KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS

Jevgenijus Sobolevas

RBAC modelio papildymo erdvine bei vietos informacija galimybių tyrimas

Baigiamasis magistro projektas

Vadovas
Doc. dr. Ingrida Lagzdinytė-Budnikė

KAUNAS, 2016

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS

RBAC modelio papildymo erdvine bei vietos informacija galimybių tyrimas

Baigiamasis magistro projektas

Programų sistemų inžinerija (kodas 621E16001)

Vadovas
Doc. dr. Ingrida Lagzdinytė-Budnikė
2016 05 23

Recenzentas
dr. Darius Matulis
2016 05 23

Projektą atliko
IFM-4/2 gr. studentas
Jevgenijus Sobolevas
2016 05 23

KAUNAS, 2016

KAUNO TECHNOLOGIJOS UNIVERSITETAS

Informatikos fakultetas

(Fakultetas)

Jevgenijus Sobolevas

(Studento vardas, pavardė)

Programų sistemų inžinerija (kodas 621E16001)

(Studijų programos pavadinimas, kodas)

Baigiamojo projekto „RBAC modelio papildymo erdvine bei vietos informacija galimybių tyrimas“

AKADEMINIO SĄŽININGUMO DEKLARACIJA

20 16 m. _____ _____ d.

Kaunas

Patvirtinu, kad mano, **Jevgenijaus Sobolevo**, baigiamasis projektas tema „RBAC modelio papildymo erdvinė bei vietos informacija galimybių 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)*

Turinys

LENTELĖS

PAVEIKSLAI

Sobolevas, J. The research study about opportunities of the RBAC model extension with location and time information: Master‘s thesis in Informatics / supervisor assoc. doc. dr. Ingrida Lagzdinytė-Budnikė. The Faculty of Informatics, Kaunas University of Technology.

Key words: Radius; STRBAC; Centralized; Wi-Fi; Wireless network; access control; RBAC; location based authorization; time based authorization;

Kaunas, 2016. 83 p.

SUMMARY

Nowadays wireless networks are widespread and their usage is steadily increasing. Therefore the spread of wireless networks increases a prevalence of hacking or unauthorized access risks, thus complicating an access control. An access to wireless networks is not always properly protected, secured and managed. Widespread of the wireless networks and wide usage of the mobile devices creates the need of such applications and services that can use time and location information to improve their existing functionality.

This type of software can be useful in different domains, i.e. for business. Also user location information and connection time can be used to improve protection of network access control.

To support above mentioned functionality it would be required more complex access control systems. And there is growing need to modify existing access control models to support advanced features.

This work examines the RBAC model extensions implementations with time and location information. Designed and developed centralized network access control system based on time (temporal) and location (spatial) information – an extended RBAC model. RBAC model extensions also are related to system functioning in wireless network specifics. The system allows distributing of access rights to the wireless network users based on the location and time when attempt to gain network access has occurred. Authorization result for network user will depend on actual location of the user and current date or time. The system supports Radius protocol, which provides compatibility with various network devices. Work including experimental studies with the developed system that demonstrates the operation of the system characteristics under different conditions. Test cases designed in such way, where different numbers of users are trying to gain access simultaneously, and in case of successful connections accounting sessions will be simulated. The work also provides presentation of the proposals to reduce the number of queries to the location positioning system, at the same time supporting time and location based RBAC model specifics.

Sobolevas, J. RBAC modelio papildymo erdvinė bei vietos informacija galimybių tyrimas. Magistro baigiamasis projektas / vadovas doc. dr. Ingrida Lagzdinytė-Budnikė; Kauno technologijos universitetas, Informatikos fakultetas.

Kaunas, 2016. 83 p.

SANTRAUKA

Šiuo metu belaidžiai tinklai labai paplitę, jų naudojimas nuolat auga. Toks tinklų paplitimas didina įsilaužimo arba nesankcionuotų prisijungimų riziką ir apsunkina prieigos prie tokių tinklų kontrolę. Taip pat prieiga prie belaidžio tinklo ne visuomet tinkamai valdoma arba apsaugota. Atsiradus ir išpopuliarėjus belaidžiam ryšiui ir mobiliems įrenginiams atsirado poreikis, tokioms taikomosioms programoms (ar paslaugoms), kurios naudotų laiko ir vietos informaciją jau esamo funkcionalumo pagerinimui.

Tokia programinė įranga gali būti aktuali įvairiuose srityse. Taip pat informaciją apie vartotojo buvimo vietą ir prisijungimo laiką taip pat galima panaudoti norint labiau apsaugoti prieigą prie tinklo.

Tokie taikymai reikalauja sudėtingesnio prieigos valdymo, kuriame autorizuojant sistemos naudotoją/vartotoją taip pat turi būti atsižvelgta į laiko ir vietos informaciją. Todėl atsiranda poreikis, modifikuoti esamus prieigos valdymo modelius.

Darbe nagrinėjamos RBAC modelio papildymo vietos ir laiko informacija galimybės. Suprojektuotas ir sukurtas tokio papildyto RBAC modelio pagrindu veikiančios sistemos prototipas. Sukurta sistema vykdo vartotojų prisijungimo prie bevielio tinklo kontrolę (autentifikaciją ir autorizaciją) atsižvelgiant į besijungiančio prie tinklo vartotojo vietą ir laiką. Sistema, leidžia skirstyti tinklo vartotojams prieigos prie belaidžio tinklo teises atsižvelgiant į tai, kokiu laiku ir kokioje vietoje/erdvėje besikreipiantis į tinklą vartotojas yra, t.y. autorizuoti vartotoją tinkle pagal jo buvimo vietą bei laiką. Sistema palaiko „Radius“ protokolą, kuris leidžia suderinti sistemos veikimą su įvairiais tinklo įrenginiais. Darbe aprašyti sukurtos sistemos tyrimo rezultatai, kurie parodo tokios sistemos veikimo charakteristikas esant skirtingoms sąlygoms (kintantis besijungiančių prie tinklo vartotojų skaičius, kintantis aptarnaujamų vartotojų skaičius). Pateikti pasiūlymai, kaip sumažinti užklausų kiekį į vartotojų vietos nustatymo sistemą, tuo pačiu įvertinant ir vietos bei laiko informacija papildyto RBAC modelio specifiką

1. Įžanga

Šiuo metu bevieliai tinklai labai paplitę, jų naudojimas nuolat auga [1, 2]. Bevieliai tinklai naudojami privačiai (namuose), viešoje erdvėje (parduotuvėse, restoranuose, lauke ir t.t.), švietimo bei administracinėse institucijose. Toks bevielių tinklų paplitimas didina įsilaužimo arba nesankcionuotų prisijungimų riziką ir apsunkina prieigos prie tokių tinklų kontrolę. Taip pat prieiga prie bevielio tinklo ne visuomet tinkamai valdoma arba apsaugota [3].

Atsiradus ir išpopuliarėjus bevieliam ryšiui ir mobiliems įrenginiams atsirado poreikis tokioms taikomosioms programoms (ar paslaugoms), kurios naudotų laiko ir vietos informaciją jau esamo funkcionalumo pagerinimui. Pavyzdžiui, universitete vykstant egzaminui būtų patogu turėti galimybę egzaminą rašantiems studentams uždrausti prieigą prie bevielių tinklų iš auditorijų, kuriuose egzaminas yra rašomas, tačiau tokie draudimai negaliotų toje pačioje auditorijoje esančiam dėstytojui. Tokia programinė įranga gali būti aktuali ir verslui, pavyzdžiui, viešbučiuose suteikiant prieigą prie bevielio tinklo resursų tik tam tikruose viešbučio numeriuose esantiems klientams. Panašaus pobūdžio funkcionalumas gali būti aktualus restoranuose, bankuose, renginiuose ir kitose srityse, kuriuose reikia skirstyti prieigą prie bevielio tinklo pagal vietą ir laiką. Informaciją apie vartotojo buvimo vietą ir prisijungimo laiką taip pat galima panaudoti norint labiau apsaugoti prieigą prie tinklo.

Tokie taikymai reikalauja sudėtingesnio prieigos valdymo, kuriame autorizuojant sistemos naudotoją/vartotoją taip pat turi būti atsižvelgta į laiko ir vietos informaciją. Todėl atsiranda poreikis modifikuoti esamus prieigos valdymo modelius.

Vienas iš dažniausiai organizacijose naudojamų standartinių prieigos valdymo mechanizmų yra Rolėmis grįstas prieigos kontrolės (angl. RBAC, „Role-based Access Control“) modelis [4, 5]. Panaudojant šį modelį kiekvienam vartotojui yra priskiriama rolė, o kiekvienai rolei leidimai. Tokiu būdu įvairiems vartotojams galima priskirti įvairias prieigos teises.

Šiuo metu egzistuoja eilė RBAC modelio praplėtimų, kurie leidžia autorizuoti vartotoją atsižvelgti į papildomą informaciją apie jį [6, 7, 8, 9, 10, 11]. Šių tyrimų autoriai daugiau dėmesio skiria RBAC praplėtimams konceptualiame lygmenyje, tačiau gana mažai informacijos pateikiama kaip šie modeliai turėtų adaptuojami įvairioms aplinkoms, pavyzdžiui, funkcionavimui bevieliame tinkle.

1.1. Darbo tikslas, sistemos aktualumas

Darbo tikslas yra išnagrinėti RBAC modelio papildymo vietos ir laiko informacija galimybes bei sukurti ir ištirti papildyto RBAC modelio pagrindu veikiančios sistemos, kuri leistų centralizuotai autorizuoti bevielio tinklo vartotojus nagrinėjant papildomą informaciją (vartotojo buvimo vietą, bei prisijungimo laiką) apie vartotoją, prototipą. Potencialūs sistemos

vartotojai/užsakovai gali būti bet kokia organizacija, kuri nori centralizuotai autorizuoti bevielio tinklo vartotojus pagal jų buvimo vietą. Pavyzdžiui, tokia sistema gali būti panaudojama tam, kad autorizuoti KTU elektronikos rūmų tinklo vartotojus. Reikia pabrėžti, kad vietos nustatymo sistema, vykdanti vartotojo vietos nustatymą, yra visiškai atskira problema, kuri nėra šio darbo objektas ir šio darbo metu nėra plačiai analizuojama. Tačiau tai yra labai svarbus komponentas, be kurio tyrimas nebūtų apskritai įmanomas. Todėl vartotojo vietos nustatymo procesą, kuriant autorizacijos sistemos prie bevielio tinklo resursų prototipą, numatoma imituoti/simuliuoti.

1.2. Mokslinis naujumas

1. Pasiūlytas bevielio tinklo vartotojų centralizuotos autorizacijos procesas, kuriame atsižvelgiama į papildomą, vartotojo prisijungimo prie tinklo vietos ir laiko, informaciją.
2. Papildyto RBAC modelio pagrindu sukurtos sistemos prototipo tyrimų rezultatai nustato rekomendacijas, skirtas tokios sistemos naudojimui realiomis sąlygomis.
3. Pateikti pasiūlymai, kaip sumažinti užklausų kiekį į vartotojų vietos nustatymo sistemą, tuo pačiu įvertinant ir vietos bei laiko informacija papildyto RBAC modelio specifiką.

1.3. Darbo uždaviniai

Magistro tiriamojo darbo uždaviniai yra šie:

1. Išanalizuoti vartotojų vietos ir laiko informacijos gavimo būdus bei ištirti RBAC modelio papildymo vietos ir laiko informacija galimybes;
2. Išanalizavus kuriamos autorizavimo sistemos belaidžio tinklo vartotojo buvimo vietos informacijos poreikį, tipą ir panaudojimo ypatumus, sukurti vietos nustatymo sistemos imitatorių, kuris leistų autorizavimo sistemai nepertraukiamai veikti ir atlikti vartotojų autorizacijas.
3. Suprojektuoti ir realizuoti papildyto RBAC modelio pagrindu veikiantį sistemos prototipą, leidžianti centralizuotai autorizuoti bevielio tinklo vartotojus vertinant papildomą informaciją apie juos (vartotojo buvimo vieta ir prisijungimo laiką).
4. Realizuotą sistemą ištirti ir įvertinti šios sistemos savybes. Gautų tyrimų rezultatų pagrindu pateikti rekomendacijas sistemos veikimo efektyvumo gerinimui, panaudojant realiomis sąlygomis.

2. ANALITINĖ DALIS

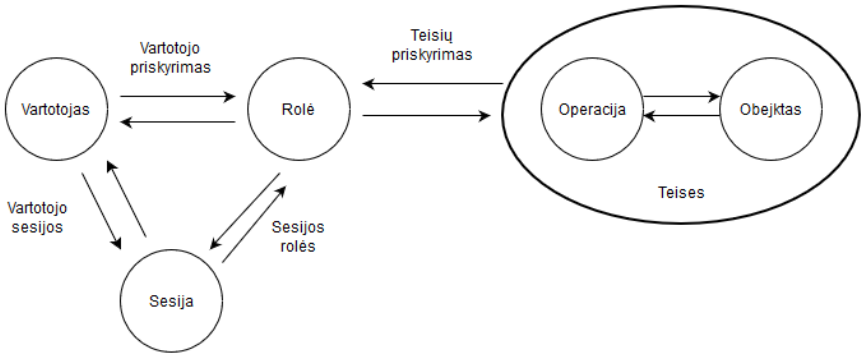
Toliau šiame skyriuje pateikiama mokslinių publikacijų trumpa apžvalga, kuriuose aprašomos panašios sistemos arba naudojami modeliai. Taip pat trumpai aprašomas RBAC modelis bei vietos nustatymo technologijos.

2.1. Rolėmis pagrįstas autorizuotų vartotojų prieigos valdymo modelis (angl. Role-Based Access control - RBAC)

RBAC (angl. Role Based Access Control) – rolėmis pagrįstas autorizuotų vartotojų prieigos valdymo modelis. Šis modelis yra pagrįstas vidinės organizacijos ar vartotojo individualiais vaidmenimis ir atsakomybe. Vaidmenų priskyrimo procesas yra pagrįstas organizacijos struktūros ir tikslų analizavimu. Modelis pagrįstas vartotojų vaidmenų/rolių sukūrimu, roles siejasi su vartotojų pareigomis, teisės vartotojams nėra suteikiamos tiesiogiai, bet priskiriant vieną ar kelias vaidmenis/roles, kuriuos apibrėžia konkrečias pareigybės arba teisės (pvz., priklausomai nuo jų darbo pareigų). RBAC prieigos kontrolės modelis yra labai plačiai taikomas verslo sektoriuje. Pavyzdžiui, medicinos įstaigoje vartotojai turi skirtingus vaidmenis: daktaras, seselė, pacientas ir t. t. Šiems elementams reikalingi skirtingi kontrolės, prieigos lygiai, kad galėtų atlikti savo funkcijas, tačiau jų tarpusavio ryšys skiriasi priklausomai nuo saugumo politikos ir reguliavimo. [4, 5]

2.1.1. RBAC modelio struktūra

RBAC modelio struktūra pavaizduota 1 paveikslėlyje.



1 pav. RBAC modelio struktūra [12]

Šioje struktūroje galima išskirti šiuos komponentus:

- vartotojas – žmogus, kuris nori atlikti tam tikrus veiksmus;
- rolė – vartotojui priskiriama teisė arba atsakomybė (pvz., organizacijoje atliekamo darbo funkcija);
- teisė – leidimas atlikti veiksmą su tam tikru objektu;
- objektas – esybė, kuri turi arba gauna informaciją (pvz.: duomenų bazės lentelė);

- operacija – vykdomasis programos atvaizdas, kurį iškvietus atliekamos tam tikros vartotojui reikalingos funkcijos [12].

Panaudojant tokį modelį, kiekvienam vartotojui yra priskiriama tam tikra rolė, kuri susieta su tam tikra teise ir objektu. Pavyzdžiui, tarkime mes turime 2 objektų aibes (O1 ir O2). Tarkime darbuotojai kurie priklauso rolei R1 galės atlikti veiksmus/operacijas (V1) su objektais iš aibės O1, tačiau objektai iš aibės O2 jiems bus nepasiekiami. Tuo tarpu darbuotojai kurie priklauso rolei R2 galės atlikti veiksmus V1 tiek su objektais iš aibės O1 tiek su objektais iš aibės O2.

2.1.2. Modelio taikymo sritis

Pagal NIST (National Institute of Standards and Technology) pateiktą ataskaitą [5], RBAC modelis pasižymi žemiau pateiktais privalumais:

- Leidžia efektyviau kontroliuoti ir prižiūrėti prieigos politiką;
- Palengvina darbą sistemos/tinklo administratoriams;
- Padidina organizacijos arba produkto produktyvumą;
- Padidina organizacijos arba produkto saugumą ir vientisumą;

Dėl aukščiau aptartų privalumų RBAC modelis gali būti taikomas įvairiose organizacijose arba sprendimuose, kuriuose reikia skirstyti prieigą prie įvairių resursų ir valdyti vartotojų teises/leidimus. RBAC modelis vienoje arba kitoje formoje gali būti panaudojamas įvairiuose srityse, tiek IT, tiek kitose. Pavyzdžiui, medicinoje, šeimos gydytojas gali pasiekti tik savo pacientų, ligų arba kitą asmeninę informaciją, o skyriaus vedėjas gali peržiūrėti viso skyriaus pacientų ligų istoriją.

RBAC modelis yra pripažintas kaip viena iš geriausių praktikų valdyti vartotojo teises. Jis yra panaudojamas skirtingomis formomis, tokiose pasaulinėse sistemose kaip: „Oracle DBVS“, „PostgreSQL 8.1“, „SAP R / 3“, „ISIS Papyrus“, „FusionForge“, „Wikipedia“ ir t. t. Pasak 2010 metų NIST (National Institute of Standards and Technology) ataskaitos, RBAC modelio panaudojimas žymiai palengvina/optimizuoja organizacijos arba kažkokių tiekiamų paslaugų administravimo procesą.

2.2. RBAC modelio papildymai vietos ir laiko informacija

Taip pat buvo atliekami įvairūs moksliniai tyrimai [10, 11, 14] siekiant formaliai patobulinti RBAC modelį, papildant jį vietos ir laiko informacija. Tokiu būdu papildytas RBAC modelis skirstant roles/teises atsižvelgtų į papildomus apribojimus (vietos ir laiko apribojimus). Papildant RBAC modelį laikina informacija (čia laikina informacija suprantama kaip vartotojo buvimo vieta ir prisijungimo laikas) galima nagrinėti organizacijos politiką. Pavyzdžiui, toks RBAC modelis leistų nustatyti politiką, kai vieni organizacijos resursai bus pasiekiami nuo 9 val. iki 12 val., o kiti tik nuo 12 val. iki 17 val. Tokiu būdu vartotojo teises apibrėžia ne tik rolė, bet ir laikas.

Kita vertus platus nešiojamųjų kompiuterių ir mobiliųjų prietaisų paplitimas leidžia tinklo naudotojams prisijungti prie bevielio tinklo iš įvairiausių įmonės vietų (kuriuose pasiekiamas bevielis ryšys). Taigi RBAC modelis taip pat turi nagrinėti ir naudotojo vietos informaciją, tam, kad vartotojų rolės būtų priskiriamos arba suvaržomos pagal jų (tinklo vartotojų) buvimo vietą. Tokius apribojimus savo darbuose aprašinėjo Hansen ir Oleshchuk, Wilikens et al.[15], [16]. Tokie papildyti RBAC modeliai dar vadinami erdviniais RBAC modeliais. Panaudojant tokius modelius, roles galima skirstyti priklausomai nuo vartotojo buvimo vietos. Pavyzdžiui, administratorius gali pasiekti organizacijos duomenų bazę arba kokią kitą kritinę sistemą tik būdamas savo kabinete.

2.2.1. Egzistuojantys RBAC modelio papildymai vieta ir laiku

Šio metu egzistuoja keletas darbų, kuriuose nagrinėjamos RBAC modelio papildymo vietos ir laiko informacija galimybės. Toliau trumpai apžvelgsime keletą jų vertindami darbus pagal kriterijus, kurie svarbūs siekiant sukonstruoti praplėstu RBAC modeliu paremtą sistemos prototipą:

- Darbe aprašomo modelio formalizavimo būdas/metodas.
- Vietos informacijos požymiai (kaip išreiškiama).
- Architektūrinis sprendimas.
- Parametrai, naudojami skirstant leidimus.
- Taikymo sritis.

2.2.1.1. Pitsburgo universiteto sukurtas prototipas, panaudojantis praplėstą RBAC modelį

Yue Zhang ir James B.D. Joshi nagrinėjo įvairių resursų saugumo problemą, bandė papildyti įprastą RBAC modelį praplėsdami jį laikina informacija. Autoriai naudojo GTRBAC (angl. Generalized Temporal Role Based Access Control) modelį. Tai RBAC modelio papildymas/išplėtimas, kuris palaiko laikinus leidimus arba autorizaciją. Toks funkcionalumas gali ženkliai palengvinti tinklo arba sistemos administravimą. Tačiau GTRBAC modelis panaudojamas gana retai dėl jo sudėtingo įgyvendinimo/realizavimo.

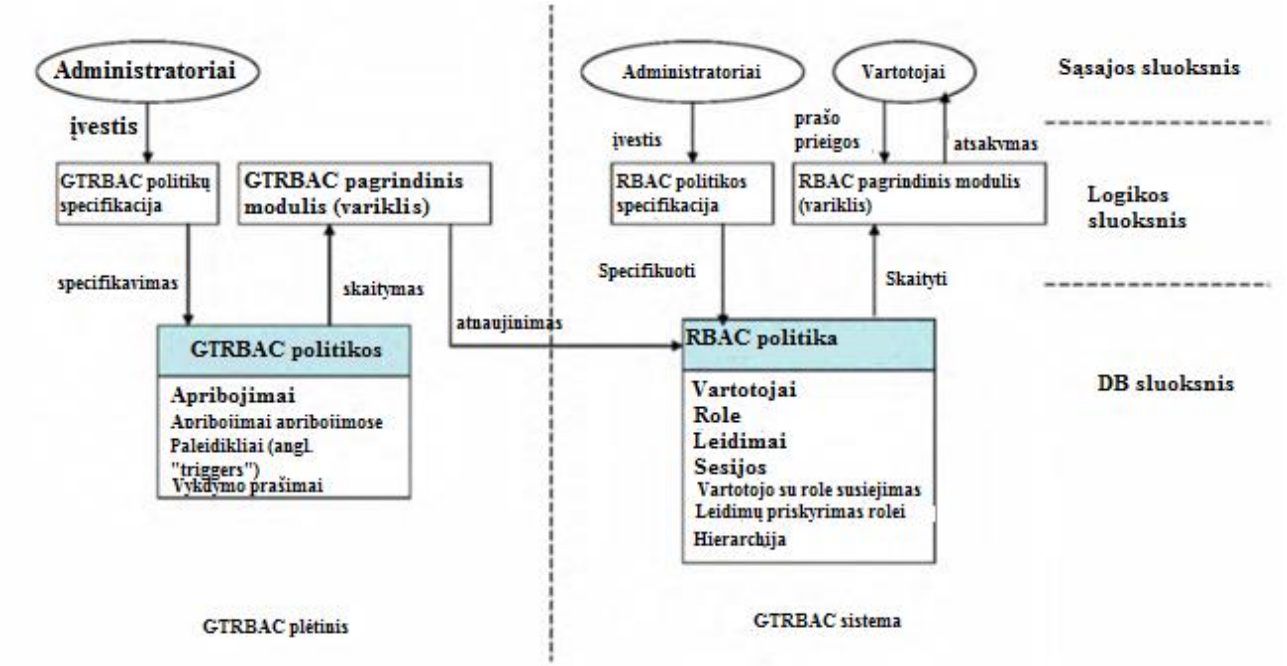
GTRBAC modelyje galima išskirti šiuos kintamus parametrus: periodiškumą, laiką, kiekį/kiekybinį suvaržymą. Šie parametrai naudojami skirstant leidimus. Toliau pateikiamas trumpas šių parametrų paaiškinimas:

- *Laikas* – yra galimybė skirti leidimus arba apriboti naudotojo veiksmus pagal laiką. Pavyzdžiui, darbuotojo darbo laikas yra nuo 9 val. iki 17 val., šiuo laiku sistema darbuotojui yra pasiekiama, po 17 val. sistema tampa nebepasiekiama.
- *Periodiškumas* – galimybė skirti periodiškus leidimus arba apribojimus. Pavyzdžiui, darbuotojas naudojasi sistema tik pirmadieniais, o kitomis dienomis prieiga jam yra draudžiama.

- *Kiekis arba kiekybinis parametras* – leidžia nustatyti, kiek kartų gali būti panaudojamas tam tikras resursas arba paslauga. Pavyzdžiui, jei leista sistema vienu metu naudotis 5 darbuotojams, tai kiti norintys turi laukti eilėje, kol atsilaisvins vieta. Taip pat galima skirti apribojimus tik tam tikrai rolei. Pavyzdžiui, darbuotojas vienu metu gali naudoti ne daugiau kaip 3 resursus.

Taip pat yra galimybė sujungti parametrus, pavyzdžiui, periodiškumą ir laiką. Vienas leidimas arba apribojimas gali iškviesti kitą. Pavyzdžiui, jei pasiektas kiekybinis limitas, pradeda veikti laiko apribojimas ir, praėjus iš anksto nustatytam laikui, vartotojas atjungiamas nuo naudojamos paslaugos. Taip atlaisvinama paslauga ir kiti vartotojai gali ja naudotis. Tačiau, atsiradus tokiems apribojimams, tampa sudėtinga suvaldyti bent 2 apribojimų tipus, jau nekalbant apie visus.

Autorių GTRBAC modelio architektūrinis sprendimas yra pavaizduotas 2 pav.:



2 pav. „GTRBAC“ modelio architektūrinis sprendimas [17]

Kaip matome iš 2 pav., vertikaliai sistema gali būti sudalinama į 3 sluoksnius: sąsajos sluoksnis, loginis ir duomenų bazės sluoksniai.

- *Sąsajos sluoksnis* – skirtas administruoti (keisti arba pridėti) vartotojų/rolių leidimus, panaudojant leidimų specifikavimo modulį (angl. Policy specification). Vartotojai taip pat naudoja šį sluoksnį autorizavimui (2 pav.).
- *Loginis sluoksnis* – loginiame sluoksnyje yra politikos (prieigos teisių) specifikavimo moduliai, kurie transformuoja vartotojo pateiktą informaciją į esančią duomenų bazėje.
- *Duomenų bazės sluoksnis* – duomenų bazės sluoksnyje saugomos esamos politikos (prieigos teisės) reliacinėje duomenų bazėje.

Panaudojant GTRBAC modelį autoriais buvo sukurtas prototipas, kuris leido skirstyti leidimus arba draudimus priklausomai nuo laikinos informacijos. Taip pat autoriai teigia, kad jų sukurtame prototipe yra paprasta skirstyti/priskirti leidimus arba apribojimus naudotojams. Vis dėlto aprašytame sistemos prototipe didesnis dėmesys skiriamas su laiku susijusių apribojimų analizei ir architektūriniams tokiu modeliu paremtos sistemos sprendimams aptarti. Darbe trumpai pristatomas papildomo modulio, kuris vertina ir vietos informaciją, kaip parametrą skirstant leidimus, integravimas, tačiau jo veikimo logika detaliau neaprašoma ir nenagrinėjama. Taip pat nėra aptariama, kaip vienu metu gali būti derinami keli skirtingi (pavyzdžiui, vieta ir laikas) parametrai [17].

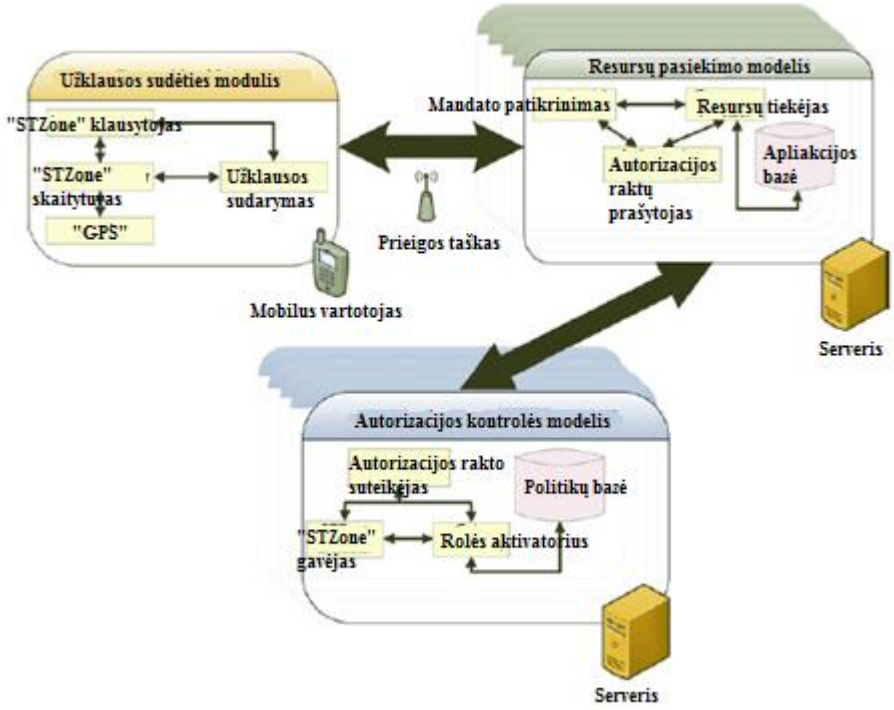
2.2.1.2. Papildyto RBAC modelio panaudojimas išmaniųjų telefonų aplikacijoje „iMedik“

Atsiradus bevieliam ryšiui ir mobiliem įrenginiam buvo sukurta daug įvairių programų, kuriose vietos ir laiko informacija yra naudojama tam, kad suteikti geresnį funkcionalumą. Tokios programos taip pat reikalauja sudėtingesnio prieigos valdymo, kuriame autorizuojant naudotoją/vartotoją taip pat turi būti atsižvelgta į laiko ir vietos informaciją. Todėl atsiranda poreikis modifikuoti esamus prieigos valdymo modelius.

Ramadan Abdunabi ir kiti, sprendė kaip apsaugoti klinikos pacientų asmeninę informaciją. Esmė tame, kad gydytojai naudojosi programėle „iMedik“, kuri skirta delniniams kompiuteriams, tam, kad pasiekti savo pacientų asmeninę informaciją (pvz. ligos aprašymą, namų adresą ir t.t.). Tačiau atsirado problema – kaip apsaugoti pacientų asmeninę informaciją, tam kad medikai galėtų pasiekti ligonių informaciją tik klinikoje ir tik darbo metu. Nes gydytojas gali pamesti delninį kompiuterį (prisijungimo duomenys gali būti išsaugoti), todėl bet koks kitas pašalinis asmuo, radęs pamestą mobilų įrenginį, galėtų pasiekti gydytojo pacientų asmeninę informaciją. Tradiciniai, rolėmis(vaidmenimis) grįstos prieigos kontrolės, modeliai - tokie kaip RBAC, yra netinkami siekiant apibrėžti tokią prieigos politiką.

Tokios problemos sprendimui reikia papildyti paprastą RBAC modelį, kad jis nagrinėtų ne tik vartotojo rolę, bet ir vietos bei laiko informaciją. Tokiu būdu su vartotoju susiejami 2 papildomi parametrai - laikas ir jo buvimo vieta. Toks papildymas leidžia priskirti kada ir kur konkreti vartotojo rolė gali būti aktyvuota. Taigi, šios problemos sprendimui autoriai naudoja GSTRBAC (angl. Generalized Spatio-Temporal Role-Based Access Control) modelį. Tai yra RBAC modelis, kuris papildytas vietos ir laiko informacija. Kai bandoma pasiekti paciento asmeninę informaciją yra patikrinamas laikas ir darbuotojo buvimo vieta. Tokiu būdu, jei klinikos darbuotojas arba asmuo radęs pamestą įrenginį, bandytų pasiekti paciento informaciją, ne klinikos viduje arba ne gydytojo darbo metu, prieiga jam nebūtų suteikta. Vietos informacijai nustatyti autoriai naudojo GPS koordinates, kadangi tai buvo mobili aplikacija.

Autoriai pateikia GSTRBAC modelio realizaciją į mobilios aplikacijos architektūrą:



3 pav. „GSTRBAC“ modelio realizacija „iMedik“ aplikacijoje [18]

Toliau pateikiamas trumpas 3 pav. pateiktų modulių aprašymas:

- Užklausos sudėties modulis (angl. „Request Composition Module“ RCM) – yra atsakingas už vartotojo prieigos prašymo formavimą ir prieigos palaikymą.
- Resursų pasiekimo modulis (angl. „Resource Access Module“ RAM) – yra tarpinis serveris tarp vartotojo ir ACM serverio. RAM serveris gauna vartotojo prieigos prašymą ir užklausia ACM serverį, ar šiam vartotojui leistina autorizuotis.
- Autorizacijos kontrolės modulis (angl. „Authorization Control Module“ ACM) – atsakingas už rolių skirstymą.

Autorių pristatytas GSTRBAC modelio prototipas ir jo architektūriniai aspektai atsako į nemažai šiame darbe iškeltų klausimų. Tačiau autorių pristatomoje sistemoje praktiškai neskiriamas dėmesys į vartotojų autorizacijos bevieliame tinkle specifiką, taip pat plačiau nenagrinėjami centralizuoto autentifikavimo ir autorizavimo aspektai [18].

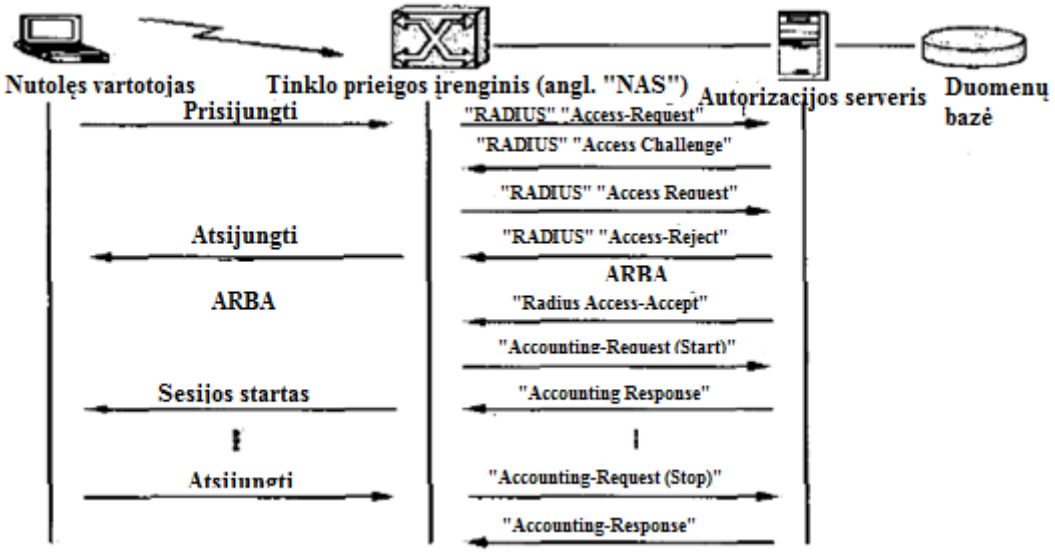
2.2.1.3. Vietos ir laiko informacija pagrista prieigos kontrolė 802.11 bevieliame tinkle

Šiuo metu bevieliai tinklai yra labai plačiai paplitę. Viena iš svarbiausių vertybių, kurias suteikia organizacijoms bevieliai tinklai, yra universali prieiga prie informacijos. Bevieliai tinklai leidžia pasiekti reikiamą informaciją iš bet kurios vietos, kur tik yra pasiekiamas bevielio tinklo ryšys. Tai leidžia pagerinti darbo efektyvumą. Tačiau yra ir trūkumų – dažniausiai pagrindinė priežastis dėl kurios atsisakoma diegti bevielį tinklą - tai jo saugumas. Pagrindinis skirtumas, kuris skiria laidinio tinklo saugumą nuo belaidžio yra tai, kad neįmanoma kontroliuoti fizinę prieigą prie

bevielio tinklo dėl to, kad bevielis tinklas sklinda radijo bangomis. Šis faktas daro belaidį tinklą ypač pažeidžiamu pasiklausymo atakoms.

Taip pat didelėse organizacijose egzistuoja įvairių lygių vartotojai (administratoriai, programuotojai, analitikai ir t.t.), kurie naudojasi įvairiais tinklo resursais. Pavyzdžiui, administratorius, panaudojant bevielį tinklą turi pasiekti visus tinklo resursus, o įprastas darbuotojas pasiekia tik savo el. paštą. Taip pat organizacijos bevieliu tinklu gali naudotis ir svečiai, jiems taip pat turi buti suteiktos tinklo resursų pasiekiamumo lygis/teisės (pvz. organizacijos svečiai gali pasiekti bevielį tinklą tik iš svečių kambario).

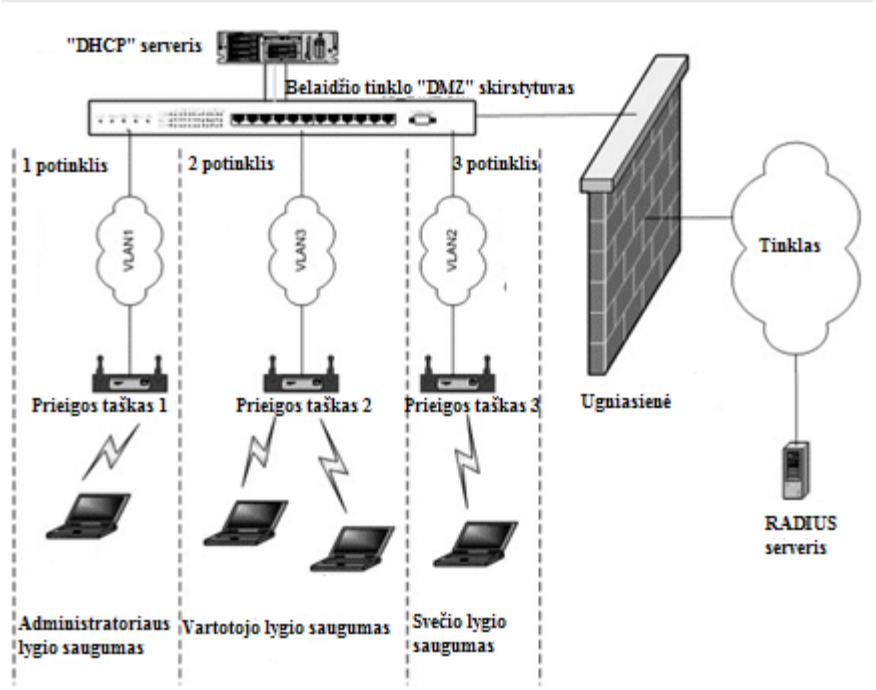
Siekiant padidinti bevielio tinklo saugumo lygį Emrah Tomur ir Yusuf Murat Erten panaudojo ugniasienę, „Radius“ autorizacijos ir autentifikacijos serverį (kuris jau įrodė savo efektyvumą laidiniuose tinkluose). „Radius“ - tai kompiuterių tinklo protokolas/servisas, kuris leidžia centralizuoti prieigą prie tinklo. Programinė „Radius“ protokolo realizacija dažnai tapatinama su Autentifikacijos, Autorizavimo ir Apskaitos paslauga (AAA). „Radius“ paslaugos veikimą galima paaiškinti taip: kai tinklo vartotojas prijungiamas prie tinklo, įvyksta autentifikacija. Tada tinklą skirstantis įrenginys kreipiasi į „Radius“ serverį (siusdamas prieigos prašymo užklausą angl. „Access-Request“), o pastarasis jau autorizuoja tinklo vartotoją ir nusiunčia prieigos leidimo (angl. „Access-Accept“) arba draudimo žinutę (angl. „Access-Reject“) tinklo stočiai. Toks autorizavimo būdas bei galimi „Radius“ serviso bendravimo žinučių tipai yra parodyti 4 pav. [19, 20].



4 pav. „RADIUS“ protokolo galimų žinučių apsikeitimas [19]

Taip pat tinklo resursų pasiekiamumas buvo ribojamas panaudojant modifikuotą RBAC modelį, kuris buvo papildytas vietos ir laiko informacija (tam, kad galima būtų skirstyti teises priklausomai nuo vartotojo buvimo vietos). Vietos informacijos nustatymas buvo realizuotas pagal bevielio tinklo vartotojo potinklio IP adresą. Tačiau autoriai teigia, kad yra ir geresnių būdų vartotojo vietai nustatyti (tokie metodai aptariami 2.2.2 skyriuje). Toks papildytas prieigos teisių

skirstymo būdas leidžia išspręsti aukščiau apibrėžtas problemas/siekius. Pavyzdžiui, leidžia užtikrinti, kad bevielis tinklas iš darbui skirtų patalpų būtų pasiekimas tik darbo valandomis ir darbo dienomis, kai tuo tarpu svečių kambaryje galima būtų naudotis tinklu bet kurio metu. Jei prieiga leidžiama tik darbo dienomis ir darbo metu, tai toks prieigos kontrolės būdas gali apsaugoti nuo neteisėtos prieigos savaitgaliais (tokiu būdu didinamas bevielio tinklo saugumas). Autorių naudota architektūra yra pavaizduota 5 pav.:



5 pav. Bevielio tinklo architektūra **[**21**]**

Tokios architektūros panaudojimas leidžia išspręsti aukščiau aptartas tinklo organizacijos problemas ir tuo pačiu padidinti saugumą. Tokioje architektūroje saugumo lygį nusako bevielio tinklo naudotojų (tinklo administratorius, svečio arba įprasto darbuotojo) rolės ir teisės, jų (vartotojų) buvimo vieta ir prisijungimo laikas. Toliau pateikiamas trumpas prisijungimo~~,~~ prie bevielio tinklo, naudojančio aukščiau (5 pav.) aprašytą architektūrą, scenarijus:

1. Tinklo naudotojo įrenginys (pvz. nešiojamas kompiuteris) bando prisijungti prie bevielio tinklo, komunikuojant su jam matomu prieigos tašku.
2. Vartotojas nustatomas pagal iš anksto numatytą metodą (priklausomai nuo jo rolės).
3. Remiantis vartotojo įrenginio potinklio ir laiko informacija vartotojui išduodamos iš anksto nustatytos teisės.
4. Vartotojo įrenginio srautas, šifruojamas panaudojant iš anksto numatytą algoritmą/metodą.

Kitaip tariant, kai vartotojas bando pasiekti tam tikrus tinklo resursus, yra patikrinama jo buvimo vieta, laikas ir prieigos teisės.

Autorių sukurta bevielio tinklo prieigos architektūra buvo panaudojama bankininkystės reglamentavimo ir priežiūros agentūroje (angl. „Banking Regulation and Supervision Agency (BRSA)“). Aprašyta sistema buvo sėkmingai įdiegta ir naudojama daugiau nei metus.

Sukurtos sistemos architektūriniai sprendimai atsako į bevielio tinklo specifikos, centralizuoto autentifikavimo ir autorizavimo klausimus, tačiau sistemoje operuojama vieninteliu vietos informacijos požymiu – vartotojo potinklio IP adresu, tačiau plačiau neanalizuojami tokie vietos informacijos požymiai kaip taškas ar zona, neaptariami vietos informacijos gavimo iš trečiųjų šalių klausimai ir su jais susiję sistemos procesai [21].

2.2.2. Vietos ir laiko informacijos gavimo būdai ir priemonės

Visi aukščiau minėti metodai naudoja vietos informaciją. Nors vartotojo buvimo vietos nustatymas nėra šio darbo tikslas, tačiau šis aspektas taip pat yra svarbus. Todėl tam, kad parodyti kaip yra gaunama vartotojo buvimo vieta trumpai aptarsime vietos informacijos gavimo būdus.

Šiuo metu egzistuoja eilė vietos nustatymo technologijų. Vietos nustatymo technologijose svarbiausia yra ieškomo prietaiso padėtis (jo buvimo koordinatės), nes ji leidžia gauti informaciją reikalinga nustatyti prietaiso buvimo vietą (pvz., patalpą, miestą, gatvę ir t.t.). Palydovinių sistemų (GPS, „Galileo“, GLONASS) plėtojimas nuolat vyksta tobulinant tikslumą, tačiau daugumai paslaugų/programų jau pakanka ir esamo tikslumo. Rinkodaros požiūriu pozicionavimo poreikis/populiarumas patalpų viduje nuolat auga, suteikia vertingas panaudojimo perspektyvas oro uostose, dideliuose prekybos centruose, įvairiose valstybinėse organizacijose. „Google“ 2011 m. lapkritį pristatė pirmąją žemėlapio versiją su pozicionavimo patalpų viduje galimybėmis. Kitos pasaulinės organizacijos, taip pat plečiasi ir atlieka įvairius tyrimus šioje srityje. Tokia pasaulinių organizacijų veikla (susidomėjimas pozicionavimu patalpų viduje) parodo, kad ši sritis yra perspektyvi ir naudinga dabartinei rinkai [22].

Toliau yra pateikiamos populiariausios vietos nustatymo technologijos (1 lentelė):

Lentelė 1. Populiariausios vietos nustatymo technologijos

<table>
<tr><th rowspan="2">Veikimo pagrindas</th><th colspan="2">Technologija</th></tr>
<tr><th>Pastato viduje</th><th>Lauko / esantis lauke</th></tr>
<tr><td>Tinklo pagrindu
(angl. „Network based“)</td><td colspan="2">„Cell-ID“</td></tr>
<tr><td></td><td colspan="2">„Cell Tower-Triangulation“</td></tr>
<tr><td>Reikalaujantis tik prietaiso/telefoną
(angl. „Handset based“)</td><td rowspan="2"></td><td>GPS</td></tr>
<tr><td>Hibridinės
(angl. „Hybrid“)</td><td>A-GPS</td></tr>
<tr><td>Paremta infrastruktūra
(angl. „Infrastructure</td><td colspan="2">Belaidis tinklas (angl. Wi-Fi)</td></tr>
</table>

based“)	„Bluetooth“	

Toliau trumpai apžvelgsime kiekvieną 1 lentelėje paminėtą technologiją.

2.2.2.1. „Cell-ID“

„Cell-ID“ (Cell-of-origin) – yra paprasčiausias korinio ryšio lokalizacijos metodas. Tinklo ryšio aprėpties zona suskaidoma į celes, tada mobiliojo ryšio operatorius nustato/apskaičiuoja įrenginio buvimo vietą, panaudodamas bazinių mobiliojo ryšio stotelių signalų stiprumus, prie kurių vartotojas yra prisijungęs. Tokiu būdu vartotojo buvimo vieta nustatoma celės tikslumu [22], [23].

2.2.2.2. GPS sistema (angl. Global Positioning System)

GPS sistema (angl. Global Positioning System) – palydovinė padėties nustatymo sistema, kontroliuojama JAV Gynybos departamento. Sistemą sudaro 31 palydovas (2012 m. informacija). Yra ir kitų alternatyvių projektų („Galileo“, GLONASS, „Beidou“), bet labiausiai pasaulyje paplitusi yra ši sistema. Sistema nustato prietaiso buvimo vietą, apskaičiuojant signalų skirtumus. Tam reikalingi mažiausiai 3 palydovų signalai. Vėliau yra panaudojamos matematinės formulės (angl. „Trilateration“), siekiant nustatyti (apskaičiuoti) naudotojo (įrenginio) padėtį, greitį, aukštį virš jūros lygio. Nepaisant puikaus tikslumo GPS turi ir trūkumų: tikslumas priklauso nuo matomų palydovų skaičiaus, pasiruošimo laikas gali būti gana ilgas, GPS neveikia patalpose arba kai palydovai yra nematomoje zonoje (šešėlyje) [22], [24].

2.2.2.3. „Assisted GPS“ (A-GPS)

A-GPS – susieja (papildo) palydovinį pozicionavimą su GSM ryšio operatoriaus vietos nustatymu. A-GPS, lyginant su GPS, sumažina vietos nustatymo laiką ir energijos suvartojimą, taip pat gali užtikrinti geresnį tikslumą. Tačiau reikalauja, kad mobiliojo ryšio stotelėse būtų įrengti GPS moduliai, taip pat šis metodas padidina stotelių apkrovimą [22], [25].

2.2.2.4. Belaidis tinklas (angl. Wi-Fi) ir „Bluetooth“

Visuotinis Wi-Fi stotelių paplitimas leido naudoti šias technologijas naudotojo vietai nustatyti. Ši technologija naudoja panašius metodus kaip ir „Cell-ID“ metodas, tačiau panaudojant Wi-Fi ryšio prieigos taškus. Kai prietaisas aptinka Wi-Fi signalą, iš anksto įdiegta vietos nustatymo įranga nuskaito jį ir palygina su ataskaitos duomenimis (kontroliniais duomenimis iš informacinės duomenų bazės). Tada, remiantis stotelių signalo stiprumais, apskaičiuojama naudotojo buvimo vieta.

Vietos nustatymas panaudojant „Bluetooth“ veikia panašiai, tačiau reikalauja papildomo antenų tinklo [22].

2.2.2.5. Vietos nustatymo sistemos

Šiuo metu egzistuoja eilė vartotojo buvimo pastato viduje vietos nustatymo sistemų, kurios naudoja įvairias vietos nustatymo metodikas. Taip pat ir aukščiau aprašytus būdus. Visų šių sistemų vietos nustatymo: tikslumas, kaina, greitaveika ir kiti parametrai skiriasi priklausomai nuo naudojamo metodo. Kadangi tai nėra šio darbo objektas mes neaptarinėsime tokių sistemų veikimo specifikos. [27]

2.2.3. Standartizacija

Siekiant išlaikyti vientisumą ir sąveiką, tarpusavio sąveiką ir patikimumą tų sistemų, kurios labai svarbios vartotojų požiūriu, yra pristatyta keletas standartų. Audito organizacijos, kurios atsakingos už LBS (angl. „Location Based Service“) paslaugų standartizaciją, yra: „Open Mobile Alliance“ (OMA), „Open Geospatial Consortium“ (OGC). Be to, yra keletas kitų organizacijų, kurios teikia svarbius komponentus LBS standartams [22], [26], [27].

2.2.5. Vietos ir laiko informacijos panaudojimo apribojimai (privatumo klausimai)

Panaudojant vietos nustatymo technologijas, privatumo klausimai taip pat yra svarbūs, o ypač jeigu naudojama vietos ir laiko informacijos kombinacija. Kadangi vietos nustatymo technologijos dažniausiai naudojamos mobiliuose/nešiojamuose įrenginiuose, užtikrinti privatumą yra labai sudėtinga, todėl nemažai tyrimų vykdoma ir šioje srityje [28], [29]. Dažniausiai, kai kažkoks servisas ruošiasi nustatyti vartotojo buvimo vietą arba naudoja vartotojo vietos informaciją, apie tai pranešama vartotojui. Pavyzdžiui, prieš pradėdamas naudotis PĮ, vartotojas turi patvirtinti, kad jis sutinka perduoti savo vietos informaciją (arba, kad sistema galės naudoti jo vietos informacijos duomenis).

2.3. Skyriaus išvados

Literatūros analizės metu buvo:

- Susipažinta su RBAC modeliu, jo taikymo sritimi. Atlikta analizė parodė, kad RBAC modelis sėkmingai naudojamas įvairiose srityse – nuo medicinos arba organizacijos valdymo iki IT srities.
- Susipažinta su populiariausiomis ir labiausiai paplitusiomis vietos nustatymo sistemomis ir technologijomis. Vietos nustatymo sistemų ir technologijų analizė parodė, kad egzistuoja daug įvairių vartotojų įrenginių vietos nustatymo būdų. Tačiau pastato viduje vietai nustatyti labiausiai tinka „Wi-Fi“ arba „Bluetooth“ technologijomis paremti metodai, kurie dažniausiai susiję su tokiais vietos informacijos požymiais kaip taškas ir zona.

- Išnagrinėtos su RBAC modelio papildymo laiko ir vietos informacija galimybės. Atlikta analizė parodė, kad nemažai tyrimų šia kryptimi jau atlikta, įvairių autorių siūlomi skirtingi RBAC modelio praplėtimo būdai. Visgi didžioji dalis vykdytų tyrimų daugiau dėmesio skiria RBAC praplėtimams konceptualiame lygmenyje, tačiau gana mažai informacijos pateikiama kaip šie modeliai turėtų adaptuojami įvairioms aplinkoms, pavyzdžiui, funkcionavimui bevieliame tinkle, gana ribota naudojamų vietos informacijos požymių aibė.
- Nustatyta, kad išgrynintas ir apjungtas, skirtingų autorių darbuose aprašytas idėjas galima sėkmingai panaudoti kuriant centralizuotą, vietos ir laiko apribojimais praplėsto RBAC modelio pagrindu veikiantį bevielio tinklo vartotojų autorizavimo sistemos prototipą. Tokia sistema leistų autorizuoti tinklo vartotoją pagal jo buvimo vietą, ir leistų naudotis įvairiais tinklo resursais, priklausomai nuo jo (tinklo vartotojo) rolės. Atsižvelgiant į aukščiau apžvelgtus panašių sistemų prototipus, naujoje (kuriamoje) sistemoje tikslinga naudoti modulinę architektūrą, kad jos funkcionalumas būtų nesudėtingai plečiamas. Sistemoje turi būti įvertinta galimybė operuoti vietos informacijos požymiu, apibrėžiančiu tam tikrą zoną bei gauti vietos informaciją iš trečiųjų šalių. Taip pat sistemoje turi būti vertinami centralizuoto autentifikavimo ir autorizavimo aspektai.
- Sistemai keliamų reikalavimų išpildymui tikslinga panaudoti tokias technologijas kaip: „Radius“ protokolą - bendravimo su prieigos taškais užtikrinimui, RMI – užtikrins bendravimą tarp sistemos posistemių, „Hibernate“ – sistemos lankstumo, pasirenkant duomenų bazę, įgyvendinimui, „Java“ programavimo kalbą – dėl įvairių OS palaikomumo. Kuriama autorizavimo sistemos komunikacija su vietos nustatymo sistema galėtų būti organizuojama RMI technologija. Taip pat sistema privalo turėti valdymo skydą, kurio pagalba būtų galima lengvai valdyti sistemos vartotojus, jų grupes bei priskirti vartotojams galimas prisijungimo vietas (t.y. skirtingoms rolėms leisti kurti skirtingus vietos ir laiko apribojimus)

3. Projektinė dalis

Šiame skyriuje yra pateikiama sukurto sistemos prototipo architektūra. Architektūra apibrėžiama panaudojant šiuos modelius:

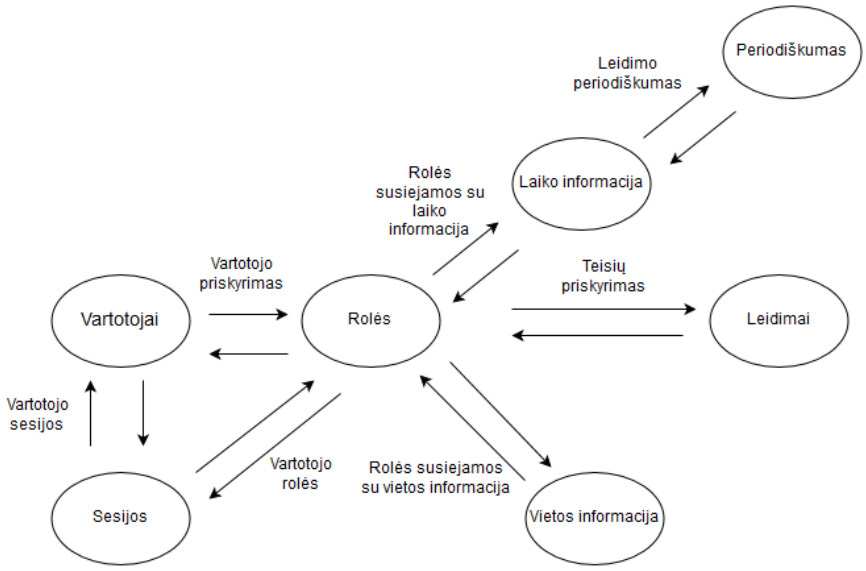
- Panaudojimo atvejų;
- Sistemos statinis modelis – sistemos paketai ir jų klasių diagramos;
- Sistemos dinaminis vaizdas – veiklos, sekų diagramos;
- Diegimo diagrama.

3.1. Sistemos apibūdinimas

3.1.1. Vietos ir laiko informacija praplėstas „RBAC“ modelis

6 pav. pavaizduotas laiko ir vietos informacija praplėstas RBAC modelis. Modelyje išskirti sekantys komponentai:

- *Vartotojas* – žmogus arba įrenginys, kuris naudosis sistema.
- *Rolė* – tai vartotojui priskiriama teisė/atsakomybė (pvz. organizacijoje atliekamo darbo funkcija).
- *Teisė* – leidimas atlikti veiksmą su tam tikru objektu.
- *Laiko informacija* – praplečia rolę laiko informacija, leidžia skirti leidimus arba apriboti naudotojo veiksmus pagal laiką.
- *Periodiškumas* – leidžia skirti periodiškus apribojimus/leidimus.
- *Lokacijos* – leidžia skirti apribojimus/leidimus pagal vartotojo buvimo vietą. Vartotojo buvimo vieta yra gaunama iš kitos sistemos, kuri praneša sukurtai sistemai patalpą, kurioje randasi vartotojas, pavyzdžiui, vartotojas A yra 302 auditorijoje. Žinant, kad 302 auditorija yra 3 aukšte, galima teigti, kad vartotojo buvimo vieta nustatoma „*x;y;z*“ koordinatėse.



6 pav. Laiko ir vietos informacija praplėstas RBAC modelis

Panaudojant tokį modelį, kiekvienam vartotojui yra priskiriama tam tikra rolė, kuri susieta su laiko bei vietos informacija. Papildomai leidimai gali būti periodiški.

Toks modelis leidžia suskirstyti vartotojus į grupes (roles), tada kiekvienai grupei galima nurodyti prieigos teises bei galimą prisijungimo vietą ir laiką, o taip pat teisių/leidimų periodiškumą. Pavyzdžiui, darbuotojai kurie priklauso grupei G1 galės naudotis tinklu iš patalpos P1, tik pirmadieniais ir penktadieniais nuo 8 val. iki 17 val., o visomis kitomis dienomis prieiga bus draudžiama. Tačiau, grupės G2 nariai galės naudotis tinklu patalpoje P1 visomis savaitės dienomis.

3.1.2. Pagrindinis sistemos funkcionalumas

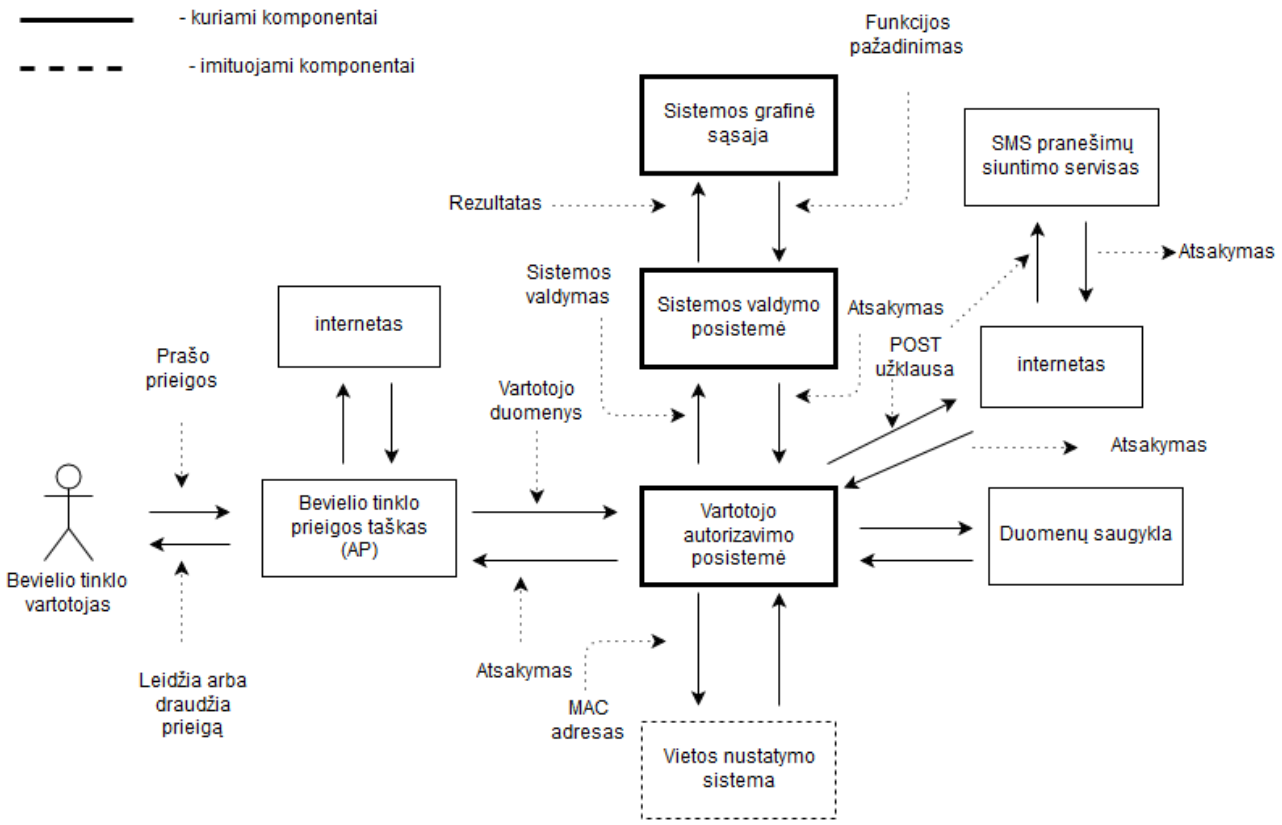
Pagrindinis sistemos funkcionalumas – sistema turi teikti centralizuotą bevielio tinklo prieigos kontrolę. Autorizuojant tinklo vartotojus atsižvelgiant į jų buvimo vietą bei prisijungimo laiką.

Sistemos veikimą trumpai galima aprašyti taip. Vartotojas, norėdamas naudotis tinklo ištekliais, kreipiasi į interneto skirstymo serverį (pvz., prieigos tašką), serveris kreipiasi į „Radius“ posistemę (sistemos autorizavimo posistemė), prašydamas prieigos. „Radius“ posistemėje pirmiausia yra apdorojami iš vartotojo gauti duomenys, tada vartotojas patikrinamas duomenų bazėje. Jei vartotojo duomenų bazėje rasti nepavyko - grąžinamas prieigos draudimo (angl. „Access-Reject“) atsakymas. Jei toks vartotojas duomenų bazėje egzistuoja - kreipiamasi į vietos nustatymo sistemą (kreipiamasi į vietos nustatymo sistemos imitatorių). Jei vietos nustatymo sistemos (imitatoriaus) grąžinta vieta bei prisijungimo laikas yra tarp vartotojui leistinų - prieiga leidžiama (angl. „Access-Accept“). Priešingu atveju prieiga draudžiama (angl. „Access-Reject“). Taip pat yra galimybė informuoti vartotoją per trumpąją „SMS“ žinutę dėl ko prieiga buvo draudžiama. Jeigu prieiga buvo sėkminga pagal poreikį ir vartotojo norą, tinklo vartotoją galima informuoti iš anksto nustatytais trumpųjų „SMS“ žinučių šablonais apie vienas arba kitas naujienas.

Šios sistemos tikslas - pagerinti bevielio tinklo vartotojų autorizavimo procesą, t.y. leisti autorizuoti bevielio tinklo vartotojus atsižvelgiant į jų buvimo vietą bei prisijungimo laiką (gaunant buvimo vietą iš kitos sistemos).

3.1.3. Sistemos veiklos kontekstas

Toliau (7 pav.) yra pateikiama veiklos konteksto diagrama, kuri pavaizduoja sistemos veiklos procesus.



7 pav. Sistemos veiklos kontekstas

Duomenų srautai tarp sistemos posistemių (valdymo posistemės grafinės sąsajos ir valdymo posistemės) siunčiami panaudojant „RMI“. Bendravimas tarp bevielio tinklo prieigos taško ir vartotojo autorizavimo posistemės bus vykdomas „Radius“ protokolu. Vartotojo autorizavimo posistemė atsakinga už gauto „Radius“ paketo apdorojimą ir tinklo vartotojų autorizavimą. Valdymo posistemė – atsakinga už vartotojų, grupių, vietos informacijos valdymą. Valdymo posistemę sudaro kliento (sistemos grafinė sąsaja) ir serverio dalys. Sistemos grafinė sąsaja (valdymo posistemės kliento dalis) ir autorizavimo posistemės yra fiziškai atskirti ir gali veikti kaip tame pačiame kompiuteryje, taip ir skirtinguose (nutolę viena nuo kitos).

3.1.4. Vartotojų charakteristikos

Sistemoje galima išskirti 2 vartotojų tipus: sistemos administratorių ir belaidžio tinklo vartotoją (žmogus, kuris nori naudotis belaidžiu tinklu). Kažkokių specifinių kompiuterinių žinių vartotojams nekeliama, kadangi sistemos administratorius galės administruoti sistemos vartotojus panaudojant grafinę sąsają. Bevielio tinklo vartotojui jokių papildomų reikalavimų nekeliama (jo savybės neaktualios), kadangi prisijungimas prie bevielio tinklo bus vykdomas standartiniais metodais. Kita vertus galima teigti, kad pagrindiniai sistemos vartotojai yra tik sistemos administratoriai, kadangi belaidžio tinklo vartotojas tiesiogiai sistemos nenaudos. Taip pat tinklo vartotojas gali nežinoti kaip jis yra autorizuojamas, prie belaidžio tinklo jis jungiasi jam įprastu būdu.

3.1.5. Vartotojų problemos

Sistemos pagrindinis tikslas yra autorizuoti tinklo vartotoją, atsižvelgiant į jo buvimo vietą (kuri yra gaunama iš vietos nustatymo sistemos, šiuo atveju iš vietos nustatymo sistemos simuliatoriaus), taip pat leisti administratoriui valdyti vartotojų leidimus (pvz. vietas, iš kurių vartotojai galės naudotis bevieliu tinklu). Administratorius turėtu nesudėtingai valdyti vartotojų leidimus, tam tikslui sistemos administravimui bus sukurta grafinė vartotojo sąsaja.

3.1.6. Pagrindiniai funkciniai reikalavimai

1. Sistema turi užtikrinti vietos informacijos gavimą iš vietos nustatymo sistemos (šiuo atveju iš vietos nustatymo sistemos imitatoriaus).
2. Sistema turi autorizuoti vartotoją/įrenginį atsižvelgiant į jo vietą ir prisijungimo laiką.
3. Sistema turi leisti priskirti sistemos vartotojams roles (priskirti vartotojus prie grupių).
4. Sistema turi leisti priskirti skirtingoms rolėms skirtingus apribojimus prisijungimui prie belaidžio tinklo resursų atsižvelgiant į rolę, vietą ir laiką.

Pagrindinių funkcinių reikalavimų detalizacija pateikiama prieduose - „8.2 .Pagrindiniai funkciniai reikalavimai“ skyriuje.

3.1.7. Pagrindiniai nefunkciniai reikalavimai sprendimui

3.1.7.1. Naudojimosi paprastumas, panaudojamumas

Bevielio tinklo vartotojo autorizavimas turi vykti standartiniu būdu, t.y. vartotojas neturėtu atlikti kažkokių papildomų veiksmų (vartotojas turi suvesti tik prisijungimo vardą ir slaptažodį).

3.1.7.2. Reikalavimai veikimo sąlygoms

Sistema turi gebėti bendrauti su įvairiais prieigos taškais (maršrutizatoriais), tam yra panaudojamas „Radius“ protokolas. Taip pat, kad gauti belaidžio tinklo vartotojo įrenginio buvimo vietą, sistema turi bendrauti su vietos nustatymo sistema.

Sistema turi veikti tiek „Windows“ tik „Linux“ aplinkoje, todėl bus panaudojama „Java“ programavimo kalbą. Tam, kad užtikrinti nepriklausomumą nuo naudojamos duomenų bazės, panaudojama „Hibernate“ technologija.

3.1.7.3. Reikalavimai saugumui

Tik autorizuoti vartotojai (sistemos administratoriai) gali prieiti prie sistemos valdymo skydo ir vidines, sistemoje išsaugotos informacijos. Užtikrinti sistemos prototipo būsenos stebėjimą, naudojant vykdomų veiksmų sekimą, rašant įvykius į įvykių (angl. „log“) failą.

3.2. Panaudotos technologijos

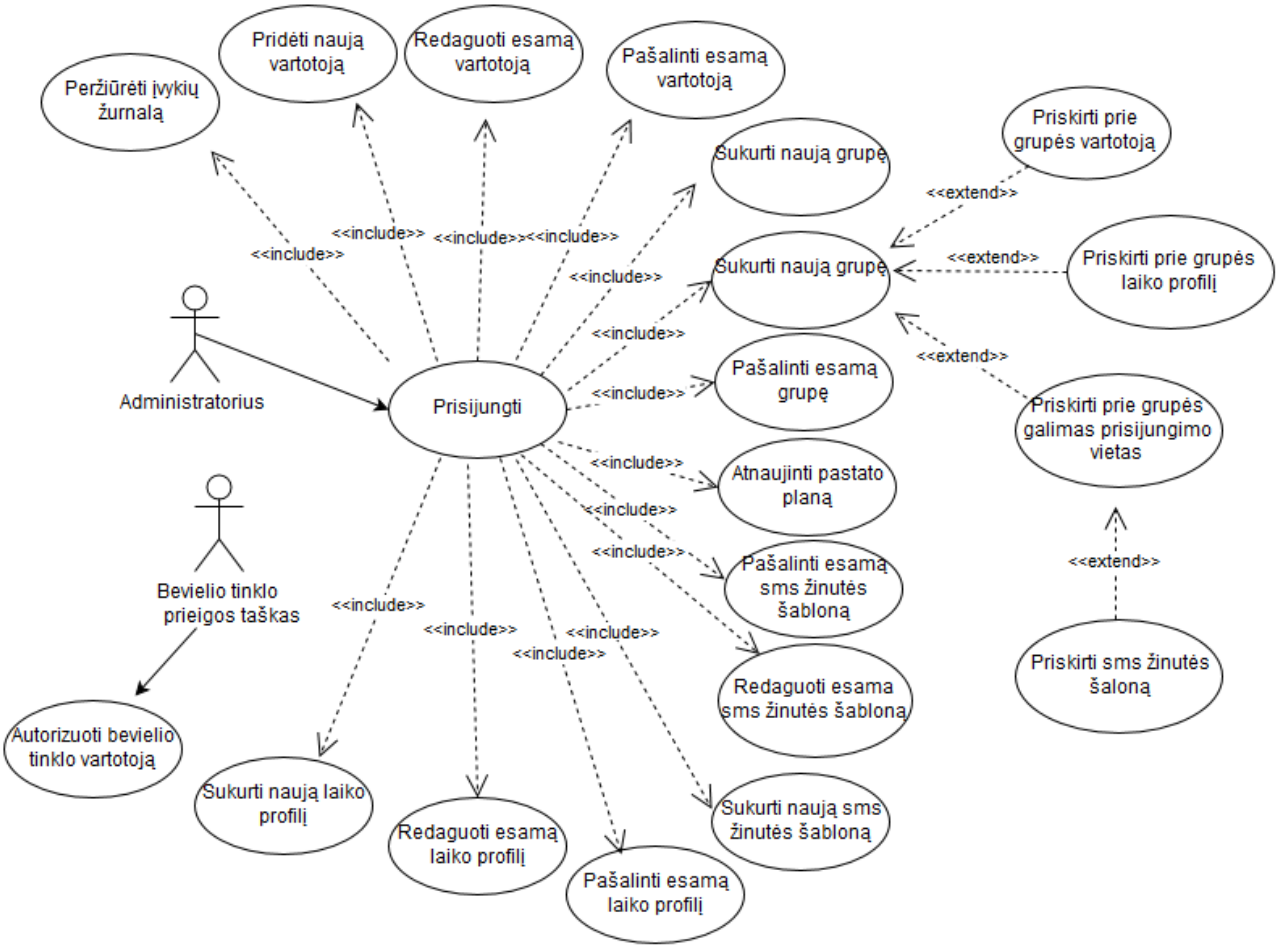
Architektūros tikslai ir apribojimai:

- Reikia užtikrinti, kad sistemos prototipas galėtu bendrauti su įvairių gamintojų maršrutizatoriais, todėl bendravimui bus panaudojimas „Radius“ protokolas.
- Sistemos prototipo architektūra turi būti parenkama taip, kad būtų galima lengviau išplėsti ar prijungti naujus komponentus.

Kuriant sistemos prototipą atsižvelgiant į aukščiau iškeltus tikslus ir apribojimus buvo naudojamos sekančios technologijos:

- „Java“ programavimo kalba (nepriklausomumas nuo naudojimo platformos).
- „Hibernate“ – užtikrina lankstumą duomenų bazės pasirinkime, taip pat esant reikalui leidžia paprasčiau migruoti prie kitos DB.
- „Java RMI“ - užtikrina bendravimą tarp sistemos posistemių.
- TinyRadius biblioteka – užtikrina „Radius“ protokolo palaikymą.
- Įvairus programavimo šablonai (angl. „Patterns“) - suteikia kodo lankstumą, paprastumą, išplėčiamumą (naudojamu šablonų pvz.: „DAO“, „Factory“, „Singletone“).

3.3. Panaudos atvejų diagrama



8 pav. Sistemos PA modelis

Pateiktoje aukščiau PA diagramoje (8 pav.) sistemoje galima išskirti 2 vartotojus: sistemos administratorių ir belaidžio tinklo prieigos tašką. Belaidžio tinklo vartotojas diagramoje neatvaizduotas, todėl, kad jis su sistema tiesiogiai nekomunikuoja. Sąveika vyksta per belaidžio tinklo prieigos tašką. Todėl galima teigti, kad pagrindinis (tiesioginis) sistemos naudotojas yra sistemos administratorius, kuriam yra pasiekiamas visas sistemos funkcionalumas.

Toliau pateikiamas PA aprašymas:

Lentelė 2. PA, „Prisijungti“

1. Panaudojimo atvejis: Prisijungti	
Tikslas:	Prisijungti prie valdymo posistemės.
Aktoriai:	Administratorius.
Prieš sąlygos:	Paleista sistema, atidarytas prisijungimo langas.
Sužadinimo sąlygos:	Spaudžiamas prisijungimo mygtukas.
Po sąlygos:	Administratorius autentifikuojamas ir gali naudotis valdymo posisteme.
Pagrindinis scenarijus:	1. Administratorius suveda vartotojo vardą ir slaptažodį. 2. Sistema patikrina duomenis. 3. Administratorius prijungiamas prie sistemos.
Alternatyvinis scenarijus:	Esant neteisingiems duomenims, sistema siūlo patikrinti duomenis ir bandyti dar kartą.

Lentelė 3. PA, „Pridėti naują vartotoją“

2. Panaudojimo atvejis: Pridėti naują vartotoją	
Tikslas:	Pridėti naują vartotoją.
Aktoriai:	Administratorius.
Prieš sąlygos:	Administratorius prisijungęs prie valdymo posistemės.
Sužadinimo sąlygos:	Spaudžiamas naujo vartotojo pridėjimo mygtukas.
Po sąlygos:	Sistemoje pridedamas naujas vartotojas.
Pagrindinis scenarijus:	1. Administratorius yra prisijungęs prie valdymo posistemės. 2. Administratorius suveda vartotojo informaciją. 3. Sistema patikrina duomenis. 4. Sukuriamas vartotojas.
Alternatyvinis scenarijus:	Esant neteisingiems duomenims, sistema siūlo patikrinti duomenis ir bandyti dar kartą.

Lentelė 4. PA, „Redaguoti esamą vartotoją“

3. Panaudojimo atvejis: Redaguoti esamą vartotoją	
Tikslas:	Redaguoti esamą vartotoją.
Aktoriai:	Administratorius.
Prieš sąlygos:	Administratorius prisijungęs prie valdymo posistemės.
Sužadinimo sąlygos:	Spaudžiamas vartotojo redagavimo mygtukas.
Po sąlygos:	Vartotojo duomenis atnaujinami.
Pagrindinis scenarijus:	1. Administratorius yra prisijungęs prie valdymo posistemės. 2. Administratorius pasirenka reikiamą vartotoją. 3. Administratorius suveda vartotojo informaciją. 4. Sistema patikrina duomenis. 5. Vartotojo informacija atnaujinama.
Alternatyvinis scenarijus:	Esant neteisingiems duomenims, sistema siūlo patikrinti duomenis ir bandyti dar kartą.

Lentelė 5. PA, „Pašalinti esamą vartotoją“

4. Panaudojimo atvejis: Pašalinti esamą vartotoją	
Tikslas:	Pašalinti sistemos DB esamą vartotoją.
Aktoriai:	Administratorius.
Prieš sąlygos:	Administratorius prisijungęs prie valdymo posistemės.
Sužadinimo sąlygos:	Spaudžiamas vartotojo pašalinimo mygtukas.
Po sąlygos:	Vartotojas pašalinamas iš sistemos duomenų bazės.
Pagrindinis scenarijus:	1. Administratorius yra prisijungęs prie valdymo posistemės. 2. Iš sąrašo pasirenkamas reikiamas vartotojas. 3. Šalinimas. 4. Parodomas rezultatas (Atnaujinamas esamų vartotojų sąrašas).
Alternatyvinis scenarijus:	Esant klaidai išvedamas apie tai informuojantis pranešimas, modifikuoti duomenis DB grąžinami atgal (angl. “roll back”).

Lentelė 6. PA, „Pridėti naują grupę“

5. Panaudojimo atvejis: Pridėti naują grupę	
Tikslas:	Pridėti naują grupę.
Aktoriai:	Administratorius.
Prieš sąlygos:	Administratorius prisijungęs prie valdymo posistemės.
Sužadinimo sąlygos:	Spaudžiamas naujos grupės sukūrimo/pridėjimo mygtukas.
Po sąlygos:	Sukuriama nauja grupė.
Pagrindinis scenarijus:	1. Administratorius yra prisijungęs prie valdymo posistemės. 2. Administratorius suveda grupės informaciją. 3. Sistema patikrina duomenis. 4. Sukuriama nauja grupė.
Alternatyvinis scenarijus:	Esant neteisingiems duomenims, sistema siūlo patikrinti duomenis ir bandyti dar kartą.

Lentelė 7. PA, „Redaguoti esamą grupę“

6. Panaudojimo atvejis: Redaguoti esamą grupę (Priskirti vartotoją / pranešimo šabloną / galimas prisijungimo vietas / laiko profilį)	
Tikslas:	Redaguoti esamą grupę.
Aktoriai:	Administratorius.
Prieš sąlygos:	Administratorius prisijungęs prie valdymo posistemės.
Sužadinimo sąlygos:	Spaudžiamas esamos grupės redagavimo mygtukas.
Po sąlygos:	Grupės duomenis atnaujinami.
Pagrindinis scenarijus:	1. Administratorius yra prisijungęs prie valdymo posistemės. 2. Administratorius pakeičia grupės informaciją (priskiria vartotoją / pranešimo šabloną / laiko profilį / galimas prisijungimo vietas). 3. Sistema patikrina duomenis. 4. Grupės informacija atnaujinama.
Alternatyvinis scenarijus:	Esant klaidai išvedamas apie tai informuojantis pranešimas, modifikuoti duomenis DB grąžinami atgal (angl. “roll back”).

Lentelė 8. PA, „Pašalinti esamą grupę“

7. Panaudojimo atvejis: Pašalinti esamą grupę	
Tikslas:	Redaguoti esamą grupę.
Aktoriai:	Administratorius.
Prieš sąlygos:	Administratorius prisijungęs prie valdymo posistemės.
Sužadinimo sąlygos:	Spaudžiamas esamos grupės pašalinimo mygtukas.
Po sąlygos:	Grupė pašalinama iš sistemos duomenų bazės.
Pagrindinis scenarijus:	1. Administratorius yra prisijungęs prie valdymo posistemės. 2. Iš sąrašo pasirenkama reikiamą grupę. 3. Šalinimas. 4. Parodomas rezultatas.
Alternatyvinis scenarijus:	Esant klaidai išvedamas apie tai informuojantis pranešimas, modifikuoti duomenis DB grąžinami atgal (angl. “roll back”).

Lentelė 9. PA, „Atnaujinti pastato planą“

8. Panaudojimo atvejis: Atnaujinti pastato planą.	
Tikslas:	Atnaujinti sistemoje išsaugotą pastato planą.
Aktoriai:	Administratorius.
Prieš sąlygos:	Administratorius prisijungęs prie valdymo posistemės.
Sužadinimo sąlygos:	Spaudžiamas pastato plano atnaujinimo mygtukas.
Po sąlygos:	Sistemoje esantis pastato planas atnaujinamas.
Pagrindinis scenarijus:	1. Panaudojant „RMI“ technologiją kreipiamasi į vietos nustatymo sistemą. 2. Sulyginami pastato planai. 3 Atliekamas skirtuminis plano kopijavimas. 4. Pakeitimai išsaugomi.
Alternatyvinis scenarijus:	Esant klaidai išvedamas apie tai informuojantis pranešimas, modifikuoti duomenis DB grąžinami atgal (angl. “roll back”).

Lentelė 10. PA, „Peržiūrėti įvykių žurnalą“

9. Panaudojimo atvejis: Peržiūrėti įvykių žurnalą.	
Tikslas:	Peržiūrėti įvykių žurnalą.
Aktoriai:	Administratorius.
Prieš sąlygos:	Administratorius prisijungęs prie valdymo posistemės.
Sužadinimo sąlygos:	Spaudžiamas įvykių peržiūrėjimo mygtukas.
Po sąlygos:	Parodomas įvykių sąrašas.
Pagrindinis scenarijus:	1. Pasirenkamas įvykių tipas. 2. Išvedamas įvykių sąrašas.
Alternatyvinis scenarijus:	Esant klaidai išvedamas apie tai informuojantis pranešimas.

Lentelė 11. PA, „Sukurti naują laiko profilį“

10. Panaudojimo atvejis: Sukurti naują laiko profilį.	
Tikslas:	Sukurti naują laiko profilį.
Aktoriai:	Administratorius.
Prieš sąlygos:	Administratorius prisijungęs prie valdymo posistemės.
Sužadinimo sąlygos:	Spaudžiamas naujo profilio sukūrimo mygtukas.
Po sąlygos:	Sukuriamas naujas laiko profilis.
Pagrindinis scenarijus:	1. Administratorius yra prisijungęs prie valdymo posistemės. 2. Administratorius suveda laiko profilio informaciją. 3. Sistema patikrina duomenis. 4. Sukuriamas naujas profilis.
Alternatyvinis scenarijus:	Esant klaidai išvedamas apie tai informuojantis pranešimas.

Lentelė 12. PA, „Pašalinti esamą laiko profilį“

11. Panaudojimo atvejis: Pašalinti esamą laiko profilį	
Tikslas:	Pašalinti esamą laiko profilį.
Aktoriai:	Administratorius.
Prieš sąlygos:	Administratorius prisijungęs prie valdymo posistemės.
Sužadinimo sąlygos:	Spaudžiamas esamo profilio pašalinimo mygtukas.
Po sąlygos:	Esamas profilis pašalinamas.
Pagrindinis scenarijus:	1.Administratorius yra prisijungęs prie valdymo posistemės. 2. Iš sąrašo pasirenkamas reikiamas profilis. 3. Šalinimas. 4. Parodomas rezultatas.
Alternatyvinis scenarijus:	Esant klaidai išvedamas apie tai informuojantis pranešimas.

Lentelė 13. PA, „Redaguoti esamą laiko profilį“

12. Panaudojimo atvejis: Redaguoti esamą laiko profilį	
Tikslas:	Redaguoti esamą laiko profilį.
Aktoriai:	Administratorius.
Prieš sąlygos:	Administratorius prisijungęs prie valdymo posistemės.
Sužadinimo sąlygos:	Spaudžiamas esamo profilio redagavimo mygtukas.
Po sąlygos:	Pakeičiama esamo profilio redaguota informacija.
Pagrindinis scenarijus:	1. Administratorius yra prisijungęs prie valdymo posistemės. 2. Administratorius pakeičia profilio informacija. 3. Sistema patikrina duomenis. 4. Profilio informacija atnaujinama.
Alternatyvinis scenarijus:	Esant klaidai išvedamas apie tai informuojantis pranešimas.

Lentelė 14. PA, „Sukurti nauja SMS žinutės šabloną“

13. Panaudojimo atvejis: Sukurti nauja SMS žinutės šabloną	
Tikslas:	Sukurti naują „SMS“ žinutės šabloną.
Aktoriai:	Administratorius.
Prieš sąlygos:	Administratorius prisijungęs prie valdymo posistemės.
Sužadinimo sąlygos:	Spaudžiamas „SMS“ žinutės šablono sukūrimo mygtukas.
Po sąlygos:	Sukuriamas naujas „SMS“ žinutės šablonas.
Pagrindinis scenarijus:	1. Administratorius yra prisijungęs prie valdymo posistemės. 2. Administratorius suveda „SMS“ žinutės šablono informaciją. 3. Sistema patikrina duomenis. 4. Sukuriamas naujas žinutės šablonas.
Alternatyvinis scenarijus:	Esant klaidai išvedamas apie tai informuojantis pranešimas.

Lentelė 15. PA, „Redaguoti esamą SMS žinutės šabloną“

14. Panaudojimo atvejis: Redaguoti esamą SMS žinutės šabloną	
Tikslas:	Pakeisti esamo šablono informaciją.
Aktoriai:	Administratorius.
Prieš sąlygos:	Administratorius prisijungęs prie valdymo posistemės.
Sužadinimo sąlygos:	Spaudžiamas „SMS“ žinutės šablono redagavimo mygtukas.
Po sąlygos:	Pakeičiama esamo šablono informacija.
Pagrindinis scenarijus:	1. Administratorius yra prisijungęs prie valdymo posistemės. 2. Administratorius pakeičia šablono informaciją. 3. Sistema patikrina duomenis. 4. Šablono informacija atnaujinama.
Alternatyvinis scenarijus:	Esant klaidai išvedamas apie tai informuojantis pranešimas.

Lentelė 16. PA, „Pašalinti esamą SMS žinutės šabloną“

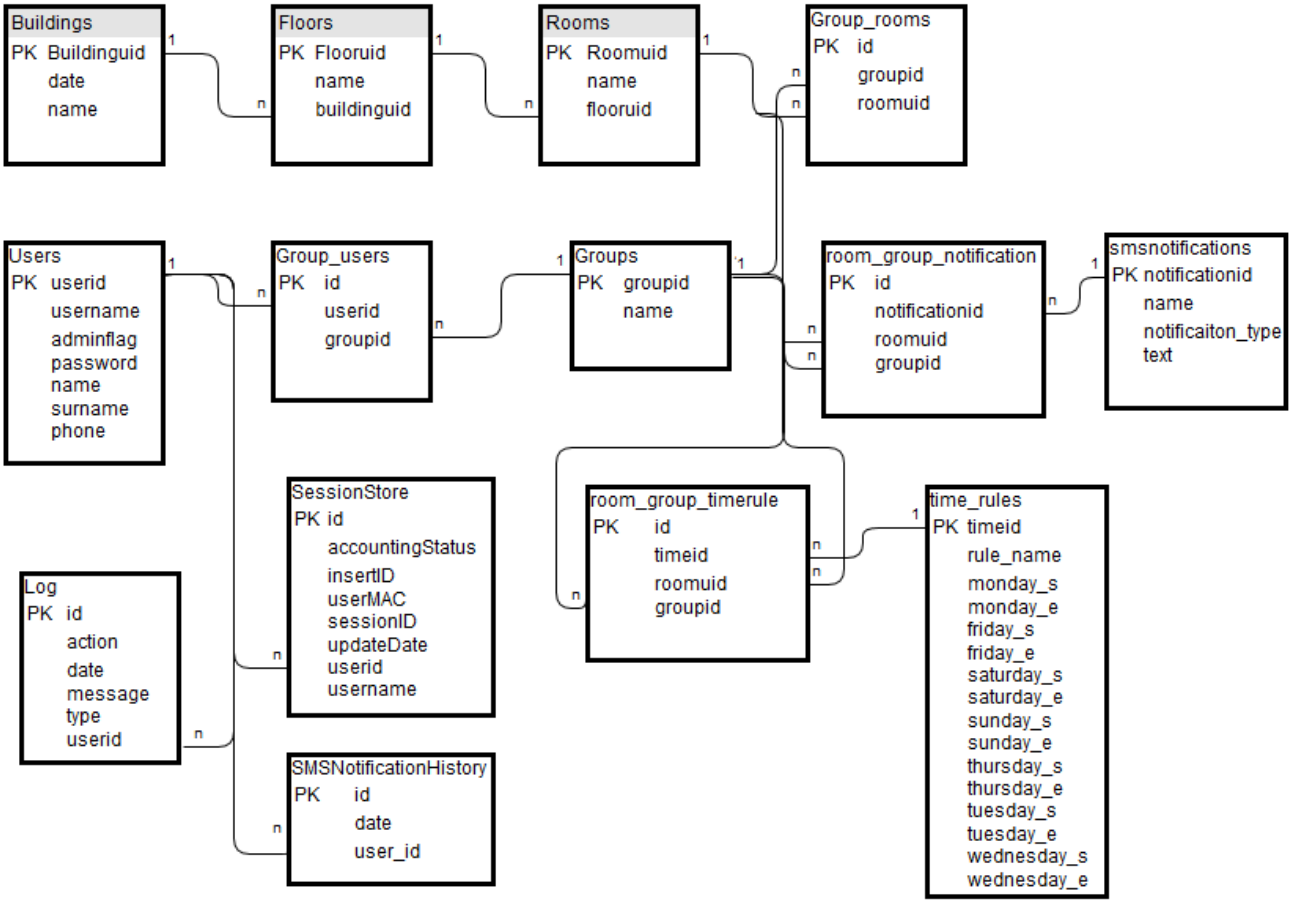
15. Panaudojimo atvejis: Pašalinti esamą SMS žinutės šabloną	
Tikslas:	Pašalinti esamą „SMS“ žinutės šabloną.
Aktoriai:	Administratorius.
Prieš sąlygos:	Administratorius prisijungęs prie valdymo posistemės.
Sužadinimo sąlygos:	Spaudžiamas „SMS“ žinutės šablono pašalinimo mygtukas.
Po sąlygos:	Esamas šablonas pašalinamas.
Pagrindinis scenarijus:	1. Administratorius yra prisijungęs prie valdymo posistemės. 2. Iš sąrašo pasirenkamas reikiamas šablonas. 3. Šalinimas. 4. Parodomas rezultatas.
Alternatyvinis scenarijus:	Esant klaidai išvedamas apie tai informuojantis pranešimas.

Lentelė 17. PA, „Autorizuoti tinklo vartotoją“

16. Panaudojimo atvejis: Autorizuoti tinklo vartotoją.	
Tikslas:	Autorizuoti tinklo vartotoją.
Aktoriai:	Maršrutizatorius.
Prieš sąlygos:	Tinklo vartotojas bando prisijungti įprastu būdu prie belaidžio interneto (per maršrutizatorių).
Sužadinimo sąlygos:	Maršrutizatorius atsiunčia (persiunčia) tinklo vartotojo duomenis.
Po sąlygos:	Siunčiamas patvirtinimo arba paneigimo atsakymas maršrutizatoriui.
Pagrindinis scenarijus:	1.Maršutizatorius naudojant „Radius“ protokolą kreipiasi į autorizavimo posistemę (siųsdamas reikiamą vartotojo/kompiuteriaus informaciją - „MAC“ adresą). 2. Autorizavimo posistemė patikrina gautą informaciją DB. 3. Kreipiamasi į vietos nustatymo sistemą, kad gauti vartotojo įrenginio buvimo vietą. 4. Patikrinamas priskirtas laiko profilis. 5. Autorizavimo posistemė siunčia maršrutizatoriui atsakymą. 6. Priklausomai nuo serverio nustatymu belaidžio tinklo vartotojui išsiunčiamas „SMS“ žinutės pranešimas (jo grupei priskirtas „SMS“ žinutės šablonas).
Alternatyvinis scenarijus:	-

3.4. Duomenų modelis ir jo elementų žodynas

Toliau (9 pav.) pateikiamas sistemos duomenų bazės modelis:



9 pav. Sistemos duomenų modelis

Žemiau (18 lentelė) pateikiamas trumpas duomenų bazės lentelių aprašymas.

Lentelė 18. Duomenų bazės lentelių aprašymas

Lentelės pavadinimas	Aprašymas
Buildings	„Buildings“ lentelė - skirta saugoti iš vietos nustatymo sistemos parsisiunčiamus pastatų objektus.
Floors	„Floors“ lentelė – skirta saugoti pastatų aukštus.
Rooms	„Rooms“ lentelė – skirta saugoti aukštų kambarius.
Group_rooms	„Group_rooms“ lentelė – skirta saugoti prie grupės priskirtus kambarius (iš kurių grupės nariai galės naudotis bevieliu ryšiu).
Groups	„Groups“ lentelė – skirta saugoti vartotojų grupes.
Group_users	„Group_users“ lentelė – skirta saugoti prie grupės priskirtus vartotojus.
Users	„Users“ lentelė – skirta saugoti sistemos vartotojus.
Log	„Log“ lentelė – skirta saugoti įvykių žurnalo įrašus.

SessionStore	„SessionStore“ lentelė – skirta saugoti vartotojo prisijungimo sesijas.
SMSNotificationHistory	„SMSNotificationHistory“ lentelė – skirta saugoti išsiustų pranešimų istoriją.
TimeRules	„TimeRules“ lentelė – skirta saugoti laiko profilius.
SMSNotifications	„SMSNotifications“ lentelė – skirta saugoti laiko žynučių šablonus.
Room_group_notification	„Room_group_notification“ lentelė – skirta saugoti prie patalpos priskirtą pranešimą.
Room_group_timeRule	„Room_group_timeRule“ lentelė – skirta saugoti prie patalpos priskirtą laiko profilį.

3.5. Komunikuojančios sistemos

Sukurtas sistemos prototipas (7 pav.) komunikuoja su belaidžio tinklo vartotojo vietos nustatymo sistemos imitatoriumi ir servisu, kuris geba siusti „SMS“ trumpąsias žinutes. Autorizavimo sistema išsiuntę vietos nustatymo sistemos imitatoriui belaidžio tinklo vartotojo įrenginio MAC adresą, turi gauti jo fizinę buvimo vietą. Bendravimas su „SMS“ žinučių išsiuntimo servisu realizuojamas panaudojant „HTTP POST“ užklausas. Sistema siunčia „POST“ užklausą su „SMS“ žinutės tekstu bei numeriu kuriam reikia išsiusti žinutę.

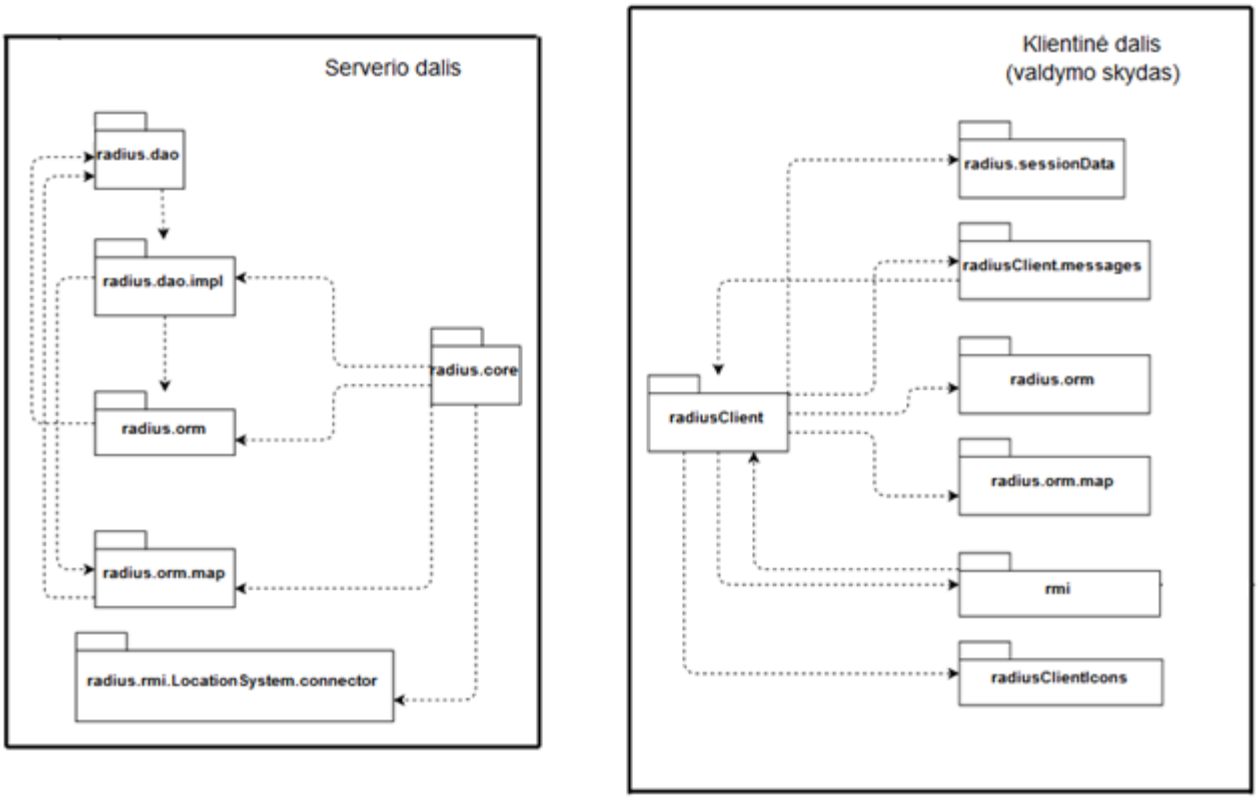
3.6. Sistemos architektūros modelis

3.6.1. Sistemos statinis vaizdas

Sistemoje galima išskirti serverio ir kliento dalis. Serverio dalis atsakinga už „Radius“ paketo apdorojimą ir tinklo vartotojų autorizavimą. Taip pat serverio dalyje yra vykdomi iš kliento siunčiamos komandos (panaudojant „RMI“ technologija).

Valdymo skydas (kliento dalis) – atsakinga už vartotojų, grupių, vietos informacijos valdymą. Panaudojant valdymo skydo grafinę sąsają sistemos administratorius gali kreiptis į serveryje realizuotus metodus.

Toliau (10 pav.) yra pateikiama sistemos apibendrinta paketų diagrama (susidedanti iš serverio ir valdymo skydo dalių):



10 pav. Sistemos paketų diagramos

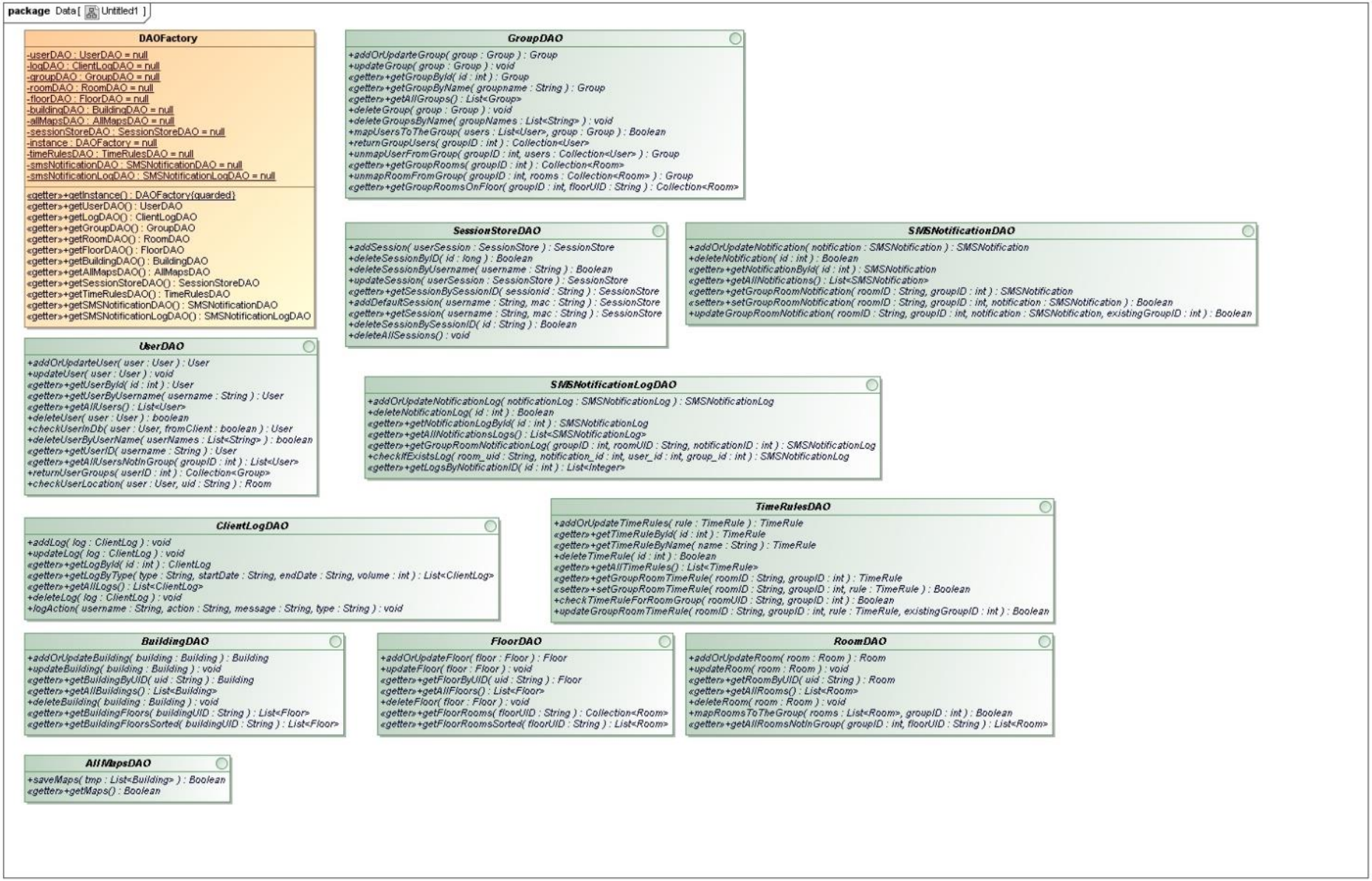
Toliau („3.7 Serverio dalies paketų detalizavimas“ skyriuje) trumpai aprašyti ir detalizuoti sistemos paketai.

3.6.2 Serverio dalies paketų detalizavimas

3.6.2.1. Paketo “radius.dao“ detalizacija

Paketas skirtas DAO (angl. „Data Access object“) sąsajom (angl. „interface“) saugoti, panaudojant šias sąsajas vyksta komunikavimas tarp valdymo skydo ir serverinės sistemos dalies. Tam, kad valdymo skydas galėtu tinkamai funkcionuoti, sąsajos turi būti importuotos į valdymo skydą bei sutapti su serveryje esančiomis. Taip pat toks realizavimas leidžia atskirti žemo lygio duomenų priėjimo logiką nuo aukšto lygio logikos. Visos šios sąsajos yra realizuojamos pakete „radius.dao.impl“ esančiomis klasėmis. Paketas sąveikauja su „radius.dao.impl“ pakete esančiomis realizacijomis.

Klasė „*DAOFactory*“ skirtą kurti arba atiduoti sąsajų objektus. Visos kitos šio paketo klasės yra sąsajos. Klasės pavadinimas atitinka pagrindinį funkcionalumą, su kuriuo ši sąsaja yra susiję. Pavyzdžiui, sąsaja „*GroupDAO*“ apima pagrindinius veiksmus susijusius su vartotojų grupėmis. Toliau yra pateikiamas paketo turinys:

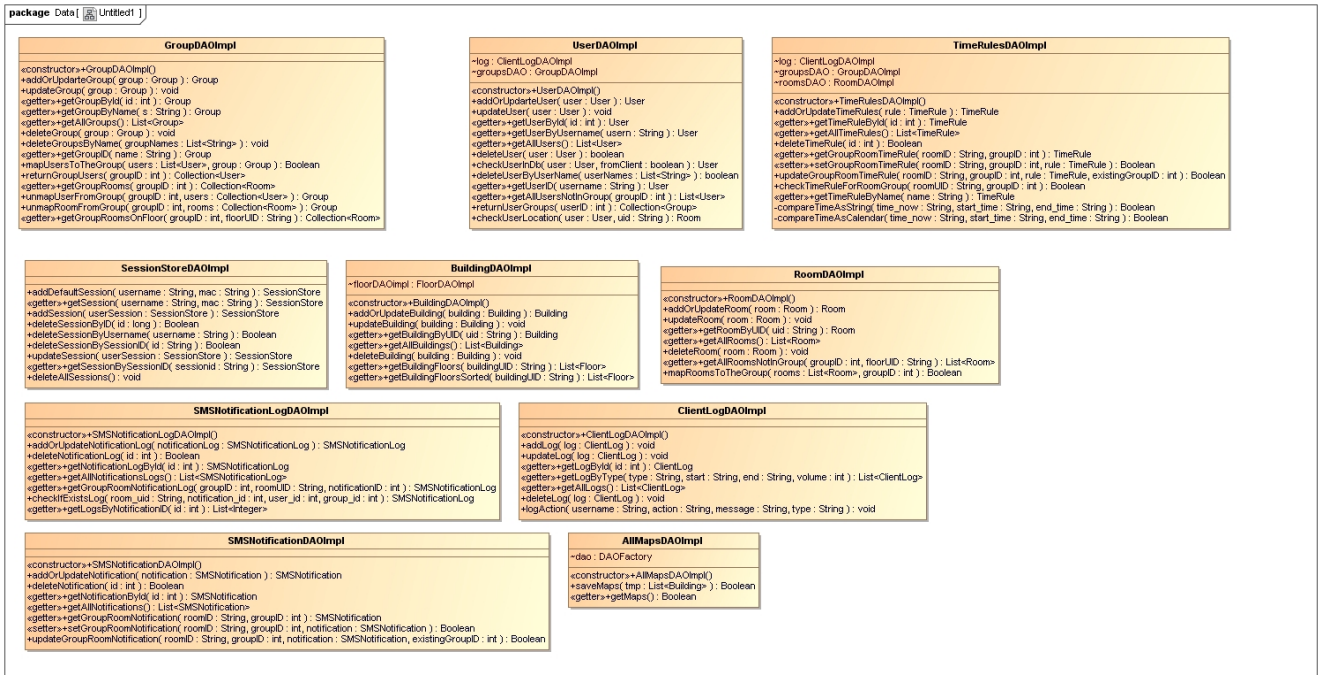


11 pav. Paketo „radius.dao“ sudėtis

3.6.2.2. Paketo „ radius.dao.impl“ detalizacija

Paketas skirtas „radius.dao“ paketo sąsajom realizacijoms saugoti. Šiame pakėtę pateiktos klasės yra atsakingos realizuoti „radius.dao“ paketo sąsajų metodus. Pavyzdžiui, klasė „*GroupDAOImpl*“, klasė atsakinga realizuoti visus metodus, kurie apibrėžti „*GroupDAO“* sąsajoje. Paketas sąveikauja su „radius.orm“ bei „radius.orm.map“ paketais.

Toliau pateikiama paketo sudėtis:

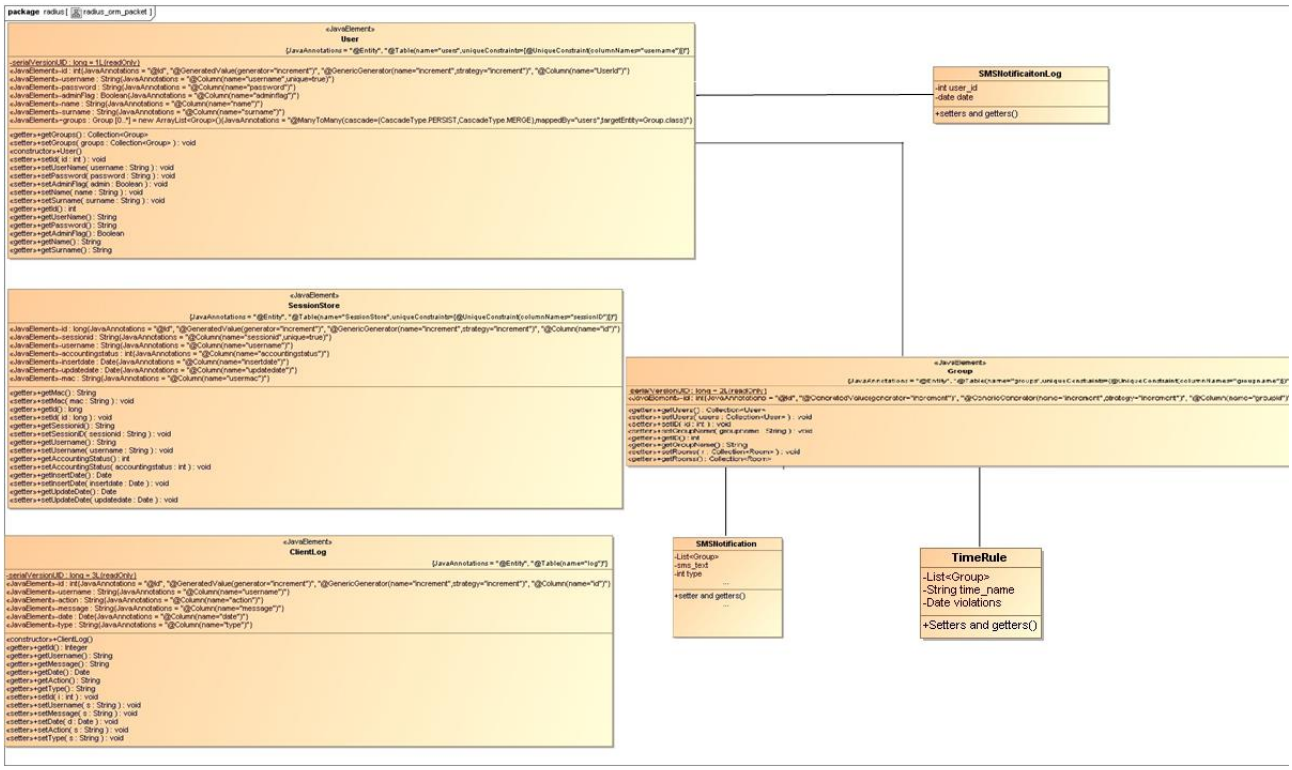


12 pav. Paketo „radius.dao.impl“ sudėtis

3.6.2.3. Paketo „radius.orm“ detalizacija

Paketas skirtas saugoti duomenų objektus, kurie atvaizduoja reliacinės DB lenteles. Pavyzdžiui, klasė „*User*“ atsakinga atvaizduoti duomenų bazės lentelę „*User*“ į sistemos objektą/klasę (klasės kintamieji atitinka duomenų bazės „*User*“ lentelės atributus). Paketas sąveikauja su „*radius.dao*“ ir „*radius.core*“ paketais.

Toliau pateikiama paketo sudėtis:

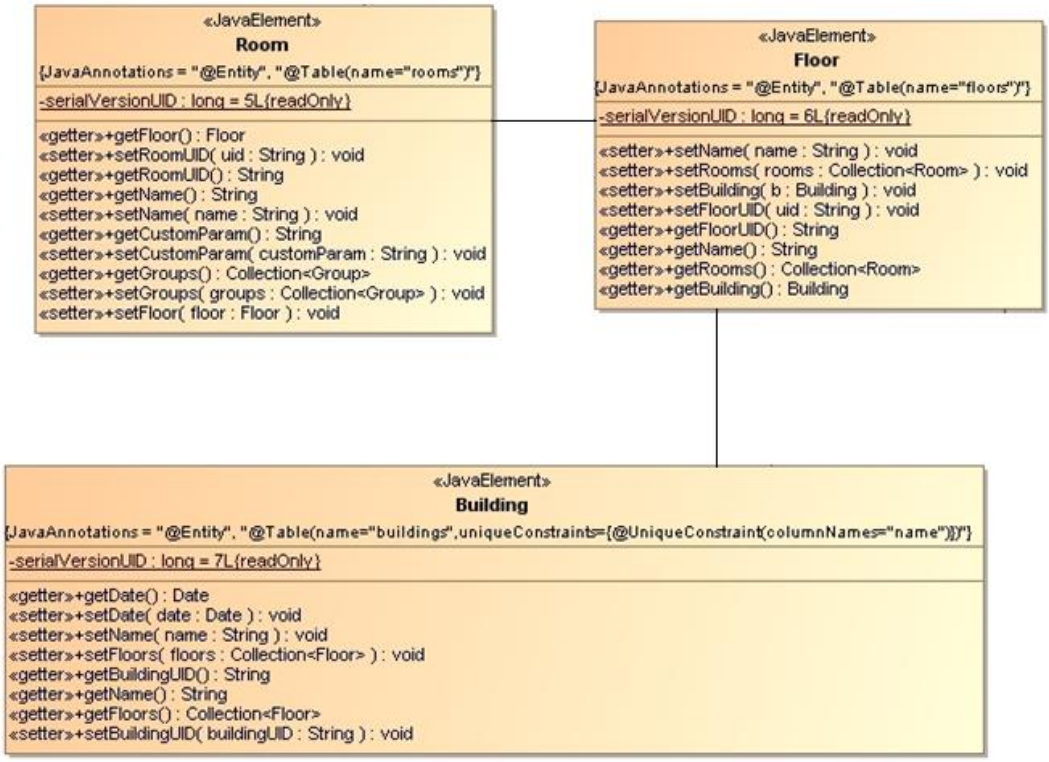


13 pav. Paketo „radius.orm“ sudėtis

3.6.2.4. Paketo „radius.orm.map“ detalizacija

Paketas skirtas saugoti pastato plano duomenų objektus, kurie atvaizduoja reliacinės DB lenteles. Pavyzdžiui, klasė „*Room*“ atsakinga atvaizduoti duomenų bazės lentelę „*Room*“ į sistemos objektą/klasę (klasės kintamieji atitinka duomenų bazės „*Room*“ lentelės atributus). Paketas sąveikauja su „*radius.dao*“ ir „*radius.core*“ paketais.

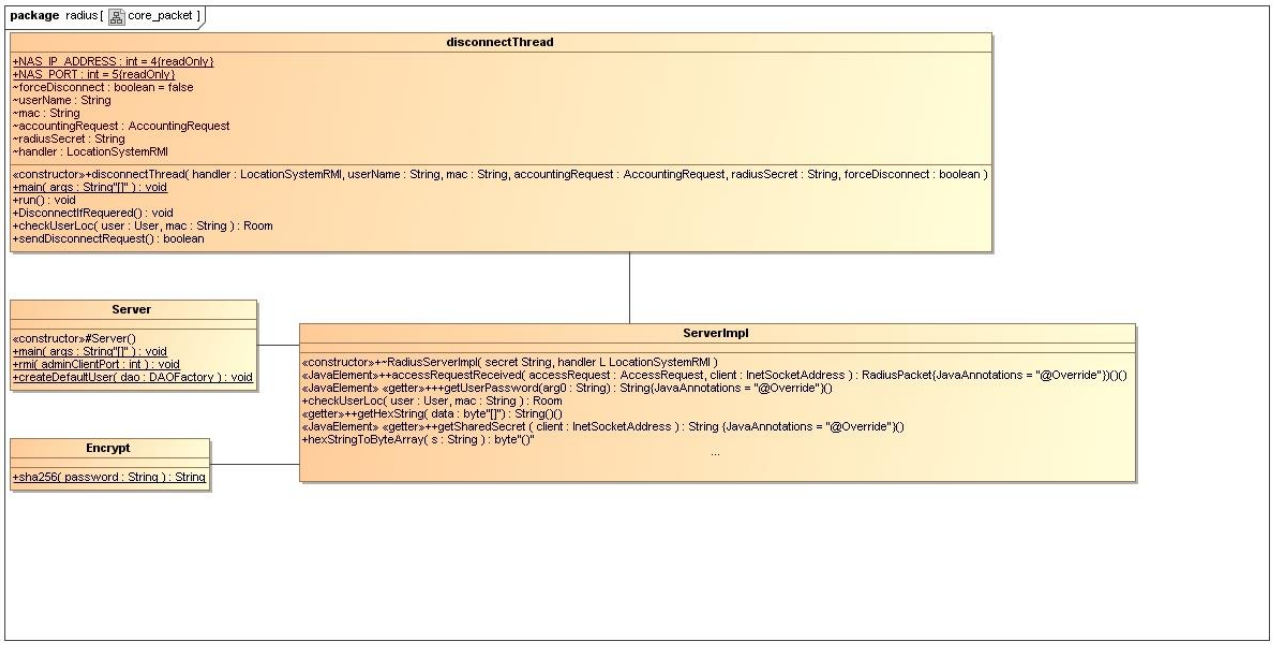
Toliau pateikiama paketo sudėtis:



14 pav. Paketo „radius.orm.map“ sudėtis

3.6.2.5. Paketo „radius.core“ detalizacija

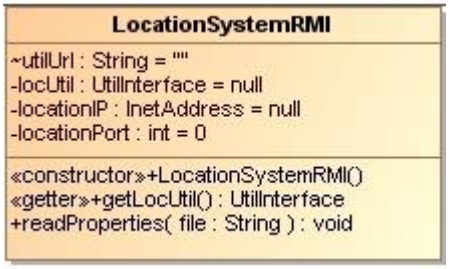
Paketas skirtas saugoti serverio paleidimo klasę ir susijusias klases. Klasė „*ServerImpl*“ skirta įgyvendinti metodus susijusius su „Radius“ paketo apdorojimu/formavimu, bei serverio paleidimu. Taip pat klasė įgyvendina metodus skirtus apdoroti gautą „Radius“ paketą, bei pagrindinį serverio paleidimo metodą. Klasė „*Server*“ - tai pagrindinė serverio klasė atsakinga už sistemos serverio paleidimą. Klasė „*DisconnectThread*“ skirta formuoti atjungimo nuo tinklo paketą. Toliau pateikiama paketo sudėtis:



15 pav. Paketo „radius.core“ sudėtis

3.6.2.6. Paketo „radius.rmi.LocatiosSystem.connector“ detalizacija

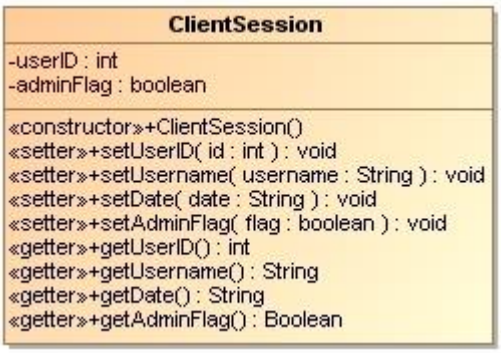
Paketas skirtas saugoti klasę/klases skirtas užtikrinti komunikavimą su vietos nustatymo sistemos imitatoriumi. Klasė „*LocationSystemRMI*“ atsakinga užtikrinti komunikavimą su vietos nustatymo sistemos imitatoriumi. Paketas sąveikauja su „radius.core“ paketu. Toliau pateikiama paketo sudėtis:



16 pav. Paketo „radius.rmi.LocationSystem.connector“ sudėtis

3.6.2.7. Paketo „radius.SessionData“

Paketas skirtas saugoti reikalingą informaciją susijusia su aktyvia vartotojo sesija. Klasė „*ClientSession*“ skirta saugoti reikiamus duomenys susijusius su aktyvaus vartotojo sesija. Toliau pateikiama paketo sudėtis:



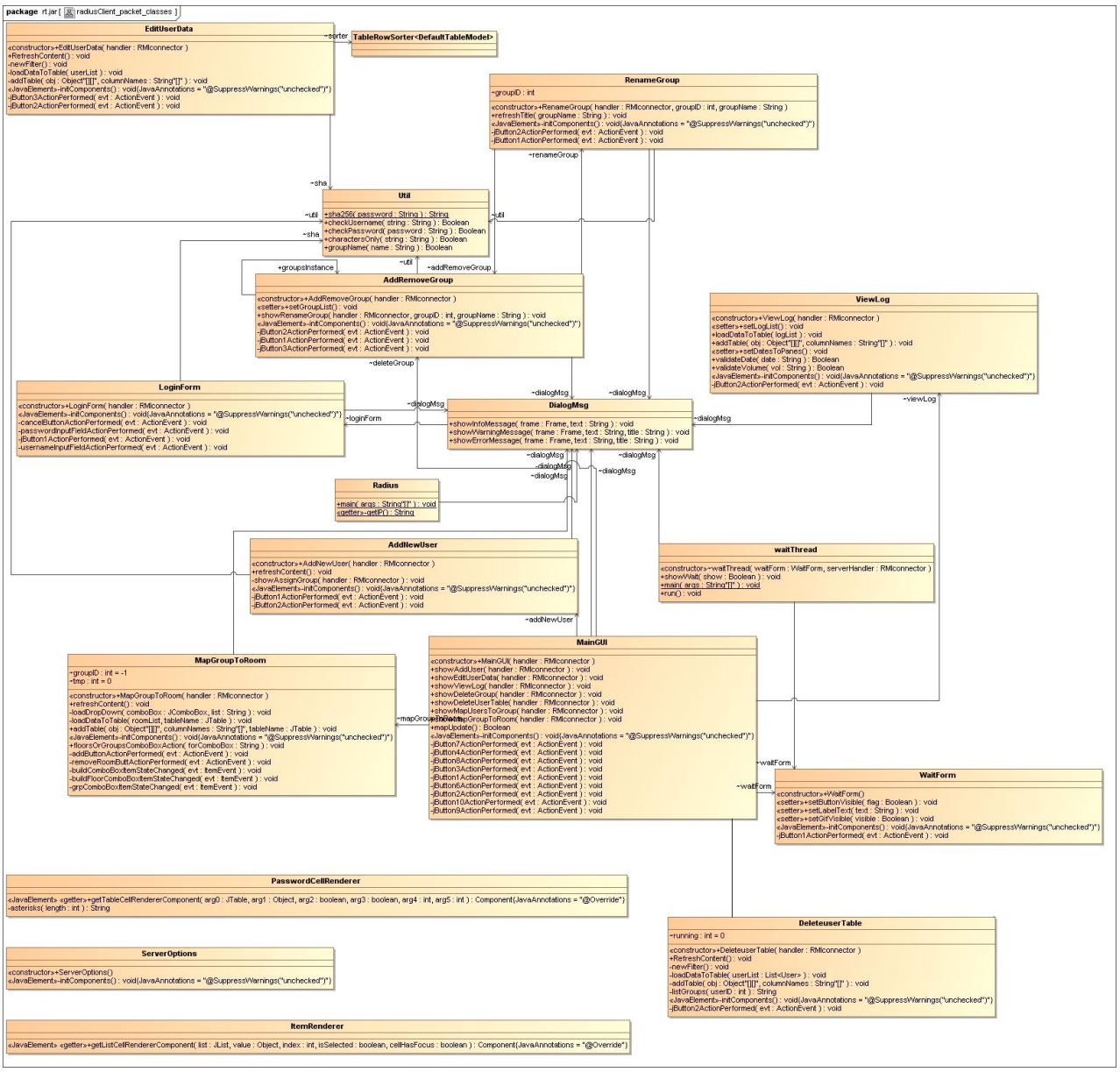
17 pav. Paketo „radius.SessionData“ sudėtis

3.6.3. Kliento dalies paketų detalizavimas

Toliau šiame skyriuje pateikiami sistemos kliento dalies paketų detalizavimas. Paketai, kurių detalizacija čia nepateikiama, yra labai panašus arba atitinka sistemos serverio dalies paketus.

3.6.3.1. Paketo „radiusClient“ detalizacija

Paketas skirtas saugoti sistemos kliento dalies paleidimo klasę ir susijusias klases. Taip pat šiame pakete saugomos klasės, kurios realizuoja vartotojui matomas grafines formas.



18 pav. Paketo „radiusClient“ sudėtis

3.6.4 Sistemos dinaminis vaizdas

3.6.4.1 Veiklos diagramos

Toliau šiame skyriuje pateikiami PA veiklos diagramos. Diagramos, kurios nepateikiamos yra intuityviai suprantamos arba labai panašios į pateiktas.

3.6.4.2. Prisijungti prie sistemos grafinės vartotojo sąsajos (valdymo skydo)

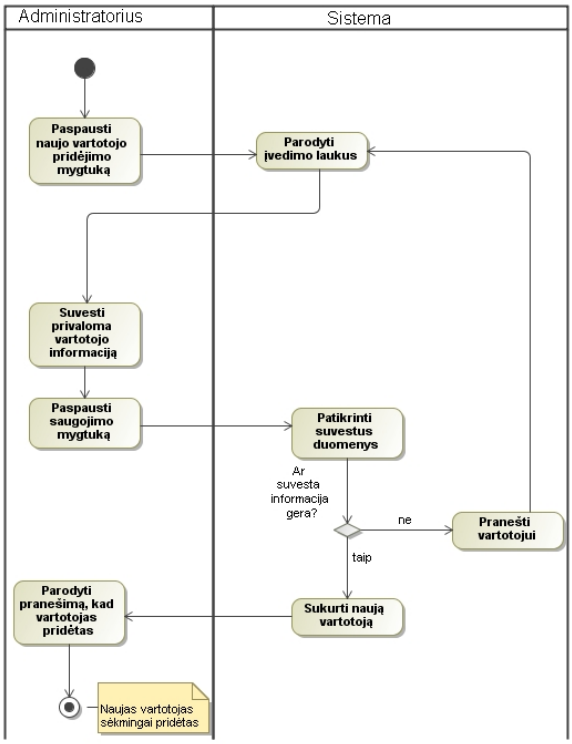
Tam, kad prisijungti prie sistemos valdymo skydo (grafinės vartotojo sąsajos), sistemos administratorius iš pradžių suveda prisijungimo duomenys. Šie duomenis yra patikrinami, jeigu tai yra tinkami duomenys, administratorius įleidžiamas į valdymo skydą. Prisijungus iškart yra matomas administratoriui pasiekiamas funkcionalumas. Detaliau šis procesas pavaizduotas žemiau:

19 pav. „Prisijungti prie valdymo posistemės“ veiklos diagrama

3.6.4.3. Pridėti naują vartotoją

Tam, kad pridėti naują vartotoją sistemos administratorius turi atlikti prisijungimo veiksmą pavaizduota aukščiau (19 pav.). Sistemos valdymo skyde spaudžiamas vartotojo pridėjimo mygtukas, įvedami būtini duomenys apie vartotoją. Jeigu suvesti vartotojo duomenys atitinka duomenų įvedimo šabloną - vartotojas pridedamas. Apie sėkmingą veiksmą parodomas pranešimas. Jeigu administratoriaus

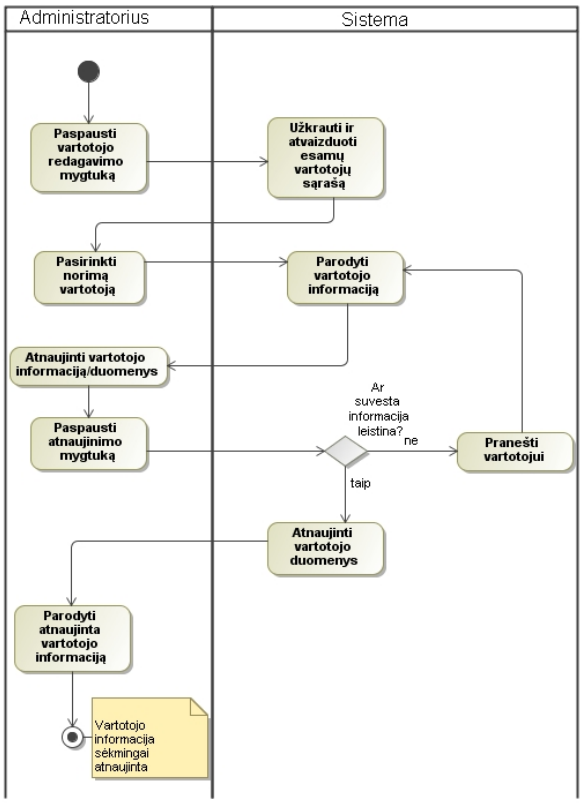
suvesta informacija apie vartotoją yra netinkama, sistema praneša apie tai prašydama įvesti tinkamus duomenys. Detaliau šis procesas yra pavaizduotas žemiau:



20 pav. „Pridėti naują vartotoją“ veiklos diagrama

3.6.4.4. Redaguoti esamą vartotoją

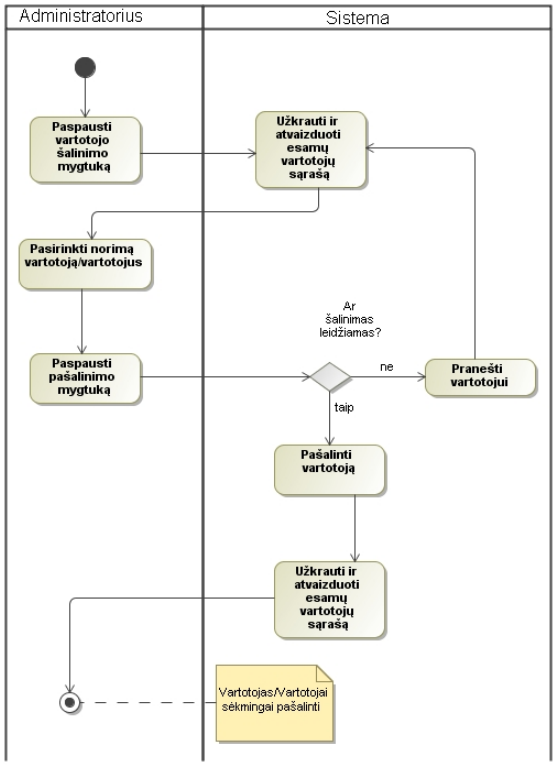
Tam, kad redaguoti esamą vartotoją sistemos administratorius turi atlikti prisijungimo veiksmą (19 pav.). Sistemos valdymo skyde spaudžiamas vartotojo redagavimo mygtukas, administratorius pasirenka norimą vartotoją ir atnaujina jo duomenys. Jei duomenys yra tinkami, tai sistema parodo atnaujintą vartotojo informaciją. Priešingu atveju išvedamas pranešimas apie blogai įvesta informaciją. Detaliau šis procesas yra pavaizduotas žemiau:



21 pav. „Redaguoti esamą vartotoją“ veiklos diagrama

3.6.4.5. Pašalinti esamą vartotoją

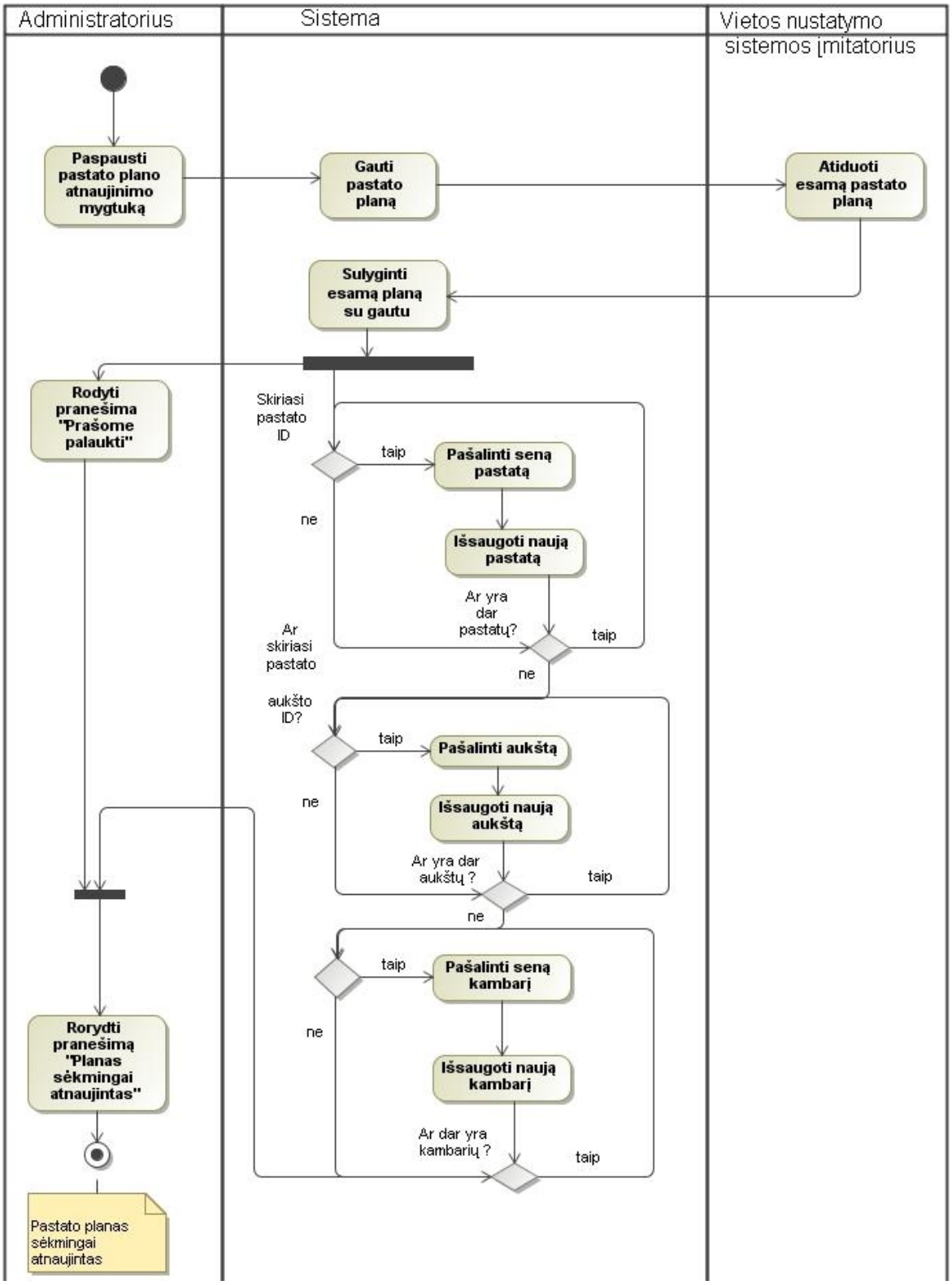
Tam, kad pašalinti esamą vartotoją sistemos administratorius turi atlikti prisijungimo veiksmą (19 pav.). Sistemos valdymo skyde spaudžiamas vartotojo pašalinimo mygtukas. Pasirenkamas norimas vartotojas arba vartotojai ir spaudžiamas pašalinimo mygtukas. Jeigu šalinimas draudžiamas apie tai pranešama, priešingu atveju vartotojas pašalinamas ir atvaizduojamas atnaujintas sistemos vartotojų sąrašas. Detaliau šis procesas pavaizduotas žemiau:



22 pav. „Pašalinti esamą vartotoją“ veiklos diagrama

3.6.4.6. Atnaujinti pastato planą

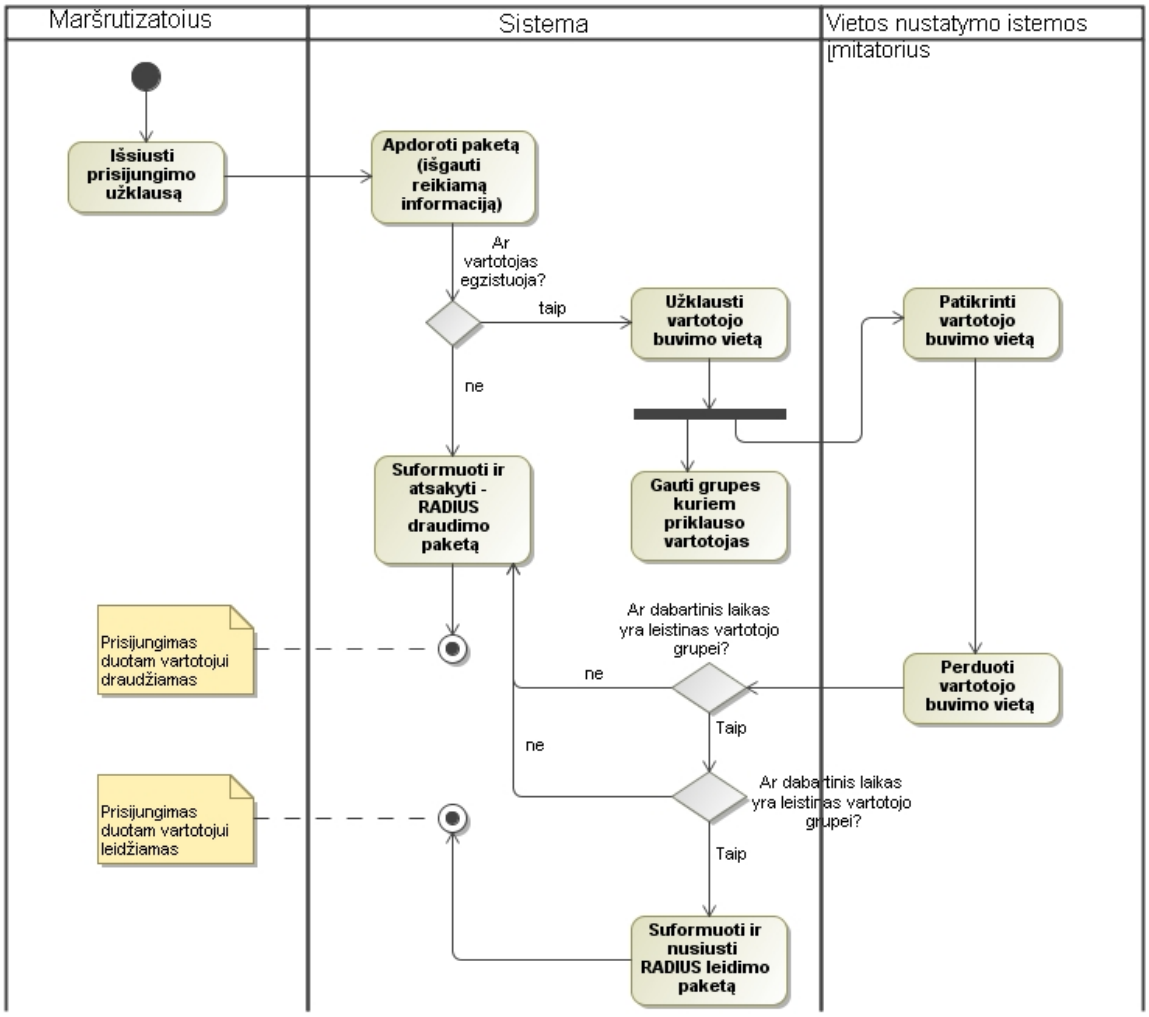
Tam, kad atnaujinti pastato planą sistemos administratorius turi atlikti prisijungimo veiksmą (19 pav.). Sistemos valdymo skyde spaudžiamas pastato plano atnaujinimo mygtukas. Iš vietos nustatymo sistemos (šiuo atveju iš vietos nustatymo sistemos imitatoriaus) parsiunčiamas pastato planas, sistemoje išsaugotas ir parsiųstas planas yra sulyginami ir esant reikalui pasenę objektai yra pašalinami, o nauji išsaugomi. Pastato plano objektai parsiunčiami pastato objekto pavidalu (abstrakčiausias vietos objektas), o tada „išvyniojami“ iki patalpos lygio (detaliausias vietos objektas). Detaliau šis procesas yra pavaizduotas žemiau:



23 pav. „Atnaujinti pastato planą“ veiklos diagrama

3.6.4.7. Tinklo vartotojo autorizacija

Detalesnis tinklo vartotojo aprašymas yra pateiktas panaudojant sekų diagramą „3.9.2.1 Tinklo vartotojo autorizacija“ skyriuje. Žemiau (24 pav.) pateikiamas apibendrintas šio proceso vaizdas:



24 pav. „Tinklo vartotojo autorizavimas“ veiklos diagrama

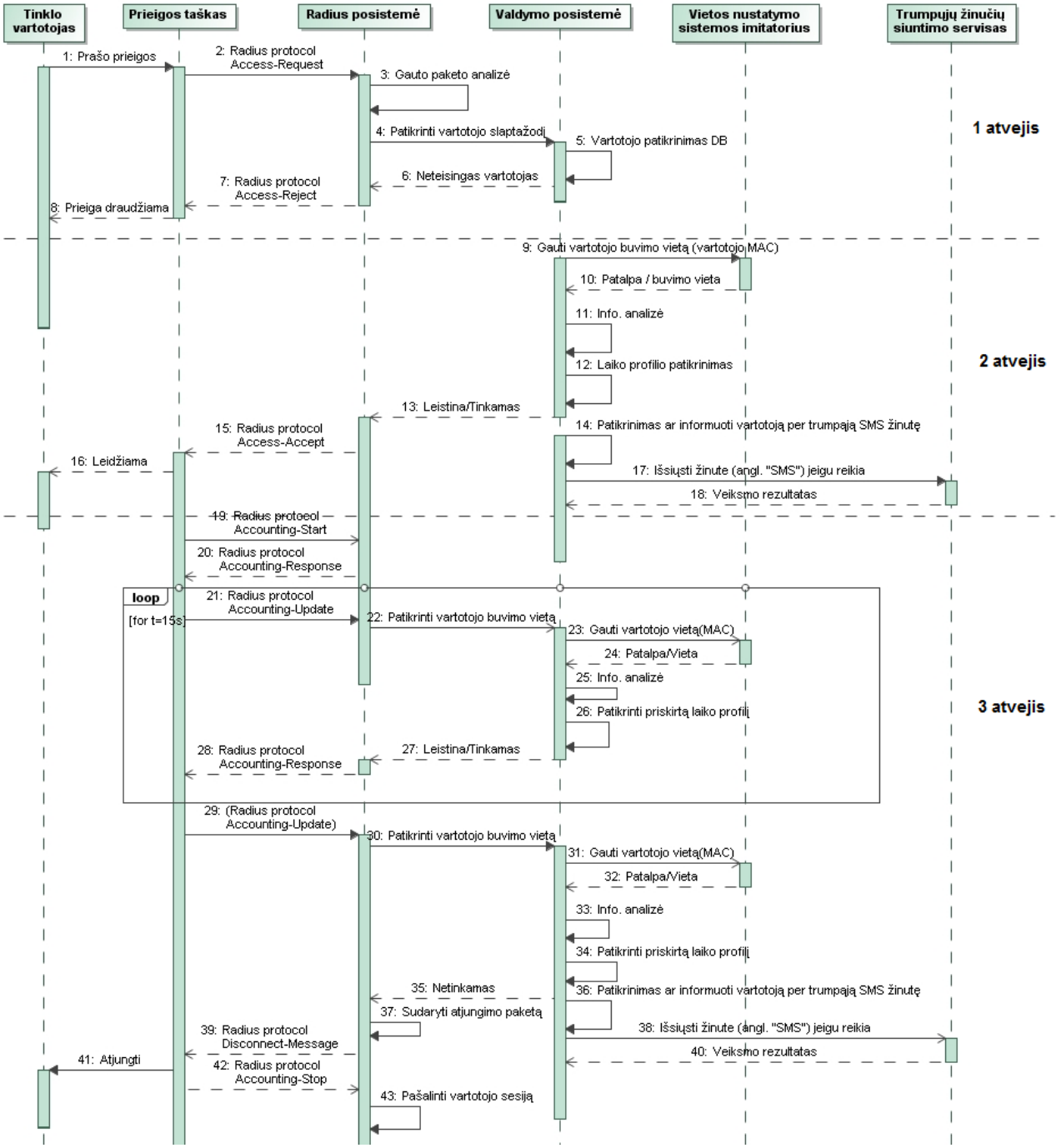
3.6.5. Sąveikos diagramos

3.6.5.1. Tinklo vartotojo autorizacija

Tinklo vartotojo autorizacijos bei apskaitos procesą galima pavaizduoti supaprastinta sekų diagrama (25 pav.). Tinklo vartotojo aptarnavimo rezultatai gali būti:

- Prieiga leidžiama.
- Prieiga draudžiama.
- Prieiga leidžiama su tolimesne vartotojo apskaitos paslauga.

Iš pradžių tinklo vartotojas jungiasi prie belaidžio tinklo prieigos taško. Tada prieigos taškas užklausia sistemą ar šį vartotoją galima įleisti į tinklą, siųsdamas sistemos autorizavimo posistemei „Radius“ protokolo užklausą „Access-Request“. Autorizavimo posistemė panaudojant valdymo posistemės funkcionalumą pirmiausiai patikrina ar įvesti vartotojo duomenys (vartotojo vardas ir slaptažodis) yra teisingi. Jeigu duomenys neteisingi, autorizavimo posistemė atsako „Radius“ „Access-reject“, atitinkamai prieiga draudžiama. Jeigu nustatyta, bei vartotojas sutinka gauti pranešimus, jam bus išsiusta „SMS“ žinutė, kodėl jam buvo uždrausta naudotis tinklu (1 autorizavimo sekų diagramas atvejis). Jei pirmame autorizavimo sekų diagramos atvejyje bus nustatytas tinkamas vartotojas, tai po sėkmingo prisijungimo sistema gali teikti vartotojo apskaitą (jeigu tokia galimybė palaiko aptarnaujamas prieigos taškas, bei sistemos nustatymuose ši paslauga aktyvuota). Apie apskaitos pradžią maršrutizatorius parsiunčia „Radius“ „Accounting-Start“ užklausą, į kurią pagal protokolą sistema atsako – „Radius“ „Accounting-Response“. Toliau kas tam tikrą laiko intervalą (priklauso nuo nustatymų, pavyzdžiui intervalas yra 15 s) bus parsiunčiamos apskaitos atnaujinimo užklausos („Radius“ „Accounting-Update“), kurios metu bus patikrinta vartotojo vieta bei laiko profiliai. Jeigu bus nustatyta, kad vartotojas yra draudžiamoje vietoje arba šiuo metu jam draudžiama naudotis tinklu, bus suformuotas taip vadinamas atjungimo paketas („Radius“ „Disconnect Message“). Šis paketas bus išsiustas prieigos taškui, kuris reaguodamas į gautą nurodymą atjungs duotą vartotoją nuo tinklo, ir praneš sistemai apie apskaitos pabaigą („Radius“ „Accounting-Stop“). „Radius“ posistemės apskaitos kvietiniai (25 pav. diagramos, 21 ž., 28 ž.) ir atjungimo kvietiniai (25 pav. diagramos, 22 – 27 ž. ir 30 - 39 ž.) veikia nepriklausomose lygiagrečiose gijose. Tai leidžia nepriklausomai nuo atjungimo kvietinio vykdymo laiko ir atjungimo rezultato gražinti atsakymą į prieigos tašką. Apskaitos kvietinių gyvavimo ciklas nepriklauso nuo atjungimo kvietinių. Taip pat atsižvelgiant į notifikacijų nustatymus vartotojas/administratorius gali būti informuotas trumpąją „SMS“ žinutę apie įvykį (2 ir 3 25 pav. sekų diagramos atvejai).

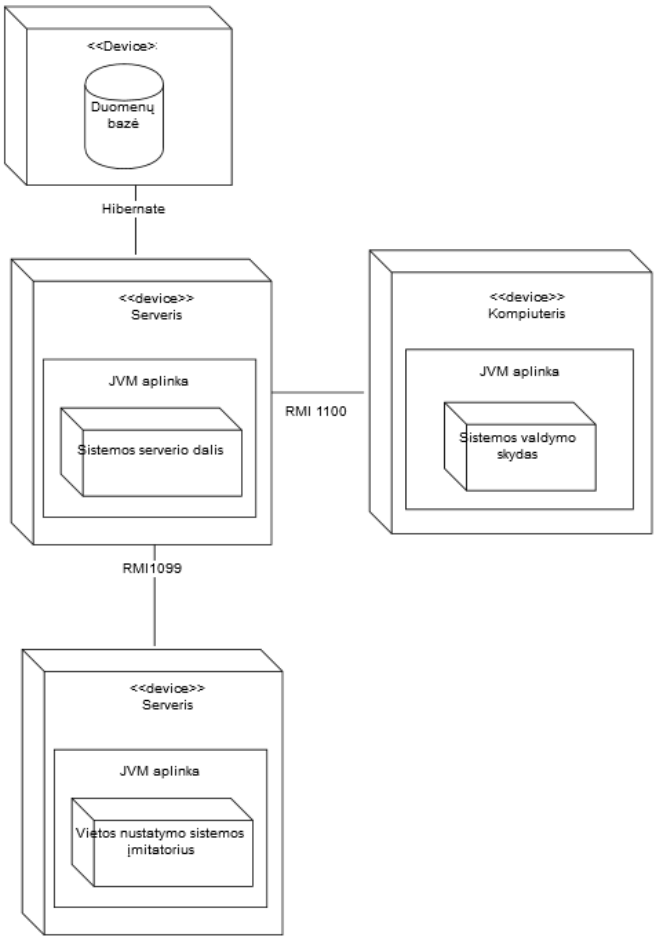


25 pav. Tinklo vartotojo autorizacijos procesas

3.7. Sistemos išdėstymo vaizdas

Sistemos veikimui užtikrinti (bet kuriai posistemei) reikia: Java aplinkos, Interneto ryšio (jeigu diegiama taip kaip pavaizduota paveiksle, t.y. posistemės diegiamas skirtinguose įrenginiuose). Serverio posistemei reikia DB.

Sistemos komponentai gali būti išsidėstę skirtingoje techninėje įrangoje. Toliau (26 pav.) yra pateikiama sistemos diegimo diagrama:



26 pav. Sistemos diegimo modelis

3.8. Vietos nustatymo sistemos imitatorius

Belaidžio tinklo vartotojo buvimo vietos nustatymas nėra šio darbo objektas. Tačiau sistemos veikimui pademonstruoti yra reikalinga vietos nustatymo sistema, dėl to yra sukurtas tokios sistemos imitatorius. Žemiau trumpai aptarsime pagrindinius jo veikimo principus bei funkcionalumą.

Vietos nustatymo sistemos imitatorius teikia sekančias funkcijas:

- Panaudojant nustatymų failą, leidžia nurodyti generuojamų pastatų, aukštų, kambarių skaičių. Kiekvienas iš šių objektų turi savo unikalų identifikatorių, kuris yra grąžinamas kai užklausiama vartotojo buvimo vieta.
- Panaudojant nustatymų failą, leidžia nurodyti vartotojo įrenginio buvimo vietą. Pavyzdžiui, įrenginys, kurio „MAC“ adresas yra „aa-ee-ff-cc“ yra patalpoje su pavadinimu „auditorija 318“, o jos unikalus identifikatorius yra sugeneruota reikšmė - „fd1887sdfae6c“. Tada nustatymų faile nurodoma „aa-ee-ff-cc=fd1887sdfae6c“.

- Galimybė grąžinti visus sugeneruotus objektus: pastatus, pastato aukštus, aukšto patalpas arba kambarius autorizavimo sistemai.
- Konfigūracija gali būti keičiama imitatoriaus veikimo metu ir užkraunama dinamiškai.

Imitatorius grąžina vartotojo įrenginio buvimo vietą kiekvieną kartą kai tik gauna užklausą iš autorizavimo sistemos. Pavyzdžiui, autorizavimo sistema užklausia „aa-ee-ff-cc“ buvimo vietą, tada imitatorius patikrina nustatymo failą ieškodamas nurodyto „MAC“ adreso ir grąžina prie adreso priskirtą patalpos unikalų identifikatorių. Jeigu nurodyto „MAC“ adreso rasti nepavyko - grąžinama reikšmė „null“.

3.9. Skyriaus išvados

1. Kadangi sistemos prototipas realizuotas panaudojant Java programavimo kalbą, jis gali veikti skirtingose platformose.
2. Sistemos naudojama architektūra turėtų palengvinti integruoti į sistemą naują funkcionalumą arba kitus patobulinimus.
3. Sistemos posistemes galima diegti paskirstytoje aplinkoje: autorizavimo posistemė ir valdymo skydas gali veikti kaip viename serveryje taip ir skirtinguose.
4. Bendravimas su duomenų baze yra abstrahuotas panaudojant Hibernate technologiją, tai leidžia neprisirišti prie konkrečios duomenų bazės, galima panaudoti skirtingas duomenų bazes: PostgreSQL, MySQL, Oracle, Sybase, Microsoft SQL bei kitas (žr. Gamintojo puslapyje) [30].

4. Eksperimentinė tiriamoji dalis

4.1. Eksperimentinio tyrimo tikslai

Darbo eksperimentinio tyrimo tikslai yra:

a. nustatyti belaidžio tinklo vartotojų autorizavimo laiką kai sistema naudojasi skirtingas vartotojų skaičius;
b. nustatyti vidutinį belaidžio tinklo vartotojų apskaitos laiką kai sistema naudojasi skirtingas vartotojų skaičius;
c. nustatyti tinklo vartotojo apskaitos minimalų bei maksimalų laiką, kai prie tinklo yra prisijungęs skirtingas vartotojų skaičius;
d. identifikuoti užklausų skaičiaus į vietos nustatymo sistemą (šiuo atveju į sistemos imitatorių) minimizavimo galimybes.

a – c punktuose įvardinti tyrimai leis įvertinti sistemos našumo savybes - parodys kiek laiko ilgiausiai gali užtrukti vartotojo autentifikacija, priklausomai nuo vienu metu besijungiančių vartotojų skaičiaus bei atsakys į klausimą ar šis skaičius įtakoja ir kiek įtakoja apskaitos procesą.

d punkte įvardintas tyrimas skirtas atsakyti į klausimą ar galima suminimizuoti užklausų vartotojo vietos informacijai gauti, skaičių ir jei galima – kokį efektą tai gali duoti. Mažinti užklausų į vietos nustatymo sistemą skaičių yra svarbu ne tik dėl tinklo resursų taupymo, bet tai pat ir dėl ekonominių priežasčių, kadangi tokios vietos nustatymo paslaugos trečiųjų šalių yra apmokestinamos priklausomai nuo generuojamų užklausų srauto dydžio [31].

4.2. Eksperimentinio tyrimo aprašymas

Aukščiau aprašytiems tikslams pasiekti papildomai buvo sukurti 2 įrankiai, kurių veikimas yra trumpai aprašytas žemiau.

4.2.1. Įrankis skirtas tinklo vartotojų imitavimui

Įrankis skirtas formuoti reikiamą kiekį „Radius“ užklausų (tinklo vartotojų). Taip pat šis įrankis geba palaikyti apskaitos (angl. Radius Accounting) paslaugą. Pavyzdžiui, jeigu yra siunčiama „RADIUS“ „Access-Request“ užklausa į kurią atsakoma „Radius“ „Access-Accept“, yra startuojama vartotojo apskaita. Kas tam tikrą laiko intervalą (nurodoma įrankyje) bus siunčiamos apskaitos atnaujinimo užklausos. Tokiu būdu yra imituojama belaidžio tinklo vartotojo autorizacija ir aktyvi sesija.

4.2.2. Įrankis skirtas užklausų skaičiaus į vietos nustatymo sistemos imitatorių sumažinimo tyrimui

Įrankis, kuris skirtas sumažinti užklausų (kreipinių) skaičių į vietos nustatymo sistemą (šiuo atveju į sistemos imitatorių) veikia podėlio (angl. „cache“) principu. Reikia paminėti, kad apskaitos atnaujinimo žinutės laiko intervalas nustatomas visiems vartotojams vienodas (pagal „Radius“ „Accounting“ protokolą). Jeigu mes norime intensyviai stebėti tam tikrą patalpą, laiko intervalas tarp apskaitos atnaujinimo žinučių turėtų būti pakankamai mažas. Esant mažam laiko intervalui atitinkamai išauga užklausų į vietos nustatymo sistemą skaičius iš visų patalpų.

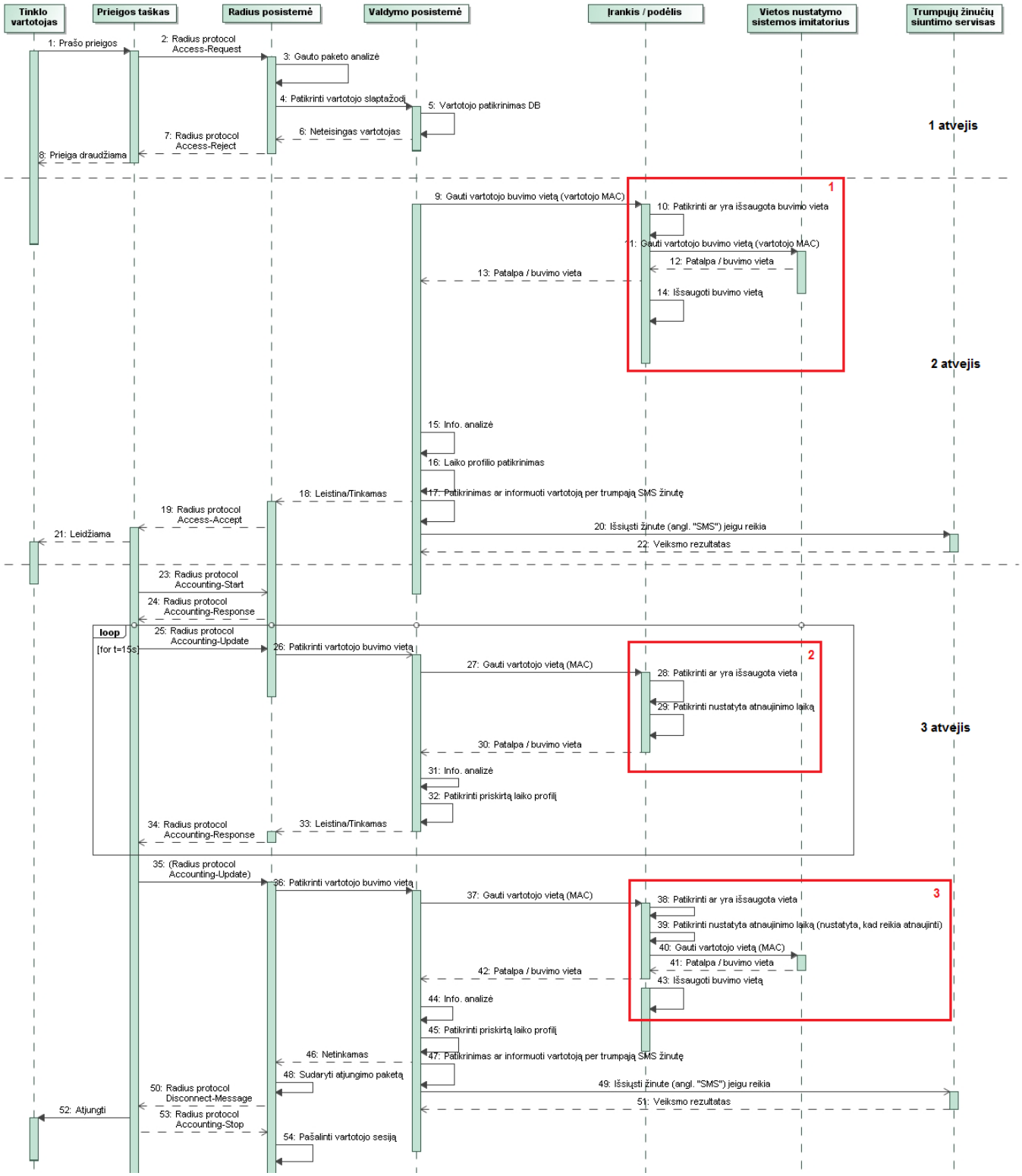
Panaudojant šį įrankį sukurtas sistemos prototipas kiekvieną kartą gavęs apskaitos atnaujinimo žinutę. Norėdamas sužinoti vartotojo buvimo vietą, vietoj to, kad kreiptųsi tiesiai į vietos nustatymo sistemą (imitatorių), jis kreipiasi į sukurtą įrankį.

Taip pat įrankyje (podėlio) kiekvienai sistemoje išsaugotai patalpai/vietai nurodomas atnaujinimo laikas. Pavyzdžiui, sistemoje išsaugotai 318 auditorijai, priskiriamas atnaujinimo laikas 15 s. Tada, kai tinklo vartotojas autorizuojasi, sukurtas sistemos prototipas kreipiasi į šį įrankį, norėdamas gauti tinklo vartotojo buvimo vietą. Jeigu įrankyje (podėlyje) nurodyto vartotojo nerasta - jis kreipiasi į vietos nustatymo sistemą ir įsimena jo buvimo vietą (tarkime buvimo vieta yra 318 auditoriją) 15 s. Tada, kai po sėkmingos autorizacijos bus vykdoma vartotojo apskaitą (tarkime apskaitos atnaujinimo žinutės bus siunčiamos kas 5 s) nebereikės kreiptis į vietos nustatymo sistemą. Kadangi vieta bus saugoma podėlyje 15 s (tik praėjus 15 s, podėlis atnaujins vartotojo buvimo vietą). Tokiu būdu yra sumažinamas kreipinių į vietos nustatymo sistemą kiekis/skaičius.

27 pav. pateikiama podėliu papildyta autorizacijos proceso supaprastinta sekų diagrama. Iš pradžių tinklo vartotojas jungiasi prie belaidžio tinklo prieigos taško. Tada prieigos taškas užklausia sistemą ar šį vartotoją galima įleisti į tinklą, siųsdamas sistemos autorizavimo posistemei „Radius“ protokolo užklausą „Access-Request“. Autorizavimo posistemė panaudojant valdymo posistemės funkcionalumą pirmiausiai patikrina ar įvesti vartotojo duomenys (vartotojo vardas ir slaptažodis) yra teisingi. Jeigu duomenys neteisingi autorizavimo posistemė atsako „Radius“ „Access-reject“, atitinkamai prieiga draudžiama. Jeigu nustatyta bei vartotojas sutinka gauti pranešimus, jam bus išsiusta „SMS“ žinutė, kodėl jam buvo uždrausta naudotis tinklu (1 autorizavimo sekų diagramas atvejis).

Jeigu pirmame autorizavimo sekų diagramos atvejyje bus nustatytas tinkamas vartotojas, tai sistema kreipsis į tyrimo metu sukurtą podėlį, kad gauti vartotojo buvimo vietą. Jeigu podėlyje nurodytam „MAC“ adresui nebus rasta buvimo vieta, podėlis kreipsis į vietos nustatymo sistemą ir grąžins bei išsaugos vartotojo buvimo vietą (27 pav. 10-14 diagramos žingsniai). Po sėkmingo prisijungimo sistema gali teikti

vartotojo apskaitą (jeigu tokią galimybę palaiko aptarnaujamas prieigos taškas, bei sistemos nustatymose ši paslauga aktyvuota). Apie apskaitos pradžią maršrutizatorius parsiunčia „Radius“ „Accounting-Start“ užklausą, į kurią pagal protokolą sistema atsako – „Radius“ „Accounting-Response“. Taip pat, kai atsiunčiama „Accounting-Start“ užklausa yra patikrinama vartotojo buvimo vieta bei laiko profilis, šie veiksmai atitinka, 27 pav. 27-30 diagramos žingsnius (diagramoje dėl paprastumo šie žingsniai neatvaizduojami). Toliau kas tam tikrą laiko intervalą (priklauso nuo nustatymų, pavyzdžiui intervalas yra 15 s) bus parsiunčiamos apskaitos atnaujinimo užklausos (Radius „Accounting-Update“), kurios metu bus patikrinta vartotojo vieta bei laiko profiliai. Tačiau, tikrinant vietą šiuo atveju jau bus kreipiamasi į podėlį, o ne į vietos nustatymo sistemą. Podėlyje pirmiausiai bus patikrinta ar vieta vis dar galioja (t.y. ar patalpai nustatytas atnaujinimo laikas nepraėjo) ir grąžinama vartotojo buvimo vieta. Jeigu bus nustatyta, kad išsaugota vietos informacija yra pasenusi, podėlis kreipsis į vietos nustatymo sistemą, kad ją atnaujinti (27 pav. 38-43 diagramos žingsniai). Jeigu bus nustatyta, kad vartotojas yra draudžiamoje vietoje arba šiuo metu jam draudžiama naudotis tinklu, bus suformuotas taip vadinamas atjungimo paketas („Radius“ „Disconnect Message“). Šis paketas bus išsiustas prieigos taškui, kuris reaguodamas į gautą nurodymą – atjungs duotą vartotoją nuo tinklo ir praneš sistemai apie apskaitos pabaigą („Radius“ „Accounting-Stop“). Taip pat atsižvelgiant į informavimo pranešimų nustatymus vartotojas/administratorius gali būti informuotas trumpąja „SMS“ žinute apie įvykį (2 ir 3 sekų diagramos atvejai).



27 pav. Tinklo vartotojo autorizacija naudojant podėlį

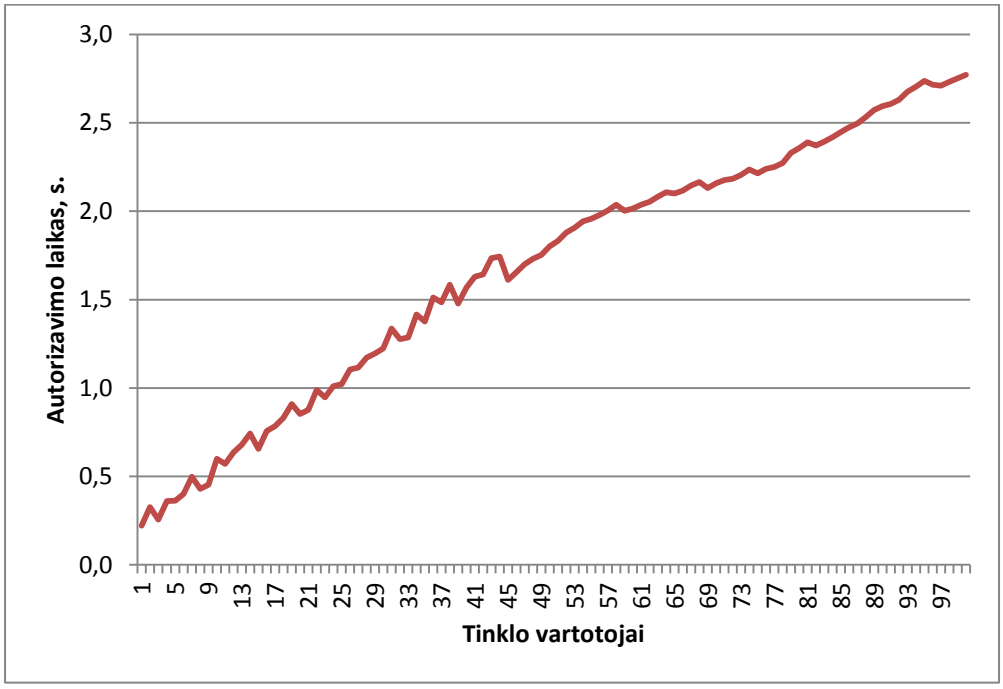
4.3. Eksperimentinio tyrimo eiga ir rezultatai

Visi įrankiai, reikalingi eksperimentiniams tyrimams atlikti (Autorizavimo serveris, vietos nustatymo sistemos imitatorius bei eksperimentams atlikti sukurti įrankiai) buvo paleidžiami vienoje aplinkoje/mašinoje. Mašinos specifikacija:

- Operacinė sistema: „Windows 7“.
- Procesorius: „Core 2 Duo“, 2,00 Ghz.
- Operatyvioji atmintis: 2 Gb.
- Duomenų bazė: „Postgress“.

4.3.1. Sistemos našumo savybių tyrimas ir rezultatai

Testuojant tinklo vartotojų autorizavimo bei apskaitos greitaveiką, buvo autorizuojami lygiagrečiai 100 vartotojų, kuriems po autorizacijos buvo aktyvuojama apskaitos paslauga. Tokio vienu metu lygiagrečiai besijungiančių vartotojų skaičiaus pakanka bendroms laiko, sugaišto autorizacijai, tendencijoms nustatyti. Eksperimento metu buvo nustatyta, kad lygiagrečiai jungiantis 100 vartotojų, vidutinis jų autorizavimo laikas yra apie 1,67123 s. 28 pav. pateikiama autorizavimo laiko kreivė kiekvienam iš lygiagrečiai besijungiančių prie bevielio tinklo vartotojų.



28 pav. Tinklo vartotojo autorizavimo greitaveika

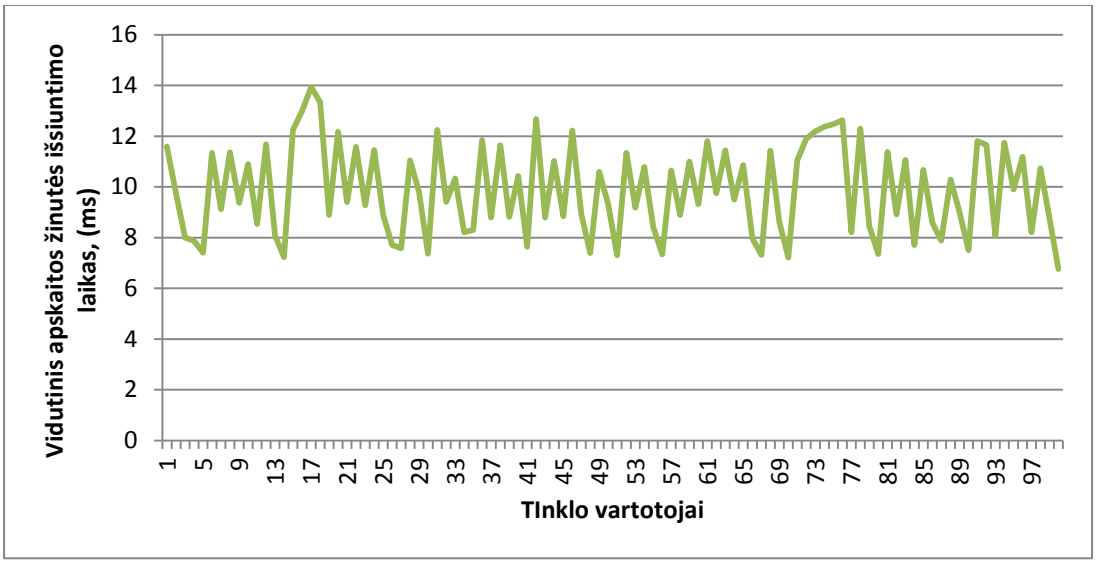
28 pav. pateiktame grafike lygiagrečiai autorizuojamas pakankamai didelis vartotojų kiekis ir laiko sąnaudos autorizacijai auga beveik tiesiškai. Tokį gana spartų tiesišką augimą gali sąlygoti laiko prastovos,

susidarančios dėl galimo užklausų sustatymo į vieną eilę. Tačiau vienu metu (lygiagrečiai) pastoviai didelio kiekio besijungiančių vartotojų tikimybė yra gana maža. Taip pat kuriamam prototipui griežtų greitaveikos reikalavimų keliama nebuvo.

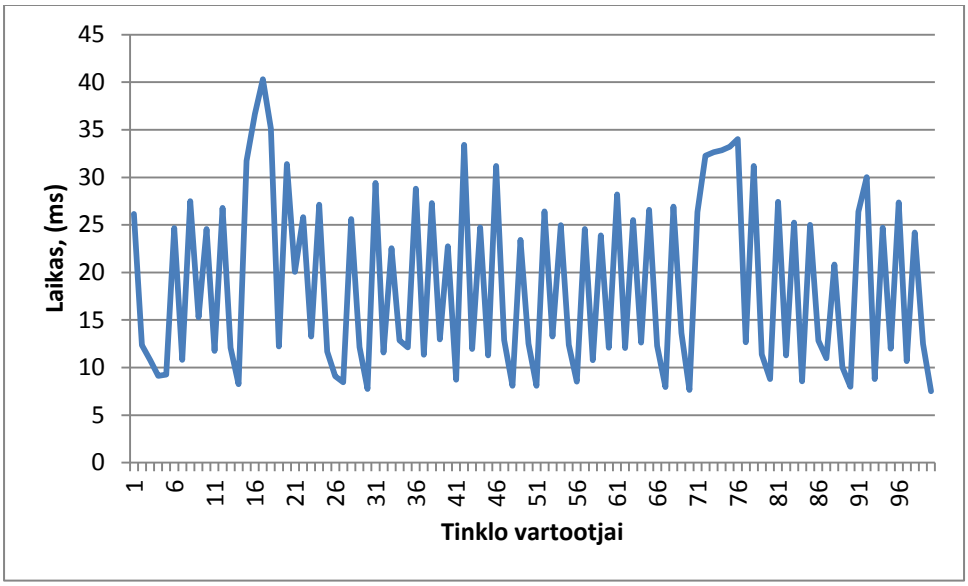
Žemiau pateikiamas 100 vartotojų apskaitos žinučių atsakymų (25 pav. diagramos 21,28 žingsniai) greitaveikos grafikas (29 pav.). Eksperimento metu apskaitos užklausų siuntimo intervalas buvo nustatytas 6s, eksperimento laikas – 1 min. Pagrindiniai apskaitos laiko reikšmes pateikiami 19 lentelėje.

Lentelė 19. Pagrindiniai apskaitos žinučių nusiuntimo laiko intervalai

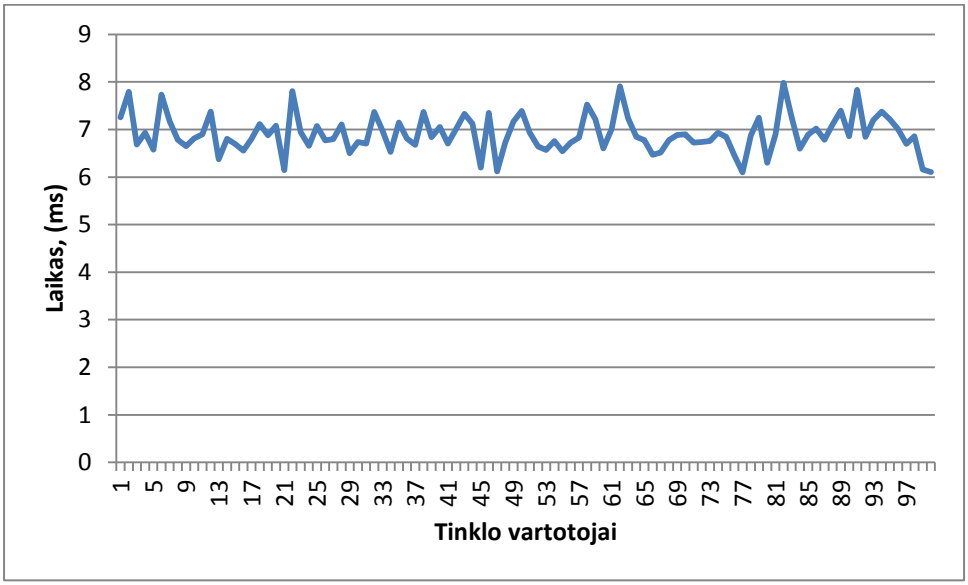
Aprašymas	Reikšmė (ms)
Vidutinis 100 vartotojų apskaitos atsakymo laikas:	~ 9,88
Maksimalus 1 vartotojo apskaitos atsakymo laikas:	40
Minimalus 1 vartotojo apskaito atsakymo laikas:	6



29 pav. Vidutiniai apskaitos atsakymų laikai



30 pav. Maksimalus apskaitos atsakymų laikai



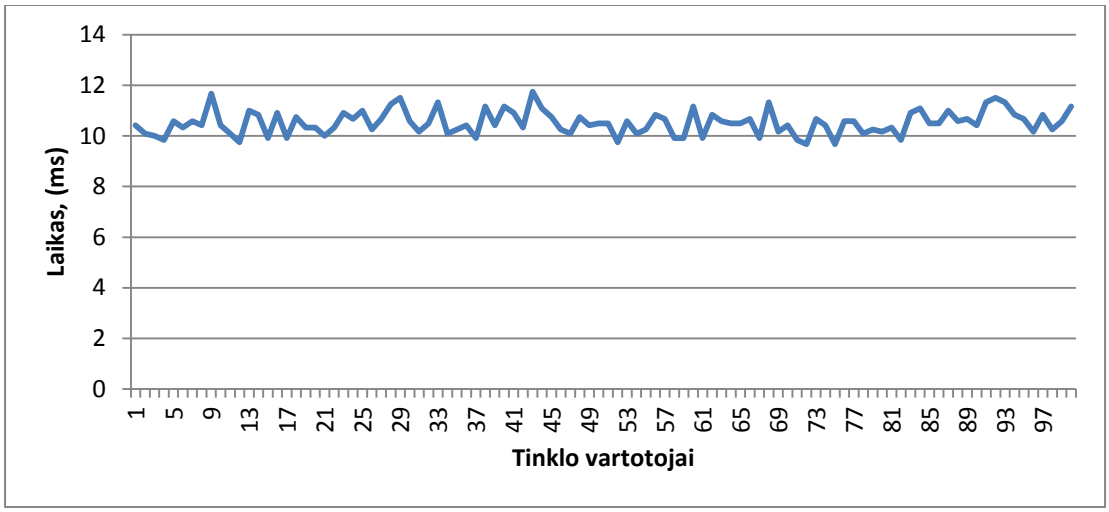
31 pav. Minimalus apskaitos atsakymų laikai

Kadangi visas vartotojo duomenų analizės procesas (25 pav. diagramos 22-27, 30-35 žingsniai), apskaitos paslaugos metu vyksta nepriklausomai nuo apskaitos žinučių atsakymų, todėl tikslinga pateikti ir šio proceso laiko sąnaudas (32 pav.). Šis laikas atitinka reakcijos laiką per kuri vartotojas gali būti atjungiamas nuo tinklo.

Vidutinis analizės proceso laikas: 10,52 ms.

Maksimalus analizės proceso laikas: 11,75 ms.

Minimalus analizės proceso laikas: 9,66 ms.



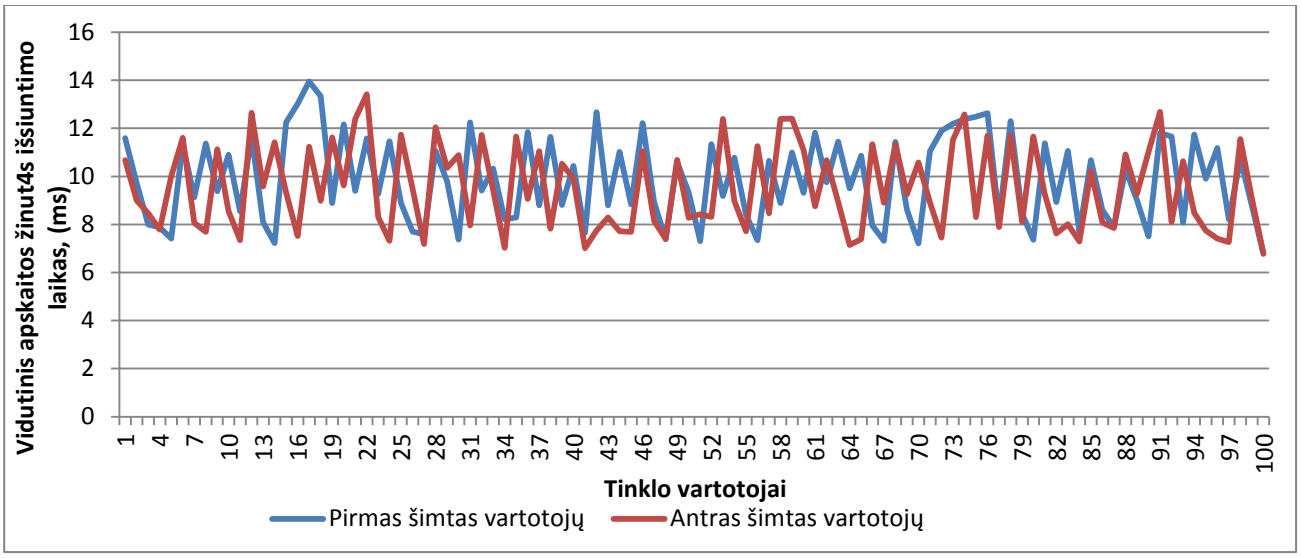
32 pav. Vidutiniai vartotojų apskaitos analizės laikai

Kaip matome iš aukščiau pateiktų grafikų apskaitos žinučių atsakymai (angl. Radius „Accounting-Response“) siunčiami ir vartotojų duomenų analizės procesai vyksta pakankamai greitai. Aptarnavimo laikas nuolat svyruoja, tačiau tai yra normalu, kadangi laiko svyravimai yra nedideli. Tai vyksta dėl to, kad neįmanoma užtikrinti testavimo aplinkos pastovumo, dėl aplinkoje egzistuojančių su tiriama sistema nesusijusių procesų (pvz., OS sisteminių procesų).

Taip pat buvo išanalizuotos 100 lygiagrečiai besijungiančių vartotojų laiko sąnaudos autorizacijai - kai sistema teikia apskaitos paslaugą 100 vartotojų. Iš pradžių prijungiami 100 vartotojų. Praėjus 3 s prijungiami dar 100 vartotojų. Tokiomis pradinėmis sąlygomis gautas vidutinis antro vartotojų šimto autorizacijos laikas lygus 1,77231 s. Šis laikas yra labai panašus į aukščiau pateiktą (28 pav.), todėl šio bandymo grafikas nebus pateikiamas. Tai parodo, kad sistema pajėgi aptarnauti pakankamai didelį kiekį vartotojų, jeigu jie nesijungia lygiagrečiai. Toliau pateikiami pagrindiniai apskaitos žinučių atsakymo laikai, kai sistema naudojasi 200 vartotojų:

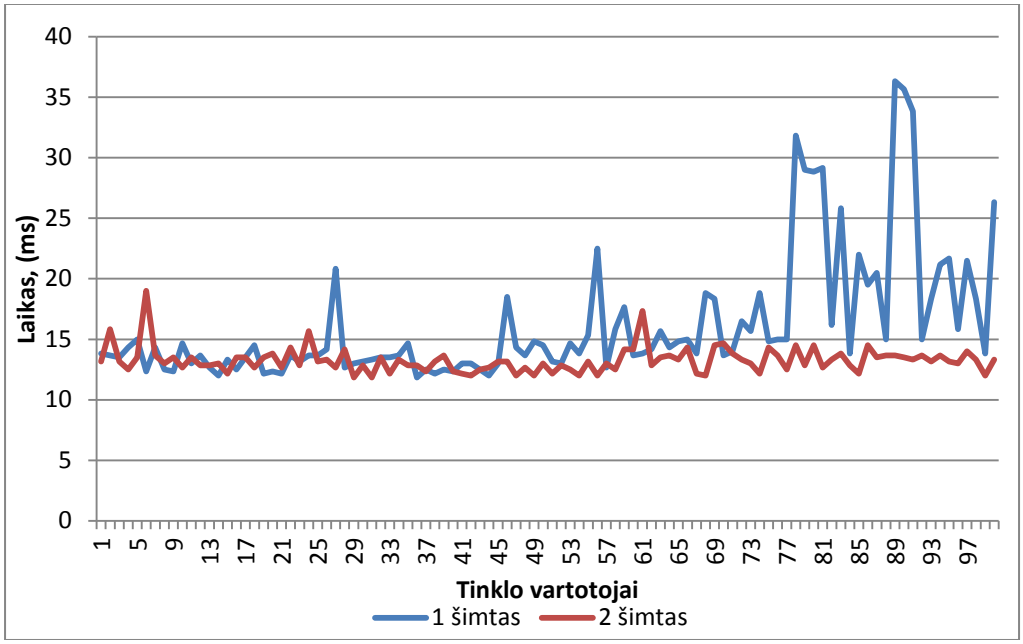
Lentelė 20. Pagrindiniai apskaitos žinučių išsiuntimo laikai

Aprašymas	Reikšmė(ms)
Vidutinis antro 100 vartotojų apskaitos laikas:	~9,5
Minimalus antro 100 vartotojų apskaitos laikas:	38
Maksimalus antro 100 vartotojų apskaitos laikas:	5



33 pav. Apskaitos laiko palyginimas

Žemiau (34 pav.) pateikiama vidutinių vartotojų apskaitos laikų priklausomybės nuo vienodo dydžio lygiagrečiai besijungiančių vartotojų grupių diagrama. Eksperimento metu gauti laikai parodo per kiek laiko po apskaitos žinutės gavimo duotas vartotojas gali būti atjungtas nuo tinklo. Nors pateiktame grafike stebime laiko šuoliai, tačiau reikia pastebėti, kad sistema nuolat reagavo (angl. „responsive“) į gautas užklausas, sistemos darbo metų trikdžių (angl. „system timeouts“) pastebėta nebuvo. Galimai tokie laiko šuoliai įvyko būtent tuo metu kai buvo prijungiamas (autorizuojamas) 2 vartotojų šimtas.



34 pav. Vidutinių vartotojų apskaitos analizės laikai

4.3.2. Podėlio įtakos užklausų į vietos nustatymo sistemą skaičiui tyrimas ir rezultatai

Toliau (21 lentelė) pateikiamas podėlio naudingumo patikrinimas, testavimo laikas – 60 s. Tikrinant podėlį buvo patikrinami 2 atvejai. Idealus atvejis - kai visi vartotojai yra patalpoje kurioje atnaujinimo laiko intervalas yra pakankamai didelis palyginus su apskaitos laiko intervalu. Labiau realesnis atvejis kai vartotojai pasiskirstę po patalpas su skirtingais atnaujinimo laiko intervalais. Podėlio atnaujinimo laikas yra laikas kuris turi praeiti tarp duomenų atnaujinimo kreipinio į vietos nustatymo sistema. Podėlio atnaujinimo laikas yra priskiriamas kiekvienai patalpai.

Lentelė 21. 1 podėlio efektyvumo tyrimo rezultatai

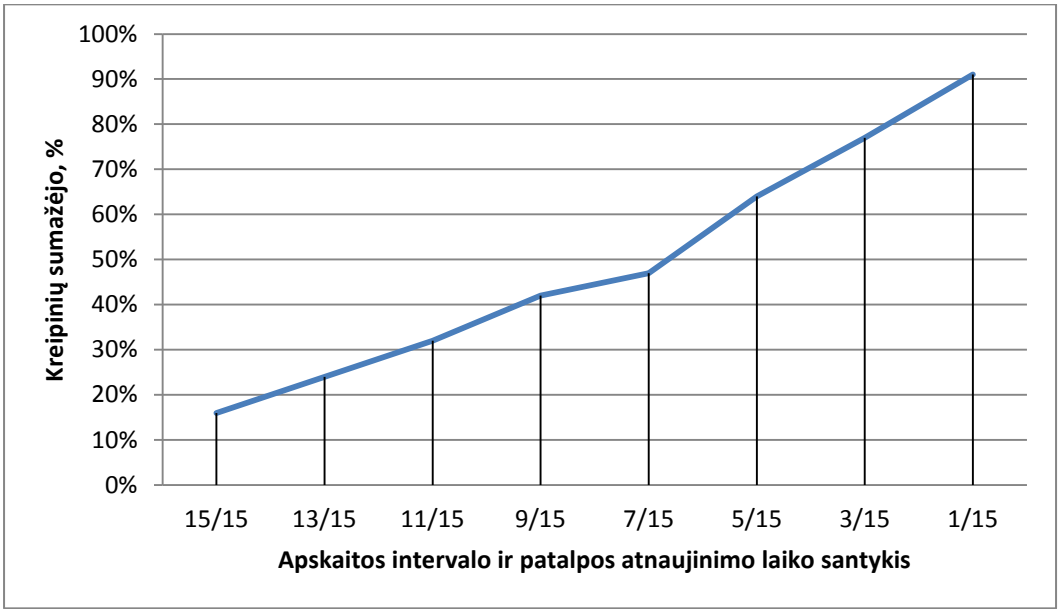
Vartotojų skaičius patalpoje	Patalpai priskirtas atnaujinimo laikas (s)	Intervalas tarp apskaitos žinučių (s)	Kreipinių skaičius į vietos nustatymo sistemos imitatorių. Naudojant podėlį	Kreipinių skaičius į vietos nustatymo sistemos imitatorių. Nenaudojant podėlio	Kreipinių sumažėjo, (%)
Kai visi vartotojai vienoje patalpoje					
100	15	5	500	1400	64
Kai vartotojai pasiskirstę per patalpas					
30	15	5	880	1400	37
30	10	5			
40	5	5			

Toliau (22 lentelė) pateikiamas atvejis kai visi vartotojai yra vienoje patalpoje su podėlio atnaujinimo laiku – 15 s., o apskaitos žinučių siuntimo intervalas yra keičiamas. Toks eksperimentas parodo apskaitos žinučių siuntimo laiko intervalo priklausomybė nuo podėlio patalpos atnaujinimo laiko. Eksperimento trukmė yra 60 s.

Lentelė 22. 2 podėlio efektyvumo tyrimo rezultatai

Vartotojų skaičius patalpoje	Patalpai priskirtas atnaujinimo laikas (s)	Intervalas tarp apskaitos žinučių (s)	Kreipinių skaičius į vietos nustatymo sistemos imitatorių. Naudojant podėlį	Kreipinių skaičius į vietos nustatymo sistemos imitatorių. Nenaudojant podėlio.	Kreipinių sumažėjo, (%)
100	15	1	500	6200	91
100	15	3	500	2200	77
100	15	5	500	1400	64
100	15	7	500	1057	47
100	15	9	500	866	42
100	15	11	500	754	32
100	15	13	500	661	24
100	15	15	500	600	16

Iš žemiau pateikto grafiko (35 pav.) galime pastebėti, kad sutaupytu kreipinių į vietos nustatymo sistema skaičius tiesiogiai priklauso nuo intervalų tarp apskaitos atnaujinimo žinučių ir podėlio patalpos atnaujinimo laiko santykio. Tendencijos yra tokios, kad kuo mažesnis intervalas tarp apskaitos siunčiamų užklausų (angl. „Accounting“) ir kuo didesnis yra podėlio patalpos atnaujino laikas tuo didesnis kreipinių į vietos nustatymo sistema sumažėjimas. Reikia pabrėžti, kad netgi kai apskaitos žinučių siuntimo intervalas ir podėlio patalpos atnaujinimo laikas sutampa kreipinių sumažėjimas yra apie 16%. Tokį kreipinių sumažėjimą sąlygoja tai, kad pagal „Radius“ protokolą, po sėkmingos autorizacijos, apie apskaitos pradžia yra pranešama iškarto (t. y. nepriklausomai nuo nustatyto apskaitos laiko intervalo) siunčiant (angl. „Accounting-start“) užklausą (27 pav. diagramos 23 žingsnis). Tačiau po sėkmingos autorizacijos podėlyje yra išsaugota vartotojo buvimo vieta, todėl į vietos nustatymo sistema kreiptis nebereikia. Todėl kiekvienas vartotojas „sutaupo“ po viena kreipinį į vietos nustatymo sistema, kai yra siunčiamos apskaitos pradžios užklausos (angl. „Accounting-start“).



35 pav. Kreipinių skaičiaus į vietos nustatymo sistema priklausomybė

4.4. Eksperimentinio tyrimo išvados

- Sistemos našumo savybių eksperimentiniai tyrimai parodė, kad apskaitos užklausų aptarnavimo laikas yra pakankamai mažas. Mažą apskaitos užklausų aptarnavimo laiką sąlygoja tai, kad apskaitos atsakymai vyksta nepriklausomai nuo atjungimo kvietinių.
- Vidutinis vartotojų autorizavimo laikas taip pat nėra labai didelis, tačiau tyrimo rezultatai rodo, kad esant didesnei apkrovai, gali atsirasti autorizacijos greitaveikos trūkumai. Tokie trūkumai gali būti susiję su nepakankamai optimizuotu prototipo ir trečios šalies bibliotekų programiniu kodu. Apibendrinant, galima daryti išvadą, kad sistemos prototipas nėra pakankamai paruoštas naudojimui

tinkluose su dideliu vartotojų kiekiu ir sistemą eksploatuojant realiomis sąlygomis, reikėtų atlikti nuodugnesnį priklausomų bibliotekų ir autorizacijos proceso greitaveikos tyrimą, identifikuojant „siauras“ vietas. Pagal šių tyrimų rezultatus galima būtų spręsti apie prototipo tobulinimo strategijas arba kitų alternatyvių sprendimų panaudojimo tikslingumą. Kadangi šiame darbe sistemos prototipui griežti greitaveikos reikalavimai keliami nebuvo prototipo greitaveikos gerinimo klausimai galėtų būti vienas iš tolesnių šio darbo vystymo krypčių.

- Podėlio įtakos užklausų į vietos nustatymo sistemą skaičiui tyrimas parodė, kad papildant sistemą šiuo elementu galima žymiai sumažinti kreipinių į vietos nustatymo sistemą skaičių, kas leistų atitinkamai sumažinti tinklo apkrovą bei vietos nustatymo sistemos resursų išnaudojimą.

5. Darbo rezultatai ir išvados

- RBAC modelio bei egzistuojančių tyrimų, siekiant šį modelį papildyti laiko ir vietos informacija, analizė parodė, kad didelis dėmesys skiriamas RBAC praplėtimams konceptualiame lygmenyje, tačiau gana mažai informacijos pateikiama kaip šie modeliai turėtų būti adaptuojami įvairioms aplinkoms, pavyzdžiui, funkcionavimui bevieliame tinkle, gana ribota naudojamų vietos informacijos požymių aibė.
- Išgryninant, apjungiant ir papildant skirtingų autorių darbuose aprašytas idėjas sukurtas centralizuotas, vietos ir laiko apribojimais praplėsto RBAC modelio pagrindu veikiantis bevielio tinklo vartotojų autorizavimo sistemos prototipas, leidžiantis autorizuoti tinklo vartotoją pagal jo buvimo vietą ir laiką, ir, priklausomai nuo jo (tinklo vartotojo) rolės, naudotis įvairiais tinklo resursais.
- Sukurta modulinės architektūros sistema užtikrina lankstumą sistemą plečiant ar į ją integruojant papildomus reikiamus modulius. Sistemoje įvertinta bevielio tinklo specifikos padiktuota galimybė operuoti vietos informacijos požymiu, apibrėžiančiu tam tikrą zoną bei gauti vietos informaciją iš trečiųjų šalių.
- Bendravimo su prieigos taškais užtikrinimui panaudotas „Radius“ protokolas, bendravimui tarp sistemos posistemių - RMI, sistemos lankstumui - Hibernate technologijos. Sistemos prototipas realizuotas Java programavimo kalba, kuri užtikrina sistemos pernešimą ir suderinamumą skirtingose kompiuterinėse platformose. Manipuliacijos rolėmis ir apribojimų skyrimas joms (taip pat ir kitas reikalingas funkcionalumas) - vykdomi sistemos grafinės sąsajos pagalba.
- Darbe pasiūlytas sukurtos sistemos prototipo papildymas-podėlis įvertinantis pastato planą ir siūlantis skirtingoms pastato zonoms priskirti skirtingus autorizacijos apskaitos laikus. Podėlio įtakos užklausų į vietos nustatymo sistemą skaičiui tyrimas parodė, kad papildant sistemą šiuo elementu galima žymiai sumažinti kreipinių į vietos nustatymo sistemą skaičių nuo 16% iki 90%, kas leistų atitinkamai sumažinti tinklo apkrovą bei vietos nustatymo sistemos resursų išnaudojimą.
- Sistemos našumo eksperimentiniai tyrimai parodė, kad bevielio tinklo vartotojų autorizacijos ir apskaitos procesai vykdomi greitai, tačiau esant didesnei apkrovai, gali atsirasti autorizacijos greitaveikos trūkumai. Tokie trūkumai gali būti susiję su nepakankamai optimizuotu prototipo ir trečios šalies bibliotekų programiniu kodu. Sistemą eksploatuojant realiomis sąlygomis, reikėtų atlikti nuodugnesnį priklausomų bibliotekų ir autorizacijos proceso greitaveikos tyrimą, identifikuojant „siauras“ vietas.

6. Literatūra

[1] Office for Nation Statistics, „Internet Access – Households and Individuals“, 2013. Prieiga per internetą: http://www.ons.gov.uk/ons/dcp171778_322713.pdf [Žiūrėta: 2016 05 07]

[2] The Statistics Portal, „Global number of public hotspots“, 2009-2015. Prieiga per interneta: http://www.statista.com/statistics/218596/global-number-of-public-hotspots-since-2009/ [Žiūrėta: 2016 05 07]

[3] Bogdan Botezatu, HOTforSecurity, „25 Percent of Wireless Networks are Highly Vulnearable to Hacking Atacks, Wi-Fi Security Survey Reveals“, 2009 – 2015. Prieiga per internetą: http://www.hotforsecurity.com/blog/25-percent-of-wireless-networks-are-highly-vulnerable-to-hacking-attacks-wi-fi-security-survey-reveals-1174.html [Žiūrėta: 2016 05 07]

[4] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, “Role-based access control models,” IEEE Comput., vol. 29, no. 2, pp. 38–47, Feb. 1996.

[5] Alan C. O`Cornor, Ross J.Loomis, „2010 Economic Analysis of Role-Based Access Control“, National Institute of Standards and Technology, December 2010. Prieiga per internetą: http://csrc.nist.gov/groups/SNS/rbac/documents/20101219_RBAC2_Final_Report.pdf [Žiūrėta: 2016 05 07]

[6] Xiutao Cui, Yuliang Chen, Junzhong Gu, „Ex-RBAC : An Extended Role Based Access Control Model for Location-aware Mobile Collaboration System“, Second International Conference on Internet Monitoring and Protection (ICIMP 2007)

[7] Yu Wanjun, Wang Yong, "Research on Security Status Recovery in Temporal Role-Based Access Control System", 2009 International Conference on Information Management, Innovation Management and Industrial Engineering

[8] Xun Li, Sang Bong Yoo, "Extended Role-Based Security System using Context Information", 2008 Second International Conference on Future Generation Communication and Networking DOI 10.1109/FGCN.2008.14

[9] Hsing-Chung Chen, Yung-Fa Huang, Syuan-Zong Lin, "Generalized Associated Temporal and Spatial Role-Based Access Control Model for Wireless He terogeneous Networks", 2011 Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. E-ISBN 978-0-7695-4372-7

[10] Elisa bertino, Barbara Catania, Maria Luisa Damiani, "GEO-RBAC: A Spatially Aware RBAC",SACMAT’05, June 1–3, 2005, Stockholm, Sweden. DOI 10.1145/1210263.1210265

[11] Kai Ouyang, James B.D. Joshi, "CT-RBAC: A Temporal RBAC Model with Conditional Periodic Time", 2007, IEEE. ISBN 1-4244-1137-8

[12] Tautvydas Čepas, Prieigos kontrolė ir jos vaidmuo sistemos saugumui užtikrinti, Vilniaus Gedimino technikos universitetas, 2011m. ISBN - 978-9955-28-834-3.

[13] Moyer, M.J. ; Abamad, M, Distributed Computing Systems, 2001. 21st International Conference on, Apr 2001.

[14] M. Koch, L.V. Mancini, F. Parisi-Presicce, “A graph-based formalism for RBAC”, 2002. DOI 10.1145/545186.545191

[15] Hansen F, Oleshchuk V.,Spatial role-based access control model for wireless networks. In: Vehicular technology conference, 2003.

[16] Wilikens M, Feriti S, Sanna A, Masera M. „A context-related authorization and access control method based on RBAC: a case study from the health care domain. In: Seventh ACM symposium on access control models and technologies“, 2002m. DOI 10.1145/507711.507730

[17] YueZhang, James B.D. Joshi. An Implementation Architecture of the GTRBAC Model (2010). Information Science Department University of Pittsburgh Pittsburgh, P A, US. DOI 10.1109/ICCDA.2010.5541433

[18] Ramadan Abdunabi, Mustafa Al-Lail, Indrakshi Ray, and Robert B. France Specification, Validation, and Enforcement of a Generalized Spatio-Temporal Role-Based Access Control Model (September 2013). DOI 10.1109/JSYST.2013.2242751

[19] Matija Sorman,Tomislav Kovac,Damir Maurovic, Implementing improved WLAN security.

[20] C. Rigney, S. Willens, A. Rubens, W. Simpson, RFC 2865, Remote Authentication Dial In User Service (RADIUS), 2000m. [Žiūrėta: 2016 05 01]

[21] Emrah Tomura, Y.M. Ertenb, Application of temporal and spatial role based access control in 802.11 wireless networks. DOI 10.1016/j.cose.2006.05.007

[22] Aleksander Buczkowski, Location-Based Services – Technologies,(2011-2012). Prieiga per internetą: http://geoawesomeness.com/knowledge-base/location-based-services/location-based-services-technologies/ [Žiūrėta: 2016 04 27]

[23] Jingyuan Zhang, A Cell ID Assignment Scheme and Its Applications, Computer Science DepartmentThe University of Alabama. ISBN 0-7695-0771-9

[24] Department of Electrical Engineering, University of The Punjab, Lahore, Pakistan. An Overview of the Factors Responsible for GPS Signal Error: Origin and Solution (2009). ISBN: 978-0-7695-3901-0

[25] Ricardo Matos, Daniel F. Santos, Jose E. Sanguino, Ant6nio Rodrigues. IT - Inst. de Telecomun., Lisbon. A GPS-based Mobile Coordinated Positioning System for Firefighting Scenarios. ISBN 978-9957-486-00-6

[26] Open Mobile Alliance. Prieiga per internetą: http://openmobilealliance.org/about-oma/ [Žiūrėta: 2016 05 07]

[27] Hui Liu, Houshang Durabi, Pat Banerjee, Jing Liu.“ Survey of Wireless Indoor Positioning Techniques and Systems“. IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART C: APPLICATIONS AND REVIEWS, VOL. 37, NO. 6, NOVEMBER 2007. DOI 10.1109/TSMCC.2007.905750

[28] Wenyan Zhang1,Ximing Cui,Dengfeng Li, Debao Yuan, Mengru Wang. China University of Mining & Technology (Beijing). The Location Privacy Protection Research in Location-based Service.

[29] Xinxin Liu (Ph.D. Student, Second Year) and Xiaolin Li (Advisor).Scalable Software Systems Laboratory University of Florida, Gainesville. Privacy Preserving Techniques for Location Based Services in Mobile Networks. DOI 10.1109/IPDPSW.2012.306

[30] „SQL Dialects“. Prieiga per internetą: http://docs.jboss.org/hibernate/core/3.3/reference/en/html/session-configuration.html [Žiūrėta: 2016 03 21]

[31] „SkyHook“ Prieiga per internetą: http://www.skyhookwireless.com/ [Žiūrėta: 2016 04 17]

7. Terminų ir santrumpų žodynas

DB – duomenų bazė.

OS – operacine sistema.

MAC – kompiuteriaus / telefono / įrenginio fizinis adresas.

Role-based access control (RBAC) - vaidmenimis pagrįsta prieigos valdymo kontrolė.

GPS (angl. Global Positioning System) – Visuotinė padėties nustatymo sistema, arba Globali pozicionavimo sistema. Leidžia nustatyti objekto koordinates bet kurioje pasaulio vietoje.

Galileo - palydovinė navigacinė sistema, kuriama Europos palydovinės navigacijos industrijos, konsorciumo.

GLONASS – globali navigacinė Sistema, rusiška GPS ir „Galileo“ alternatyva.

LBS (Location Based Service) – vietos nustatymo paslaugos.

GTRBAC (Generalized Temporal Role-Based Access Control Model) – praplėstas laikiną informacija apibendrintas (formalus)RBAC modelis.

GSTRBAC (Generalized Spatio-Temporal Role-Based Access Control Model) – apibendrintas laiko ir vietos informacija praplėstas RBAC modelis.

UML (Unified Modeling Language) - vieninga modeliavimo ir specifikacijų kūrimo kalba, skirta specifikuoti, atvaizduoti ir konstruoti objektiškai orientuotų programų dokumentus.

OCL (Object Constraint Language) - deklaratyvi ribojimų kalba, skirta aprašyti taisykles taikomas UML modeliams.

RADIUS (Remote Authentication Dial In User Service) - kompiuterių tinklo protokolas, leidžiantis centralizuoti autentifikacijos (prieigos), autorizacijos ir apskaitos valdymą tinklo naudotojams arba įrenginiams, besijungiantiems prie tam tikrų tinklo paslaugų.

RMI (Remote Method Invocation) - standartų sistema koordinuotam Java kalba parašytų programų darbui Internete.

IDE (Integrated Development Environment) – integruote kūrimo aplinka.

JDK (Java development kit) – java programavimo aplinka.

RADIUS serveris – serveris, kuris veikia RADIUS protokolo pagrindų ir leidžia centralizuoti autentifikaciją ir autorizaciją.

8.Priedai

8.1. Parengtas straipsnis

Centralized network access control system based on the Spatio-Temporal-RBAC model and Radius protocol

Ingrida Lagzdinyte-Budnike
Kaunas University of Technology
Kaunas, Lithuania
Ingrida.lagzdinyte@ktu.edu

Jevgenijus Sobolevas
Kaunas University of Technology
Kaunas, Lithuania
Eugenijus07@gmail.com

***Abstract* — Paper describes designed and developed centralized network access control system based on time (temporal) and location (spatial) information – an extended RBAC model. RBAC model extensions also are related to system functioning in wireless network specifics. The system allows to distribute access rights to the wireless network users based on the location and time of network access, authorization result for network user depends on actual location and current date/time. The system supports Radius protocol, which provides compatibility with various network devices. System has modular architecture that makes it easier to extend or replace existing functionality. System operations are described using context and sequence diagrams.**

Keywords — Radius; STRBAC; Centralized; Wi-Fi; Wireless network; access control; RBAC; location based authorization; time based authorization;

I. *Introduction*

Nowadays wireless networks are widespread and their usage is steadily increasing [1, 2]. Wireless networks are used privately, at home, at public areas (shopping malls, restaurants, outdoors), in the educational and administrative authorities and etc. The spread of wireless networks increases a prevalence of hacking or unauthorized access risks, thus complicating an access control. Access to wireless networks is not always properly protected, secured and managed [3].

Widespread of the wireless networks and wide usage of the mobile devices creates the need for such applications and services that can use time and location information to improve their existing functionality. For example, in the university during exams there would be convenient to have the possibility to deny access to the wireless network for the group of students who are passing exam only for the classrooms where exam is hold. At same time the access restrictions would not be applied for the lectors in the same classrooms. The access control can be accomplished even if students and teachers are connected to wireless network via same access point. The software can be useful and for business entities, i.e. hotels providing wireless network access for certain customers in the hotel rooms. Similar type of functionality can be useful or even important for the restaurants, banks, various public events and areas with the requirement to allocate access to wireless network by location, limiting area of permitted access for relevant users, including allowed access time information. User location information and connection time can be used to improve protection of network access control.

To support above mentioned functionality it would be required more complex access control systems. There is growing need to modify existing access control models to support advanced features.

One of the most commonly used practices for the standard access control implementation is based on the role-based access control (RBAC) model [4, 5]. Using this model, a role is assigned to each user, and then permissions are set to each role. In such case different users can have different access rights.

There are several extensions of the RBAC model that allow including of the additional information about the users in the process of the authorization [6-9].

There are various studies and researches that focus on possibilities of RBAC model extensions [10, 11]. In these studies, authors make focus on the RBAC extension on the conceptual level, but in the most cases they are not providing at all or providing very little information about how the following models should be adopted to the different environments or integrated with other systems, i.e. the model adaptation to use with the wireless network.

Further in this paper similar other researches are discussed in chapter II. The architecture and basic principles of our implementation of the centralized access control system based on STRBAC model are described in chapter III. Testing process of the developed software and further work required

for the system improvement, including parameters optimization tasks are specified in chapter IV.

II. *Related works*

Similar researches have been executed by Yue Zhang and his team. They offer RBAC model extension with time information (called "Generalized Temporal Role Based Access Control - GTRBAC"). In the research work of Abdunabi and authors RBAC model was extended with space and time information, then it was used in smart phone application "iMedik" [12, 13]. Further these two case studies will be discussed.

A. *Deployment of the GTRBAC model*

Yue Zhang and James B.D. Joshi studied security issues of the various resources and were trying to extend regular RBAC model with temporal information. They proposed additional RBAC model extension which supported rules and authorization based on the temporary information. Studies have shown that such functionality and features greatly facilitates system administration. However, GTRBAC model quite rarely is used in real environments, because of complexity in the implementation stage. Authors have mentioned, that GTRBAC model has a lot of constraints, which should be taken into account and makes implementation challenging and complicated, especially when it is applied to the real world environments.

In GTRBAC model we can distinguish the following variable constraints:

- *Time* – the ability to assign permissions or restrict user actions by the time. For example, the employee's working hours are from 9 a.m. to 5 p.m. At these time employers can use system resources, after work hours the system will deny access.
- *Periodicity* – the possibility for the periodical authorizations or restrictions. For example, an employee uses the system only on Mondays. On other days access might be restricted.
- *Quantity or quantitative restriction* – allows to set the number of how many times the certain resource or service can be used.

Above mentioned constraints define restrictions, which are used for the allocation of allowance. Using GTRBAC model co-authors have developed a prototype system, which allows to distribute permissions and restrictions depending on the temporal information. However, user location information usage for RBAC model was not discussed.

B. *GSTRBAC model usage in mobile application "iMedik"*

Ramadan Abdel Nabi and co-authors were solving how to improve private information protection of clinic patients. Doctors in the clinic used mobile and handheld computers with "iMedik" application which allowed to observe personal information like disease description, home address and etc. However, there was a problem – how to protect patients' personal information in such a way, that doctors could reach personal data of the patients only in the clinic place and only during working hours. Doctor can lose a mobile device with all patients' personal data (online data can be saved), and any other ineligible person who will found lost mobile device would be able to access patients' personal information and use it by his own needs. Traditional role based access control models, such as RBAC does not solve such problem.

The authors' proposed solution was GSTRBAC model that takes into account not only the user's role, but also the location and time information. During the attempt to reach personal information of the patient, the time and location of the doctor is being checked. If the doctor or other person finds the lost mobile device and attempts to access the patient's information outside the clinic or after working hours he would be blocked. To identify location of the user, authors have used GPS coordinates. Therefore, GPS is not the best solution for location determination *inside buildings*.

III. *Developed system description*

The main system goal is to improve the wireless network authorization process by allowing to authorize network users depending on their location and connection time. The user location is obtained by other external system. To achieve that it was decided to use RBAC model concepts:

a) By extending RBAC with the location and time information;

b) By evaluating if extended RBAC can be applied on the functions of the wireless network specifics;

A. *Spatio Temporal Role Base Access Control (RBAC) model*

The RBAC model extended with time and location information (STRBAC) is shown below in Fig. 1. The components of the model are:

- *User* – a person or device that will use the system.
- *Role* – right or responsibility that is assigned to the user (e.g. any work function in the organization).
- *Permission* – right or permission to perform an action with an object or resource.
- *Time information* – extends the role or permission with time information that allows configuring permissions or restrictions for the user actions depending on the time.
- *Periodicity* – allows configuring restrictions or permissions periodicity (e.g. on each Monday).
- *Location information* – allows to configure restrictions or permissions depending on the location of the user. The user's location is obtained by another system, which informs developed system by providing to it exact room name where user is located. For example, the user *A* is in 302 classroom. We know that the 302 classroom is located on the 3rd

floor. So it can be said that location detection supports *x;y;z* coordinates.

Using such model each user is linked with a certain role (permissions), which is then linked with time and location information. In addition, such permissions may be periodic, e.g. user *A* can use resource *R1* every Monday at 2 p.m. from location *L1*.

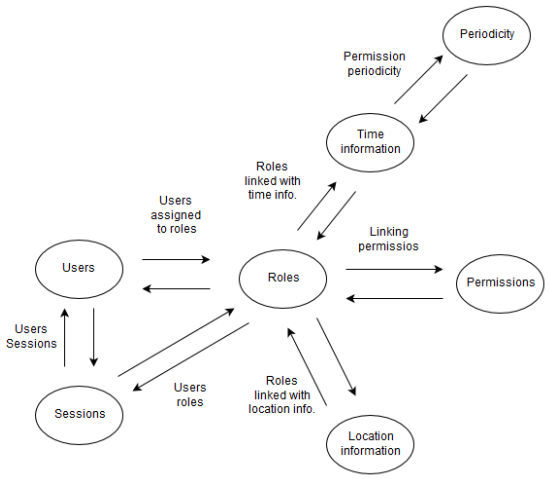


Figure 1. "STRBAC model"

This model allows dividing users into groups (roles), where each group is linked with the specific access rights. Moreover, permissions are linked with permissive access, time and location information, as well as the periodical permits. For example, employees who belong to group *G1* will be able to use the network from the place *L1*, only on Mondays and on Fridays from 8 a.m. to 5 p.m. The access on all other days will be denied. However, the group *G2* members will be able to use the network from *L1* on any day.

B. *Developed system functinallity*

System management is made through a graphical user interface, which allows:

1. *Manage network users.* Network user management includes: creation of the user, user personal information editing, deleting existing user.

2. *Manage user groups.* Management of the user groups (groups corresponds to roles) includes: assign or remove a user to or from one or more groups. Creating new or deleting existing group, changing group description. Group management includes linking of the group with permitted network access places and time profiles. Each group optionally can be linked with the notification template.

3. *Event log*. System tracks all important events such as administrator actions and system actions, including actions of the network user (authorization, accounting, disconnecting), sent notifications and other information. Event log is provided within graphic user interface with search and different filters features. On each log event it provides additional information about events, such as why the network user is prohibited to grant network access or why the user has been disconnected from the network.

4. *Update of the building, location plans or places.* Location information of the network users is requested from other external system (positioning service). In order to ensure smooth communication between developed authorization and positioning systems, building plans in both systems should be synchronized. If the location maps (contains all buildings, floors and rooms) are updated in positioning service, then they should be synchronized with the developed authorization system. This action can be triggered from graphic control panel and processed automatically. Update of location maps in developed system consists of removing the outdated locations and downloading, updating, saving the updated ones. Such process ensures that location objects in both systems are synchronized.

5. *Manage time profiles.* Time profiles management consists of creating a new profile, editing current profile and removal of existing profile. Time profiles enable identification of permissive connection time range and weekday for the certain location. The system allows to link different time profiles with multiple locations which are also assigned with certain group. For example, the group *G1* members are allowed to use network from room *R1* only on Mondays from 9 a.m. To 5 p.m., and the *G2* group members are allowed to use network from the same room all day long.

6. *Manage SMS notifications templates.* System provides notifications via SMS, custom notification template can be defined for each supported notification type. SMS notifications can be sent to the system administrator providing important information or to certain group members providing relevant information. Each location assigned to the group can have different SMS notification. For example, user *U1* is a member of group *G1*. Notification template *T1* is assigned to room *R1* and *G1*. When user *U1* will be granted to access the network and his location would be *R1*, he will get notification *T1*. It is possible to determine notification by type. The notification message can be sent when user gets right to access the network. Another notification can be sent when user is disconnected or user is connected from the specific room.

Above listed system features allows to have user groups, that could be assigned different access permissions with the exact location and time profile. Each network user can be assigned to one or more groups, location and time profile can be assigned to each user group.

Network user authorization process is fully automatic and does not require any action of system

administrator. This process is explained in more detail in chapter III section D “Network user authorization process”.

C. *System architecture*

The system has a modular architecture where functionality can be easily extended or improved.

System was developed using Java DAO (Data Access Object) pattern [14], which allows to separate system business logic from database layer. The pattern also helps to reduce system maintenance or replacement costs.

In order to migrate existing database vendor to other, Hibernate technology was used. It ensures a smooth migration to the supported databases.

System context is shown on Fig. *2*. It shows system business processes. The developed system components are marked in gray. Data between the sub systems (system management subsystem and control sub system) is transferred using RMI. Communication between target network devices, routers or access points, user authentication subsystem is organized by RADIUS protocol.

The system communicates with the SMS notifications messaging service via HTTP POST requests.

We can distinguish 3 subsystems in the system:

1) Network user authentication subsystem;

2) The control subsystem;

3) System control panel with graphical user interface.

Network user *authentication subsystem* is responsible for processing and analysing the RADIUS packets, network user authorization process. Management subsystem is responsible for users, user groups, locations mappings and time profiles administration.

Location positioning service is responsible for obtaining user location and providing it to our proposed authorization system. By now instead of the location system its simulator is used. Authorizaiton system communicates with location positioning system simulator via RMI. In the future proposed system can be tuned up (implemented) to work with real positioning service and communicating for example via HTTP requests or in other way. Today there are different ways to obtain indoor user location. For example, Wi-Fi based positioning system (WPS) [19], Received signal strength indication (RSSI) [20] and other ways [21, 22].

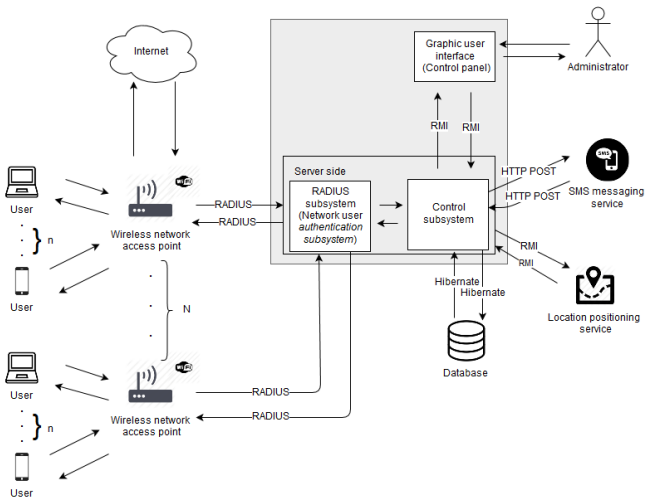


Figure 2. “System context model”

Control subsystem consists of client and server sides. Client side delivers the graphical interface, which provides functions for system management (system control panel). Server side includes all functionality which is required to ensure system smooth work.

The control subsystem and system control panel are physically separated and may be running either on the same system node or on the different one.

Main users of the developed system are system administrators, which have a pre-configured account and can access the control panel. Wireless network users can be interpreted as non-direct system users. User credentials and pre-configured access rules for network access should present in the developed system, however users might not be aware of the developed system in place, since they are not communicating with the system directly.

D. *Network user authorization proccess*

The authorization process based on STRBAC model is wrapped by Radius protocol. This allows smooth system integration with the whole range of the different level wireless network devices (enterprise level routers or switches, as well as low level consumer equipment) which supports Radius protocol (RFC-2866, RFC-2138) [15, 16].

Network user authorization and accounting process is shown in a simplified sequence diagram (Fig. 3). System responses to the network user are:

- Access-Accept.
- Access-Reject.
- Access-Accept with further user accounting process.

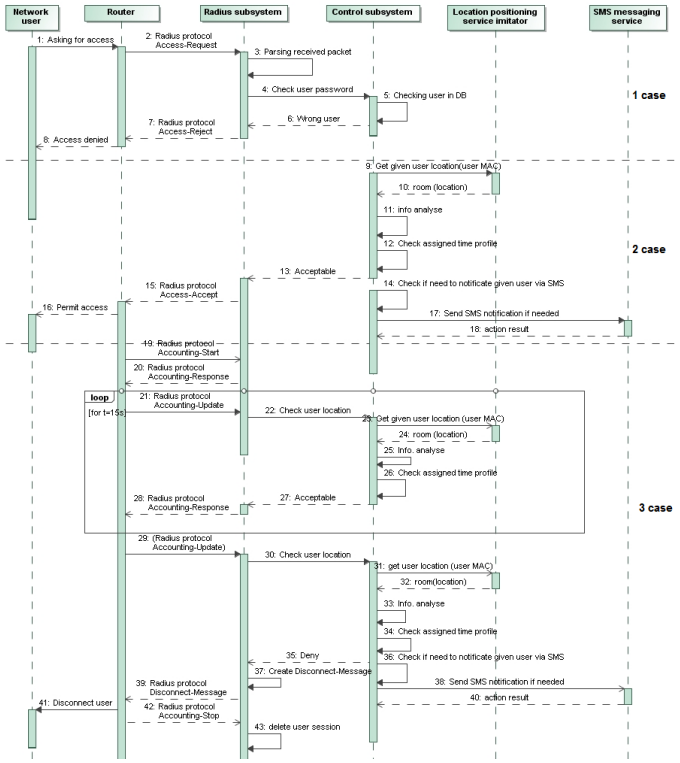


Figure 3. "Authorization process of the network users"

Initially, the network users connect to the wireless access point in usual way. Then router requests developed system authorization subsystem, to check if certain user can access the network, by sending Radius "Access-Request" packet. The authorization subsystem using control subsystem functionality checks certain user username and password in the database. If given user credentials are incorrect, system denies access, sending to router - Radius "Access-Reject" packet, access for given network user is prohibited. If the SMS notification is configured and SMS sending in the user profile is allowed (user has agreed to receive notifications via SMS messaging), he will get SMS notification explaining why his attempt to get access was rejected (Fig. 3, 1-8 steps in 1st authentication sequence diagram case).

If during authentication phase user was granted to access the network, system would provide accounting feature (in case Radius Accounting feature is supported and enabled in the router) (Fig. 3, 9-41 steps in the sequence diagram. Router sends "Accounting-Start" request and system replies with Radius "Accounting-Response". Further periodically (time interval depends on the router configuration) router will be sending Radius "Accounting-Update" requests and on each request system will check user location and time. If it will be detected that location of the user or connection time is denied by assigned time profile to the current user group, access to the network will be prohibited. System will send back Radius "Disconnect-Message". This packet should trigger disconnect of the appropriate user from the wireless network and inform system about accounting end (Radius "Accounting-Stop"). According to the configured notifications settings, user can be notified via SMS about any event. For example, after successful connection he can get an advertisement. If the forced disconnect occurred (by the system) from the network, he can get extra information why this has happened, i.e. room which he entered is prohibited for his group.

Accounting feature is also important if existing Wi-Fi network infrastructure is using Wi-Fi controller and fast roaming feature. In this case accounting will help to track clients migration and disconnect them from network if required. For example clients do not do reauthentication when fast roaming. Once authorized, client can move to different building if it is covered by same network. But accounting feature will check (periodically e.g. every 2m) client role (group) and assigned permissions to this role (group) if it will be noticed that this client using network at his group restricted place or time, he will be disconnected.

IV. *Developed system tests and future works*

System testing was performed by using NTradPing [17] tool, which is designed to make and send a single Radius requests.

Unit testing automatization was made by jUnit [18] library. During unit testing individual system units and functions were tested.

Network user authorization process was tested using combined functional testing with NTradPing tool and location system simulator. For example, we can describe shortened test scenario as further: during accounting session, in the location system simulator user location was manually changing to restricted area. Simultaneously system was checking if this user was disconnected from the network. Time based restrictions were checked similarly also. Functional testing has been applied in order to test the graphical user interface (control panel).

During integration tests, several router manufacturers (*D-Link* and *Mikrotik)* were tested. All errors and inaccuracies founded during testing were successfully corrected.

In future it is necessary to create the tool that will be able to simulate the required amount of network users. Such tool will help to perform a stress test for testing average service time of network users when a lot of wireless network users are connected.

In order to fully prepare system for the effective functioning it is necessary to make following additional experimental studies:

- To detect optimal Accounting and Authorization service configurations, by analyzing servicing times and durations (average and maximal) of network users and finding correlation of those times and number of user requests (system load). Such study should show how long it may take to authenticate a single user, depending on a number of simultaneously connecting and connected to the network users.

- To identify minimal required hardware resources that are required to run system.
- Additional experimental studies might be required to give recommended time interval value for the Radius accounting requests in router configuration.

V. *Conclusions*

Centralized network access control system that allows authorizing network users relying on their location and weekday including time range of network access was developed and described. System provides graphical user interface that makes easier to manage users, user groups, and their access rights. System fully supports Radius protocol.

RBAC model extensions related with location and time attributes were offered and described. Model was successfully integrated and adopted to the developed system. System functioning in wireless network specifics was estimated by processing only spatial area-type attributes.

The developed system can be used for institutions, various other public places or organizations with the requirement to separate access to wireless network by location, week days, time information or to provide centralized expanded access control. System is integrated with notifications via SMS service, which not only informs network users or system administrators about various system events, but also opens unlimited marketing possibilities.

Functionality of the system was tested using the location system simulator.

The future experimental studies should include tuning up system parameters considering different system users' location and time, including different number of system users.

References

[1] Office for Nation Statistics, "Internet Access - Households and Individuals", 2013. Internet access: http://www.ons.gov.uk/ons/dcp171778_322713.pdf

[2] The Statistics Portal, "Global number of pulic hotspots", 2009 - 2015. Internet access: http://www.statista.com/statistics/218596/global-number-of-public-hotspots-since-2009/

[3] Bogdan Botezatu, HOTforSecurity, "25 Percent of Wireless Networks are Highly Vulnerable to Hacking Attacks, Wi-Fi Security Survey Reveals", 2009 - 2015. Internet access: http://www.hotforsecurity.com/blog/25-percent-of-wireless-networks-are-highly-vulnerable-to-hacking-attacks-wi-fi-security-survey-reveals-1174.html

[4] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, "Role-based access control models," IEEE Comput., vol. 29, no. 2, pp. 38–47, Feb. 1996.

[5] Alan C. O`Connor, Ross J.Loomis, "2010 Economic Analysis of Role-Based Access Control", National Institute of Standards and Technology, December 2010. Internet access: http://csrc.nist.gov/groups/SNS/rbac/documents/20101219_RBAC2_Final_Report.pdf

[6] Xiutao Cui, Yuliang Chen, Junzhong Gu, „Ex-RBAC : An Extended Role Based Access Control Model for Location-aware Mobile Collaboration System", Second International Conference on Internet Monitoring and Protection (ICIMP 2007)

[7] Yu Wanjun, Wang Yong, "Research on Security Status Recovery in Temporal Role-Based Access Control System", 2009 International Conference on Information Management, Innovation Management and Industrial Engineering

[8] Xun Li, Sang Bong Yoo, "Extended Role-Based Security System using Context Information", 2008 Second International Conference on Future Generation Communication and Networking

[9] Hsing-Chung Chen, Yung-Fa Huang, Syuan-Zong Lin, "Generalized Associated Temporal and Spatial Role-Based Access Control Model for Wireless He terogeneous Networks", 2011 Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing

[10] Elisa bertino, Barbara Catania, Maria Luisa Damiani, "GEO-RBAC: A Spatially Aware RBAC",SACMAT'05, June 1–3, 2005, Stockholm, Sweden.

[11] Kai Ouyang, James B.D. Joshi, "CT-RBAC: A Temporal RBAC Model with Conditional Periodic Time", 2007, IEEE

[12] YueZhang, James B.D. Joshi. An Implementation Architecture of the GTRBAC Model (2010). Information Science Department University of Pittsburgh Pittsburgh, P A, US.

[13] Ramadan Abdunabi, Mustafa Al-Lail, Indrakshi Ray, and Robert B. France Specification, Validation, and Enforcement of a Generalized Spatio-Temporal Role-Based Access Control Model (September 2013).

[14] Oracle, "Core J2EE Patterns - Data Access Object". Internet access: http://www.oracle.com/technetwork/java/dataaccessobject-138824.html

[15] Network Working Group - Request for Comments:2866, "RADIUS Accounting", Livingston June 2000. Internet access: https://tools.ietf.org/html/rfc2866

[16] Network Working Group - Request for Comments:2838, "Remote Authentication Dial In User Service (RADIUS)", Livingston April 1997. Internet access: https://tools.ietf.org/html/rfc2138

[17] Novell, masterSoft "NTRadPing 1.5 RADIUS Test Utility" Internet access: https://www.novell.com/coolsolutions/tools/14377.html

[18] JUnit framework. Internet access: http://junit.org/

[19] Binghao Li, James Salter, Andrew G. Dempster and Chris Rizos, "Indoor Positioning Techniques Based on Wireless LAN", School of Computer Science and Engineering, Sydney, Australia.

[20] Chang N, Rashidzadeh R, Ahmadi M. 2010. Robust indoor positioning using differential Wi-Fi access points. IEEE Transactions on Consumer Electronics.

[21] Houshang Darabi, Pat Banerjee, Jing Liu,"Survey of Wireless Indoor Positioning Techniques and Systems", IEE Transactions on systems, man, and cybernetics - part C, VOL. 37, NO.6, November 2007

[22] Reza AW, Geok TK. 2009. Investigation of indoor location sensing via RFID reader network utilizing grid covering algorithm. Wireless Personal Communications.

8.2 .Pagrindiniai funkciniai reikalavimai

Toliau pateikiama pagrindinių funkcinių reikalavimų detalizacija:

Reikalavimas: 9.1	Reikalavimo tipas: 9	Įvykis/panaudojimo atvejis: PA1
Aprašymas: Administratoriaus įvesti prisijungimo duomenys (vartotojo vardas ir slaptažodis) turi būti sulyginami su sistemos DB esančiais.		
Pagrindimas: Neautorizuoti vartotojai neturi matyti sistemos vidinės informacijos bei administruoti sistemą.		
Šaltinis: Administratorius.		
Tinkamumo kriterijus: Prisijungus administratoriui tampa pasiekiamas valdymo skydas (parodomas pagrindinis langas).		
Užsakovo patenkinimas: 1	Užsakovo nepatenkinimas: 5	
Priklausomybės: nėra.	Konfliktai: nėra.	
Papildoma medžiaga: nėra.		
Istorija: sukurtas 2014 03 01		

Reikalavimas: 9.2	Reikalavimo tipas: 9	Įvykis/panaudojimo atvejis: PA2
Aprašymas: Pridedant naują vartotoją visi privalomi laukai turi būti pažymėti ir užpildyti. Taip pat turi būti galimybė iškarto priskirti vartotoją prie sistemoje esančios grupės (pvz. pasirenkant iš grupių sąrašo).		
Pagrindimas: Administratorius turi gebėti greitai bei lengvai pridėti naują vartotoją.		
Šaltinis: Administratorius.		
Tinkamumo kriterijus: Pridedant naują vartotoją privalomi laukai pažymėti ir užpildyti.		
Užsakovo patenkinimas: 2	Užsakovo nepatenkinimas: 5	
Priklausomybės: 9.3	Konfliktai: nėra.	
Papildoma medžiaga: nėra.		
Istorija: sukurtas 2014 03 01		

Reikalavimas: 9.3	Reikalavimo tipas: 9	Įvykis/panaudojimo atvejis: PA2, PA3, PA7
Aprašymas: Turi būti suformuojamas ir atvaizduojamas sistemoje esančių grupių sąrašas.		
Pagrindimas: Panaudojant sąrašą galima lengvai manipuliuoti esančiomis grupėmis		
Šaltinis: Administratorius.		
Tinkamumo kriterijus: Sėkmingai suformuojamas ir atvaizduojamas sistemoje esančių grupių sąrašas.		
Užsakovo patenkinimas: 2	Užsakovo nepatenkinimas: 5	
Priklausomybės: nėra	Konfliktai: nėra.	
Papildoma medžiaga: nėra.		
Istorija: sukurtas 2014 03 01		

Reikalavimas: 9.4	Reikalavimo tipas: 9	Įvykis/panaudojimo atvejis: PA3
Aprašymas: Redaguojant esamą vartotoją, visi prieš tai užpildyti laukai turi būti automatiškai užpildomi.		
Pagrindimas: Administratorius turi gebėti greitai ir patogiai redaguoti esamą vartotoją.		
Šaltinis: Administratorius.		
Tinkamumo kriterijus: Redaguojant esamą vartotoją laukai automatiškai užpildomi.		
Užsakovo patenkinimas: 2	Užsakovo nepatenkinimas: 5	
Priklausomybės: 9.3, 9.5	Konfliktai: nėra.	
Papildoma medžiaga: nėra.		
Istorija: sukurtas 2014 03 01		

Reikalavimas: 9.5	Reikalavimo tipas: 9	Įvykis/panaudojimo atvejis: PA3
Aprašymas: Redaguojant esamą vartotoją, turi būti parodoma vartotojo asmeninė informacija ir grupių sąrašas kurioms jis priklauso (galimybė keisti asmeninę informaciją/šalinti iš grupių).		
Pagrindimas: Administratorius turi gebėti greitai ir patogiai redaguoti esamą vartotoją.		
Šaltinis: Administratorius.		
Tinkamumo kriterijus: Redaguojant esamą vartotoją laukai automatiškai užpildomi, parodoma vartotojo asmeninė informacija.		
Užsakovo patenkinimas: 2	Užsakovo nepatenkinimas: 5	
Priklausomybės: 9.3, 9.4	Konfliktai: nėra.	
Papildoma medžiaga: nėra.		
Istorija: sukurtas 2014 03 01		

Reikalavimas: 9.6	Reikalavimo tipas: 9	Įvykis/panaudojimo atvejis: PA4
Aprašymas: Šalinant esamą vartotoją sistema turi automatiškai jį pašalinti iš grupių, kuriuose jis buvo pridėtas. Vartotojo šalinimas vyksta per sąrašą (pasirenkant vartotojo iš sąrašo). Taip pat turi būti galimybė administratoriui šalinti vartotoją įvedant konkretu vartotojo vardą (paieška).		
Pagrindimas: Administratorius turi gebėti greitai pašalinti sistemoje esančius vartotojus nesudarant „šiukšlių“.		
Šaltinis: Administratorius.		
Tinkamumo kriterijus: Tam, kad pašalinti vartotoją nereikia iš pradžių jį „išimti“ iš grupės.		
Užsakovo patenkinimas: 4	Užsakovo nepatenkinimas: 5	
Priklausomybės: 9.7	Konfliktai: nėra.	
Papildoma medžiaga: nėra.		
Istorija: sukurtas 2014 03 01		

Reikalavimas: 9.7	Reikalavimo tipas: 9	Įvykis/panaudojimo atvejis: PA4, PA5, PA6
Aprašymas: Turi būti rodomas bei suformuojamas esamų vartotojų sąrašas.		
Pagrindimas: Panaudojant sąrašą galima lengvai manipuliuoti esančiais vartotojais.		
Šaltinis: Administratorius.		
Tinkamumo kriterijus: Sėkmingai suformuojamas bei atvaizduojamas sistemoje esančių vartotojų sąrašas.		
Užsakovo patenkinimas: 4	Užsakovo nepatenkinimas: 5	
Priklausomybės: nėra.	Konfliktai: nėra.	
Papildoma medžiaga: nėra.		
Istorija: sukurtas 2014 03 01		

Reikalavimas: 9.8	Reikalavimo tipas: 9	Įvykis/panaudojimo atvejis: PA5
Aprašymas: Pridedant naują grupę, turi būti galimybė iškarto priskirti jai sistemoje esančius vartotojus. Taip pat turi būti grupės pavadinimo validavimas.		
Pagrindimas: Administratorius turi gebėti greitai sukurti naują grupę.		
Šaltinis: Administratorius.		
Tinkamumo kriterijus: Sukuriant naują grupę, galima iškarto priskirti vartotojus.		
Užsakovo patenkinimas: 4	Užsakovo nepatenkinimas: 5	
Priklausomybės: 9.7, 9.9	Konfliktai: nėra.	
Papildoma medžiaga: nėra.		
Istorija: sukurtas 2014 03 01		

Reikalavimas: 9.9	Reikalavimo tipas: 9	Įvykis/panaudojimo atvejis: PA5, PA6
Aprašymas: Pridedant naują grupę arba redaguojant esamą, turi būti patikrinta ar grupė su nurodytu pavadinimu jau egzistuoja, jei bus rasta tokia pati grupė (grupės pavadinimas) sistema turi neleisti sukurti tokią grupę, bei maloniai paprašyti pakeisti grupės pavadinimą.		
Pagrindimas: Grupės vardai neturi dubliuotis.		
Šaltinis: Administratorius.		
Tinkamumo kriterijus: Jeigu pavyko rasti grupę su tokiu pačiu pavadinimu išvedamas pranešimas.		
Užsakovo patenkinimas: 4	Užsakovo nepatenkinimas: 5	
Priklausomybės: nėra.	Konfliktai: nėra.	
Papildoma medžiaga: nėra.		
Istorija: sukurtas 2014 03 01		

Reikalavimas: 9.10	Reikalavimo tipas: 9	Įvykis/panaudojimo atvejis: PA6
Aprašymas: Redaguojant esamą grupę turi būti automatiškai užkraunamas grupėje esančių vartotojų sąrašas, taip pat turi būti galimybė pridėti arba pašalinti vartotojus. Taip pat priskirinėti prie grupės galimas prisijungimo vietas (zonas), pasirenkant iš sistemoje esančių zonų sąrašo.		
Pagrindimas: Administratorius turi gebėti greitai redaguoti grupę (keisti grupės pavadinimą, priskirinėti arba šalinti vartotojus).		
Šaltinis: Administratorius.		
Tinkamumo kriterijus: Redaguojant grupę galima keisti jos pavadinimą, priskirinėti vartotojus arba šalinti grupėje esančius vartotojus. Priskirinėti prie grupės galimas prisijungimo vietas/zonas.		
Užsakovo patenkinimas: 4	Užsakovo nepatenkinimas: 5	
Priklausomybės: 9.7, 9.9, 9.11	Konfliktai: nėra.	
Papildoma medžiaga: nėra.		
Istorija: sukurtas 2014 03 01		

Reikalavimas: 9.11	Reikalavimo tipas: 9	Įvykis/panaudojimo atvejis: PA6
Aprašymas: Turi būti suformuotas ir atvaizduotas sistemoje esančių zonų sąrašas.		
Pagrindimas: Panaudojant sąrašą galima lengvai manipuliuoti esančiomis zonomis		
Šaltinis: Administratorius.		
Tinkamumo kriterijus: Sėkmingai suformuotas ir atvaizduotas sistemoje esančių zonų sąrašas.		
Užsakovo patenkinimas: 4	Užsakovo nepatenkinimas: 5	
Priklausomybės: nėra.	Konfliktai: nėra.	
Papildoma medžiaga: nėra.		
Istorija: sukurtas 2014 03 01		

Reikalavimas: 9.12	Reikalavimo tipas: 9	Įvykis/panaudojimo atvejis: PA7
Aprašymas: Šalinant esamą grupę, priskirtos prie grupės galimos prisijungimo zonos turi būti automatiškai „atrišamos“, kad nesusidarytu „šiukšles“. Grupės šalinimas vyksta pasirenkant reikiamą grupę iš grupių sąrašo.		
Pagrindimas: Administratorius turi gebėti greitai pašalinti esamą grupę. Neturi būti papildomų veiksmų, pavyzdžiui, kad nereikėtu iš pradžių „atrišti“ galimas prisijungimo zonas, o tik paskui pašalinti grupę.		
Šaltinis: Administratorius.		
Tinkamumo kriterijus: Šalinant sistemoje esančią grupę galimos prisijungimo zonos automatiškai „atrišamos“.		
Užsakovo patenkinimas: 4	Užsakovo nepatenkinimas: 5	
Priklausomybės: 9.3, 9.13	Konfliktai: nėra.	
Papildoma medžiaga: nėra.		
Istorija: sukurtas 2014 03 01		

Reikalavimas: 9.13	Reikalavimo tipas: 9	Įvykis/panaudojimo atvejis: PA7
Aprašymas: Šalinant esamą grupę, priskirti prie grupės vartotojai turi būti automatiškai „atrišami“, kad nesusidarytu „šiukšles“.		
Pagrindimas: Administratorius turi gebėti greitai pašalinti esamą grupę. Neturi būti papildomų veiksmų, pavyzdžiui, kad nereikėtu iš pradžių „atrišti“ vartotojus, o tik paskui pašalinti grupę.		
Šaltinis: Administratorius.		
Tinkamumo kriterijus: Šalinant sistemoje esančią grupę grupės vartotojai sėkmingai „atrišami“.		
Užsakovo patenkinimas: 4	Užsakovo nepatenkinimas: 5	
Priklausomybės: 9.12	Konfliktai: nėra.	
Papildoma medžiaga: nėra.		
Istorija: sukurtas 2014 03 01		

Reikalavimas: 9.14	Reikalavimo tipas: 9	Įvykis/panaudojimo atvejis: PA8
Aprašymas: Atnaujinant pastato planą, turi būti sulyginami sistemoje išsaugotas ir vietos nustatymo sistemoje esantis planai, pasenę objektai turi būti automatiškai pašalinami iš sistemos, o jei atsirado naujų, jie turi būti parsiusti ir išsaugoti.		
Pagrindimas: Atnaujinant sistemoje esanti pastato planą, administratorius neturi atlikti papildomų veiksmų pats (atnaujinimas turi būti automatizuotas).		
Šaltinis: Administratorius.		
Tinkamumo kriterijus: Pastato planas sėkmingai atsinaujinamas, pašalinant pasenusius objektus ir parsiunčiant naujus.		
Užsakovo patenkinimas: 4	Užsakovo nepatenkinimas: 5	
Priklausomybės: 9.11	Konfliktai: nėra.	
Papildoma medžiaga: nėra.		
Istorija: sukurtas 2014 03 01		

Reikalavimas: 9.15	Reikalavimo tipas: 9	Įvykis/panaudojimo atvejis: PA9
Aprašymas: Įvykiai pateikiami sąrašu, rūšiavimo galimybe, taip pat turi būti galimybė pritaikyti filtrą (rodyti įvykius pagal jų tipą).		
Pagrindimas: Administratorius turi aiškiai ir patogiai matyti įvykių sąrašą.		
Šaltinis: Administratorius.		
Tinkamumo kriterijus: Jei įvykių nėra, apie tai turi būti pranešta. Ekrane turi būti rodoma bent dešimt įvykių.		
Užsakovo patenkinimas: 4	Užsakovo nepatenkinimas: 5	
Priklausomybės: 9.16	Konfliktai: nėra.	
Papildoma medžiaga: nėra.		
Istorija: sukurtas 2014 03 01		

Reikalavimas: 9.16	Reikalavimo tipas: 9	Įvykis/panaudojimo atvejis: PA9
Aprašymas: Suformuoti ir atvaizduoti įvykių sąrašą.		
Pagrindimas: Administratorius turi aiškiai ir patogiai matyti įvykių sąrašą.		
Šaltinis: Administratorius.		
Tinkamumo kriterijus: Parodomas suformuotas įvykių sąrašas.		
Užsakovo patenkinimas: 4	Užsakovo nepatenkinimas: 5	
Priklausomybės: nėra.	Konfliktai: nėra.	
Papildoma medžiaga: nėra.		
Istorija: sukurtas 2014 03 01		

Reikalavimas: 9.17	Reikalavimo tipas: 9	Įvykis/panaudojimo atvejis: PA16
Aprašymas: Kai iš maršrutizatoriaus gaunamas RADIUS paketas, pirmiausiai jis apdorojamas, išgaunami reikiami vartotojo duomenis. vartotojas patikrinimas DB, jeigu toks egzistuoja -kreipiamasi į vietos nustatymo sistemą. Visi veiksmai turi būti pilnai automatizuoti. Kai vartotojas praeina arba nepraeina autorizaciją, apie tai yra informuojamas maršrutizatorius.		
Pagrindimas: vartotojo autorizacijos procesas turi būti automatizuotas.		
Šaltinis: Administratorius.		
Tinkamumo kriterijus: Maršrutizatorius gauna patvirtinimo arba paneigimo atsakymą.		
Užsakovo patenkinimas: 4	Užsakovo nepatenkinimas: 5	
Priklausomybės: 9.18, 9.19, 9.20	Konfliktai: nėra.	
Papildoma medžiaga: nėra.		
Istorija: sukurtas 2014 03 01		

Reikalavimas: 9.18	Reikalavimo tipas: 9	Įvykis/panaudojimo atvejis: PA16
Aprašymas: Išgauta iš maršrutizatoriaus atsiusto paketo vartotojo informacija turi būti patikrinta sistemos DB (ar toks vartotojas egzistuoja). Jei vartotojo rasti nepavyko atsakoma maršrutizatoriui, kad vartotojas nepraėjo autorizacijos.		
Pagrindimas: vartotojo autorizacijos procesas turi būti automatizuotas.		
Šaltinis: Administratorius.		
Tinkamumo kriterijus: Maršrutizatorius gauna paneigimo atsakymą. Arba grąžinami rasto vartotojo duomenys.		
Užsakovo patenkinimas: 4	Užsakovo nepatenkinimas: 5	
Priklausomybės: 9.20	Konfliktai: nėra.	
Papildoma medžiaga: nėra.		
Istorija: sukurtas 2014 03 01		

Reikalavimas: 9.19	Reikalavimo tipas: 9	Įvykis/panaudojimo atvejis: PA16
Aprašymas: Gauta iš vietos nustatymo sistemos vartotojo buvimo vieta patikrinama su jam (vartotojui) leistinom vietom.		
Pagrindimas: vartotojo autorizacijos procesas turi būti automatizuotas.		
Šaltinis: Administratorius.		
Tinkamumo kriterijus: Sėkmingai gauta vartotojo (įrenginio MAC) buvimo vieta.		
Užsakovo patenkinimas: 4	Užsakovo nepatenkinimas: 5	
Priklausomybės: 9.20	Konfliktai: nėra.	
Papildoma medžiaga: nėra.		
Istorija: sukurtas 2014 03 01		

Reikalavimas: 9.20	Reikalavimo tipas: 9	Įvykis/panaudojimo atvejis: PA16
Aprašymas: Suformuojamas atsakymas kuris turi būti perduotas maršrutizatoriui. Jei vartotojas nebuvo rastas sistemos DB, sistema turi atsakyti „Access-Reject“ jei vartotojas buvo rastas DB, ir vietos nustatymo sistema grąžino leistina jo įrenginio buvimo vietą atsakoma „Access-Accept“		
Pagrindimas: vartotojo autorizacijos procesas turi būti automatizuotas.		
Šaltinis: Administratorius.		
Tinkamumo kriterijus: Sėkmingai suformuojamas vienas iš galimų atsakymų.		
Užsakovo patenkinimas: 4	Užsakovo nepatenkinimas: 5	
Priklausomybės: 9.17	Konfliktai: nėra.	
Papildoma medžiaga: nėra.		
Istorija: sukurtas 2014 03 01		

Reikalavimas: 9.21	Reikalavimo tipas: 9	Įvykis/panaudojimo atvejis: PA10, PA 12, PA13, PA14
Aprašymas: Pridedant naują laiko profilį / SMS žinutės šabloną arba redaguojant esamą, turi būti patikrinta ar laiko profilis su nurodytu pavadinimu jau egzistuoja, jei bus rastas toks pats laiko profilis (profilio pavadinimas) sistema turi neleisti sukurti tokį profilį, bei maloniai paprašyti pakeisti profilio pavadinimą.		
Pagrindimas: Profilio vardai neturi dubliuotis.		
Šaltinis: Administratorius.		
Tinkamumo kriterijus: Jeigu pavyko rasti profilį/šabloną su tokiu pačiu pavadinimu išvedamas pranešimas.		
Užsakovo patenkinimas: 4	Užsakovo nepatenkinimas: 5	
Priklausomybės: nėra.	Konfliktai: nėra.	
Papildoma medžiaga: nėra.		
Istorija: sukurtas 2014 03 01		