*) ir charakteristikomis. Kiekviena paslauga yra sudaryta iš tam tikro kiekio charakteristikų ir kiekviena charakteristika turi tam tikras operacijas. Operacijos gali būti įrašymo ar nuskaitymo. Šios operacijos yra identifikuojamos pagal visuotinį unikalų identifikatorių UUID, kuris yra unikalus kiekvienai tarnybai ir charakteristikai. UUID reikšmė gali kisti nuo 16 iki 128 bitų [36].

Saugumo valdymas (angl. *Security Management*) „Bluetooth smart“ duomenų perdavime yra sudarytas iš protokolų ir algoritmų, skirtų šifruotam sujungimui sudaryti. Tai atliekama apsikeičiant privačiu raktu, kuris skirtas šifruoti komunikaciją tarp įrenginių. Yra apibrėžiamos dvi įrenginių rolės:

a. iniciatorius - valdantysis (angl. *Master*) OSI lygmens, centrinis GAP įrenginys;
b. atsakovas - valdomasis (angl. *Slave*) OSI lygmens, periferinis GAP įrenginys.

Iniciatorius visados pradeda komunikacijos procedūras, bet atsakovas asinchroniškai gali pareikalauti iniciatoriaus pakartotinai atlikti „saugumo procedūras“. Šis pareikalavimas gali būti atliktas suklastoto įrenginio, norint inicializuoti pakartotinį rakto apsikeitimą. Yra trys saugumo procedūros:

a. ryšio poros sudarymas - procedūra, kai yra sukuriamas laikinasis raktas LR, kuris yra naudojamas trumpalaikei šifruotai komunikacijai sudaryti. Šis raktas nėra išsaugomas, tad yra nenaudojamas nuolatiniam ryšiui sudaryti;
b. jungties sudarymas - procedūra, kai yra sudaromas nuolatinis šifravimo raktas, skirtas perduodamiems duomenims šifruoti ir nuolatiniai jungčiai sudaryti. Šis raktas yra saugomas abiejuose įrenginiuose, kad nereikėtų pakartotinai atlikti jungimosi procedūros;
c. šifravimo atkūrimas (angl. *Encryption reestablishment*) - procedūra skirta nuolatinio rakto apsikeitimui.

Ryšio poros sudarymas yra laikinas, iki tol, kol vyksta komunikacija tarp įrenginių. Bet ryšio jungties sudaryme sukurtas raktas išlieka visą laiką, iki tol, kol patys įrenginiai nusprendžia jį ištrinti.

Rakto apsikeitimas vyksta trimis etapais. Pirmame etape yra apsikeičiama informacija, skirta laikinai komunikacijai sudaryti. Antrame etape iniciatorius ir atsakovas nepriklausomai sukuria laikinuosius raktus (angl. S*hort term key*). Paketai yra šifruojami laikinuoju raktu, apskaičiuojama

reikšmė, kuri patvirtina, kad abu komunikuojantys įrenginiai naudoja tą patį raktą. Trečiame etape yra apsikeičiama privačiu raktu, kuris yra naudojamas nuolatiniam duomenų šifravimui. Antrame etape yra trys LR sudarymo metodai [35]:

a. tiesiog veikia (angl. *Just Works*) - LR raktas yra 0, tad duomenų apsikeitimas vyksta nešifruotu tekstu. Šis metodas neapsaugotas nuo MIMT atakos;
b. rakto generavimas (angl. *Passkey Display*) - sukuriamas LR, kuris fiziškai įvedamas į abu komunikuojančius įrenginius. Šis metodas yra negalimas, jei vienas iš įrenginių neturi ekrano ir klaviatūros. Laikinasis raktas generuojamas nuo 0 iki 999999, tad šis metodas neapsaugo nuo jėgos atakos (angl. *Brute force attack*), bandant atspėti visus galimus slaptažodžio variantus;
c. dažnių juostos sujungimas (angl. O*ut of band pairing*) - LR raktas yra perduodamas kita perdavimo technologija, kaip NFC.

Tad 1 ir 2 laikinojo rakto sudarymo metodai neapsaugo nuo pasyvaus, neteisėto informacijos perėmimo (angl. *Passive eavesdropping*) [26].

Laikinojo rakto reikšmę galima gauti atliekant jėgos ataką (angl. *Brute force attack*), bandant visus galimas reikšmes, nuo 0 iki 999999 [36]. O turint laikinąjį raktą, galima atkurti nuolatinį raktą. Turint nuolatinį rakta galima atkurti sesijos raktus, kurie yra naudojami kiekvienos komunikacijos metu.

Ataka atliekama pasyviu duomenų pasiklausymu. Gavus duomenis bitų pavidalu, juos galima analizuoti. Įrenginio 4 oktetų MAC kreipties adresas yra žinomas, nes jis yra visados transliuojamas prieš įrenginiui užmezgant ryšį. Tad norint rasti PDU, reikia skenuoti bitus iki tol, kol bus rastas 4 oktetų MAC adresas, o po juo yra šifruoti duomenys. Perduodami duomenys, kaip jutiklių rodmenys, yra šifruoti AES algoritmu, o likusios paketo dalys nešifruojamos.

Tyrime atlieku prisijungimo metodo saugumo pagerinimą įdiegiant papildomus saugumo sprendimus (3.2 lent.). Siekiamas sprendimas turi išpildyti 1.5 lentelėje pateiktus užsibrėžtus tikslus.

4.3. Išmaniojo įrenginio programinės įrangos realizacija

Išmaniojo įrenginio atrakinimo ir duomenų šifravimo metodų tyrimui naudoju AES algoritmą. Tiriama duomenų perdavimo technologija yra „Bluetooth“.

Komunikacija naudojant „Bluetooth“ perdavimo protokolą atliekama naudojantis atributų protokolu (angl. *Attribute protocol*) ir bendru atributų protokolu (angl. *Generic attribute protocol*), kuris yra atributų protokolo meta sluoksnis skirtas kuriamai paslaugos programai kurti. Išmaniojo įrenginio paslaugos profilis apibūdina bendras atributų protokolo paslaugas ir charakteristikas, kurios yra naudojamos tam tikram funkcionalumui įgyvendinti.

Atributai yra sudaryti iš 16 bitų prižiūrėtojo (angl. *Bit handler*), 16, 32 arba 128 bitų ilgio unikalaus identifikatoriaus UUID (angl. *Universally unique identifier*) ir iki 512 bitų duomenų lauko. Apibendrinus, atributų protokolas aprašo atributus, kurie susidaryti iš:

a. bitų prižiūrėtojo - atributo adresas, kuris naudojamas atributų protokolo atpažinimui;
b. unikalaus identifikatoriaus - apibūdina atributo tipą;
c. duomenų lauko - bitų masyvas, kuris priklausomas nuo unikalaus identifikatoriaus.

Reikalingi keli atributai norint apibrėžti paslaugos charakteristikas. Charakteristika susideda bent iš deklaracijos ir duomenų lauko, kuriame yra konfigūruojama profilio reikšmė. Deklaracija visados pateikiama prieš duomenų lauko atributą ir ji apibūdina kada duomenų lauko reikšmė gali būti nuskaitoma ar įrašoma. Ji susideda iš unikalaus charakteristikos identifikatoriaus UUID ir bitų prižiūrėtojo. Charakteristikos deskriptoriai apibūdina jos formatą, kaip duomenys yra apdorojami ir kaip nustatomas siunčiamų pranešimų dažnumas. Charakteristikos yra naudojamos atributų kūrimui.

Kuriamai informacinei sistemai sukuriu naują profilį, skirtą AES rakto apsikeitimui. Kuriamo profilio charakteristikos pateiktos 4.2 lent.

4.2 lentelė. Kuriamo profilio charakteristikos

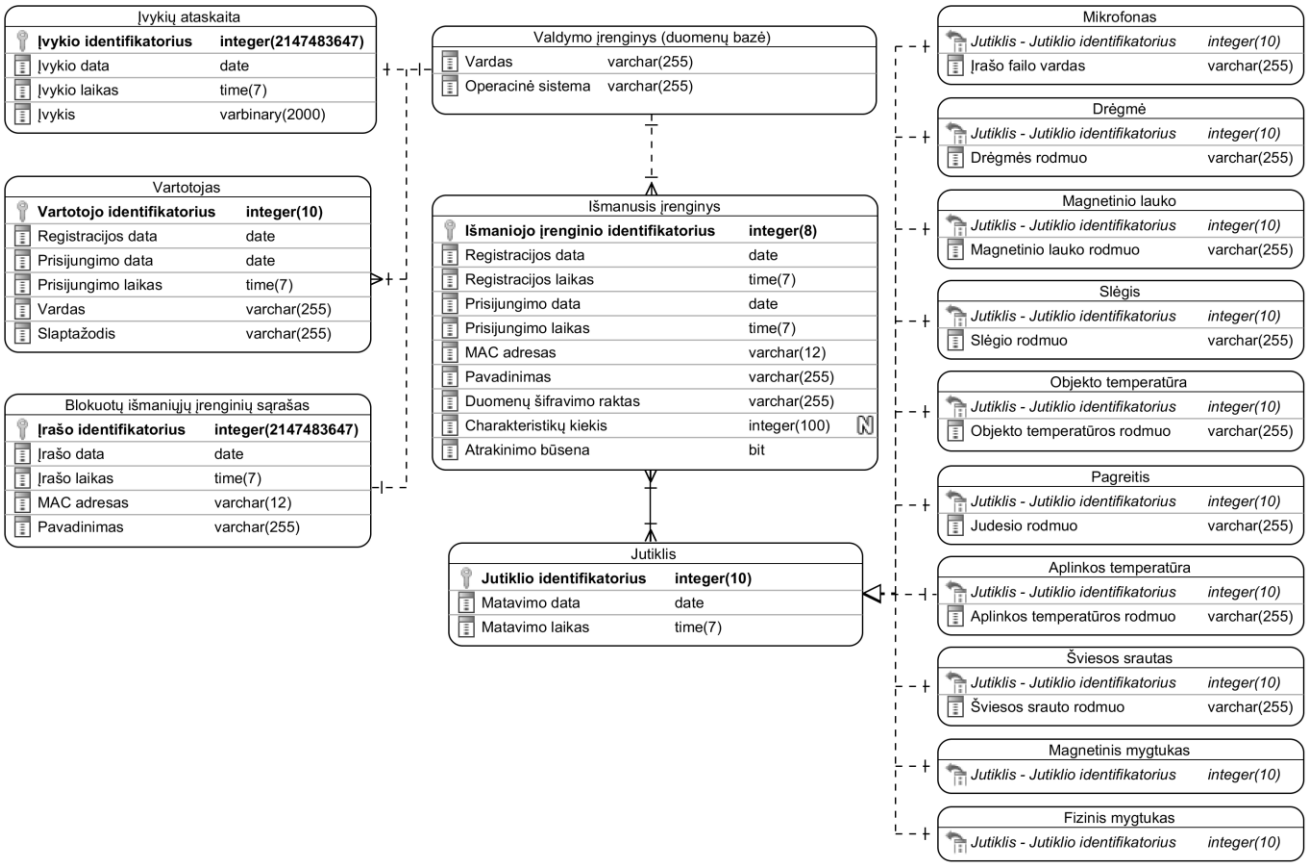
Sutrumpintas unikalaus identifikatoriaus UUID	**Duomenų leidimai**	**Paskirtis**
0xbeef	Nuskaityti	Skirta perskaityti užšifruotą AES raktą iš išmaniojo įrenginio.
0xbeff	Įrašyti	Skirta išmaniojo įrenginio atrakinimui ir naujo rakto įrašymui.

Esamas profilis sudarytas iš dviejų charakteristikų (4.2 lent.). Pirmoji charakteristika skirta užšifruoto AES rakto gavimui iš išmaniojo įrenginio. Antroji skirta įrenginio atrakinimui ir AES rakto pakeitimui, kai įrenginys jau yra atrakintas. Valdymo įrenginys gali stebėti atributus pagal jų prižiūrėtojus, kurie yra automatiškai priskiriami išmaniojo įrenginio ir jie nesikeičia.

4.4. Valdymo įrenginio duomenų bazės realizacija

Duomenų bazė talpinama valdymo įrenginyje ir naudojama iš išmaniųjų įrenginių gautų duomenų talpinimui. Šie duomenys gali būti panaudojami vėlesniam duomenų istorijos peržiūrėjimui arba atakų aptikimo bei saugumo užtikrinimo metodams.

Tiriamos sistemos duomenų bazės lentelių skaičius priklauso nuo išmaniųjų įrenginių ir jutiklių skaičiaus. Duomenų bazės esybių diagrama pateikta 4.4 pav.

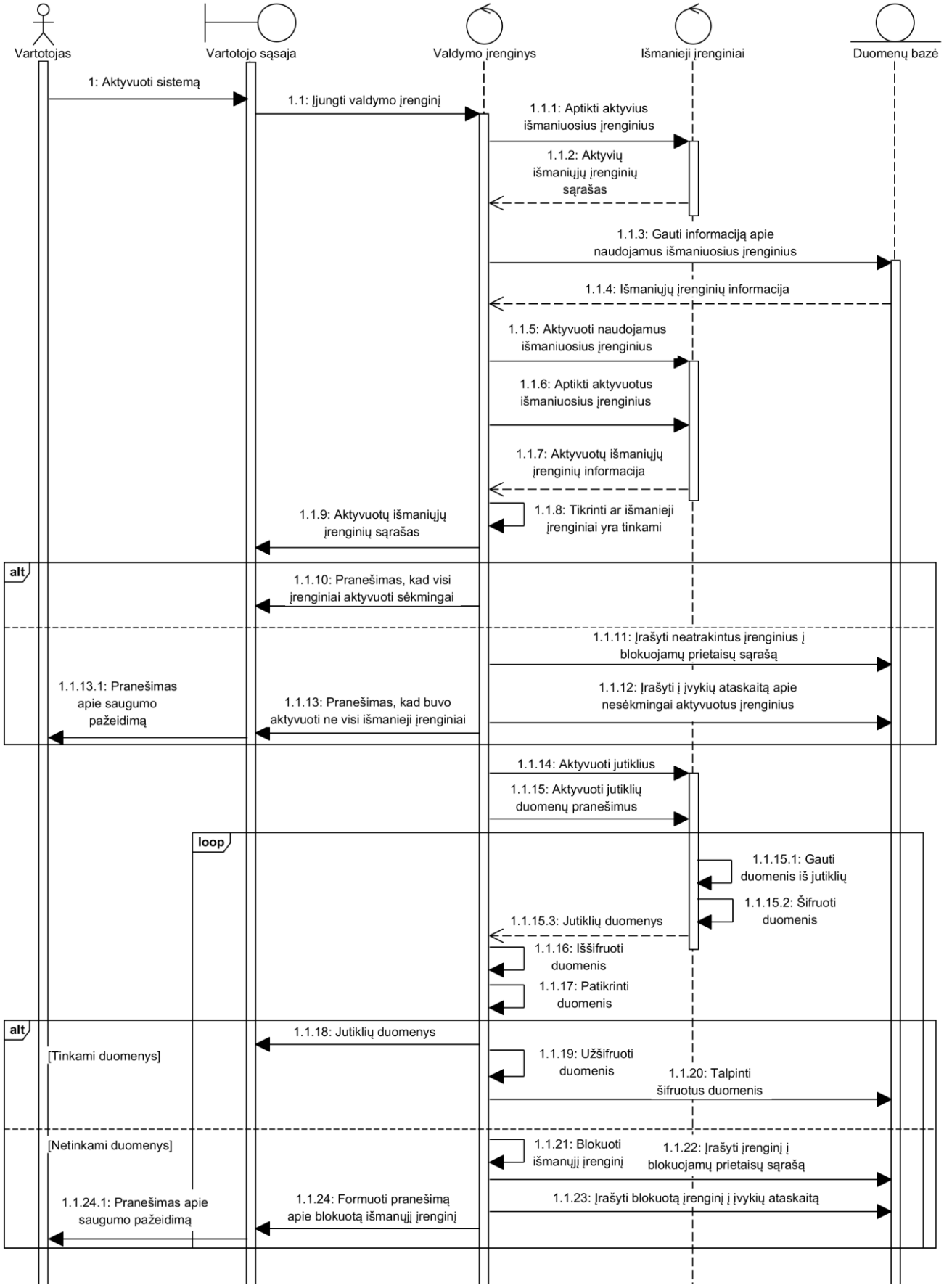


4.4 pav. Duomenų bazės esybių diagrama

Duomenų bazės esybių diagrama (4.4 pav.) atvaizduoja valdymo įrenginyje esančios, tiriamos informacinės sistemos duomenų bazės struktūrą. Esant vienam vartotojui ir išmaniajam įrenginiui, sudaroma penkiolika lentelių. Dešimt lentelių yra skirta kiekvieno jutiklio šifruotiems duomenims saugoti.

4.5. Informacinės sistemos realizacija

Kuriama daiktų interneto informacinė sistema susideda iš vartotojo sąsajos, išmaniųjų įrenginių ir valdymo įrenginio su integruota duomenų baze (3.1 pav.). Šie komponentai komunikuoja tarpusavyje ir keičiasi informacija. Valdymo įrenginys apdoroja informaciją ir formuoja pranešimus vartotojui per vartotojo sąsaja. Realizuojamos daiktų interneto informacinės sistemos sekų diagrama pateikta 4.5 pav.



4.5 pav. Realizuojamos daiktų interneto informacinės sistemos sekų diagrama

Realizuojamos daiktų interneto informacinės sistemos sekų diagramoje (4.5 pav.) tikrinama ar aktyvuoti išmanieji įrenginiai yra tinkami (1.1.8 punktas). Tinkamumas apibrėžiamas pagal šiuos kriterijus:

a. išmaniojo įrenginio vardas ir MAC adresas atitinka saugomą duomenų bazėje;
b. išmaniojo įrenginio šifravimo raktas toks pat kaip ir duomenų bazėje;
c. išmaniojo įrenginio aptiktų jutiklių kiekis atitinka saugomą duomenų bazėje;
d. nėra pasikartojančių įrenginių;

Aktyvuotiems išmaniesiems įrenginiams siunčiama užklausa iš valdymo įrenginio, kad būtų aktyvuotas duomenų nuskaitymas iš jutiklių kas viena sekundė. Nuskaityti duomenys yra šifruojami išmaniajame įrenginyje ir iššifruojami bei patikrinami valdymo įrenginyje (4.5 pav. 1.1.17 punktas). Iššifruotų duomenų tinkamumas apibrėžiamas pagal šiuos punktus:

a. ar duomenys iššifruoti sėkmingai;
b. ar jutiklio duomenys yra numatyto dydžio (skaičiuojama baitais);
c. ar išmatuota jutiklio duomenų reikšmė yra įprasto dydžio (palyginama su prieš tai saugotais duomenų bazėje jutiklių rodmenimis).

Blokuoti išmanieji įrenginiai yra registruojami duomenų bazėje ir apie tai yra pranešamas vartotojas grafinėje sąsajoje. Šie įvykiai registruojami kaip galimai vykdomos atakos prieš informacinę sistemą.

5. DAIKTŲ INTERNETO INFORMACINĖS SISTEMOS TESTAVIMAS

Išmaniųjų įrenginių informacinės sistemos testavime pateikiu realizuotų saugumo metodų bei atakos simuliacijos testavimą.

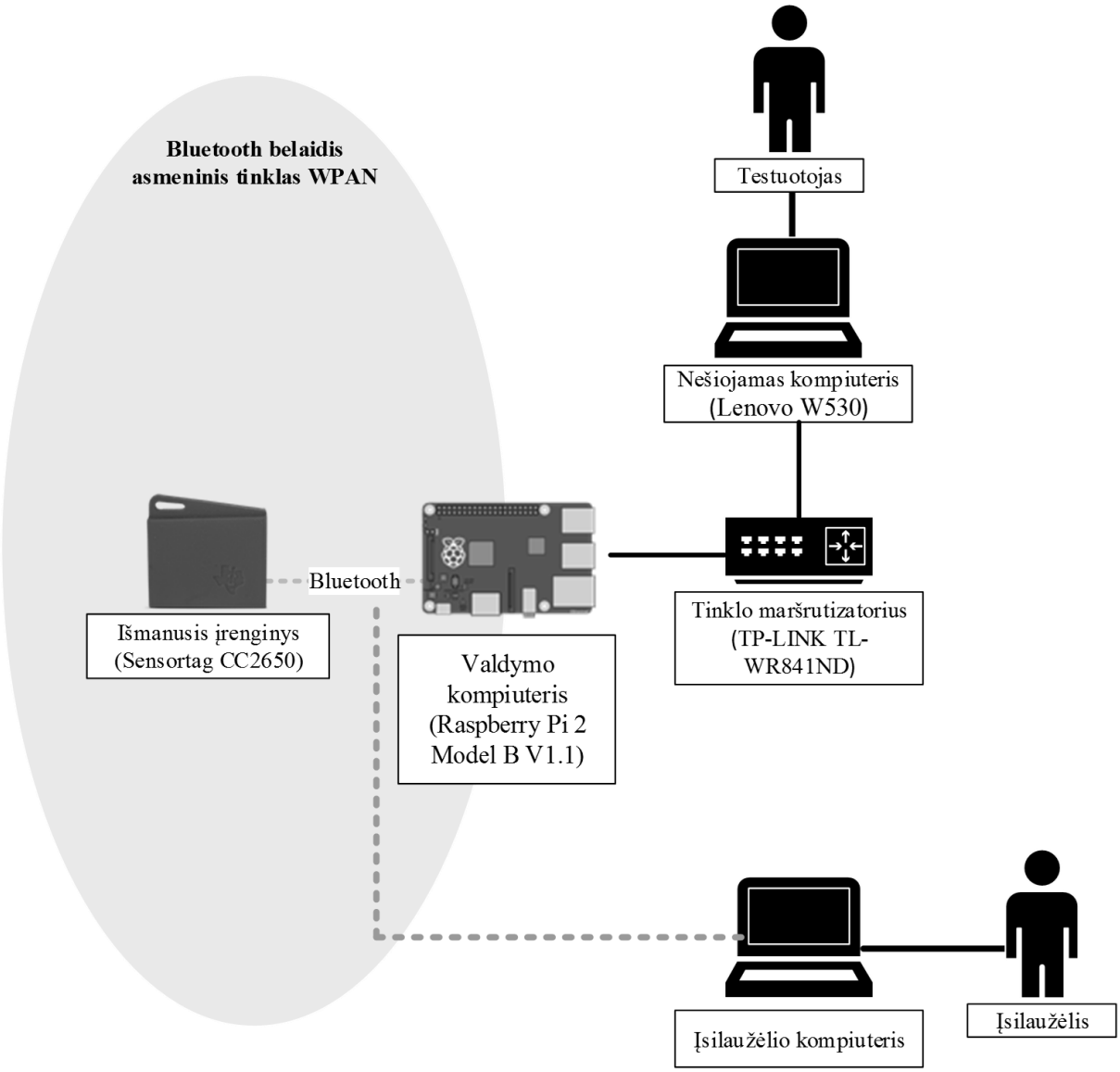
5.1. Testavimo programinė ir aparatinė įranga

Testavimui naudoju „Raspbian GNU/Linux 8“ operacinę sistemą įrašytą „Raspberry Pi 2 Model B V1.1“ kompiuteryje. Taip pat naudoju „Bluez 5.23-2+rpi1“ programinę įrangą ir jos GATTOOL funkciją. Atakai simuliuoti naudoju „CC2540EMK-USB“ įrenginį [37], skirtą perduodamų „Bluetooth“ duomenų perėmimui. Naudojama aparatinė įranga pateikta 5.1 lent.

5.1 lentelė. Naudojama aparatinė įranga

Įranga	**Informacija**
Išmanusis įrenginys (Sensortag CC2650)	Testavimui naudojamas išmanusis įrenginys „Sensortag CC2650“ [28].
Kompiuteris (Raspberry Pi 2 Model B V1.1)	Kompiuteris naudojamas komandoms siųsti į išmanųjį įrenginį.
Maršrutizatorius (TP-LINK TL-WR841ND)	Vietinio tinklo maršrutizatorius.
Kompiuteris (Lenovo W530)	Naudojamas kompiuteris skirtas komandoms perduoti į valdymo kompiuterį.
Adapteris (LogiLink USB Bluetooth V4.0)	Adapteris skirtas valdymo kompiuterio „Bluetooth“ komunikacijai.
„Bluetooth“ duomenų pasiklausymo įrenginys (CC2540EMK-USB)	Įsibrovėlio naudojamas įrenginys skirtas atlikti atakai prieš sukurtą informacinę sistemą.
Atminties kortelė (MicroSD 2GB)	Vidinė įrenginio atmintinė skirta duomenų saugojimui.

Testavimo platformos architektūra pateikta 5.1 pav.



5.1 pav. Testavimo platformos architektūra

Testuojamas išmanusis įrenginys yra sujungiamas su „Raspberry Pi 2 Model B V1.1“ valdymo įrenginiu. Nešiojamas kompiuteris ir valdymo kompiuteris sujungtas naudodamas SSH protokolą ir terminalą. Naudojantis terminalo langą nešiojamajame kompiuteryje (5.1 pav.), testuotojas kontroliuoja perduodamas komandas išmaniajam įrenginiui iš valdymo kompiuterio.

5.2. Testavimo metodika

Norint atlikti jutiklių duomenų įrašymą ir nuskaitymą iš išmaniojo įrenginio „Sensortag CC2650“ naudojama „GATTTOOL“ programinė įranga. Ji apibrėžia galimas paslaugas, naudojamas „Sensortag CC2650“ įrenginyje. Naudojant „GATTTOOL“ įrankį, atliekamas duomenų nuskaitymas ir įrašymas. Visos testavimui naudojamos komandos pateiktos 5.2 lent.

5.2 lentelė. Naudojamos testavimo komandos

Komanda	**Paskirtis**
gatttool -b <išmaniojo įrenginio MAC adresas> -I	Programos „GATTTOOL“ aktyvavimas panaudojus išmaniojo įrenginio MAC adresą.
connect	Prisijungimo aktyvavimas prie išmaniojo įrenginio.

char-write-cmd <prižiūrėtojas> <šešioliktainis numeris>	Jutiklio aktyvavimas įrašant šešioliktainį numerį ir panaudojus charakteristikos prižiūrėtoją.
char-read-hnd <prižiūrėtojas>	Vienos reikšmės nuskaitymo komanda.
char-write-cmd <prižiūrėtojas> <šešioliktainis numeris>	Pranešimų aktyvavimo komanda.
char-write-cmd <prižiūrėtojas> <šešioliktainis numeris>	Pranešimų nutraukimo komanda.
char-desc	Funkcija skirta išvardinti visas aktyvias išmaniojo įrenginio charakteristikas.

Atributų prižiūrėtojas (angl. *Handle*) skirtas numeruoti išmaniojo įrenginio atributus. Jie yra automatiškai numeruojami ir išlieka tie patys, jei programinė įranga nesikeičia. Naudojant prižiūrėtojo šešioliktainį numerį yra atskiriamos naudojamos charakteristikos. Įrašant duomenis į tam tikras charakteristikas yra atliekama komunikacija tarp išmaniojo įrenginio ir valdymo kompiuterio.

5.3. Įrenginio autorizacijos metodo testavimas

Atlieku išmaniojo įrenginio atrakinimo metodų testavimą. Išmanusis įrenginys yra su įdiegtu autorizacijos metodu, kurį aprašo (3.4 pav.) sekų bei (3.6 ir 5.2 pav.) veiklos diagramos.

Prieš atliekant testavimą yra aptinkami aktyvūs išmanieji įrenginiai ir jų MAC adresai (4.5 pav. 1.1.1 punktas). Aktyvius įrenginius aptinku naudojantis komanda „sudo hcitool lescan“. Įrenginio aptikimo procesas valdymo įrenginyje pateiktas 5.3 lent.

5.3 lentelė. Išmaniojo įrenginio aptikimas

```
administratorius@sensortagserver:~ $ sudo hcitool lescan
LE Scan ...
B0:B4:48:BE:2E:07 (unknown)
B0:B4:48:BE:2E:07 CC2650 SensorTag
…
^Z
[1]+  Stopped                 sudo hcitool lescan
```

Aptikto išmaniojo įrenginio vardas yra „CC2650 SensorTag“ ir MAC adresas „B0:B4:48:BE:2E:07“. Šie duomenys yra talpinami duomenų bazės „Išmanusis įrenginys“ lentelėje (4.4 pav.).

Norint naudotis išmaniuoju įrenginiu reikia žinoti jo paslaugų charakteristikų unikaliuosius identifikatorius arba prižiūrėtojus (angl. *Handle*). Gaunu visas aptikto išmaniojo įrenginio charakteristikas naudojantis komandą „char-desc“. Gautos užrakinto išmaniojo įrenginio charakteristikos pateiktos 5.4 lent.

5.4 lentelė. Visos užrakinto išmaniojo įrenginio charakteristikos

```
administratorius@sensortagserver:~ $ sudo gatttool -b B0:B4:48:BE:2E:07 -I
[B0:B4:48:BE:2E:07][LE]> connect
Attempting to connect to B0:B4:48:BE:2E:07
Connection successful
[B0:B4:48:BE:2E:07][LE]> char-desc
```

handle = 0x0001, uuid = 00002800-0000-1000-8000-00805f9b34fb
handle = 0x0002, uuid = 00002803-0000-1000-8000-00805f9b34fb
handle = 0x0003, uuid = f000**beef**-0451-4000-b000-000000000000
handle = 0x0004, uuid = 00002902-0000-1000-8000-00805f9b34fb
handle = 0x0005, uuid = 00002803-0000-1000-8000-00805f9b34fb
handle = 0x0006, uuid = f000**beff**-0451-4000-b000-000000000000
handle = 0x0007, uuid = 00002902-0000-1000-8000-00805f9b34fb

Norint atrakinti išmanųjį įrenginį, reikia gauti užšifruotą AES raktą (4.5 pav. 1.1.2 punktas). Tam skirta charakteristika yra su „0x0003“ prižiūrėtoju ir „f000**beef**-0451-4000-b000-000000000000“ unikaliuoju identifikatoriumi (5.4 lent.). Užšifruoto rakto nuskaitymui naudota „char-read-hnd 0x0003“ funkcija. Užšifruoto rakto nuskaitymo procedūra pateikta 5.5 lent.

5.5 lentelė. Užšifruoto rakto nuskaitymo procedūra

administratorius@sensortagserver:~ $ sudo gatttool -b B0:B4:48:BE:2E:07 -I
[B0:B4:48:BE:2E:07][LE]> connect
Attempting to connect to B0:B4:48:BE:2E:07
Connection successful
[B0:B4:48:BE:2E:07][LE]> char-read-hnd 0x0003
Characteristic value/descriptor: a9 13 29 af 99 a7 8d 02 ae c1 7c 50 77 57 aa ef

Užšifruoto rakto nuskaitymo procedūroje (5.5 lent.) matome, kad užšifruotas raktas yra „a91329af99a78d02aec17c507757aaef“. Kadangi tai pirmas prisijungimas prie išmaniojo įrenginio, yra žinoma, kad šifravimo raktas yra „61626364656667686 96a6b6c6d6e6f70“. Atrakinamas išmanusis įrenginys naudojantis funkcija „char-write-req 0x0006 61626364656667686 96a6b6c6d6e6f70“ (4.5 pav. 1.1.5 punktas). Atrakinimo procedūra pateikta 5.6 lent.

5.6 lentelė. Išmaniojo įrenginio atrakinimo procedūra

[B0:B4:48:BE:2E:07][LE]> char-write-req 0x0006 61626364656667686 96a6b6c6d6e6f70
Characteristic value was written successfully

Išmaniojo įrenginio atrakinimo procedūroje (5.6 lent.) matome, kad duomenys buvo įrašyti sėkmingai, bet nežinome ar duomenys buvo įvesti teisingi. Norint patikrinti ar išmanusis įrenginys atrakintas, pakartojama charakteristikų nuskaitymo funkcija „sudo gatttool -b B0:B4:48:BE:2E:07 --char-desc“ (4.5 pav. 1.1.6 punktas). Išmaniojo įrenginio atrakintos charakteristikos pateiktos 5.7 lent.

5.7 lentelė. Išmaniojo įrenginio atrakintos charakteristikos

[B0:B4:48:BE:2E:07][LE]> char-desc
handle: 0x0001, uuid: 00002800-0000-1000-8000-00805f9b34fb
handle: 0x0002, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0003, uuid: f000beef-0451-4000-b000-000000000000
handle: 0x0004, uuid: 00002902-0000-1000-8000-00805f9b34fb
handle: 0x0005, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0006, uuid: f000beff-0451-4000-b000-000000000000
handle: 0x0007, uuid: 00002902-0000-1000-8000-00805f9b34fb
handle: 0x0008, uuid: 00002800-0000-1000-8000-00805f9b34fb

```
handle: 0x0009, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x000a, uuid: 00002a00-0000-1000-8000-00805f9b34fb
handle: 0x000b, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x000c, uuid: 00002a01-0000-1000-8000-00805f9b34fb
handle: 0x000d, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x000e, uuid: 00002a04-0000-1000-8000-00805f9b34fb
handle: 0x000f, uuid: 00002800-0000-1000-8000-00805f9b34fb
handle: 0x0010, uuid: 00002800-0000-1000-8000-00805f9b34fb
handle: 0x0011, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0012, uuid: 00002a23-0000-1000-8000-00805f9b34fb
handle: 0x0013, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0014, uuid: 00002a24-0000-1000-8000-00805f9b34fb
...
```

Išmaniojo įrenginio atrakintų charakteristikų kiekis padaugėjo (5.7 lent.), tai reiškia, kad AES raktas buvo sėkmingai įvestas ir išmanusis įrenginys yra atrakintas. Pirmo konfigūravimo metu, charakteristikų skaičius yra talpinamos duomenų bazės „Išmanusis įrenginys“ lentelėje (4.4 pav.).

Atrakinto įrenginio charakteristikų skaičius turi sutapti su talpinamu duomenų bazėje. Jei yra neatitikimų, išmanusis įrenginys yra įrašomas į duomenų bazės „Blokuotų išmaniųjų įrenginių sąrašas“ lentelę (4.4 pav.). Taip pat yra registruojamas šis įvykis (4.5 pav. 1.1.11 punktas) ir pranešamas vartotojas (4.5 pav. 1.1.13.1 punktas).

5.4. Rakto pakeitimo metodo testavimas

Kadangi įrenginys yra atrakinamas numatytuoju šifravimo raktu yra atrakinamos visos įrenginio paslaugos, ir įrenginio AES rakto pakeitimo galimybė. Pakeičiamas numatytasis AES raktas atliekant šiuos punktus:

a. valdymo įrenginys siunčia išmaniajam įrenginiui naują AES raktą naudodamasis tam skirta charakteristika (4.2 lent.);
b. AES raktas yra užšifruojamas tuo pačiu AES raktu ir talpinamas vidinėje atmintyje.

Norint kitą kartą prisijungti prie išmaniojo įrenginio, reikalinga turėti unikalų AES raktą. Norint pakeisti numatytąjį AES raktą, naudoju tą pačią paslaugą su unikaliuoju identifikatoriumi „f000**beff**-0451-4000-b000-000000000000“ kaip ir atrakinant įrenginį. Raktą galimą pakeisti tik jau atrakintame įrenginyje. Pakeičiu AES raktą naudodamas funkciją „sudo gatttool -b B0:B4:48:BE:2E:07 --char-write-req 0x0006 <naujas šifravimo raktas>“. Rakto pakeitimo procedūra pateikta 5.8 lent.

5.8 lentelė. AES rakto keitimo procedūra

```
[B0:B4:48:BE:2E:07][LE]> char-write-req 0x0006 6162636465666768696a6b6c6d6e6f71
Characteristic value was written successfully
```

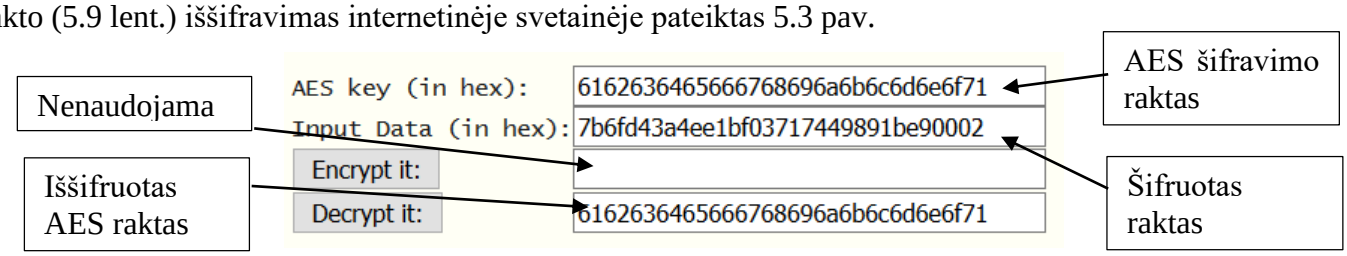
Gautas pranešimas, kad raktas buvo įrašytas sėkmingai (5.8 lent.). Patikrinama ar AES raktas buvo pakeistas išmaniajame įrenginyje. Tai atliekama nuskaitant raktą naudojantis funkciją „sudo

gatttool -b B0:B4:48:BE:2E:07 --char-read-hnd 0x0003“. Naujo rakto nuskaitymo procedūra pateikta 5.9 lent.

5.9 lentelė. Naujo rakto nuskaitymo procedūra

[B0:B4:48:BE:2E:07][LE]> char-read-hnd 0x0003 Characteristic value/descriptor: 7b 6f d4 3a 4e e1 bf 03 71 74 49 89 1b e9 00 02

Norint įsitikint, kad šifravimo algoritmas išmaniajame įrenginyje veikia taisyklingai ir šifruotas raktas (5.9 lent.) yra teisingas, naudoju internetinėje svetainėje esančią AES šifravimo programą [38]. Rakto (5.9 lent.) iššifravimas internetinėje svetainėje pateiktas 5.3 pav.



5.3 pav. Duomenų iššifravimas internetinėje svetainėje

Internetinėje svetainėje iššifruotas AES raktas „616263646566768696a6b6c6d6e6f71“ (5.3 pav.) atitinka naudojamą raktą (5.8 lent.). Tai reiškia, kad algoritmas veikia taisyklingai.

5.4.1. Išmaniojo įrenginio funkcionalumo testavimas

Norint patikrinti ar įrenginys išsisaugojo savyje naujai nustatytą AES raktą, atjungiamas išmaniojo įrenginio maitinimo šaltinis ir po to vėl įjungiamas. Testuojama ar prietaisas veikia taip kaip numatyta. Testuoju prisijungimą prie išmaniojo įrenginio, charakteristikų nuskaitymą ir įrenginio atrakinimą. Visa testavimo procedūra SSH terminale pateikta 5.10 lent.

5.10 lentelė. Išmaniojo įrenginio funkcionalumo testavimas

administratorius@sensortagserver:~ $ sudo gatttool -b B0:B4:48:BE:2E:07 -I **[B0:B4:48:BE:2E:07][LE]>** connect Attempting to connect to B0:B4:48:BE:2E:07 Connection successful **[B0:B4:48:BE:2E:07][LE]>** char-desc handle: 0x0001, uuid: 00002800-0000-1000-8000-00805f9b34fb handle: 0x0002, uuid: 00002803-0000-1000-8000-00805f9b34fb handle: 0x0003, uuid: f000beef-0451-4000-b000-000000000000 handle: 0x0004, uuid: 00002902-0000-1000-8000-00805f9b34fb handle: 0x0005, uuid: 00002803-0000-1000-8000-00805f9b34fb handle: 0x0006, uuid: f000beff-0451-4000-b000-000000000000 handle: 0x0007, uuid: 00002902-0000-1000-8000-00805f9b34fb **[B0:B4:48:BE:2E:07][LE]>** char-write-req 0x0006 616263646566768696a6b6c6d6e6f71 Characteristic value was written successfully **[B0:B4:48:BE:2E:07][LE]>** char-write-char-desc handle: 0x0001, uuid: 00002800-0000-1000-8000-00805f9b34fb handle: 0x0002, uuid: 00002803-0000-1000-8000-00805f9b34fb handle: 0x0003, uuid: f000beef-0451-4000-b000-000000000000 handle: 0x0004, uuid: 00002902-0000-1000-8000-00805f9b34fb handle: 0x0005, uuid: 00002803-0000-1000-8000-00805f9b34fb handle: 0x0006, uuid: f000beff-0451-4000-b000-000000000000 handle: 0x0007, uuid: 00002902-0000-1000-8000-00805f9b34fb

```
handle: 0x0008, uuid: 00002800-0000-1000-8000-00805f9b34fb
handle: 0x0009, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x000a, uuid: 00002a00-0000-1000-8000-00805f9b34fb
handle: 0x000b, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x000c, uuid: 00002a01-0000-1000-8000-00805f9b34fb
handle: 0x000d, uuid: 00002803-0000-1000-8000-00805f9b34fb
...
```

Prisijungimas prie išmaniojo įrenginio (5.10 lent.) sėkmingai įvykdytas naudojantis 5.8 lentelėje nurodytu „6162636465666768696a6b6c6d6e6f71“ AES raktu, tad galime daryti išvadas, kad sukurtas metodas veikia taisyklingai.

5.5. Atakų aptikimo ir išmaniojo įrenginio užrakinimo metodo testavimas

Atakų aptikimo ir išmaniojo įrenginio užrakinimo metodo testavimas vyksta bandant tris kartus perduoti neteisingą AES raktą. Po trijų neteisingų bandymų, charakteristika kurios unikalus identifikatorius yra „f000beef-0451-4000-b000-000000000000“ turi gražinti vertę „ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff“, kas reikštų, kad išmanusis įrenginys yra užblokuotas. Išmaniojo įrenginio užrakinimo metodo testavimas pateiktas 5.11 lent.

5.11 lentelė. Atakų aptikimo ir išmaniojo įrenginio užrakinimo metodo testavimas

```
administratorius@sensortagserver:~ $ sudo gatttool -b B0:B4:48:BE:2E:07 -I
[B0:B4:48:BE:2E:07][LE]> connect
Attempting to connect to B0:B4:48:BE:2E:07
Connection successful
[B0:B4:48:BE:2E:07][LE]> char-desc
handle: 0x0001, uuid: 00002800-0000-1000-8000-00805f9b34fb
handle: 0x0002, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0003, uuid: f000beef-0451-4000-b000-000000000000
handle: 0x0004, uuid: 00002902-0000-1000-8000-00805f9b34fb
handle: 0x0005, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0006, uuid: f000beff-0451-4000-b000-000000000000
handle: 0x0007, uuid: 00002902-0000-1000-8000-00805f9b34fb
[B0:B4:48:BE:2E:07][LE]> char-read-hnd 0x0003
Characteristic value/descriptor: a9 13 29 af 99 a7 8d 02 ae c1 7c 50 77 57 aa ef
[B0:B4:48:BE:2E:07][LE]> char-write-req 0x0006 6162636465666768696a6b6c6d6e6f71
Characteristic value was written successfully
[B0:B4:48:BE:2E:07][LE]> read-hnd 0x0003
Characteristic value/descriptor: a9 13 29 af 99 a7 8d 02 ae c1 7c 50 77 57 aa ef
[B0:B4:48:BE:2E:07][LE]> char-write-req 0x0006 6162636465666768696a6b6c6d6e6f71
Characteristic value was written successfully
[B0:B4:48:BE:2E:07][LE]> read-hnd 0x0003
Characteristic value/descriptor: a9 13 29 af 99 a7 8d 02 ae c1 7c 50 77 57 aa ef
[B0:B4:48:BE:2E:07][LE]> char-write-req 0x0006 6162636465666768696a6b6c6d6e6f71
Characteristic value was written successfully
[B0:B4:48:BE:2E:07][LE]> read-hnd 0x0003
Characteristic value/descriptor: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
 [B0:B4:48:BE:2E:07][LE]> char-desc
handle: 0x0001, uuid: 00002800-0000-1000-8000-00805f9b34fb
handle: 0x0002, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0003, uuid: f000beef-0451-4000-b000-000000000000
handle: 0x0004, uuid: 00002902-0000-1000-8000-00805f9b34fb
```

handle: 0x0005, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0006, uuid: f000beff-0451-4000-b000-000000000000
handle: 0x0007, uuid: 00002902-0000-1000-8000-00805f9b34fb

Atakų aptikimo ir išmaniojo įrenginio užrakinimo metodo testavime (5.11 lent.) panaudojus funkciją „read-hnd 0x0003“ yra gaunama „ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff“ reikšmė. Tai informuoja, kad prie įrenginio buvo bandyta netaisyklingai prisijungti tris kartus. Panaudota „char-desc“ funkcija tam, kad būtų įsitikinta, jog įrenginys išliko užrakintas. Užrakintame išmaniajame įrenginyje nebegalima pasinaudoti esamomis paslaugomis.

Atakos identifikavimas valdymo įrenginyje vyksta, kai yra bandoma aptikti išmanųjį įrenginį (4.5 pav. 1.1.1 punktas). Apie įvykusią ataką yra pranešamas vartotojas (4.5 pav. 1.1.13.1 punktas).

5.6. Jutiklio duomenų šifravimo testavimas

Jutiklių duomenų šifravimo testavimui, pasirinktas šviesos srauto jutiklis. Palyginimui atliekamas testavimas neįdiegus šifravimo algoritmo. Šviesos srauto sutrumpintas unikalusis identifikatorius yra „AA70“. Jutiklio duomenys nuskaitomi naudojant šešioliktainį prižiūrėtoją „0x41“ ir komandą „char-read-hnd 0x41“. Atliekama jutiklio aktyvacija naudojant komandą „char-write-cmd 0x44 01“ (4.5 pav. 1.1.14 punktas). Automatiniai jutiklio pranešimai aktyvuojami naudojant „0x42“ šešioliktainį valdiklį ir naują reikšmę „01:00“ (4.5 pav. 1.1.15 punktas). Sustabdomi pranešimai įrašant naują reikšmę „00:00“. Testavimui panaudotos komandos pateiktos 5.12 lent.

5.12 lentelė. Naudojamos duomenų šifravimo metodo testavimo komandos

Komanda	**Paskirtis**
gatttool -b B0:B4:48:BE:2E:07 -I	Programos „*gatttool*“ aktyvavimas panaudojus išmaniojo įrenginio MAC adresą.
connect	Prisijungimui prie išmaniojo įrenginio.
char-write-cmd 0x44 01	Jutiklio aktyvavimas įrašant „*01*” šešioliktainį numerį ir panaudojus „*0x44*“ prižiūrėtoją.
char-read-hnd 0x41	Vienos reikšmės nuskaitymo komanda.
char-write-cmd 0x42 01:00	Pranešimų aktyvavimo komanda. Pranešimai atnaujinami kas viena sekundė.
char-write-cmd 0x42 00:00	Pranešimų nutraukimo komanda.

Atliekamas jutiklio testavimas pagal 5.12 lentelėje pateiktas komandas. Testavimo rezultatai pateikti 5.13 lent.

5.13 lentelė. Jutiklio funkcionalumo testavimas

administratorius@sensortagserver:~ $ gatttool -b B0:B4:48:BE:2E:07 -I
[B0:B4:48:BE:2E:07][LE]> connect
Attempting to connect to B0:B4:48:BE:2E:07
Connection successful
[B0:B4:48:BE:2E:07][LE]> char-write-cmd 0x44 01
[B0:B4:48:BE:2E:07][LE]> char-read-hnd 0x41
Characteristic value/descriptor: d1 1d
[B0:B4:48:BE:2E:07][LE]> char-write-cmd 0x42 01:00

Notification handle = 0x0041 value: c9 1d
Notification handle = 0x0041 value: 88 1d
Notification handle = 0x0041 value: e5 0c
Notification handle = 0x0041 value: 9f 19
[B0:B4:48:BE:2E:07][LE]> char-write-cmd 0x42 00:00

Jutiklių duomenys (5.13 lent.) yra pateikti šešioliktainiu pavidalu. Norint apskaičiuoti jutiklio rodmenis liuksais, reikia panaudoti formulę, pateiktą [39] šaltinyje. Iš gautų dviejų šešioliktainių skaitmenų reikia atskirti du kintamuosius *m* ir *e*. Kintamųjų apskaičiavimas pateiktas 5.14 lent.

5.14 lentelė. Šviesos srauto kintamųjų apskaičiavimas

Kintamasis	**Duomenys bitų pavidalu**	**Naudojama funkcija**	**Rezultatas bitų pavidalu**	**Rezultatas dešimtainiu formatu**
m	00011101 11010001 00001111 11111111	Loginė bitų operacija „arba“.	00001101 11010001	3537
e	00011101 11010001 11110000 00000000	Loginė bitų operacija „arba“ ir postūmis į dešinę per 12 bitų.	00000000 00000001	1

Apskaičiuojame šviesos srauto reikšmę ŠS, pritaikant funkciją:

$$Š\boldsymbol{S} = \boldsymbol{m} \cdot (\mathbf{0,01} \cdot \mathbf{2}^{\boldsymbol{e}}) = \mathbf{3537} \cdot (\mathbf{0,01} \cdot \mathbf{2}^{\mathbf{1}}) = \mathbf{70.74}\ [\boldsymbol{Lux}]; \quad (1)$$

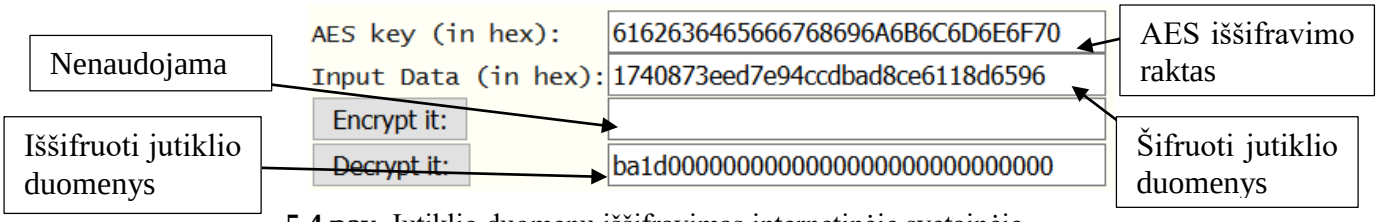
čia *ŠS* - šviesos srautas liuksais; *m* ir *e* kintamieji iš 5.14 lent.

Išmaniajame įrenginyje įdiegiamas duomenų šifravimo algoritmas ir atliekamos tos pačios komandos (5.13 lent.). Duomenys yra šifruojami išmaniajame įrenginyje ir išsiunčiami valdymo įrenginiui (4.5 pav. 1.1.15.2 punktas). Duomenų šifravimui panaudotas „61626364656667686 96A6B6C6D6E6F70“ AES raktas. Testavimo rezultatai pateikti 5.15 lent.

5.15 lentelė. Jutiklio duomenų šifravimo testavimas

administratorius@sensortagserver:~ $ gatttool -b B0:B4:48:BE:2E:07 -I
[B0:B4:48:BE:2E:07][LE]> connect
Attempting to connect to B0:B4:48:BE:2E:07
Connection successful
[B0:B4:48:BE:2E:07][LE]> char-write-cmd 0x44 01
[B0:B4:48:BE:2E:07][LE]> char-read-hnd 0x41
Characteristic value/descriptor: 17 40 87 3e ed 7e 94 cc db ad 8c e6 11 8d 65 96
[B0:B4:48:BE:2E:07][LE]> char-write-cmd 0x42 01:00
Notification handle = 0x0041 value: **17 40 87 3e ed 7e 94 cc db ad 8c e6 11 8d 65 96**
Notification handle = 0x0041 value: **8e 6d ae 50 60 80 d1 6c 75 2b e6 92 b2 0e 74 07**
[B0:B4:48:BE:2E:07][LE]> char-write-cmd 0x42 00:00

Jutiklio duomenų šifravimo testavime (5.15 lent.) matome dvi gautas 32 simbolių eilutes: „17 40 87 3e ed 7e 94 cc db ad 8c e6 11 8d 65 96“ ir „8e 6d ae 50 60 80 d1 6c 75 2b e6 92 b2 0e 74 07“. Vienas užšifruotas šviesos srauto rodmuo atitinka 16 šešioliktainių skaičių. Iššifruojama gauta reikšmė internetinėje programoje [38]. Rezultatas pateiktas 5.4 pav.



5.4 pav. Jutiklio duomenų iššifravimas internetinėje svetainėje

Iššifruoti 32 simboliai iš kurių 28 yra „0“ (5.4 pav.). Tai reiškia, kad duomenys iššifruoti sėkmingai. Reikalinga šviesos srauto reikšmė yra tik pirmieji 4 simboliai, kurie atitinka du šešioliktainius numerius „ba“ ir „1d“. Pavertus į dešimtainį formatą atitinkamai jie yra 186 ir 29. Apskaičiuojama šviesos srauto ŠS reikšmė liuksais naudojantis 5.14 lentelėje pateiktomis funkcijomis ir formule:

$$\check{S}\boldsymbol{S} = \boldsymbol{m} \cdot (\mathbf{0,01} \cdot \mathbf{2}^{\boldsymbol{e}}) = \mathbf{3339} \cdot (\mathbf{0,01} \cdot \mathbf{2}^{\mathbf{1}}) = \mathbf{66.78}\,[\boldsymbol{Lux}];\ (2)$$

čia *ŠS* - šviesos srautas liuksais; *m* ir *e* kintamieji apskaičiuoti pagal 5.14 lentelėje pateiktus metodus.

Gautas rezultatas (2) skiriasi nuo prieš tai gauto (1) tik 3,96 liuksais, tai reiškia, kad šifravimo funkcija ir naudojamas šviesos srauto jutiklis išmaniajame įrenginyje veikia taisyklingai. Šviesos srauto 2,8% paklaida galėjo atsirasti dėl nepastovaus apšvietimo testavimo patalpoje.

Anomalijų aptikimas vykdomas lyginant iššifruotų duomenų ir jutiklių duomenų ilgį baitais, duomenų tikrinimo etape (4.5 pav. 1.1.17 punktas). Jei gautas jutiklio rodmuo yra didesnis nei numatyta, laikoma, kad išmanusis įrenginys yra suklastotas. Šviesos srauto iššifruoti duomenys (5.4 pav.) yra sudaryti iš dviejų baitų, tai įrodo du šešioliktainiai numeriai lygūs „ba“ ir „1d“, o likę skaičiai yra lygūs „0“. Jei perdavimo metu duomenys buvo perimti ir modifikuoti, iššifruoti duomenys bus didesni nei du baitai.

5.7. Atakos simuliacijos testavimas be įdiegtų papildomų saugumo sprendimų

Duomenų pasiklausymo ataka vykdoma įsilaužėlio kompiuteryje su „SmartRF Protocol Packet Sniffer“ programinė įranga [40]. Ši įranga pateikia informaciją apie kiekvieną, duomenų perdavimo terpe „pagautą“ paketą. Tarp įsilaužėlio kompiuterio ir išmaniojo bei valdymo įrenginio yra 8 metrai (5.1 pav.). Duomenų paketų struktūros elementai „SmartRF Protocol Packet Sniffer“ programinėje įrangoje pateikti 5.16 lent.

5.16 lentelė. Duomenų paketų struktūros elementai

Eil. Nr.	Paketo elementas	Elemento paaiškinimas
1	P.nbr.	Paketo numeris „SmartRF Protocol Packet Sniffer“ programoje.
2	Time (ms)	Laiko vertė naudojama paketų sinchronizacijai.
3	Channel	Naudojamas duomenų perdavimo kanalas.
4	Access Address	Įrenginio MAC adresas.
5	Direction	Duomenų perdavimo kryptis. „M“ - valdantysis (angl. *Master*), S - valdomasis (angl. *Slave*).

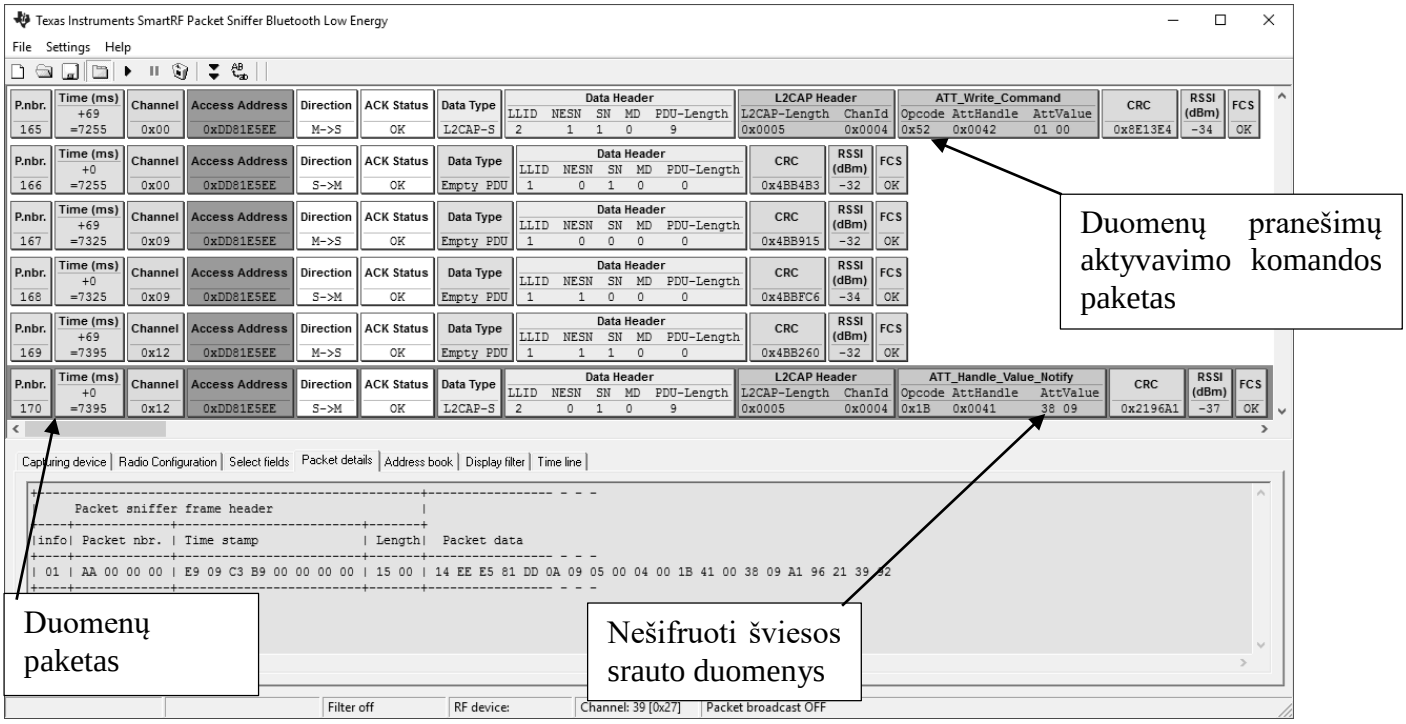
6	ACK Status	Gauto paketo patvirtinimo būsena.
7	Data type	Duomenų tipas.
8	Data Header	Duomenų antraštė.
9	L2CAP Header	Loginio ryšio kontrolės ir taikymo protokolo antraštė.
10	ATT_Write_Command	Atributų protokolo rašymo komanda.
11	ATT_Handle_Value_Notify	Atributo protokolo pranešimo reikšmė.
12	CRC	Ciklinė pertekliaus tikrinimo kontrolės reikšmė.
13	RSSI	Signalo stiprumas.
14	FCS	Perduodamo paketo kadrų tikrinimo eilė.

Atliekamas šviesos srauto jutiklio duomenų nuskaitymas iš valdymo kompiuterio naudojantis 5.12 lentelėje pateiktomis komandomis. Tuo tarpu aktyvuojama duomenų pasiklausymo sistema įsilaužėlio kompiuteryje (5.1 pav.). Atliktos komandos ir rezultatai atlikti valdymo kompiuteryje pateikti 5.17 lent.

5.17 lentelė. Neapsaugotos informacinės sistemos valdymo įrenginio atliktos komandos

administratorius@sensortagserver:~ $ gatttool -b B0:B4:48:BE:2E:07 -I
[B0:B4:48:BE:2E:07][LE]> connect
Attempting to connect to B0:B4:48:BE:2E:07
Connection successful
[B0:B4:48:BE:2E:07][LE]> char-write-cmd 0x44 01
[B0:B4:48:BE:2E:07][LE]> char-write-cmd 0x42 01:00
Notification handle = 0x0041 value: 38 09
Notification handle = 0x0041 value: 19 09
Notification handle = 0x0041 value: e8 08
[B0:B4:48:BE:2E:07][LE]> char-write-cmd 0x42 00:00

Pagal duomenų pranešimų aktyvavimo komandos „01 00“ vertę (5.17 lent.), įsilaužėlio kompiuterio programinėje įrangoje „SmartRF Protocol Packet Sniffer“ yra surandami perskaityti duomenų paketai. Duomenų pasiklausymo programos langas pateiktas 5.5 pav.



5.5 pav. Duomenų pasiklausymo programos langas

Surasto duomenų pranešimų aktyvavimo komandos paketo numeris yra 165, o šviesos srauto duomenų paketo 170 (5.5 pav.). Tarpiniai paketai (166, 167, 168 ir 169) yra skirti paketų sinchronizacijai.

Duomenų paketas (5.5 pav.) turi nešifruotus šviesos srauto duomenis „38 09“, tuos pačius kaip ir gautus valdymo įrenginyje (5.17 lent.). Tai įrodo, kad įsilaužėlis gali atlikti duomenų pasiklausymo ataką.

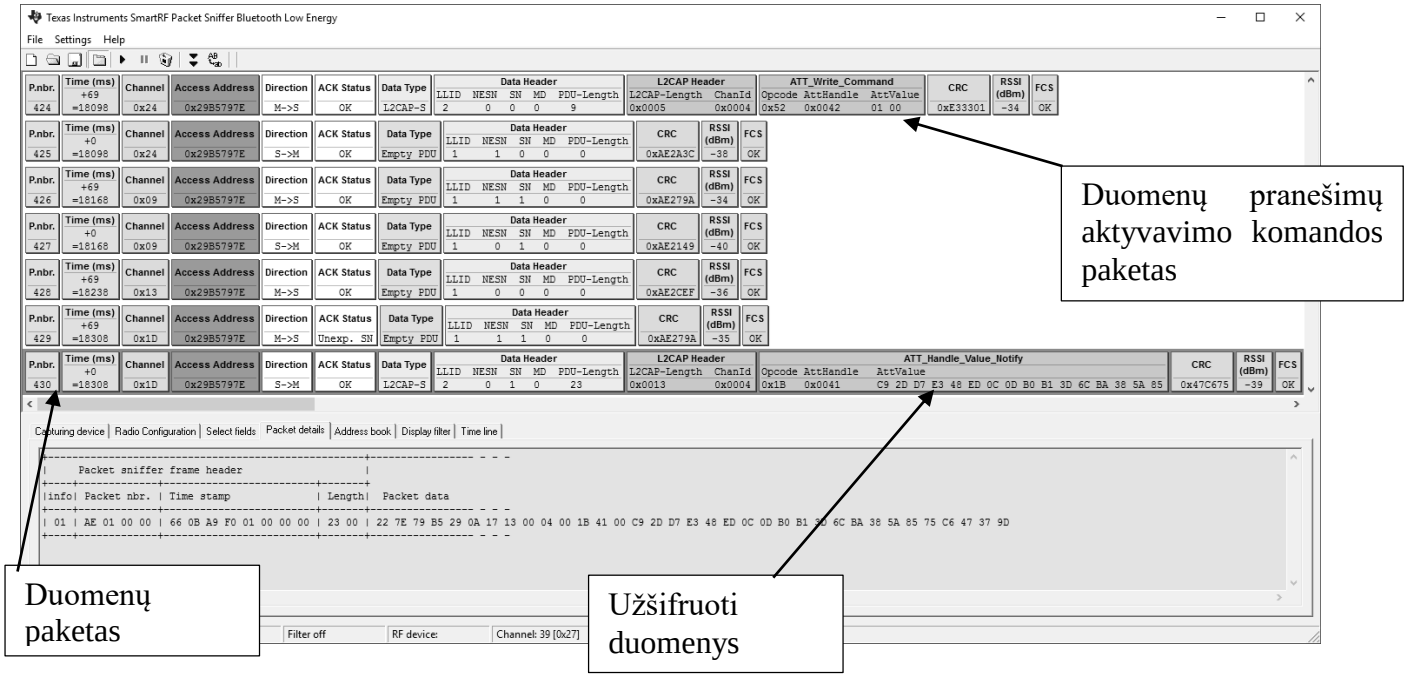
5.8. Atakos simuliacijos testavimas su įdiegtais papildomais saugumo sprendimais

Įdiegiu papildomus saugumo sprendimus (3.2 lent.) į sukurtą informacinę sistemą ir pakartoju 5.17 lentelėje pateiktas komandas. Atliktos komandos ir rezultatai valdymo kompiuteryje pateikti 5.18 lent.

5.18 lentelė. Apsaugotos informacinės sistemos valdymo įrenginyje atliktos komandos

```
administratorius@sensortagserver:~ $ gatttool -b B0:B4:48:BE:2E:07 -I
[B0:B4:48:BE:2E:07][LE]> connect
Attempting to connect to B0:B4:48:BE:2E:07
Connection successful
[B0:B4:48:BE:2E:07][LE]> char-write-cmd 0x44 01
[B0:B4:48:BE:2E:07][LE]> char-write-cmd 0x42 01:00
Notification handle = 0x0041 value: c9 2d d7 e3 48 ed 0c 0d b0 b1 3d 6c ba 38 5a 85
Notification handle = 0x0041 value: 67 8f 81 5e 22 12 79 12 5c 0f 6f a6 d7 6c 32 a6
[B0:B4:48:BE:2E:07][LE]> char-write-cmd 0x42 00:00
```

Įsilaužėlio kompiuteryje „pagaunu“ visus duomenų paketus tarp valdymo ir išmaniojo įrenginio. Duomenų pasiklausymo programos langas įsilaužėlio kompiuteryje pateiktas 5.6 pav.



5.6 pav. Duomenų pasiklausymo programos langas

Pagal duomenų pranešimų aktyvavimo komandos „01 00“ vertę (5.18 lent.), įsilaužėlio kompiuterio programinėje įrangoje „SmartRF Protocol Packet Sniffer“ yra surandami perskaityti

duomenų paketai. Surasto duomenų pranešimų aktyvavimo komandos paketo numeris yra 424, o šviesos srauto duomenų paketo 430 (5.6 pav.). Įsilaužėlio perskaityti duomenys „c9 2d d7 e3 48 ed 0c 0d b0 b1 3d 6c ba 38 5a 85“ (5.6 pav.) yra šifruoti, tad yra apsisaugoma nuo duomenų pasiklausymo atakos grėsmės.

5.9. Testavimo išvados

Tiriamas išmanusis įrenginys neturi ekrano ar tam tikros rakto apsikeitimo technologijos, tad prisijungimas vykdomas „tiesiog veikia“ metodu (1.5 lent.), be slaptažodžio ar apsaugos, tad iškyla grėsmė, kad įrenginiu bus galima pasinaudoti pašaliniams asmenims. Darbe pasiūlytas metodas išsprendžia šią problemą talpinant šifravimo raktą vidinėje išmaniojo įrenginio atmintyje. Pakeitus šį AES raktą pirmo konfigūravimo metu prietaisas yra apsaugomas nuo neteisėto panaudojimo. Prisijungimo metodų palyginimas pateiktas 1.5 lent.

Pasiūlyti algoritmai yra vykdomi „Tiesiog veikia“ metodo pagrindu. Valdymo kompiuteriui prisijungiant prie išmaniojo įrenginio yra matomas tik AES rakto apsikeitimo paslaugos (5.4 lent.). Išmaniojo įrenginio aktyvavimui naudojamas AES raktas kuris gali būti pakeistas vartotojo, kiekvieno prisijungimo metu.

Yra užtikrinama, kad išmaniuoju įrenginiu nebus galima pasinaudoti po trijų kartų neteisingai įvesto AES rakto, kas apsaugo įrenginį nuo neteisėto panaudojimo. Teisėtam valdymo kompiuteriui bandant vėl prisijungti prie išmaniojo įrenginio, jis mato, kad buvo bandyta neteisėtai prisijungti prie išmaniojo įrenginio. Tai gali informuoti apie bandytą atlikti ataką.

Papildomas duomenų šifravimas duotu AES raktu suteikia pagerintą saugumą, kai bandoma pasinaudoti atrakintu išmaniuoju įrenginiu. Duomenų nuskaitymas tampa negalimas nežinant slapto AES rakto.

Atlikus duomenų pasiklausymo atakos simuliaciją buvo nustatyta, kad perduodamų duomenų šifravimas pagerina apsaugą nuo žinomos „Bluetooth“ technologijoje esančios MIMT atakos [26].

6. REZULTATŲ APIBENDRINIMAS IR IŠVADOS

1. Atlikus analizę nustatyta, kad daiktų interneto informacinėse sistemose trūksta saugumo sprendimų, kurios naudoja išmaniuosius įrenginius be išorinio ekrano, klaviatūros ar specialios slaptažodžio apsikeitimo technologijos.
2. Darbo metu buvo pagerintas daiktų interneto informacinės sistemos saugumas sukuriant išmaniojo įrenginio autorizavimo metodą, įdiegiant atakų aptikimo metodus ir šifruojant perduodamus bei talpinamus duomenis.
3. Išmaniojo įrenginio autorizavimo metodas užtikrina saugesnį valdymo kompiuterio prisijungimą prie išmaniojo įrenginio naudojant simetrinį kriptografijos raktą, kuris taip pat naudojamas perduodamų duomenų šifravimui.
4. Atlikus sukurtos informacinės sistemos testavimą, nustatyta, kad realizuotas išmaniojo įrenginio blokavimo metodas užtikrina apsaugą nuo slaptažodžio atspėjimo atakos, o sistemos anomalijų aptikimas pagerina apsaugą nuo informacijos iškraipymo bei įrenginio klastojimo atakos.
5. Realizuotas, tarp valdymo ir išmaniųjų įrenginių, perduodamų duomenų šifravimo metodas apsaugo informacinę sistemą nuo informacijos modifikavimo, perėmimo bei suteikia apsaugą nuo duomenų pasiklausymo atakos.
6. Pasiūlyti metodai gali būti pritaikomi visiems, tirtą belaidį duomenų perdavimo protokolą palaikantiems įrenginiams, nepakeičiant standarto specifikacijų. Tai užtikrina sistemos suderinamumą su visais šią technologiją palaikančiais įrenginiais.

7. LITERATŪRA

[1] The International Telecommunication Union, „Internet of Things Global Standards Initiative," [Tinkle]. Available: http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx. [Kreiptasi 18 05 2015].

[2] „Smart Device," Janalta Interactive, [Tinkle]. Available: https://www.techopedia.com/definition/31463/smart-device. [Kreiptasi 18 05 2016].

[3] M. A. Bhabad ir S. T. Bagade, „Internet of Things: Architecture, Security Issues and Countermeasures," *International Journal of Computer Applications,* t. 125, nr. 14, 2015.

[4] S. Duhan ir P. khandnor, „Intrusion Detection System in Wireless Sensor Networks: A Comprehensive Review," *International Conference on Electrical, Electronics, and Optimization Techniques,* 2016.

[5] A. Mishra ir A. K. Srivastava, „A Modular Approach To Intrusion Detection in Homogenous Wireless Network," *Journal of Computer Engineering,* t. 14, nr. 6, pp. 53-59, 2013.

[6] A. Mishra ir A. K. Srivastava, „A Survey on Intrusion Detection System for Wireless Network," *International Journal of Computer Applications,* t. 73, nr. 21, pp. 37-40, 2013.

[7] U. A. Sandhu, S. Haider, S. Naseer ir O. U. Ateeb, „A Survey of Intrusion Detection & Prevention Techniques," *International Conference on Information Communication and Management,* t. 16, 2011.

[8] O. Singh ir J. Singh, „Comparative study of various Distributed Intrusion Detection Systems for WLAN," *Global Journal of researches in engineering electrical and electronics engineering,* t. 12, nr. 6, 2012.

[9] T. Sharma ir K. Sinha, „Intrusion Detection Systems Technology," *International Journal of Engineering and Advanced Technology,* t. 1, nr. 2, pp. 28-33, 2011.

[10] R. Mitchell ir I.-R. Chen, „A survey of intrusion detection in wireless network applications," *Computer Communications,* t. 42, pp. 1 - 23, 2014.

[11] P. Mehra, „A brief study and comparison of Snort and Bro Open Source Network Intrusion Detection Systems," *International Journal of Advanced Research in Computer and Communication Engineering,* t. 1, nr. 6, pp. 383 - 386, 2012.

[12] J. S. Whitea, T. T. Fitzsimmonsb ir J. N. Matthewsc, „Quantitative Analysis of Intrusion Detection Systems: Snort and Suricata," *Proceedings of the SPIE,* t. 8757, 2013.

[13] S. B. Ambati ir D. Vidyarthi, „A brief study and comparison of, open source intrusion detection system tools," *International Journal of Advanced Computational Engineering and Networking,* t. 1, nr. 10, pp. 26 -32, 2013.

[14] G. Khalil ir R. VandenBrink, „Open Source IDS High Performance Shootout," *SANS Institute InfoSec Reading Room,* 2012.

[15] J. M. Allen ir A. Atlasis, „Using OSSEC with NETinVM," *SANS Institute InfoSec Reading Room,* 2010.

[16] S. Ocepek, „Unraveling the Onion: A New Take on Defense-in-Depth," SecureState Consulting, 13 08 2014. [Tinkle]. Available: https://www.securestate.com/blog/2014/08/13/kill-chain. [Kreiptasi 15 04 2016].

[17] M. Yassine, „A review of security attacks and Intrusion Detection Schemes in Wireless Sensor Networks," *International Journal of Wireless & Mobile Networks,* t. 5, nr. 6, 2013.

[18] D. Miessler ir C. Smith, „OWASP Internet of Things Project," The Open Web Application Security Project, 21 04 2015. [Tinkle]. Available: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Main. [Kreiptasi 20 04 2016].

[19] M. Dener, „Security Analysis in Wireless Sensor Networks,“ *International Journal of Distributed Sensor Networks,* 2014.

[20] A. S. Wander, N. Gura, H. Eberle, V. Gupta ir S. C. Shantz, „Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks,“ *Pervasive Computing and Communications,* pp. 324 - 328, 2005.

[21] C. Karlof ir D. Wagner, „Secure routing in wireless sensor networks: attacks and countermeasures,“ *Ad Hoc Networks,* p. 293–315, 2003.

[22] R. Roman, P. Najera ir J. Lopez, „Securing the Internet of Things,“ *Article published in IEEE Computer,* t. 44, nr. 9, pp. 51-58, 2011.

[23] H. Krawczyk, „The Order of Encryption and Authentication for Protecting Communications,“ *Advances in Cryptology — CRYPTO 2001,* t. 2139, pp. 310-331, 2001.

[24] E. D. Cristofaro, H. Du, J. Freudiger ir G. Norcie, „A Comparative Usability Study of Two-Factor Authentication,“ 2014.

[25] M. Popa, „Techniques of Program Code Obfuscation for Secure Software,“ *Journal of Mobile, Embedded and Distributed Systems,* t. 3, nr. 4, pp. 205 - 219, 2011.

[26] M. Ryan, „Bluetooth: With Low Energy comes Low Security,“ *USENIX Workshop on Offensive Technologies,* 2013.

[27] J. Robertson ir S. Robertson, Volere Requirements Specification Template, Atlantic Systems Guild Limited, 2012.

[28] „SimpleLink Bluetooth Smart/Multi-Standard SensorTag,“ [Tinkle]. Available: http://www.ti.com/tool/cc2650stk. [Kreiptasi 04 03 2016].

[29] „BLE Project Zero,“ Texas Instruments, 10 03 2016. [Tinkle]. Available: http://software-dl.ti.com/lprf/simplelink_academy/modules/projects/ble_projectzero/information.html. [Kreiptasi 17 05 2016].

[30] Texas Instruments, „CC2640 and CC2650 SimpleLink Bluetooth low energy Software Stack 2.1.0/2.1.1 Developers Guide,“ 01 2016. [Tinkle]. Available: http://www.ti.com/lit/ug/swru393b/swru393b.pdf. [Kreiptasi 17 05 2016].

[31] Raspberry Pi Foundation, „Raspberry Pi 2 Model B,“ [Tinkle]. Available: https://www.raspberrypi.org/products/raspberry-pi-2-model-b/. [Kreiptasi 17 05 2016].

[32] National Institute of Standards and Technology, „ADVANCED ENCRYPTION STANDARD (AES),“ Federal Information Processing Standards Publications, 2001.

[33] „Bluetooth low energy (LE) (also called Bluetooth Smart or Version 4.0+ of the Bluetooth specification) is the power- and application-friendly version of Bluetooth that was built for the Internet of Things (IoT),“ SIG, [Tinkle]. Available: https://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-technology-basics/low-energy. [Kreiptasi 17 05 2016].

[34] C. Gomez, J. Oller ir J. Paradells, „Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology,“ *Sensor Networks,* pp. 11734-11753, 2012.

[35] P. John ir S. Karen, „Guide to Bluetooth Security,“ National Institute of Standards and Technology, 2011.

[36] Bluetooth SIG, „BLUETOOTH SPECIFICATION Version 4.0 [Vol 0],“ 30 06 2010. [Tinkle]. Available: https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=229737. [Kreiptasi 20 04 2016].

[37] „2.4-GHz Bluetooth low energy System-on-Chip,“ Texas Instruments, 06 2013. [Tinkle]. Available: http://www.ti.com/tool/cc2540emk-usb. [Kreiptasi 26 04 2016].

[38] „AES Calculator,“ [Tinkle]. Available: http://testprotect.com/appendix/AEScalc. [Kreiptasi 03 05 2016].

[39] „CC2650 SensorTag User's Guide,“ 28 03 2016. [Tinkle]. Available: http://processors.wiki.ti.com/index.php/CC2650_SensorTag_User's_Guide#Optical_Sensor. [Kreiptasi 20 04 2016].

[40] „SmartRF Protocol Packet Sniffer,“ Texas Instruments, [Tinkle]. Available: http://www.ti.com/tool/packet-sniffer. [Kreiptasi 26 04 2016].

[41] „RASPBIAN OS,“ [Tinkle]. Available: https://www.raspberrypi.org/downloads/raspbian/. [Kreiptasi 07 03 2016].

8. PRIEDAI

8.1. priedas. Tiriamų metodų testavimo įranga

Tyrimui naudojamas „Sensortag CC2650“ [28] įrenginys. Šis prietaisas pasižymi universalumu, nes gali būti perprogramuojamas ir naudojamas skirtingų topologijų tinkluose. Taip pat šį įrenginį galima asmeniškai pritaikyti įvairiems vartotojo poreikiams. Išmaniojo įrenginio „TI Sensortag CC2650“ panaudojimo atvejai:

a. namų automatizavimas;
b. išmanusis laikrodis;
c. orų stebėjimo stotelė;
d. išmaniojo telefono padėjėjas.

Išmanusis įrenginys „TI Sensortag CC2650“ turi savyje integruotus dešimt jutiklių. Šių jutiklių duomenis galima panaudoti įvairiems panaudos atvejams. Vidiniai jutikliai yra:

a. šviesos srauto jutiklis;
b. infraraudonųjų spindulių temperatūros jutiklis;
c. aplinkos temperatūros jutiklis;
d. akselerometras;
e. giroskopas;
f. magnetometras (gali būti naudojamas kaip kompasas);
g. slėgio jutiklis;
h. drėgmės jutiklis;
i. mikrofonas;
j. magnetinio lauko jutiklis.

Palaikomi skirtingi duomenų perdavimo protokolai suteikia galimybę įrenginį pritaikyti įvairioms tinklo topologijoms. Palaikomi belaidžio perdavimo protokolai:

a. IEEE 802.15.1 Bluetooth Smart;
b. IEEE 802.15.4 ZigBee;
c. IEEE 802.15.4 6loWPAN.

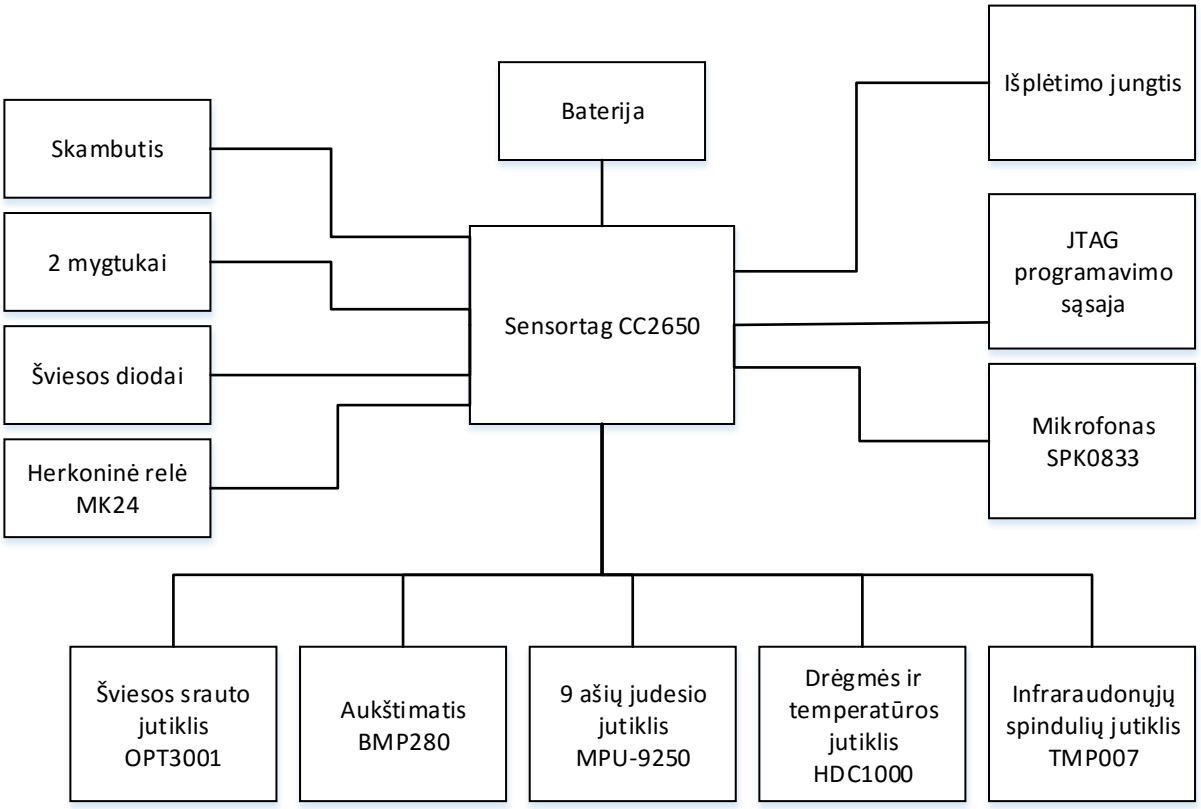
Priklausomai nuo duomenų perdavimo technologijos „Bluetooth“, „Zigbee“ ar 6loWPAN tinklo topologijos gali būti žvaigždės ar tinklelio. Žvaigždės topologija sudaroma naudojant „Bluetooth“ technologiją, o tinklelio „Zigbee“ arba 6loWPAN. Kitos išmaniojo įrenginio specifikacijos:

a. 48MHz dažnio „ARM Cortex-M3“ technologija paremtas CC2650 belaidžio duomenų perdavimo mikrovaldiklis;
b. 128KB programuojamoji atmintis;
c. 20KB laikinoji atmintis SRAM;
d. JTAG programavimo jungtis;

e. AES-128 apsaugos modulis;

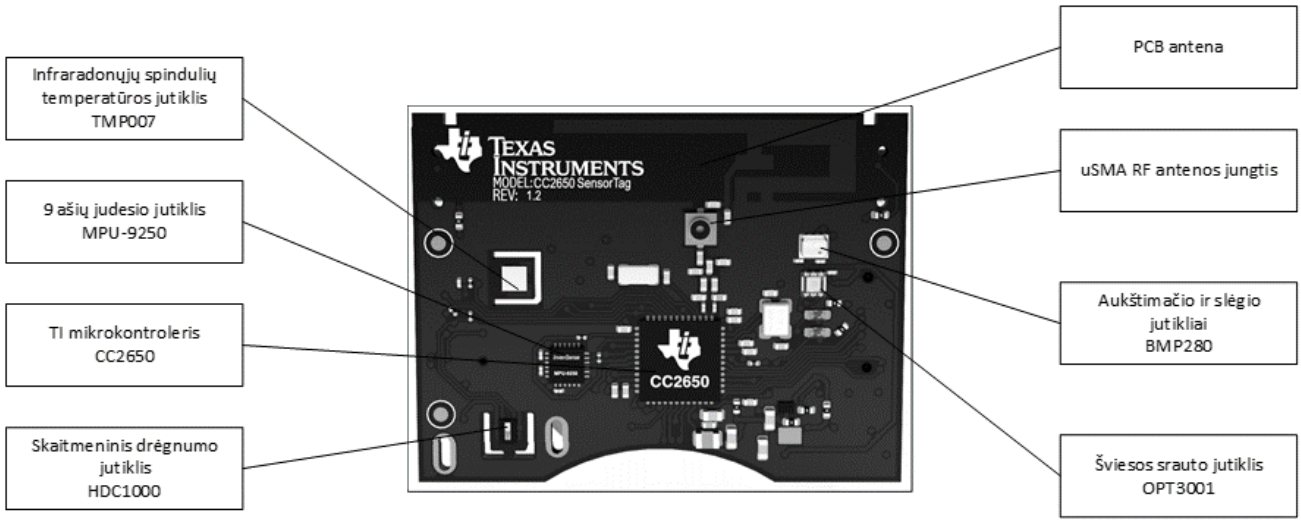
f. MQTT protokolo palaikymas.

Įrenginio blokinė diagrama pateikta 8.1 pav.



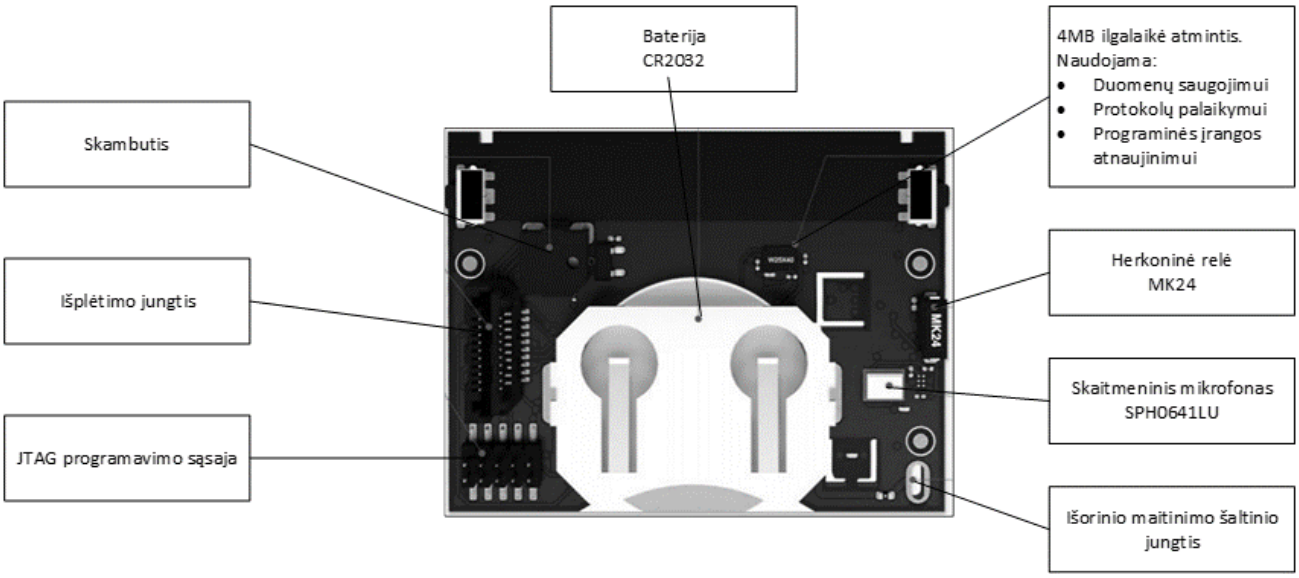
8.1 pav. Išmaniojo įrenginio blokinė diagrama

Priekinė įrenginio dalis pateikta 8.2 pav.



8.2 pav. Išmaniojo įrenginio priekinė dalis

Galinė įrenginio dalis pateikta 8.3 pav.



8.3 pav. Išmaniojo įrenginio galinė dalis

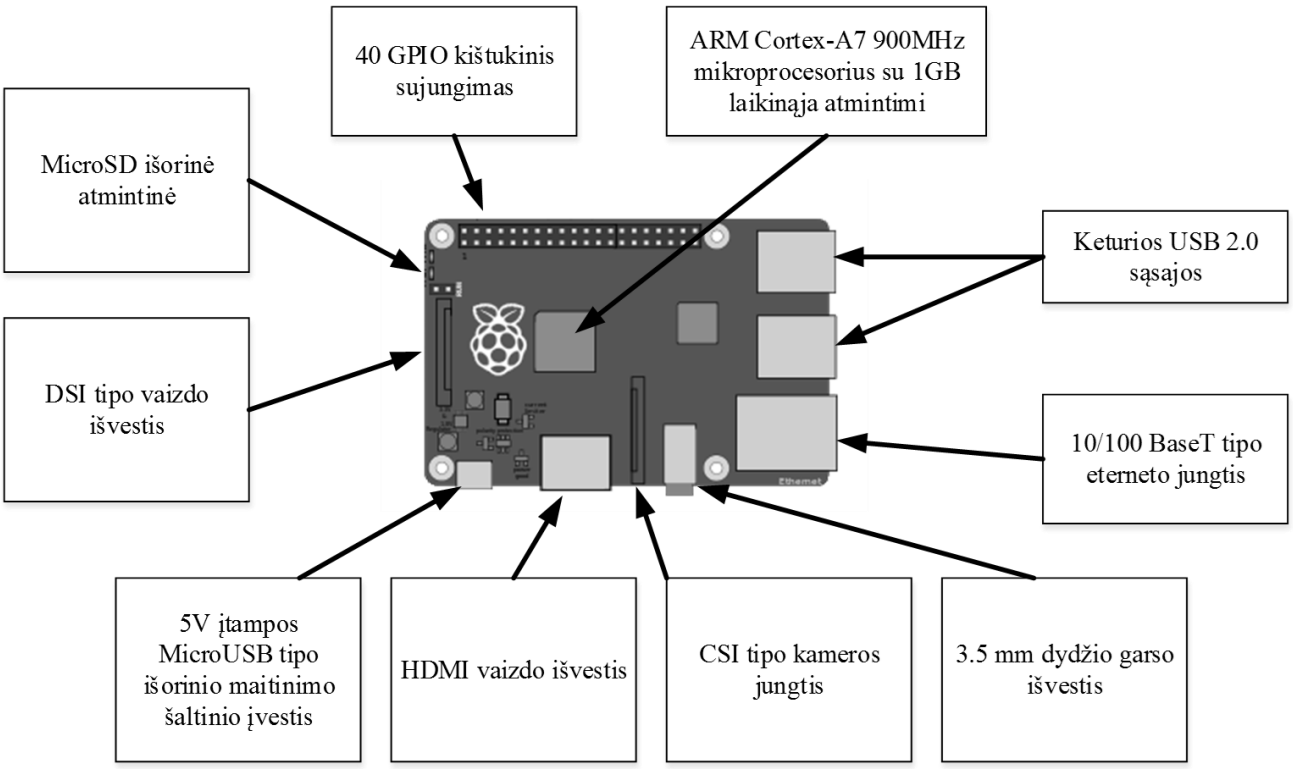
Kuriamoje išmaniųjų įrenginių informacinėje sistemoje yra naudojamas sistemos valdymo įrenginys, kuris atlieka tarpininko vaidmenį tarp „Bluetooth“ belaidžio asmeninio tinklo WPAN ir vietinio tinklo. Tyrimui valdymo kompiuteris yra „Raspberry Pi 2 Model B V1.1“. Šio įrenginio specifikacijos pateiktos 8.1 lent.

8.1 lentelė. Realizuotos informacinės sistemos valdymo įrenginio specifikacijos

Eil. Nr.	**Komponentas**	**Komponento aprašymas**
1.	Operacinė sistema	„Windows 10 IoT Core“ arba „Linux“.
2.	Wi-Fi technologija	Reikalingas USB adapteris.
3.	Bluetooth technologija	Reikalingas USB adapteris.
4.	Procesorius	ARM Cortex-A7 900MHz.
5.	Laikinoji atmintis	Atminties talpa 1GB.
6.	Ilgalaikė atmintis	MicroSD kortelė arba USB atmintukas.
7.	Baterija	Nėra
8.	Išplėtimo jungtys	Keturios USB sąsajos.
9.	Išmatavimai	85mm x 56mm.
10.	Išorinis maitinimo šaltinis	5V/2A kintančios srovės adapteris.

Iš 8.1 lentelės matome, kad valdymo įrenginiui „Raspberry Pi 2 Model B V1.1“ reikalingi papildomi išoriniai adapteriai „Bluetooth 4.0“ technologijos palaikymui.

Priekinė valdymo įrenginio dalis pateikta 8.4 pav.



8.4 pav. Valdymo įrenginio priekinė dalis

Pasirinktas valdymo įrenginys atitinka užduotus reikalavimus. Šiame įrenginyje yra instaliuojama gamintojo optimizuota „Windows 10 IoT Core“ arba „Raspbian GNU/Linux 8“ operacinė sistema [41]. Šios operacinės sistemos turi optimizuotą grafinę sąsają, tad užima mažesnį duomenų kiekį „MicroSD“ atmintinėje ir reikalauja mažiaus sistemos resursų.