KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

KOMPIUTERIŲ TINKLŲ KATEDRA

Rasa Petrauskienė

Prieigos prie bevielio tinklo resursų valdymas panaudojant vietos informaciją

Magistro baigiamasis darbas

Mokslinė vadovė –

dr. Ingrida Lagzdinytė-Budnikė

Recenzentas –

lekt. Dr. Dangis Rimkus

Kaunas

2011

Turinys

1 ĮVADAS

Dėl prieinamos kainos ir lankstumo bevieliai tinklai yra labai populiari alternatyva laidiniams tinklams. Wigle.net suskaičiuoja apie penkiolika milijonų bevielių tinklų visame pasaulyje ir šis skaičius nuolat smarkiai auga. Bevieliai tinklai diegiami daugelyje įstaigų ir įmonių, tačiau būtent dėl to, kad duomenų perdavimas vyksta atviru oru neapribotoje aplinkoje, jie yra labiausiai pažeidžiami ir atviri įvairioms atakoms, kurios gali baigtis dideliais finansiniais ir moraliniais nuostoliais. Pagal atliktus tyrimus daugelį bevielių tinklų pasaulyje saugo lengvai įveikiamas WEP (angl. WEP – *Wired Equivalent Privacy*) šifravimas. Pavyzdžiui, Londone ir Niujorke, kur buvo suskaičiuota daugiausia prieigos prie bevielio tinklo taškų, daugiau nei pusę prieigos taškų saugo viso labo WEP [1]. Lietuvoje situacija panaši, bet kadangi bevieliai tinklai čia paplito kiek vėliau, santykinai ir yra daugiau naujesnėmis bei saugesnėmis technologijomis paremtų bevielių tinklų.

Autentifikacija ir prieigos prie bevielio tinklo resursų valdymas yra vienas svarbiausių dalykų užtikrinant sėkmingą bevielio tinklo naudojimą. Vietos informacija gali padidinti teisingo vartotojo autentifikavimo tikimybę ir padėti išvengti neautorizuotų vartotojų prisijungimų bei kitų atakų. Moksliniuose darbuose yra aprašyta keletas būdų, kaip galima nustatyti mobilaus vartotojo vietą [9, 10, 22, 23, 24]. Tobulėjant mobilioms technologijoms vietos informacija tapo svarbi prieigos valdymui ir atsiranda vis daugiau mokslinių darbų šia tema. A. Mishra ir S. Banerjee [9] aprašo infrastruktūrą pavadinimu „Secure Spaces“, leidžiančią tik tam tikroje vietoje (taip vadinamoje „saugioje“ vietoje) esantiems vartotojams naudotis tinklo ištekliais. Vietos informacijos nustatymo ir autentifikacijos sistema naudoja RF signalų stipriais paremtą technologiją. Y. S. Cho ir kiti [10] pristato vietos informacija pagrįsto prieigos prie tinklo valdymo (angl. *Location-based network Access Control* – LBAC) protokolą IEEE 802.11 grupės WLAN (angl. *Wireless Local Area Network*) sistemoms saugiai autentifikuoti mobilaus vartotojo vietą ir saugiai paskirstyti bendruosius raktus, skirtus duomenų šifravimui. Autoriai siūlo, kad vietoje tikslaus vartotojų vietos nustatymo, prieiga prie WLAN sistemos būtų suteikta tik tiems vartotojams, kurie yra tam tikrose zonose, kurios atitinkamai yra padengtos kelių prieigos taškų. Naudojant kryptines antenas tokios zonos gali būti norimos formos. Ardagna ir kiti [13, 8, 7] nagrinėja, kaip į tradicinį bendrąjį prieigos valdymo mechanizmą gali būti integruojamos vietos informacija pagrįstos požymiai, kaip jie įvertinami ir pritaikomi. Autoriai taip pat nagrinėja vietos informacijos apsaugos problemą ir detaliau pristato apsaugai naudojamas supainiojimu pagrįstas technologijas. I. Ray ir M. Kumar [12] rašo, kaip formalizuoti vietos informaciją, kaip standartinio privalomojo prieigos valdymo (angl. *Mandatory Access Control*) modelio komponentus susieti su vietos

informacija ir kaip ši vietos informacija gali būti panaudojama nustatyti, ar subjektas turi prieigą prie tam tikro objekto. Darbe aptariamas ir privatumo, t.y. vietos informacijos apsaugos klausimas. Autorių siūlomas modelis yra tinkamas karinėms programoms, į kurias įeina statiniai bei dinaminiai objektai ir kuriose suteikiant prieigą turi būti įvertinta subjektų ir objektų vietos informacija. M. L. Damiani ir kiti [18] pristato Geo-RBAC – role pagrįsto prieigos valdymo (angl. *Role Based Access Control*) modelio išplėtimą įvedant į jį vietos informaciją. R. Bhatti ir kiti [14] aptaria Geo-RBAC valdymo mechanizmą. Autoriai formaliai apibrėžia Geo-RBAC ir politikos specifikavimo kalbos X-GTRBAC administravimo komandų jungimą. [15, 16] pristato LBAC politikų užrašymo kalbas.

Šio baigiamojo darbo tikslas yra sudaryti vietos informacija paremtą prieigos prie bevielio tinklo resursų valdymo modelį, kuris leistų padidinti teisingo autentifikavimo tikimybę bei išplėsti prieigos valdymo galimybes. Baigiamojo darbo uždaviniai yra šie:

1. Ištirti autentifikavimo ir prieigos prie bevielio tinklo resursų valdymo būdus bei nustatyti jų pažeidžiamumus;
2. Ištirti autentifikavimo ir prieigos prie bevielio tinklo resursų valdymo būdų derinimo su vietos informacija galimybes;
3. Pasiūlyti įprastinių autentifikavimo ir prieigos prie tinklo išteklių valdymo mechanizmų derinimo su vietos informacija būdus (-ą), pateikti galimus prieigos valdymo išplėtimus;
4. Suprojektuoti ir realizuoti vietos informacija paremtą prieigos prie bevielio tinklo resursų valdymo sistemą, kuri galėtų veikti kelių aukštų pastato viduje ir tiktų tokiai organizacijai kaip universitetas;
5. Eksperimento būdu įvertinti siūlomo prieigos valdymo būdo savybes.

Darbo struktūra yra sekanti. Pirmame skyriuje nagrinėjami autentifikacijos ir prieigos valdymo mechanizmai, naudojami bevieliuose tinkluose, jų pažeidžiamumai, skirtumai ir panašumai. Antrame skyriuje nagrinėjamos autentifikacijos ir prieigos valdymo mechanizmų derinimo su vietos informacija galimybės. Pirmoje skyriaus dalyje apžvelgiami vietos informacijos gavimo būdai, tada pristatomi egzistuojantys vietos informacijos derinimo su autentifikacija ir prieigos valdymu sprendimai. Trečioje skyriaus dalyje išskiriami vietos informacijos įvedimo į autentifikacijos ir prieigos valdymo procesus privalumai, galiausiai pateikiamas apibendrinimas ir išvados Trečiame skyriuje pristatomas sudarytas prieigos prie tinklo resursų valdymo panaudojant vietos informaciją modelis, aprašomos jo dalys. Antroje skyriaus dalyje pateikiami vietos informacija grįsto prieigos valdymo pažeidžiamumai, trečioje – specifikuojami reikalavimai projektuojamai sistemai. Likusiose dalyse pateikiama

saugos politika, aprašomos projektuojamos sistemos duomenų struktūros, architektūra, galiausiai pateikiamos programinių modulių ir objektų, panaudotos techninės ir programinės įrangos specifikacijos. Ketvirtame darbo skyriuje aprašomas sistemos testavimas ir eksperimentiniai tyrimai, o pabaigoje pateikiamos išvados.

2 BEVIELIUOSE TINKLUOSE NAUDOJAMI AUTENTIFIKACIJOS, AUTORIZACIJOS BEI PRIEIGOS VALDYMO MECHANIZMAI IR JŲ PAŽEIDŽIAMUMAI

Informatikos moksle prieigos valdymas yra paslauga arba sistema, kuri kontroliuoja informacinės sistemos išteklių panaudojimą pagal saugos politiką ir ištekliais leidžia naudotis tik autorizuotoms esybėms (vartotojams, programoms, procesams arba kitoms tinkle esančioms sistemoms) [15, 30]. Prieigos valdymas yra susijęs su autentifikacija ir autorizacija. Autentifikavimas – tai procesas, kurio metu nustatoma arba patvirtinama, kad kažkas yra autentiškas, arba kad kažkas yra tai, kuo jis skelbiasi esąs. Kitaip dar galima pasakyti, kad autentifikavimas – tai procesas, kai identifikavimo informacija yra susiejama su autentifikavimo informacija. [28, 29] Jei autentifikavimo informacija, pavyzdžiui, slaptažodis, atitinka identifikavimo informaciją, pavyzdžiui, vartotojo vardą, laikoma, kad autentifikavimo procesas yra sėkmingas ir vartotojo ar tinklo įrenginio tapatybė yra nustatyta. Autorizacija – tai procesas, kurio metu vartotojui priskiriamas galimybių pasiekti informacijos išteklius sąrašas, leidimas atlikti konkrečius veiksmus sistemoje [20, 21]. Ir autentifikacija ir autorizacija gali būti laikomos prieigos valdymo dalimis, bet kalbant apie prieigos valdymą, autentifikacijos būdas nebūtinai tiksliai nurodomas; todėl šiame skyriuje autentifikacija ir prieigos valdymas bus nagrinėjami atskirai.

2.1 Bevieliuose tinkluose naudojamų autentifikacijos būdų analizė

Autentifikavimo mechanizmas priklauso nuo konkrečių saugumo nuostatų ir leidžiamo saugumo lygio. Autentifikavimas turi būti atliktas prieš klientui suteikiant tinklo prieigą.

Autentifikacija gali būti užtikrinama šiais autentifikavimo mechanizmais:

1) paremtais žinoma informacija (slaptažodžiai, PIN (angl. *Personal Identification Number*) kodai ir panašiai);

2) priklausomais nuo turimų priemonių (kriptografinės kortelės, skaitmeniniai sertifikatai, mobilusis telefonas ir panašiai);

3) paremtais informacija, išvesta remiantis vartotojo individualiosiomis savybėmis (įvairūs biometriniai metodai – atpažinimas pagal piršto antspaudus, akies rainelę, net DNR seką ir panašiai)

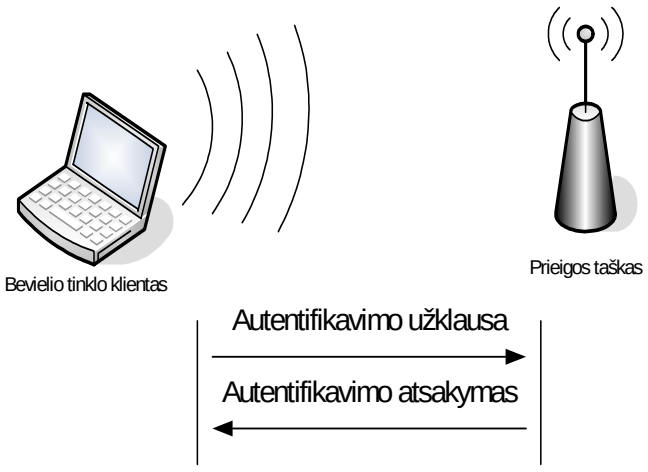
Kiekvienas iš šių autentifikavimo metodų yra pažeidžiamas. Slaptažodžiai ir PIN gali būti atspėjami, neteisėtomis priemonėmis perimami arba panaudojus specialias technologijas iššifruojami. Įrenginius, kurie patvirtina jį turinčiojo tapatybę gali būti neteisėtai ar apgaulės būdu pasisavinami. Kriptografinių sistemų ir vienkartinių slaptažodžių schemos gali sutrikti ir nepasiteisinti, net kai turi kriptografiškai labai atsparius algoritmus. Biometriniai metodai gali

būti pažeidžiami, informaciją su vartotojo individualiomis savybėmis perimant ir ją panaudojant autentifikuotis pakartotinai [20, 21]. Kai kurie autentifikavimo metodai gali turėti kitų trūkumų, pvz., gali būti nepatogūs vartotojui.

Toliau šiame skyriuje nagrinėjami įvairūs autentifikacijos mechanizmai ir jų trūkumai pradedant nuo bevieliuose tinkluose naudojamų standartinių autentifikavimo mechanizmų ir baigiant papildomais bendraisiais autentifikacijos mechanizmais. Ištyrus šiuos mechanizmus galima nustatyti, ar jie gali būti derinami su vietos informacija ir kaip vietos informacija galėtų sumažinti autentifikacijos mechanizmų pažeidžiamumus.

2.1.1 Atvira autentifikacija

Bevieliuose tinkluose nuo pat jų sukūrimo buvo naudojami du autentifikacijos būdai: atvira autentifikacija ir bendrojo rakto autentifikacija. Šie du būdai yra naudojami WEP (angl. WEP – *Wired Equivalent Privacy*) bevielio tinklo apsaugos algoritme. Atviros autentifikacijos atveju WLAN klientui nieko nereikia pristatyti prieigos taškui. Klientas, norėdamas prisijungti prie įrenginio, siunčia paketą su prieigos taško (angl. *Access Point* - AP) identifikatoriumi SSID (angl. SSID – *Sevice Set Identifier*), o jį gavęs prieigos taškas išsiunčia autentifikavimo atsakymo (patvirtinimo) paketą, jei gautasis SSID atitinka tikrąjį jo SSID (žr. 1 paveikslėlį). Visas atvirojo rakto autentifikavimo procesas yra atliekamas atviruoju tekstu (nešifruotu). Bet kuris klientas su bet kokiu WEP raktu gali autentifikuotis prieigos taškui, o WEP raktas gali būti naudojamas tik po autentifikacijos srauto tarp vartotojo ir prieigos taško šifravimui. Taigi galime sakyti, kad jokios autentifikacijos ir neįvyksta. 32 simbolių unikalus identifikatorius SSID šiuo atveju naudojamas kaip slaptažodis jungiantis prie bevielio tinklo, tačiau SSID galima lengvai sužinoti naudojantis tokiomis bevielio tinklo stebėjimo programomis kaip Kismet.



1 pav. Atvira autentifikacija bevieliame tinkle

2.1.2 Bendrojo rakto autentifikacija

Bendrojo rakto autentifikacijos atveju naudojamas WEP raktas. Kaip parodyta 2 paveikslėlyje autentifikavimo proceso metu AP klientui siunčia nešifruoto teksto paketą. Klientas, gavęs tokį paketą jį užšifruoja panaudodamas savo turimą raktą ir išsiunčia atgal prieigos taškui. Autentifikavimas nebus įvykdytas, jei AP priimtas paketas užšifruotas neteisingu raktu. Po autentifikacijos ir prisijungimo WEP raktas naudojamas paketų šifravimui naudojant RC4 šifrą.

2 pav. Bendrojo rakto autentifikacija bevieliame tinkle

Standartinis 64 bitų WEP protokolas naudoja 40 bitų raktą, kuris sujungiamas su 24 bitų inicializacijos vektoriumi. Išplėstas 128 bitų WEP protokolas naudoja 104 bitų dydžio raktus su inicializacijos vektoriumi. Tokio ilgio raktus galima nesunkiai sužinoti nuskanavus maždaug 10 MB tinklu siunčiamų duomenų. Naudojantis šiandieninėmis dešifravimo technologijomis 40 bitų ilgio raktą galima „nulaužti“ maždaug per 2 min., o ilgesnį – maždaug per valandą. Ilgesnio rakto „nulaužimui“ reikia perimti daugiau paketų, bet įsilaužėlis gali stimuliuoti didesnį paketų srautą.

Kadangi RC4 yra srautinis šifras, to paties rakto negalima panaudoti du kartus. Inicializacijos vektoriaus pagalba sukuriamas kintantis šifravimo raktas. Kaip bebūtų jei tinklas pakankamai užimtas, tokio ilgio rakto neužtenka apsisaugoti nuo įsilaužėlių. Inicializacijos vektorių kolizijos ir galimybė pakeisti paketus yra WEP pažeidžiamumai, kurių nepašalina net ir ilgesnių raktų naudojimas.

Dar vienas WEP trūkumas – statiniai raktai. Kai sukonfigūruojamas bendras raktas, gan sunku yra jį pakeisti, nes keisti reikia raktą visuose vartotojų kompiuteriuose rankiniu būdu. Retai keičiamą raktą yra didesnės galimybės „nulaužti“, o „nulaužus“ įsilaužėlis gali ilgiau

naudotis prieiga prie bevielio tinklo resursų ir perimti bei iššifruoti kitų vartotojų siunčiamus duomenis.

Bendrojo rakto autentifikacija yra labiau pažeidžiama net už atvirąją autentifikaciją, nes jos metu AP siunčia atvirą tekstą, kurį vartotojas užšifravęs atsiunčia atgal. Jei atakuotojas perima šiuos paketus, jam lengviau apskaičiuoti, koks yra slaptas raktas.

2.1.3 MAC adresų filtravimas

Vienas iš WEP naudojančių bevielių vietinių tinklų (angl. WLAN – *Wireless Local Area Network*) prieigos valdymo mechanizmų yra MAC (angl. *Ethernet Media Access Control*) adresų filtravimas. Sudaromas sąrašas MAC adresų tų kompiuterių, kuriems prieiga prie WLAN išteklių yra leidžiama (angl. *Access Control List* – ACL). Autentifikuotis leidžiama tik tam vartotojui, kurio tinklo plokštės MAC adresas atitinka vieną iš ACL sąraše esančių adresų. Šis autentifikacijos mechanizmas yra lengvai pažeidžiamas, nes piktavaliai pasinaudoję tam tikra bevielio tinklo stebėjimo programine įranga, pavyzdžiui Kismet, gali pastebėti, kokie yra prisijungusių vartotojų MAC adresai, ir suklastoti savo MAC adresą. MAC adresą kiekvienas vartotojas savo kompiuteryje gali pasikeisti į, kokį tik nori, ir pasirinktu MAC adresu jungtis prie WLAN. Be to prie vieno prieigos taško gali būti prisijungę keli vartotojai su vienodais MAC adresais.

2.1.4 PSK metodas

Bevieliuose tinkluose veikiančiuose pagal WPA (angl. WPA – *Wi-Fi Protected Access*) standartą, autentifikacija gali būti viename iš dviejų režimų: asmeniniame (angl. *Personal*) arba įmonės (angl. *Enterprise*) režime. Abiejų šių režimų metu yra vykdoma abipusė autentifikacija, kuri yra saugesnė palyginus su autentifikacija pagal WEP algoritmą.

Asmeninis režimas, dar vadinamas PSK (angl. PSK – *Pre-Shared Key*) režimu, tinka namų arba mažos įmonės tinklams, nes jo metu nenaudojamas 802.1X autentifikacijos serveris[25]. Vartotojai šiame režime iš anksto jiems žinomu 256 bitų ilgio raktu šifruoja srautą. PSK slaptas raktas gali būti „nulaužiamas“, jei raktui naudojama lengvai atspėjama frazė. Apsisaugoti nuo pilno perrinkimo atakos raktui turėtų būti naudojama tikrai atsitiktinis slaptažodis ar frazė iš 13 simbolių. Jei slaptažodis per trumpas, jis gali būti pažeistas „offline dictionary attack“, t.y. atakuotojas galės perimti kelis paketus, kai teisėtas vartotojas prisijungia prie bevielio tinklo, ir vėliau iš jų atkurti slaptažodį. Kadangi duomenų šifravimui naudojamos saugesnės technologijos, tokios kaip TKIP (angl. TKIP – *Temporal Key Integrity Protocol*) arba AES (angl. AES – *Advanced Encryption Standard*) pagrįstas CCMP (angl. CCMP – *Counter-Mode with Cipher Block Chaining Message Authentication Code Protocol*) protokolas, dešifruoti paketus pagal WPA standartą veikiančiuose tinkluose yra sunkiau arba

neįmanoma. Šiuo metu yra žinoma, kad esant pakankamai užimtam tinklui, kuriame veikia TKIP šifravimas ir naudojami pakankamai ilgi rakto keitimo intervalai (pavyzdžiui, 3600 sekundžių), galima atlikti ARP (angl. *Address Resolution Protocol*) žinučių analizę ir vadinamą „chopchop“ ataką. Atlikęs šią ataką įsilaužėlis sužino 64 bitus MIC (angl. *Message Integrity Code*), skirtus žinutės vientisumo patikrinimui, ir gali siųsti žinutes, sutrikdančias IDS (angl. *Intrusion Detection System*) sistemą, gali siųsti suklastotas ARP žinutes ir srautas bus nukreiptas kitur. Piktavalis gali bandyti padaryti abipusį dvikryptį kanalą iki kliento, tokiu atveju kliento žinučių nebus galima perskaityti bevieliame tinkle, bet jos gali būti nukreiptos atgal į internetą.

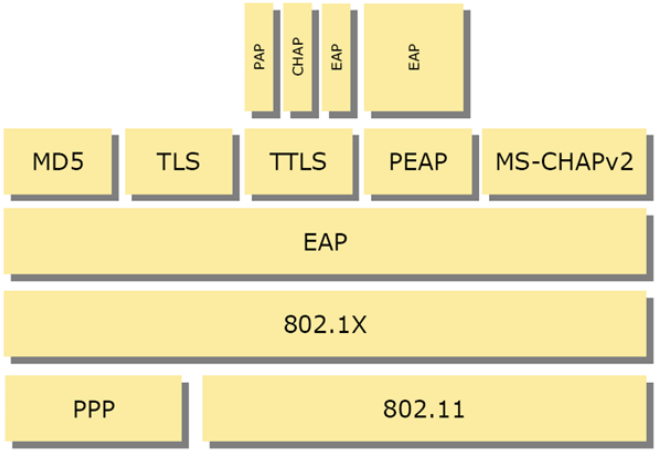
2.1.5 EAP protokolas

Kai WPA bevielis tinklas veikia įmonės režimu, autentifikacijai naudojamas EAP (angl. EAP – *Extensible Authentication Protocol*) protokolas pagal IEEE 802.1X standartą. Priešingai nei asmeniniame režime, šiame režime reikalingas autentifikacijos serveris. Darbui su autentifikacijos serveriu naudojamas koks nors autentifikacijos, prieigos valdymo ir registravimo (angl. AAA – *Authentication, Access control and Accounting*), dažniausiai RADIUS, protokolas, kuris atsakingas už autentifikaciją ir raktų paskirstymą. Įmonės režime vartotojų prisijungimo duomenys valdomi centralizuotai. EAP privalumas yra tas, kad jį galima lengvai realizuoti prieigos taške, nes prieigos taškui nereikia žinoti jokių specifinių autentifikavimo metodų ypatumų, jis tarnauja tik kaip perdavimo grandis tarp kliento ir autentifikavimo serverio [21].

3 paveikslėlyje pavaizduota EAP kadro struktūra. Patį autentifikacijos mechanizmą nusako ne EAP, o įvairūs EAP metodai, kurių šiuo metu yra apie 40. IETF RFC apibrėžti autentifikacijos mechanizmai yra šie: [6]

- EAP-MD5 (autentifikuoja tik vartotoją serveriui, yra pažeidžiamas žodyno atakų),
- EAP-OTP (naudojamas VPN ir PPP (angl. PPP – *Point to Point Protocol*), bet ne bevieliams tinklams, teikia tik vienpusę autentifikaciją),
- EAP-GTC (autentifikacijai bevieliuose tinkluose dažniausiai naudojamas viduje TLS tunelio, sukurto TTLS arba PEAP),
- EAP-TLS (naudoja saugų TLS (angl. TLS – *Transport Layer Security*) protokolą ir sertifikatus),
- EAP-IKEv2 (pagrįstas antros versijos IKE (angl. IKE – *Internet Key Exchange Protocol*) protokolu),
- EAP-SIM (naudojamas GSM (angl. GSM – *Global System for Mobile Communications*) SIM (angl. SIM – *Subscriber Identity Module*)),

- EAP-AKA (naudojamas UMTS (angl. UMTS – *Universal Mobile Telecommunications System*) USIM (angl. USIM – *Universal Subscriber Identity Module*)).



3 pav. EAP kadro struktūra

Nors bevieliuose tinkluose gali būti naudojami ir kiti, Į WPA sertifikavimo programą yra įtraukti šie EAP metodai:

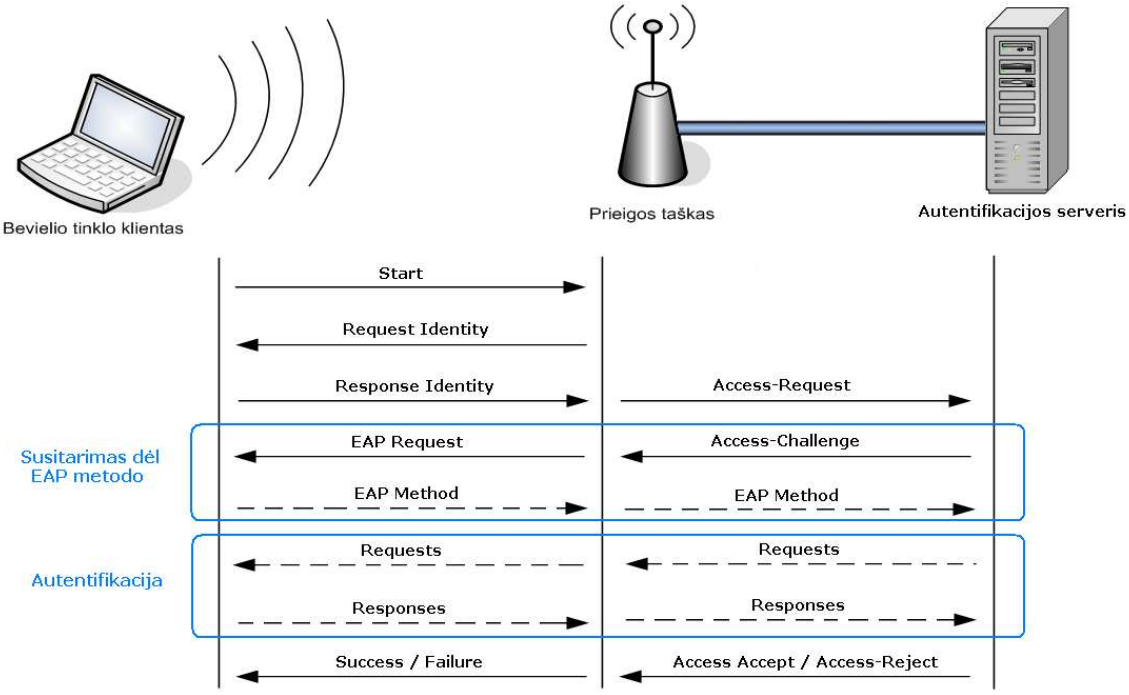
- EAP-TLS
- EAP-TTLS/MSCHAPv2
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- PEAP-TLS
- EAP-SIM

EAP-TTLS ir EAP-PEAP (dar vadinama PEAP) metodai išsiskiria tuo, kad prieš autentifikaciją sudaro TLS tunelį tarp kliento ir autentifikacijos serverio ir tada tuneliu atliekama autentifikacija kaip pagal EAP-MD5, EAP-TLS (EAP-PEAP metodo atveju) arba PAP, CHAP, MS-CHAP, MS-CHAP v2 (EAP-TTLS metodo atveju) metodus (žr. 5 paveikslėlį). Toks tuneliavimas apsaugo nuo žodyno, „man in the middle“ arba sesijos perėmimo atakų. EAP-LEAP (angl. LEAP – *Lightweight Extensible Authentication Protocol*) metodas yra paprastas, aiškus, greitai veikia, pritaikomas apribotų skaičiavimo resursų aplinkose, naudojamas bevieliams tinklams. Jis naudoja modifikuotą MS-CHAP versiją. Saugos raktai dinamiškai keičiami kiekvienai sesijai, taip apsisaugoma nuo surinktų duomenų dekodavimo. Autentifikacijai EAP-LEAP metodas naudoja slaptažodį. 1 lentelėje yra palyginti keli EAP metodai.

1 lentelė. EAP metodų savybės

Metodas	Serverio autentifikacija	Vartotojo autentifikacija	Dinaminis raktų paskirstymas	Rizikos
EAP-MD5	Nėra	Slaptažodžio santrauka	Ne	„Man-in-the-middle“ (MitM) ataka; sesijos perėmimas
LEAP	Slaptažodžio santrauka	Slaptažodžio santrauka	Taip	Tapatybės atskleidimas; žodyno ataka
EAP-TLS	Viešojo rakto (sertifikatas)	Viešojo rakto (sertifikatas arba kortelė)	Taip	Atskleista tapatybė
EAP-TTLS	Viešojo rakto (sertifikatas)	CHAP, PAP, MS-CHAPv2, EAP	Taip	MitM ataka
PEAP	Viešojo rakto (sertifikatas)	Bet koks EAP, pvz., MS-CHAPv2, arba viešojo rakto	Taip	MitM; potencialus tapatybės atskleidimas I fazėje

4 paveikslėlyje parodyta, kaip autentifikacija atliekama pagal 802.1X standartą, nepriklausomai nuo to, koks EAP metodas yra naudojamas. Autentifikacijoje pagal 802.1X standartą dalyvauja trys elementai: klientas (802.1X standartą palaiko Windows XP ir vėlesnės Windows operacinės sistemos, 10.3 ir vėlesnės MAC OS X operacinės sistemos, taip pat iPhone OS 2.0), autentifikatorius (prieigos taškas bevieliame tinkle) ir autentifikacijos serveris, pavyzdžiui, RADIUS serveris [26].



4 pav. 802.1X autentifikacija

Autentifikacija vyksta taip: iš pradžių autentifikatoriaus prievadas laikomas „neautorizuotas“ būsenoje, kurioje priimamas tik 802.1X autentifikacijos srautas, visas kitas srautas blokuojamas tinklo lygmenyje. Komunikacija tarp kliento ir autentifikatoriaus vyksta vadinamomis EAPOL (EAP over LAN) žinutėmis. Kai autentifikatorius gauna Start kadrą arba aptinka naują klientą, išsiunčia jam tapatybės užklausą (angl. *Request Identity*). Klientas atsako atsiųsdamas identifikuojančius duomenis (angl. *Response Identity*). Autentifikatorius gautas EAP žinutes įpakuoja į protokolo (pvz., RADIUS), naudojamo komunikacijai tarp autentifikatoriaus ir serverio, paketus ir persiunčia autentifikacijos serveriui [2, 6]. Tada serveris siunčia klientui (per autentifikatorių) nuorodas, kokį EAP metodą naudoti. Klientas gali pasiūlyti savo metodą arba sutikti su pasiūlytu. Toliau vyksta autentifikacija ir serveris atsiunčia atsakymą, ar klientas autentifikuotas. Jei autentifikacija sėkminga, autentifikatoriaus prievado būsena tampa „autorizuotas“ ir nebeblokuojamas bet koks srautas [26].

2.1.6 Papildomos autentifikavimo priemonės

Šiame skyrelyje pristatomos papildomos priemonės, kurios gali būti panaudotos autentifikacijai bevieliame tinkle. Šios priemonės nėra skirtos būtent bevieliam tinklui, o tėra bendros tinkančio bet kokios rūšies tinklui ir/ar papildomos, todėl tolesniuose skyriuose jos nebus nagrinėjamos.

2.1.6.1 Virtualus privatus tinklas

Kitas sprendimas vartotojams saugiai jungtis prie tinklo yra naudoti virtualiuosius privačius tinklus (VPT). Tai nėra būtent bevieliams tinklams skirtas sprendimas, jis gali būti naudojamas ir kituose tinkluose nuotoliniui prisijungimui. Autentifikacijai gali būti naudojami du faktoriai: slaptažodžiai ir elektroniniai sertifikatai. Ugniasienė teikia VPN autentifikavimo paslaugą. Yra du pagrindiniai VPT tipai: IP_{Sec} sistemos, kurioms reikia įdiegti kliento programinę įrangą, ir SSL VPT, kurie veikia per naršyklę.

2.1.6.2 WEB autentifikacija

WEB autentifikacija – autentifikacijos būdas, naudojantis HTTPS (angl. *Hypertext Transfer Protocol Secure*) protokolą, Vartotojai autentifikuojasi WWW naršyklėje įvesdami prisijungimo duomenis. Siunčiamą autentifikacijos informaciją šifruoja WWW naršyklė, naudojanti HTTPS protokolą.

2.1.6.3 Bendrųjų autentifikacijos technologijų apžvalga

Lentelėje 2 pateikta bendrų standartinių autentifikacijai naudojamų technologijų apžvalga. Kai kurios iš jų, tokios kaip slaptažodžiai ir elektroniniai sertifikatai, paprastai yra naudojamos bevieliuose tinkluose, o kitos galėtų būti papildomai panaudojamos. Autentifikacijai gali būti naudojamos ir kelios technologijos vienu metu.

2 lentelė. Autentifikacijos technologijų analizė

K.	Autentifikacijos technologijos	Privalumai	Trūkumai
Žinoma informacija	Bendras raktas	* Lengva įdiegti, veikia ir su senesniais įrenginiais	* Susikompromitavus vienam vartotojui, visiems vartotojams reikia keisti raktą
	Vienkartinis slaptažodis	* Vienąkart įsilaužus neilgai galima naudotis sistema	* Nepatogu vartotojui * Kiekvienąkart reik sugeneruoti ir perduoti naują slaptažodį
	Daugkartinis slaptažodis	* Nebrangu, * Dažniausiai nereikalauja daug papildomų priemonių įdiegiant	* Jei naudojamas silpnas slaptažodis kaip žodis iš žodyno ar trumpas žodis, galima nulaužti, * Galima nulaužti pilno perrinkimo metodu, * Slaptažodį lengva pamiršti
	PIN kodas	* Nesunku įdiegti, * Nebrangu	* Gali būti nulaužtas, * Lengva pamiršti arba pamesti
Turimos priemonės	Elektroniniai sertifikatai	* Saugu, nes sunku suklastoti	* Pažeidžiamumas kolizijos atakai, * Nepatogu vartotojui, nepopuliaru
	USB raktai	* Nereikia prisiminti, įvedinėti slaptažodžio * Nėra tikimybės, kad suklys	* Brangu ir gan sudėtinga įdiegti, * Grėsmė, kad bus pamesta, sugadinta, pavogta arba suges
	Smart cards	* Nereikia prisiminti, įvedinėti slaptažodžio * Nėra tikimybės, kad suklys	* Brangu ir gan sudėtinga įdiegti, * Grėsmė, kad bus pamesta, sugadinta, pavogta arba suges
	Slaptažodžių generatorius	* Sunkiau nulaužti palyginus su paprastu slaptažodžiu arba PIN kodu	* Brangu ir gan sudėtinga įdiegti, * Grėsmė, kad bus pamesta, sugadinta, pavogta arba suges, * Nelabai patogu naudotis
Individualios savybės	Atpažinimas pagal piršto antspaudą	* Patogu, lengva naudotis, * Suklysti priimant gali tik 0,001% atvejų, suklysti atmetant gali tik 0,5%, [19] * Ne naujas, sąlyginai ne taip sunku įdiegti	* Nepopuliaru, vartotojams reikia įsigyti papildomą įrangą, kur būtų įdiegta ši technologija
	Veido atpažinimo kamera	* Patogu naudotis	* Lengva apgauti panaudojant nuotrauką
	Garsų ir kalbos atpažinimas	* Patogus vartotojams	* Netikslumai naudojant triukšmingoje aplinkoje, * Netikslumai dėl riboto žodyno, * Nepatogu, nes kelia triukšmą (negali veikti tyliai), * Galima apgauti panaudojant įrašą
	Rainelės skanavimas	* Patogu naudotis	* Brangus sprendimas, * Naujas ir sudėtingas įdiegti

2.1.7 Autentifikavimo būdai ir jų pažeidžiamumai

Išnagrinėjus įvairius autentifikacijos metodus, galima juos palyginti ir įvertinti kiekvieno metodo pažeidžiamumus. 3 lentelėje parodyta, kokios priemonės gali būti panaudotos neteisėto autentifikavimosi įvykdymui, esant įvairiems autentifikacijos metodams. Lentelėje taip pat nurodyta, kokie yra atitinkamų autentifikacijos metodų pažeidžiamumai ir kokio standarto tinkluose tie metodai naudojami. EAP protokolu pagrįsta autentifikacija laikoma saugia, todėl lentelėje šių metodų nėra.

3 lentelė. Priemonės neteisėto autentifikavimosi įvykdymui

Tinklo standartas	Autentifikacijos metodas	Pažeidžiamumas	Priemonės neteisėto autentifikavimosi įvykdymui
WEP	Atvira autentifikacija	SSID	Tinklo srauto stebėjimas
	Bendrojo rakto autentifikacija	Raktas ir inicializacijos vektorius	Dešifravimo technologijos
	MAC adresų filtravimas	MAC adresas	MAC adreso pasikeitimas
WPA	PSK	Trumpas arba atspėjamas raktas	Žodyno ataka
		TKIP šifravimas	ARP žinučių "chopchop" analizė ir ataka

4 lentelė. Atakos bevieliame tinkle

Tinklas	Autentifikacijos metodas	Pažeidžiamumas	Atakos
WEP	Atvira autentifikacija	SSID	Slaptas klausymasis; Įsivežimas ir resursų pavogimas; Srauto nukreipimas; Netikri tinklai ir stoties nukreipimas; Denial of Service (DoS)
	Bendrojo rakto autentifikacija	Raktas ir inicializacijos vektorius	
	MAC adresų filtravimas	MAC adresas	
WPA	PSK	Trumpas arba atspėjamas raktas	Slaptas klausymasis; Įsivežimas ir resursų pavogimas; DoS ataka; Žodyno ataka
		TKIP šifravimas	Gali būti nukreiptas srautas ir sudarytas dvipusis kanalas su klientu; DoS
	EAP-TLS		Tapatybės atskleidimas
	EAP-TLS/MSCHAPv2		„Man in the Middle" ataka
	PEAPv0 EAP-MSCHAPv2		„Man in the Middle" ataka; Potencialus tapatybės atskleidimas I fazėje
	PEAPv1 / EAP-GTC		
	PEAP-TLS		
	EAP-SIM		

4 lentelėje nurodyta, kokios atakos bevieliame tinkle apskritai yra įmanomos naudojant tam tikrus autentifikacijos metodus. Kai kurias atakas galima įvykdyti net bevieliame tinkle, kuriame naudojamas naujausias EAP autentifikacijos metodas.

2.1.8 Apibendrinimas

Pasiekti saugų duomenų perdavimą nesaugiuose WEP naudojančiuose WiFi tinkluose gali būti naudojamas užšifruotas tuneliavimo protokolas, pavyzdžiui IP_{Sec}, Secure Shell, tačiau pakankamas saugumo lygis turėtų būti pasiekiamas pačiame bevieliame tinkle.

Išnagrinėjus įvairius autentifikacijos mechanizmus bevieliuose tinkluose, aišku, kad saugiausias iš jų yra naujausias EAP protokolu pagrįstas metodas. WEP algoritmo autentifikacija yra pažeidžiama dėl silpno slapto rakto. VPN gali užtikrinti saugią autentifikaciją, tačiau nėra bevieliams tinklams taikytinas sprendimas.

2.2 Bevieliuose tinkluose naudojamų autorizavimo būdų analizė

Autorizacija – tai procesas, kurio metu vartotojui priskiriamas galimybių pasiekti informacijos išteklius sąrašas, leidimas atlikti konkrečius veiksmus sistemoje ir panašiai [20, 21]. Prieigos valdymo procesas gali būti padalintas į dvi fazes: politikų apibrėžimą ir politikų vykdymą. Autorizacija atlieka politikų apibrėžimo funkciją [29, 30, 31]. Nors įvairiuose šaltiniuose autorizacija laikoma ir tuo, kas atliekama antroje fazėje, tai prieštarauja svarbiai šio žodžio prasmei. Autorizacija atskirai šiame darbe, nebus nagrinėjama, su ja susiję klausimai bus pristatyti prieigos valdymo mechanizmų analizėje.

2.3 Prieigos valdymo mechanizmų analizė

Nors autentifikacija gali būti laikoma prieigos valdymo dalimi, šiame skyrelyje terminas “prieigos valdymas” reiškia prieigos prie sistemos resursų valdymą po to, kai vartotojo paskyros informacija ir tapatybė buvo autentifikuoti ir prieiga prie sistemos suteikta. Saugos politikos įgyvendinimui svarbu pasirinkti tinkamą prieigos valdymo mechanizmą. Šiame skyriuje pristatomi standartiniai prieigos valdymo mechanizmai. Jie nepriklauso nuo to, kokios technologijos naudojamos komunikacijai (ar radijo signalai, ar optiniai kabeliai ir panašiai), jie tik apibrėžia, kaip sistemoje apibūdinami vartotojai, resursai ir kaip nusprendžiama, prie kurių resursų vartotojas gali prieiti. Prieigos valdymas glaudžiai susijęs su saugos politika, pagal kurią turi veikti sistema.

2.3.1 Privalomasis prieigos valdymas

Privalomasis prieigos valdymas (angl. *Mandatory Access Control* – MAC) yra griežčiausias iš visų ir remiasi hierarchiniu požiūriu į prieigos valdymą. Pagal jį prieiga prie visų resursų, arba objektų, tokių kaip failai, yra kontroliuojama administratoriaus sukurtomis nuostatomis. Tokiu būdu vartotojai negali pakeisti prieigos prie resursų valdymo.

Privalomasis prieigos valdymas klasifikuoja sistemos resursus (priskiria resursams saugos žymes (angl. *security lebels*)) ir prieigą leidžia tik toms esybėms (žmonėms, procesams ar įrenginiams), kurioms suteikta tam tikro lygmens autorizacija, arba kitaip vadinami saugos leidimai (angl. *clearance*). Saugos žymėse yra informacija apie objekto klasifikaciją, pavyzdžiui, "konfidencialu", "slapta" ir panašiai, ir kategoriją, pagal kurią nustatomas valdymo lygis, departamentas ar projektas, kuriam objektas turi būti prieinamas. Analogiškai kiekvieno vartotojo paskyrai taip pat yra priskirta klasifikacija ir kategorija. Vartotojui bandant prieiti prie resurso, pagal privalomąjį prieigos valdymą operacinė sistema patikrina vartotojo saugos lygį bei kategorijas ir palygina jas su resurso saugumo žyme. Jei vartotojui priskirti saugos leidimas ir kategorijos sutampa su objekto saugumo žyme, prieiga leidžiama. Turi sutapti ir klasifikacija ir kategorijos. Pavyzdžiui, aukščiausio lygio slaptumo klasifikacijos vartotojas negali pasiekti resurso, jei jis nepriklauso kategorijai, kurią turi resursas.

Privalomojo prieigos valdymo modelis dažniausiai turi šias savybes:

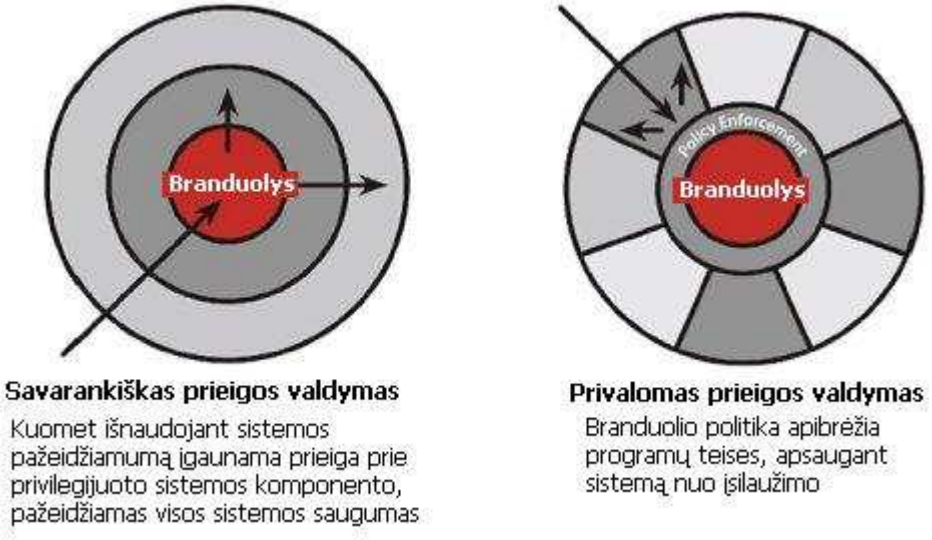
- Visi vartotojai gali skaityti žemesnės klasifikacijos resursus nei jiems suteikta. Pavyzdžiui, "slapta" klasifikacijos vartotojas gali skaityti neklasifikuotus dokumentus.
- Visi vartotojai gali rašyti į aukštesnės klasifikacijos resursus. Pavyzdžiui, "slaptas" vartotojas gali siųsti informaciją į Aukščiausio slaptumo resursą.
- Visiems vartotojams duota rašymo/skaitymo prieiga tik prie tos pačios klasifikacijos objektų. Pavyzdžiui, "slaptas" vartotojas gali skaityti ir rašyti tik slaptus dokumentus.
- Prieiga prie objektų priklausomai nuo dienos laiko yra autorizuojama arba draudžiama pagal resurso žymę ir vartotojo saugo leidimą.
- Prieiga prie objektų yra autorizuojama arba draudžiama pagal HTTP kliento saugos charakteristikas (pavyzdžiui, SSL ilgis bitais, versijos informacija, šaltinio IP adresas arba domenas ir panašiai).

Privalomasis prieigos valdymas paprastai yra tinkamas ypač saugioms sistemoms, tokioms kaip kelių lygių saugios karinės programos, tačiau nėra toks lankstus ir patogus vartotojams. Prieš įdiegiant tokį prieigos valdymą, reikia nemažai suplanuoti, o po įdiegimo sistemą taip pat reikia valdyti – pastoviai atnaujinti objektų ir vartotojų žymes įvedant naujus duomenis, naujus vartotojus arba atliekant pakeitimus jau egzistuojantiems vartotojams.

2.3.2 Savarankiškas prieigos valdymas

Savarankiškas prieigos valdymas (angl. *Discretionary Access Control* – DAC) leidžia sistemos vartotojams (pavyzdžiui, žmonėms, procesams ar įrenginiams) prieiti prie sistemos resursų pagal leidimus, kurie skirti tam tikrą tapatybę turintiems vartotojams arba tam tikrai

grupei priklausantiems vartotojams. Paprastai prieiga leidžiama arba draudžiama pagal autentifikacijos metu pateiktus kredencialus (vartotojo vardą, slaptažodį, įrenginį, bilietą). Kitaip nei privalomojo prieigos valdymo modeliu pagrįstos sistemos, dauguma tipinių savarankiško prieigos valdymo sistemų leidžia resurso savininkui pakeisti to resurso leidimus, t.y. valdyti prieigą prie savo resursų. Tokio valdymo trūkumas yra, kad administratoriai negali iš vieno taško valdyti leidimų failuose arba web serveriuose. 5 paveikslėlyje atvaizduoti prieigos valdymų skirtumai [17]. Vietoje saugos žymės kiekvienas resursas savarankiško prieigos valdymo atveju yra susietas su prieigos valdymo sąrašu (angl. *Access Control List – ACL*). Šiame sąraše nurodyta, kuriems vartotojams ir grupėms leista prieiga prie resurso, ir prieigos lygmuo kiekvienam vartotojui ar grupei. Pavyzdžiui, vartotojas A leidžia tik skaitymo prieigą prie savo failų vartotojui B, skaitymo ir rašymo prieigą vartotojui C ir pilną valdymą vartotojams, priklausantiems grupei 1. Kai kuriose operacinėse sistemose sistema arba tinklo administratorius gali nurodyti, kuriuos leidimus vartotojai gali įvesti savo resursams į prieigos valdymo sąrašą.



5 pav. MAC ir DAC mechanizmų skirtumai [17]

Savarankiško prieigos valdymo modelis dažniausiai turi šias savybes:

- Duomenų savininkai gali perduoti savininko teises į informaciją kitiems vartotojams.
- Duomenų savininkai gali nustatyti, kokio tipo prieiga (rašyti skaityti, kopijuoti ir kt.) duota kitiems vartotojams.
- Pasikartojanti nesėkminga autorizaciją prie to pačio resurso ar objekto iššaukia aliarmą arba uždraudžia vartotojo prieigą.
- Reikalinga speciali papildoma (angl. "*add on*" arba "*plug in*") programinė įranga HTTP klientui apsisaugoti nuo nepageidaujamo vartotojų kopijavimo (angl. "*cutting and pasting"*).

- Vartotojams, kurie neturi prieigos prie informacijos, turėtų būti neįmanoma nustatyti jos charakteristikų (tokių kaip failo dydis, failo pavadinimas, vieta diske ir kt.).

Savarankiškas prieigos valdymas paprastai naudojamas darbalaukio operacinėms sistemoms. Jis suteikia kur kas lankstesnę aplinką nei privalomasis prieigos valdymas, bet kartu ir padidėja tikimybė, kad duomenys taps prieinami tiems vartotojams, kuriems prieiga nebūtinai turėtų būti suteikta.

2.3.3 Role pagrįstas prieigos valdymas

Esant role pagrįstam prieigos valdymui (angl. *Role Based Access Control* – RBAC), dar žinomam kaip nesavarankiškas prieigos valdymas (angl. *Non discretionary Access Control*), vartotojų identifikacija, autentifikacija ir autorizacija yra atliekama pagal jų pareigas organizacijoje, kurioje veikia kompiuterių sistema. Kitaip sakant, prieiga apsprendžiama pagal individo roles ir pareigas organizacijoje ar vartotojų bazėje. Kad galėtų būti apibrėžtos rolės, dažniausiai reikia išanalizuoti organizacijos tikslus bei struktūrą ir susieti tai su saugos politika. Pavyzdžiui, medicinos įstaigoje rolės gali būti daktaras, seselė, pacientas, lankytojas ir panašiai Suprantama, šiems vartotojams, kad jie atliktų savo funkcijas reikia skirtingo lygio prieigos, taip pat web operacijos ir situacijos, kuriose jos leidžiamos, gali būti labai skirtingos, priklausomai nuo saugos politikos ir bet kokių kitų su tuo susijusių taisyklių. Rolės nuo grupių skiriasi tuo, kad pagal privalomąjį prieigos valdymo modelį vartotojas gali priklausyti kelioms grupėms, bet pagal role pagrįstą prieigos valdymą vartotojui gali būti paskirta tik viena rolė. Be to atskiriems vartotojams negali būti priskirta papildomų teisių šalia tų, kurios jau priskirtos jų rolėms. Pavyzdžiui, daktaras turi tokias pat teises, kokias turi visi kiti daktarai sistemoje. Esant role pagrįstam prieigos valdymui web programų saugos administratoriai turėtų turėti galimybę nustatyti, kas, kokius veiksmus, kada, iš kur, kokia tvarka ir kai kuriais atvejais net kokiomis aplinkybėmis gali atlikti. Role pagrįstam prieigos valdymui būdingos šios savybės:

- Rolės paskiriamos pagal organizacijos struktūrą laikantis organizacijos saugos politikos.
- Roles paskiria administratorius pagal organizacijoje ar vartotojų bazėje esančius ryšius. Pavyzdžiui, vadybininkas bus autorizuotas atlikti operacijas, susijusias su jo darbuotojais, o administratorius bus autorizuotas atlikti operacijas savo pareigų srityje (duomenų atkūrimas, sąskaitos sukūrimas ir panašiai).
- Kiekvienai rolei skirtas profilis, kuriame nurodyta autorizuotos komandos, operacijos ir leistina informacijos prieiga.
- Teisės rolėms suteikiamos mažiausios privilegijos principu.

- Rolės kuriamos taip, kad būtų atskirtos pareigybės. Pavyzdžiui, Vykdytojo rolė neturėtų dalinai sutapti su testuotojo role.
- Rolės aktyvuojamos statiškai arba dinamiškai.
- Rolės gali būti perkeltos arba pavestos naudojant tik griežtas procedūras.
- Rolės valdomos saugos administratoriaus arba projekto vadovo centraliai.

2.3.4 Taisyklėmis pagrįstas prieigos valdymas

Taisyklėmis pagrįstas prieigos valdymas (angl. *Rule Based Access Control* – RBAC) leidžia arba draudžia prieigą prie objektų pagal taisyklių rinkinį, kurį sukuria sistemos administratorius. Kaip ir savarankiško prieigos valdymo atveju, prieigos nuostatos yra prieigos valdymo sąrašuose (angl. *Access Control Lists* – ACL), kurie yra susieti su kiekvienu išteklių objektu. Kai kokia nors sąskaita ar grupė bando prieiti prie objekto, operacinė sistema patikrina to objekto prieigos valdymo sąraše esančias taisykles. Tokio prieigos valdymo pavyzdys yra situacija, kai prieiga prie tinklo sąskaitai ar grupei yra leidžiama tam tikromis dienos valandomis arba tam tikromis savaitės dienomis. Kaip ir privalomojo prieigos valdymo atveju taisyklėmis pagrįsto prieigos valdymo vartotojai keisti negali, visi prieigos leidimai yra valdomi tik sistemos administratoriaus.

2.3.5 Apibendrinimas

Ar atakuotojas galės įsilaužti į sistemą, labiausiai priklauso nuo autentifikacijos mechanizmo, o ne prieigos valdymo modelio. Prieigos valdymo modelis parenkamas pagal tai, kokio pobūdžio yra sistema, pavyzdžiui, ar joje vartotojams gali būti priskirtos griežtai apibrėžtos rolės, ar teises patogiau suteikti kiekvienam vartotojui atskirai, ar sistemai reikalingos įvairios taisyklės (kaip kad kuriuo metu kurie objektai gali būti prieinami), ar sistemoje reikalinga galimybė vartotojams patiems valdyti prieigą prie resursų, ar geriau, kai prieiga valdoma centraliai. Sistemoms, kurioms saugumas yra svarbiausias, pvz., karinėms sistemoms, labiau tinka privalomasis prieigos valdymas. Kaip parodyta 5 paveikslėlyje, savarankiško prieigos valdymo atveju įsilaužus į sistemą per vieno vartotojo paskyrą galima prieiti prie visų sistemos resursų ir pažeisti visą sistemą. Privalomojo prieigos valdymo atveju bus pažeista tik sistemos dalis, prieinama per įsilaužtą paskyrą. Kita vertus savarankiškas prieigos mechanizmas yra lankstesnis, reikalauja mažiau resursų, valdymo ir palaikymo. Role pagrįstas prieigos valdymas labiausiai tinka tokioms sistemos, kur rolės tiksliai apibrėžtos ir nėra jokių papildomų taisyklių, tačiau šis modelis yra ribotas, kai prieigos sprendimui yra svarbus kontekstas, pavyzdžiui, ar dabar naktis ar diena, ar karas ar taika. Role pagrįstą prieigos valdymą taip pat sunku pritaikyti kelias sritis apimančiai sistemai. Minėtų trūkumų

galima išvengti naudojant atributais pagrįstą prieigos valdymą (angl. *Attribute-based Access Control*), kuris šiame darbe nebus nagrinėjamas.

Tokios organizacijos kaip universitetas tinklui geriausiai gali būti pritaikomas role pagrįstas prieigos valdymas, nes sistemos vartotojams, kurie yra studentai, dėstytojai ir kiti darbuotojai, nesunkiai gali būti apibrėžtos rolės.

2.4 Skyriaus apibendrinimas

Išanalizuoti įvairūs autentifikacijos būdai. Bevieliams tinklams taikomi autentifikacijos metodai yra šie: atvira autentifikacija, bendrojo rakto autentifikacija, MAC adresų filtravimas, PSK metodas ir EAP protokolas. PSK metodas ir EAP protokolas yra taikomi naujesniuose WPA tinkluose ir atitinkamai vadinami namų ir įmonės režimais. Autentifikacijos metodai, naudojami senesniuose WEP bevieliuose tinkluose yra pažeidžiami, naudojamas raktas yra pakankamai trumpas, jį galima dešifruoti ir neteisėtai prisijungti prie bevielio tinklo. Su šiais bevieliuose tinkluose naudojamais autentifikacijos metodais gali būti naudojami ir kiti autentifikacijos metodai ir mechanizmai, tokie kaip VPN ir tuneliavimas, USB raktai autentifikacijai, kodų generatoriai, atpažinimas pagal pirštų antspaudus ir panašiai.

Bevieliam tinklui, kaip ir kitos rūšies tinklams, gali būti pritaikomas bet koks prieigos valdymo modelis. Prieigos valdymo modelį reikia pasirinkti pagal informacinės sistemos paskirtį, dydį, struktūrą, vartotojų veiklos pobūdį, reikalingą saugumo lygį.

3 AUTENTIFIKACIJOS IR PRIEIGOS VALDYMO MECHANIZMŲ DERINIMO SU VIETOS INFORMACIJA GALIMYBĖS

Vietos informacija – tai elektroninių ryšių tinkluose tvarkomi duomenys, nurodantys elektroninių ryšių paslaugų vartotojo galinių įrenginių geografinę padėtį. Vietos informacija gali nurodyti bevielio tinklo vartotojo galinio įrenginio geografinę platumą bei ilgumą, aukštį, kryptį, vietos nustatymo informacijos tikslumą, tinklo elementą, prie kurio galinis įrenginys yra prisijungęs, ir panašiai [20, 32].

3.1 Vietos informacijos gavimo būdai

3.1.1 Įvairios vietos nustatymo technologijos

5 lentelė. Pozicionavimo technologijų paplitimo suvestinė

Eil. Nr.	Technologija	Įdiegimo metai	Paplitimas rinkoje
1	GPS	1994	Pasaulyje
2	GPS - Block II F	2009	Pasaulyje
3	EGNOS	2004	Europoje
4	Galileo [4]	2008	Pasaulyje
5	DGPS	1994	Pasaulyje
6	Cell-ID	2002	Pasaulyje, kur yra GSM
7	Cell-ID+TA	2002	Pasaulyje, kur yra GSM
8	E-CGI	2003	Pasaulyje, kur yra GSM
9	AOA	2003	JAV
10	U-TOA	2003	JAV
11	E-OTD	2003	JAV
		2003-2005	Europoje
12	OTDOA		Tik įdiegus UMTS
13	A-GPS		JAV – duomenų nėra
		2004-2005	Europa
14	Data Base Correlation	2003	Atskiri taikymai
15	Loc. Pattern Match.	2003	JAV privatūs taikymai
16	WLAN	2003	Sveikatos apsauga ir gamyba
17	Bluetooth	Jau yra	Pasaulyje
18	UWB	Jau yra	JAV bandymai
19	DTV	2003	Europoje

Dėl greito vystymosi bevielių ir mobiliųjų tinklų srityje atsirado nauja karta įrenginių, kurie vietos informacijos technologijų gali būti naudojami kaip sekliai. Įvairiuose moksliniuose darbuose yra aprašyta ir pasiūlyta nemažai būdų nustatyti mobilaus vartotojo vietos informaciją. Pavyzdžiui, 2002 metais užregistruotame patente siūlomas metodas ir įrenginiai įvertinti mobilaus telefono geografinę vietą pagal jo signalų stiprius [3]. Mobiliųjų telefonų tinkluose vietos nustatymo paslaugos (angl. *Location Service*) yra standartizuojamos ir naudojamos visame pasaulyje. Lentelėje 5 surašytos įvairios vietos nustatymo technologijos, jų įdiegimo metai ir paplitimas rinkoje. Reikia paminėti, kad derinant GSM

(angl. *Global Standard for Mobile Communications*) ir GPS (angl.. *Global Positioning System*) vietos nustatymo metodus, vartotojo vietą galima nustatyti labai tiksliai net ir uždarose patalpose.

3.1.2 Bevieliame tinkle naudojamos vietos nustatymo technologijos

Šiame darbe orientuojamasi į WLAN vartotojų vietos informaciją. Vietos nustatymo metodai bevieliuose tinkluose nėra tiek daug plėtojami ir taikomi. WLAN vietos nustatymas gali būti atliekamas dviem pagrindiniais būdais: 1) įvertinant įrenginio signalų stiprumus [9, 11, 27, 28]; 2) matuojant laiką, per kurį duomenų paketas bevieliu tinklu nukeliauja nuo vieno įrenginio iki kito [22, 24, 28]. Šių metodų pagalba galima nustatyti objekto vietą 1-3 m tikslumu.

Sastry ir kiti [22] aprašo Echo protokolą apskaičiuoti vietą pagal žinutės kelionei sugaištą laiką ir viršgarsinius signalus. Water ir kiti [24] pasiūlė analogišką radijo bangų dažnių RF (angl. *radio-frequency*) žinučių apsikeitimu pagrįstą protokolą nustatyti suklastojimui atsparias įrenginių vietas. Zhang ir kiti [23] pasiūlė naudoti vietos informacija paremtus raktus naudojant viešojo rakto kriptografiją, kuri sprendžia Diffie-Hellman problemą. A. Mishra ir S. Banerjee [9] naudoja signalinį kadrą, kurį sistemos įrenginiai siunčia atsitiktiniu stipriu su tam tikru identifikatorium. Kai vartotojas praneša, kurį signalinį kadrą, kokiu stipriu gavo, sistema nustato jo vietą. Kappes ir kitų patente [11] aprašoma sistema, kurioje vartotojui nusiuntus užklausą prisijungti prie bevielio tinklo resursų, siuntimo-priėmimo aparatas, gavęs tą užklausą, perleidžia ją valdymo elementui, kuris išmatuoja užklausos signalo stiprį ir palygina jį su iš anksto nustatyta ir atmintinėje įrašyta ribine reikšme. Jei išmatuoto stiprio reikšmė didesnė už ribinę reikšmę, laikoma, kad vartotojas yra tam tikroje apibrėžtoje vietovėje ir jam leidžiama prisijungti prie tinklo.

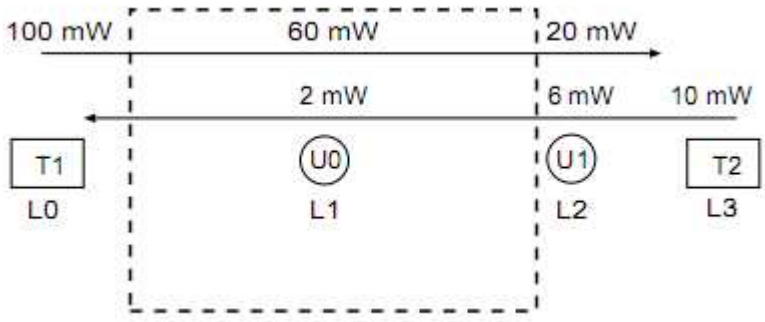
3.2 Šiuo metu egzistuojantys vietos informacijos derinimo su autentifikacija ir prieigos valdymu sprendimai

3.2.1 Vietos nustatymo ir autentifikacijos sistema „Secure Spaces“

A. Mishra ir S. Banerjee [9] pristato infrastruktūrą pavadinimu „Secure Spaces“, leidžiančią tik tam tikroje vietoje (taip vadinamoje „saugioje“ vietoje) esantiems vartotojams naudotis tinklo ištekliais. Pavyzdžiui, jei viešbučio aplinkoje vyksta verslo konferencija, įvairūs delegatai turi skirtingus mobiliuosius įrenginius ir skirtinguose konferencijos kambariuose susirenka diskutuoti verslo planų, „Secure Spaces“ infrastruktūra leidžia tik tam tikroje erdvėje (dažniausiai kambaryje) esantiems asmenims saugiai komunikuoti toje erdvėje. Taigi tokia infrastruktūra apsaugo nuo slapto klausymosi ir duomenų perėmimo. Vartotojai,

esantys „saugioje“ vietoje yra autentifikuojami ir jiems atsiunčiamas grupės raktas, kuris leidžia jiems komunikuoti tarpusavyje.

Pasiūlyta vietos nustatymo ir autentifikacijos sistema naudoja RF signalų stipriais paremtą technologiją. Prieš pradedant autentifikaciją sudaromas erdvės radijo žemėlapis. Kiekvieną fizinę erdvės vietą žemėlapis susieja su lentelėmis, kuriose nurodyta kokio stiprumo kadrai priimami toje vietoje iš skirtingų patikimų įrenginių (dažniausiai prieigos taškų, kurių reikia vieno ar daugiau) naudojant skirtingą transliavimo galią. Autentifikacijos metu kiekvienas patikimas įrenginys atsitiktinai pasirinktu stipriu transliuoja signalinį kadrą. Kadro šaltinio identifikatorius yra slepiamas, o vietoje jo kadre nurodomas unikalus identifikatorius, pagal kurį sistema supranta, kas yra kadro šaltinis ir kokiu stipriu kadras buvo išsiųstas. Vartotojas, gavęs signalinį kadrą (-us), siunčia atgal į sistemą tokią informaciją apie kiekvieną priimtą signalinį kadrą: jo unikalų identifikatorių ir signalo stiprį. Vietos nustatymo ir autentifikacijos sistema (angl. *Location Determination and Authentication System* – LDAS) palygina gautą informaciją su stiprių žemėlapiu ir duomenims atitikus autentifikuoja vartotoją. 6 paveikslėlyje yra parodytas paprastas pavyzdys vienoje dimensijoje. T_1 ir T_2 yra patikimi įrenginiai, kurie bando autentifikuoti nepatikimų įrenginių U_0 ir U_1 vietas. T_1 transliuoja signalinį kadrą b_1 su atsitiktinai parinkta galios verte, tarkim 100 *mW*. Sklindant perdavimo erdve signalas nusilpsta ir U_0 priimamas su 60 *mW* galia, o U_1 su 20 *mW* galia. Analogiškai T_2 transliuoja kadrą b_2 su atsitiktinai pasirinkta galios verte, tarkim, 10 *mW*. U_0 priima šį kadrą su 2 *mW* galia, o – su 6 *mW* galia. Jei U_0 ir U_1 grąžina signalų stiprių dedamąsias atitinkamai {<b_1, 60 *mW*>, <b_2, 2 *mW*>} ir {<b_1, 20mW>, <b_2, 6 *mW*>} vietos yra teisingai nustatomos ir autentifikuojamos pagal LDAS prieinamą radijo žemėlapį.



6 pav. Supaprastintas LDAS pavyzdys vienoje dimensijoje.

Jei U_1 nori suklaidinti LDAS, kad jo vieta yra L_1, jam reikia grąžinti signalų stiprių dedamąsias {<b_1, 60 *mW*>, <b_2, 2 *mW*>}. Kaip bebūtų, U_1 nežino, kurie patikimi įrenginiai kokius signalinius kadrus transliavo (signalinio kadro šaltinio informacija yra nuslepiama). Be to, patikimas įrenginys kiekvieną naują signalinį kadrą transliuoja su atsitiktinai priskirta galia. Tai apsaugo nuo to, kad U_1 pasinaudotų kokia nors išvadų pagal vietą darymo schema nustatyti teisingus priimamų signalų stiprius kokioje nors kitoje vietoje kitiems signaliniams kadrams. Jei U_1 gali nustatyti signalų sklidimo kryptį, jis gali pasinaudoti kokiais nors signalų silpimo modeliais prognozuoti signalo stiprį kitose vietose (pavyzdžiui, vietoje L_1), tačiau nustatyti signalo sklidimo kryptį yra labai sudėtingas uždavinys uždarose patalpose dėl keleto kelių (angl. *multi-path*) efekto, signalai gali pasiekti įrenginį atsispindėję nuo kelių paviršių.

Realiame scenarijuje, vartotojai, norėdami autentifikuoti, siunčia ne tikslius signalų stiprius, bet zoną (signalų ruožas), kuriai gautas signalas priklauso. Tiksliau vartotojas pagal zoną išveda nuo vietos priklausantį raktą, kuriuo užšifruoja gautą nešifruotą tekstą ir jį išsiunčia LDAS serveriui patikrinti. Visi „Secure Spaces“ infrastruktūroje autentifikuoti vartotojai gauna slaptą raktą, kurio pagalba gali šifruoti duomenis ir komunikuoti su kitais tinklo elementais. Kai kuris nors vartotojas išeina iš „saugios“ erdvės arba ateina naujas vartotojas, slaptasis raktas pakeičiamas ir vėl išdalinamas prisijungusiems vartotojams [9].

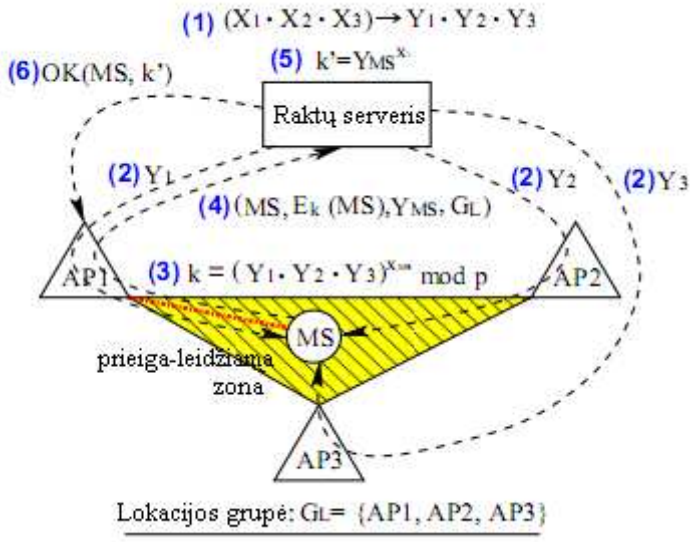
3.2.2 LBAC protokolas autentifikacijai ir šifravimui

Y. S. Cho ir kiti [10] pristato vietos informacija pagrįsto prieigos prie tinklo valdymo (angl. *Location-based network Access Control* – LBAC) protokolą IEEE 802.11 grupės WLAN sistemoms. Autoriai siūlo, kad vietoj tikslaus vartotojų vietos nustatymo, prieiga prie WLAN sistemos būtų suteikta tik tiems vartotojams, kurie yra tam tikrose zonose, kurios atitinkamai yra padengtos kelių prieigos taškų. Naudojant kryptines antenas tokios zonos gali būti norimos formos. Jų pasiūlytas LBAC protokolas naudoja Diffie-Hellman raktų apsikeitimo schemą saugiai autentifikuoti mobilaus vartotojo vietą ir saugiai paskirstyti bendruosius raktus, skirtus duomenų šifravimui. Raktų apsikeitimui naudojamas raktų serveris. LBAC protokolas gali būti naudojamas tiek pradinės prieigos prie tinklo autentifikacijos etape (jo metu naudojamas 802.1x autentifikacijos mechanizmas), tiek paprastų duomenų kadrų apsikeitimo etape. 7 paveikslėlis vaizduoja LBAC architektūrą, kurioje yra trys elementai: MS – mobilios stotys (vartotojų galiniai kompiuteriai), AP – prieigos taškai (angl. *Access Points)* ir raktų serveris. 7 paveikslėlyje MS yra zonoje, kurioje leidžiama prieiga prie tinklo resursų ir kuri apibrėžta lokacijos grupe G_L. Raktų serveris sujungtas su prieigos taškais greitais ir saugiais kanalais. Kiekvienam AP yra priskirtas (Raktų serveris periodiškai generuoja ir priskiria, kaip parodyta (1) žingsnyje) vietos raktas

(atitinkamai Y_1, Y_2, ir Y_3), kuris yra viešasis raktas Diffie-Hellman algoritme. Kaip parodyta (2) žingsnyje, gavę vietos raktus prieigos taškai transliuoja juos. Jei MS yra prieiga-leidžiama zonoje, MS surenka visus raktus iš lokacijos grupės. MS apskaičiuoja ir paskelbia savo vietos informacijos raktą *k* žingsnyje (3).

$$k = (Y_1 \cdot Y_2 \cdot Y_3)^{X_{MS}} = g^{(X_1 \cdot X_2 \cdot X_3) \cdot X_{MS}} \pmod{p}$$

Tada MS siunčia $(MS, E_k(MS), Y_{MS}, G_L)$ per prieigos tašką, prie kurio yra prisijungęs, kaip parodyta (4) žingsnyje. Raktų serveris patikrina MS raktą (5) ir autentifikuoja vartotoją. (6) žingsnyje raktų serveris sugeneruoja bendrą raktą *k'* MS ir AP, prie kurio MS prisijungęs, komunikacijai [10].



7 pav. LBAC raktų apsikeitimo protokolas

3.2.3 Vietos informacija pagrįstas prieigos valdymas

Vietos informacija pagrįsto prieigos valdymo (angl. *Location Based Access Control* – LBAC) sistemos apibrėžia infrastruktūrą, skirtą įvertinti ir tvarkyti prieigos valdymo politikas, į kurias įeina predikatai ir būsenos, paremtos vartotojų vietos informacija [8].

Vertinant vietos informacija pagrįsto prieigos valdymo politikas, reikia atsižvelgti į tai, kad vietos informacija yra apytikslė ir kintanti laike. Vietos informacijos tikslumas priklauso nuo vietos nustatymui naudojamų technologijų, tačiau naudojant bet kurias technologijas vieta nebus nustatyta visiškai tiksliai. Tam įtakos daro besikeičiančios aplinkos sąlygos. Derinant vietos informaciją su autentifikacijos mechanizmais, reikia įvertinti, kad autentifikuotas vartotojas gali judėti ir jo vietos informacija gali pasikeisti.

Vietos informacija pagrįstas prieigos valdymas moksliniuose darbuose dažniausiai yra nagrinėjamas vietos informaciją naudojančių programų kontekste. Tokių informaciją

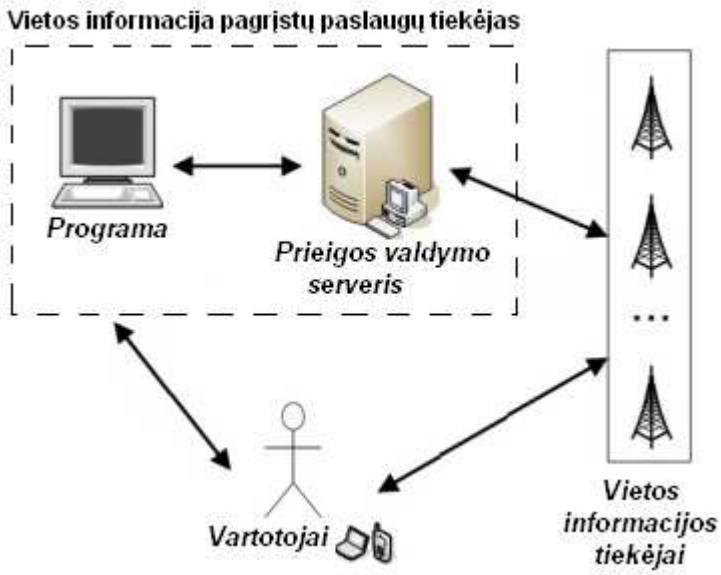
naudojančių paslaugų sėkmės esminis aspektas yra prieigos valdymas. Šiame darbe orientuojamasi į vietos informacijos panaudojimą prieigai prie bevielio tinklo resursų valdyti.

Bendrai LBAC sistemos veikimo scenarijus gali būti apibūdintas taip: vartotojas siunčia užklausą naudotis vietos informacija pagrįstomis paslaugomis (angl. *Location Based Services* – LBSs). Tiekėjas, galimai bendradarbiaudamas su vietos informacijos serveriu, surenka vietos informaciją, kad galėtų nuspręsti, ar paslauga gali būti suteikta ir kaip ji turėtų būti suteikta. Vietos informacijos serveris veikia kaip vietos nustatymo sistema, įvertinanti vartotojų mobiliųjų įrenginių vietos informaciją ir pateikdama tokią informaciją kitokiu pavidalu ir su kitokia paslaugų kokybe. Kokių tipų vietos informacijos užklausas vietos informacijos serveris gali patenkinti, priklauso nuo vartotojo naudojamų įrenginių, vartotojo vietos įvertinimui taikomų metodų ir aplinkos sąlygų [7].

Ardagna ir kiti išskiria tris pagrindinius žingsnius LBAC sistemos kūrime: 1) LBAC architektūros, kuri įvertintų ir pritaikytų vietos informacija pagrįstas politikas, projektavimas; 2) vietos informacija pagrįstų būsenų apibrėžimas; 3) vietos informacija pagrįstų būsenų įvertinimo ir pritaikymo mechanizmo apibrėžimas [7].

3.2.3.1 LBAC architektūra

Vienas iš siūlomų LBAC infrastruktūros sprendimų pavaizduotas 8 paveikslėlyje. Vartotojas yra esybė, kurios prieigos užklausą turi autorizuoti LBAC sistema. Programa yra į klientą orientuota programa tiekianti paslaugas, kurių prieinamumą reguliuoja prieigos informacija pagrįsta saugos politika. Prieigos valdymo serveris atsakingas už prieigos užklausų įvertinimą pagal kelias vietos informacija pagrįstas politikas. Prieigos valdymo serveris komunikuoja su vienu ar keliais Vietos informacijos tiekėjais, kad gautų vietos informaciją. Jis neturi tiesioginio priėjimo prie jos, bet siunčia užklausas ir gauna atitinkamus atsakymus. Vietos informacijos tiekėjai yra patikimi ir teikia duomenis apie vietą ir laiką, įvertina vietos informacija pagrįstus predikatus. Šios esybės komunikuoja užklausų ir atsakymų pagalba kaip parodyta 8 paveikslėlyje. Procesą inicijuoja Vartotojas siųsdamas prieigos užklausą Programai. Tada jie keičiasi duomenimis, kurie reikalingi įvertinti politikai. Užklausa toliau persiunčiam Prieigos valdymo serveriui, kuris reikalui esant, susisiekia su Vietos informacijos tiekėjais, įvertina politikas ir grąžina prieigos atsakymą. Komunikacija tarp Prieigos valdymo serverio ir Vietos informacijos tiekėjų atliekama pagal derybų dėl paslaugos lygio fazę. Derybų metu susitariama dėl paslaugų kokybės atributų rinkinio ir atitinkamos paslaugos kainos.



8 pav. LBAC architektūra [7]

3.2.3.2 Vietos informacija pagrįstų būsenų apibrėžimas

LBAC sistemose gali būti vertinama ne tik vartotojo vardas ir slaptažodis, bet ir jo būsena, pavyzdžiui ar vartotojas yra viename ar kitame pastate. Ardagna ir kiti išskiria tris pagrindines kategorijas vietos informacija pagrįstų būsenų, kurios gali būti naudojamos prieigos valdymo politikose ir kurias šiuolaikinės technologijos gali įvertinti: būsenos pagal vietą, būsenos pagal judėjimą ir būsenos pagal sąveiką. Būsenos gali būti išreiškiamos tokios formos boolean tipo užklausomis: `predikatas`*(parametrai, reikšmės)* [7, 8, 13].

Tokia užklausa klausia, ar su nurodytais parametrais predikatas įgyja nurodytą reikšmę. Lentelėje 6 pateikti predikatai, susiję su kiekvienos kategorijos būsenomis, ir jų paaiškinimai. Pavyzdžiui, užklausa *greitis(Aldona, 0, 3)* tikrina, ar Aldonos greitis yra tarp 0 ir 3 kilometrų per valandą.

6 lentelė. Vietos informacija paremti predikatai

Tipas	**Predikatas**	**Paaiškinimas**
Vieta	zonoje(vartotojas, zona)	Įvertina, ar vartotojas zonos ribose.
	nezonoje(vartotojas, zona)	Įvertina, ar vartotojas už zonos ribų.
	nuotolis(vartotojas, objektas, min_atstumas, max_atstumas)	Įvertina, ar atstumas nuo vartotojo iki objekto yra intervale [min_atstumas, max_atstumas].
Judėjimas	greitis(vartotojas, min_greitis, max_greitis)	Įvertina, ar vartotojo greitis yra intervale [min_greitis, max_greitis]
Sąveika	tankis(zona, min_kiekis, max_kiekis)	Įvertina, ar vartotojų kiekis tam tikroje zonoje yra ne didesnis už max_kiekis ir ne mažesnis už min_kiekis.
	vietinis_tankis(vartotojas, zona, min_kiekis, max_kiekis)	Įvertina, ar vartotojų tankis zonoje aplink vartotoją yra intervale [min_kiekis, max_kiekis]

Ardagna ir kiti [13, 8, 7] pristato kalbą, kuria aprašomos būsenos ir predikatai, šioje kalboje yra du pagrindiniai elementai: vartotojai ir zonos. Visi vartotojai yra vienareikšmiškai identifikuojami vartotojo identifikatoriumi, kuris susieja vartotojo tapatybę su galiniu mobiliuoju įrenginiu. Pavyzdžiui, GSM/3G technologijų atveju tai galėtų būti SIM kortelės numeris, o IEEE 802.11 tipo tinkle IP adresas. Zonos yra rinkinys žemėlapio vietovių, kurios identifikuojamos pagal geometrinį modelį (pavyzdžiui, sritis n dimensijų koordinačių sistemoje) arba pagal simbolinį modelį (pavyzdžiui su nuorodomis į realaus pasaulio objektus tokius kaip gatvės, miestai, zip kodai ar pastatai).

Ardagana ir kiti [13, 8, 7] siūlo bendrą sprendimą, kaip papildyti jau esamas kalbas išnaudojant vietos informaciją, bet nekuria naujos kalbos. Priimama, kad prieigos valdymo serveris atpažįsta tik priregistruotus klientus, kurie be savo vartotojo identifikatoriaus turi ir kitas savybes, tokias kaip vardas, adresas, gimimo data ir pan. Šios savybės yra išreikštos per vartotojo profilį. Objektai yra resursai (duomenys ir paslaugos), prie kurių vartotojai gali gauti prieigą. Jie taip pat turi savybes, kurios išreiškiamos objekto profiliu, objektai gali būti grupuojami pagal vienodas savybes ir į grupę objektų galima kreiptis vienu vardu. Profiliai yra susieti su tam tikro objekto ar vartotojo identifikatoriumi. Formaliai prieigos valdymo taisyklę [13, 8, 7] apibrėžia taip:

Apibrėžimas 1: *prieigos valdymo taisyklė susideda iš trijų elementų* <subj_išraiška, obj_išraiška, veiksmas>, *kur*

subj_išraiška *yra boolean tipo formulė, kuri leidžia nurodyti subjektų rinkinį pagal tai, ar jie tenkina tam tikras sąlygas, kurios gali įvertinti vartotojo profilį, priklausymą tam tikrai grupei, aktyvias roles, vietos predikatus ir pan.*

obj_išraiška *yra boolean tipo formulė, kuri leidžia nurodyti objektų rinkinį pagal tai, ar jie tenkina tam tikras sąlygas, kurios gali įvertinti objekto profilį, priklausymą tam tikrai kategorijai ir pan.*

veiksmas *yra veiksmas arba veiksmų klasė, kurią nurodo taisyklė.*

Sąlygos išreikštos subj_išraiška gali būti bendrosios sąlygos ir vietos informacijos sąlygos. Bendrosios sąlygos įvertina, ar subjektai priklauso tam tikroms klasėms ir savybes, esančias jų profiliuose.

Priimama, kad P žymi prieigos valdymo serveryje įdiegtą prieigos valdymo politiką. Kai duota prieigos valdymo taisyklė $r \in P$, *subj_išraiška(r), obj_išraiška(r), veiksmas(r)* apibrėžia atitinkamai subjekto išraišką, objekto išraišką ir veiksmą, priklausančius taisyklei *r*.

Objektų ir vartotojų profiliuose esančios atskiros savybės yra nurodomos tradiciškai naudojant taško ženklą. Pavyzdžiui, `Aldona.Adresas` reiškia Aldonos adresą. `Aldona` čia yra

vartotojo identifikatorius, taigi kartu ir atitinkamo profilio identifikatorius, `Adresas` yra savybės pavadinimas.

Lentelė 7. Prieigos valdymo taisyklių pavyzdžiai

	Subjektas		objektas	veiksmas
	Bendrosios sąlygos	**Vietos informacijos sąlygos**		
1	`lygu(vartot.rolė, admin) ∧ teisingas(vartot.vardas, vartot.slaptažodis)`	`zonoje(vartot.id, Serverinė) ∧ tankis(Serverinė, 1, 1) ∧ greitis(vartot.id, 0, 3)`	`lygu(obj.vardas, Tinklo_administr)`	`vykdyti`
2	`lygu(vartot.rolė, admin) ∧ teisingas(vartot.vardas, vartot.slaptažodis)`	`zonoje(vartot.id, ITdepartamentas) ∧ vietinis_tankis(vartot.id, šalia, 1, 1) ∧ greitis(vartot.id, 0, 3)`	`lygu(obj.kategorija, žurnalas)`	`skaityti`
3	`lygu(vartot.rolė, vadyb) ∧ teisingas(vartot.vardas, vartot.slaptažodis)`	`zonoje(vartot.id, ofisas) ∧ vietinis_tankis(vartot.id, šalia, 1, 1) ∧ greitis(vartot.id, 0, 3)`	`lygu(obj.kategorija, klientas)`	`skaityti`
4	`lygu(vartot.rolė, vadyb) ∧ teisingas(vartot.vardas, vartot.slaptažodis)`	`nezonoje(vartot.id, Konkurentų_vieta) ∧ vietinis_tankis(vartot.id, šalia, 1, 1)`	`lygu(obj.kategorija, StatistDuom)`	`skaityti`

Pavyzdys 1. Lentelėje 7 surašyti prieigos valdymo taisyklių pavyzdžiai. Tarkim, kad Tinklo_administr yra programinė įranga administruoti kompanijos tinklui. Taisyklė 1 reiškia, kad tik prisiregistravę administratoriai būdami statiški Serverinėje gali paleisti tinklo administravimo programą. Be šios privilegijos administratoriai, būdami IT departamente, gali skaityti žurnalą, kuriame yra duomenys apie vartotojų vietą (taisyklė 2). Su klientais susijusi informacija turi būti saugoma ir suteikiama tiktai tam tikriems personalo darbuotojams, todėl pagal taisyklę 3 tokią informaciją gali skaityti tik prisiregistravę vadybininkai būdami ofise statiški, kai šalia jų nėra kitų vartotojų. Statistiniai kompanijos duomenys turi būti saugomi nuo konkurentų, todėl pagal taisyklę 4 juos leidžiama skaityti prisiregistravusiems vadybininkams, kurie nėra konkurentų vietoje ir šalia jų nėra kitų vartotojų.

3.2.3.3 Vietos informacija pagrįstų būsenų įvertinimas ir pritaikymas

Kaip jau minėta anksčiau būsenos išreiškiamos tokios formos boolean tipo užklausomis: `predikatas`*(parametrai, reikšmės)*. Tokios užklausos grąžina trijų elementų atsakymus [`bool_reikšmė, patikimumas, galiojimas`], kur `bool_reikšmė` nurodo, ar predikatas yra tiesa, `galiojimas` išreiškia įvertinimo galiojimo laiką, `patikimumas` išreiškia su įvertinimu siejamą patikimumą. Patikimumas priklauso nuo tokių aspektų kaip tikslumas, aplinkos ir oro sąlygos, užklaustos vietos smulkumas, matavimui naudojamos technologijos. Parametras *patikimumas* grąžinamas dėl to, kad fizinių matavimų klaidos galėtų būti atskirtos nuo prieigos valdymo būsenų. Vietos informacijos tiekėjas gali geriau nustatyti *patikimumą,* nes

gali įvertinti matavimo reikšmių tikimybių pasiskirstymą. Kadangi vietos informacijos tiekėjai grąžina minėtas tris reikšmes, prieigos valdymo serveriui pagal `patikimumas` ir `galiojimas` reikia nuspręsti, ar gautas atsakymas gali būti laikomas tinkamu prieigos valdymui. Tam reikalui kiekvienam predikatui yra priskiriamos viršutinė ir apatinė patikimumo ribos bei *MaxBandymų* skaičius (Lentelėje 8 pateiktas pavyzdys teisingumo lentelės, kurioje nurodytos ribos kiekvienam predikatui). Jei `patikimumas` reikšmė yra didesnė už viršutinę ribą, parodymai tinkami, jei žemiau apatinės ribos, parodymai netinkami, o jei tarp apatinės ir viršutinės ribų, kviečiamas predikato įvertinimas iš naujo, bet ne daugiau nei *MaxBandymų* kartų. Jei po *MaxBandymų* atsakymas dar neįvertintas, vietos informacija paremta būsena laikoma **`neapibrėžta`**. Skaičius *MaxBandymų* nurodo, kiek daugiausia kartų Prieigos valdymo serveris pervertins predikatą dėl nepakankamo patikimumo arba pasibaigusio įvertinimo galiojimo laiko [13].

8 lentelė. Teisingumo lentelės vietos predikatams pavyzdys

Predikatas	**Patikimumo ribos**		**MaxBandymų**
	apatinė	**viršutinė**	
`Zonoje`	`0.1`	`0.9`	`10`
`Nezonoje`	`0.1`	`0.9`	`10`
`Nuotolis`	`0.2`	`0.8`	`5`
`Greitis`	`0.2`	`0.8`	`5`
`Tankis`	`0.3`	`0.7`	`3`
`vietinis_tankis`	`0.3`	`0.7`	`3`

Lentelėje 8 parodytas teisingumo lentelės pavyzdys apibrėžia Prieigos valdymo serverio veikimą. Patikimumo ribų reikšmės yra empirinės, kurias turėtų nustatyti ekspertas. Nustatant reikšmes turėtų būti atsižvelgta į tai, kaip techniškai yra sudėtinga atlikti matavimus reikalingus kiekvienam predikatui, ir į tai, kiek patikimas yra Vietos informacijos tiekėjas. Pavyzdžiui, su patikimo Vietos informacijos tiekėjo nurodytu 80% patikimumu reikšmė gali būti vertinama kaip teisinga, o su kito Vietos informacijos tiekėjo nurodytu 90% patikimumu – kaip nepatikima. Vietos informacijos tiekėjo patikimumui įtakos gali turėti tam tikros matavimų technikos, taip pat sensorių kiekis ir paskirstymas. Predikatai, kurių įvertinimui sugaištama daugiau laiko, gali būti pervertinami mažiau kartų nei kiti. Pavyzdžiui, predikatų `tankis` ir `vietinis_tankis` įvertinimas gali būti ilgiausias, nes priklauso nuo kelių subjektų pozicijos. `zonoje` ir `nezonoje` predikatai gali būti greičiau įvertinami, nes jie priklauso nuo vieno subjekto pozicijos, predikatų `nuotolis` ir `greitis` įvertinimas priklauso nuo dviejų

subjektų matavimų. Techninių aspektų, kurie gali turėti įtakos patikimumui, pavyzdžiai yra predikato jautrumas išorinėms sąlygoms, tokioms kaip aplinkos ir oro sąlygos, ir naudojamos matavimo technologijos. Pavyzdžiui, `zonoje` ir `nezonoje` predikatai yra jautresni aplinkos pokyčiams, taigi jiems reiktų nustatyti mažą patikimumo intervalą, kad būtų sumažintas netikslumas. Predikatai `tankis` ir `vietinis_tankis` yra mažiausiai jautrūs, taigi gali būti priimti didesni patikimumo intervalai, kad rezultatas, gautas Vietos informacijos tiekėjo, būtų patvirtintas. Nustatant patikimumo ribas reiktų apsvarstyti, kiek pervertinimo bandymų gali įvykti prieš pasibaigiant vertinimo galiojimo laikui. Tiems predikatams, kuriems pervertinimo bandymų gali būti daugiau, yra didesnė tikimybė sulaukti atsakymo su tinkamu patikimumo lygiu, taigi šiems predikatams gali būti nustatytos aukštesnės patikimumo ribos [13].

[13] pristato, kaip veikia prieigos valdymas. Priimama, kad Prieigos valdymo serveris iš pradžių įvertina, ar sprendimas gali būti priimtas lokaliai, t.y. ar jam taikomos taisyklės įvertina tik bendrąsias būsenas. Jei sprendimo priimti negalima (autorizacijai naudojami vietos informacija pagrįsti predikatai) atitinkamos užklausos yra siunčiamos Vietos informacijos tiekėjui. Vietos informacija pagrįstų predikatų įvertinimui reikia daugiau resursų, todėl esant galimybei to reiktų išvengti. Kadangi informacija pagrįsti predikatai gali įgyti tris reikšmes (**`taip`**, **`ne`** ir **`neapibrėžta`**), kelių predikatų jungties rezultatas gaunamas taip: **`neapibrėžta`** $\cap$ **`ne`** = **`ne`**, **`neapibrėžta`** $\cup$ **`taip`** = **`taip`**, o visais kitais atvejais konjunkcijos ir disjunkcijos su **`neapibrėžta`** rezultatas yra **`neapibrėžta`**. Prieiga yra suteikiama, jei taikomos taisyklės subjekto išraiška yra įvertinama **`taip`**, kitais atvejais prieiga yra draudžiama.

3.2.4 Privalomojo prieigos valdymo modelio papildymas vietos informacija

Standartinis privalomojo prieigos valdymo modelis gali būti išplėstas – vietos informacijos koncepcija gali būti įjungta į MAC modelį. I. Ray ir M. Kumar [12] rašo, kaip formalizuoti vietos informaciją ir kaip MAC modelio komponentus susieti su vietos informacija. Teisingas modelio elgesys išreiškiamas apribojimais, kurių turi laikytis kiekviena pagal šį modelį veikianti sistema.

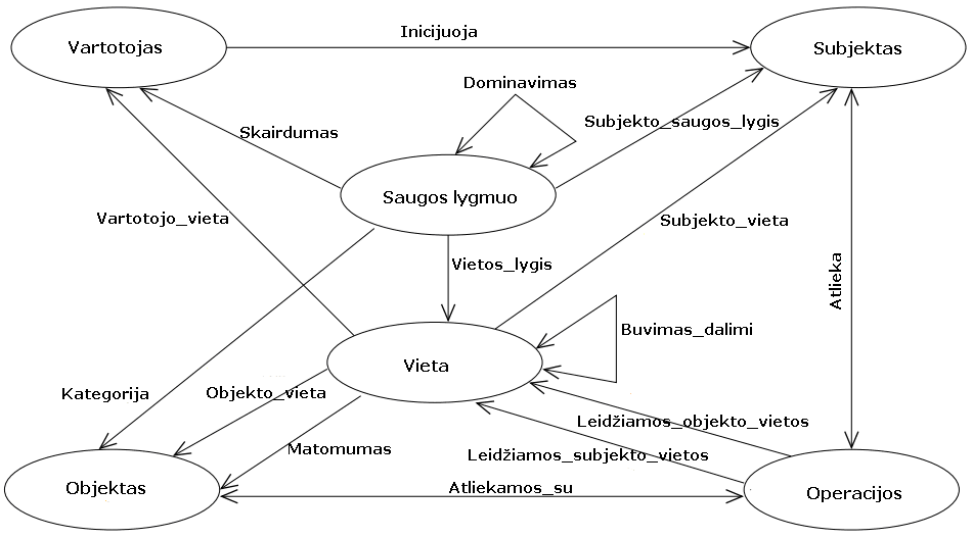
Pagrindiniai MAC modelio komponentai yra objektai (angl. *Object*), vartotojai (angl. *User*), subjektai (angl. *Subject*) ir operacijos (angl. *Operations*). Objektai savyje turi arba priima informaciją, vartotojai – tai žmonės. Kiekvienas objektas ir kiekvienas vartotojas gali būti susietas su saugumo lygiu (angl. *Security Level*). Vartotojas gali prisijungti prie objekto, jei to objekto saugos lygis yra žemesnis už vartotojo saugos lygį, t.y. vartotojo saugo lygis dominuoja (angl. *Dominance*). Kiekvienas vartotojas susietas su vienu ar daugiau subjektų.

Subjektai yra procesai vykdomi prisijungusių vartotojų vardu, jų saugos lygis toks pat kaip prisijungusių prie jų vartotojų. Operacijos, kurias subjektas gali vykdyti su objektais gali būti `skaityti` (objekto turinio atskleidimas, bet ne modifikavimas) arba `rašyti` (objekto turinio keitimas). Būtinos sąlygos skaitymui arba rašymui yra šios:

Subjektui *S* yra leidžiama skaityti objektą *O* tik tada, kai subjekto saugos lygis *L*(*S*) dominuoja objekto saugos lygio *L*(*O*) atžvilgiu, t.y. $L(O) \leq L(S)$.

Subjektui *S* galima rašyti į objektą *O* tik tada, kai objekto *O* saugos lygis *L*(*O*) yra lygus subjekto saugo lygiui *L*(*S*), t.y. $L(O) = L(S)$.

Objekto ar vartotojo vietą formaliai I. Ray ir M. Kumar [12] apibrėžia kaip netuščią taškų rinkinį $\{t_i, t_j, ..., t_n\}$. Kelios vietos gali būti susijusios vienu iš dviejų ryšiu: gali būti lygios arba viena gali būti kitos dalis. Pagal tai sudaroma vietovių hierarchija (ta vietovė, kuri yra kitos dalis, hierarchijoje yra žemiau), tada joms priskiriamas saugos lygis (jei vietovė $Viet_i$ yra $Viet_j$ dalis, $Viet_i$ vietovės saugos lygis turi dominuoti $Viet_j$ vietovės saugos lygio atžvilgiu – apribojimas 1).



9 pav. MAC komponentų ir vietos informacijos susiejimas [12]

9 paveikslėlyje parodyta, kaip MAC komponentai susiejami su vietos informacija. Ryšį parodo rodyklė – komponento, prie kurio yra rodyklės galas ➔, ryšys yra „daug“, o komponento, kuris sujungtas be ženklo➔, yra „vienas“. Dėl saugos sumėtimų vartotojai leidžiami tik į tas vietas, kurių saugos lygis yra ne aukštesnis už vartotojų saugos lygį – apribojimas 2. Prieš suteikiant subjektui priėjimą prie kokio nors objekto, patikrinama subjekto vietos informacija. Kiekvienas subjektas yra susiejamas su ta vieta, kurioje yra subjektą inicijavęs vartotojas. Vartotojui leidžiama inicijuoti subjektą tik tokioje vietoje,

kurios saugos lygis dominuoja subjekto saugo lygio atžvilgiu – apribojimas 3. Objektai gali būti fiziniai (pavyzdžiui, kompiuteris) ir loginiai (pavyzdžiui, failai). Loginiai objektai yra laikomi fiziniuose objektuose, todėl loginių objektų vieta yra fizinių objektų, kuriuose jie yra, vieta. Kai loginis objektas, toks kaip paskirstyta duombazė, yra keliose fiziniuose objektuose, jo vieta yra rinkinys taškų, susietų su skirtingais fiziniais objektais, kuriuose jis yra. Kad objektai būtų apsaugoti, jie turi būti laikomi vietose, kurių saugos lygis dominuoja objektų saugo lygio atžvilgiu – apribojimas 4. Kai vienas objektas yra sudarytas iš kelių kitų objektų, jo saugos lygis turi dominuoti jį sudarančių objektų saugos lygių atžvilgiu, o jį sudarančių objektų vietų saugos lygiai turi dominuoti to objekto vietos saugo lygio atžvilgiu, nes objekto vieta susideda iš objektą sudarančių objektų vietų – apribojimas 5.

Esant vietos informacija paremtam prieigos valdymui prieš autorizuojant operacijas būtina užtikrinti, kad subjektai ir objektai yra tam tikrose vietose, taigi kiekviena operacija susiejama su dviem vietovių rinkiniais: leistinomis subjekto vietomis $Viet_{op\_sub}$ ir leistinomis objekto vietomis $Viet_{op\_obj}$ (šie ryšiai 10 paveikslėlyje pažymėti *LeistinosSubjektoVietos* ir *LeistinosObjektoVietos* antraštėmis). Taigi kad prieiga būtų suteikta, subjekto vieta turi būti tarp leistinų subjekto vietų, o objekto vieta turi būti viena iš leistinų objekto vietų. Be to vietos saugos lygis turi dominuoti objekto saugos lygio atžvilgiu, nes objektas negali būti vietoje, kurios saugos lygis žemesnis už jo saugos lygį. Taip pat ir subjektas turi būti vietoje, kurios saugos lygis ne žemesnis už subjekto saugos lygį. Visa tai išreiškia apribojimas 6 (operacijai `skaityti`) ir apribojimas 7 (operacijai `rašyti`).

Visi prieš tai pristatyti apribojimai yra formaliai surašyti žemiau:

Apribojimas 1 $\forall\ Viet_i, Viet_j \in \mathbf{Viet} \bullet Viet_i \subseteq Viet_j \Rightarrow L(Viet_j) \leq L(Viet_i)$, kur **Viet** yra rinkinys visų galimų vietų.

Apribojimas 2 $L(Viet_V) \leq L(V)$, kur V yra vartotojas ir $Viet_V$ yra vartotojo vieta.

Apribojimas 3 $L(S) \leq L(V) \wedge Viet_S = Viet_V \wedge L(S) \leq L(Viet_S)$, kur S yra vartotojo V inicijuotas subjektas, $Viet_V$ yra vartotojo V vieta ir $Viet_S$ yra subjekto S vieta.

Apribojimas 4 $L(O) \leq L(Viet_O)$, kur O yra objektas ir $Viet_O$ yra objekto vieta.

Apribojimas 5 $(žvr(L(O_1), L(O_2), ..., L(O_n)) \leq L(O)) \wedge (L(Viet_O) \leq aar(L(Viet_{O1}), L(Viet_{O2}), ..., L(Viet_{On}))$, kur *žvr*() nurodo žemiausią viršutinę ribą iš visų saugos lygių, *aar*(...) nurodo aukščiausią apatinę ribą išvardintiems saugos lygiams, O_i yra sudėtinio objekto O dalis ir $Viet_{Oi}$ yra O_i vieta, o $1 \leq i \leq n$.

Apribojimas 6 $L(O) \leq L(S) \wedge Viet_S \subseteq Viet_{skaityti\_sub} \wedge Viet_O \subseteq Viet_{skaityti\_obj} \wedge L(O) \leq L(Viet_{skaityti\_obj}) \wedge L(S) \leq L(Viet_{skaityti\_sub})$, kur S yra subjektas, pageidaujantis skaityti objektą

O, $Viet_S$, $Viet_O$ yra tikrosios atitinkamai subjekto ir objekto vietos, o $Viet_{skaityti\_sub}$, $Viet_{skaityti\_obj}$ yra leistinos vietos subjektui ir objektui, kad būtų įvykdyta skaitymo operacija.

Apribojimas 7 $L(O) = L(S) \wedge Viet_S \subseteq Viet_{rašyti\_sub} \wedge Viet_O \subseteq Viet_{rašyti\_obj} \wedge L(O) \leq L(Viet_{rašyti\_obj}) \wedge L(S) \leq L(Viet_{rašyti\_sub})$, kur S yra subjektas, pageidaujantis rašyti į objektą O, $Viet_S$, $Viet_O$ yra tikrosios atitinkamai subjekto ir objekto vietos, o $Viet_{rašyti\_sub}$, $Viet_{rašyti\_obj}$ yra leistinos vietos subjektui ir objektui, kad būtų įvykdyta rašymo operacija.

3.2.5 Role pagrįsto prieigos valdymo modelio papildymas vietos informacija

M. L. Damiani ir kiti [18] pristato Geo-RBAC – role pagrįsto prieigos valdymo modelio išplėtimą įvedant į jį vietos informaciją.

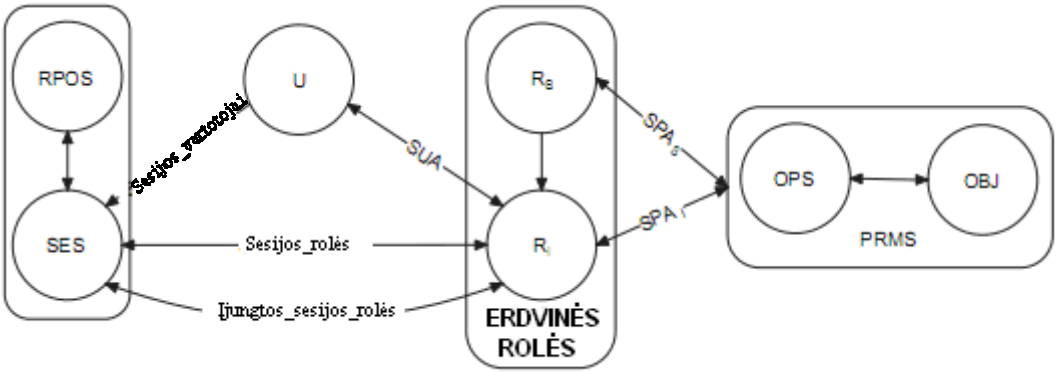
Geo-RBAC modelyje priimama, kad objektai turi geometrinę išvaizdą pagal OGC (angl. *Open GeoSpatial Consortium*) paprastų požymių (angl. *simple feature*) geometrinį modelį [31]. Tokiame modelyje objekto geometrija gali būti taško, linijos arba daugiakampio tipo arba tokių geometrijų rinkinys. Geometrijos gali būti susietos skirtingais būdais. Topologinių ryšių rinkinys yra *REL* = {*Disjoint, Touch, In, Contains, Equal, Cross, Overlap*}. Jei egzistuoja vienas ryšys, tai kiti neegzistuoja. Šie ryšiai yra patobulinimas gerai žinomo topologinių ryšių rinkinio, kurį pasiūlė Clementini ir kiti 1993 m. Priimama, kad resursai, kurie turi būti saugomi, susideda iš duomenų apie realaus pasaulio esybes, kurios gali turėti vietą. Pagal OGC terminologiją šios esybės vadinamos požymiais. Požymiai identifikuojami pavadinimais, pavyzdžiui, *Milanas*, *Mičigano* ežeras, mašina su numeriu *ZBC823*. Kai esybėms gali būti priskirta kažkokia vieta erdvėje, požymiai yra *erdviniai* (angl. *spatial*), pavyzdžiui, *Milanas* ir *Mičigano* ežeras. Požymiai yra *neerdviniai*, kai jie nėra susieti su kokia nors vieta, pavyzdžiui, mašina su numeriu *ZBC823*. Laikoma, kad erdviniai požymiai turi tokią pat geometriją, kaip ir vieta, kurioje jie yra, todėl požymio dimensija yra 0, kai jis yra taškas, 1, kai jis yra linija, 2, kai jis yra daugiakampis, ir neapibrėžta ($\perp$), kai požymis yra *neerdvinis*.

Požymiai turi nuo taikymo priklausomą semantiką, kurią išreiškia požymio tipo koncepcija. Požymio tipas nurodo esybės paskirtį. *Kelias*, *miestas*, *ežeras*, *mašina* yra požymių tipų pavyzdžiai. Priimama, kad požymių tipų rinkinyje yra du sistemos apibrėžti požymių tipai: didžiausias (aukščiausias) požymio tipas ir mažiausias (žemiausias) požymio tipas. Didžiausias požymio tipas (pažymėkime jį Top_{ft}) susideda iš visų vartotojų apibrėžtų požymių tipų, o mažiausias požymio tipas (pažymėkime jį Bot_{ft}) yra visų vartotojų apibrėžtų požymių tipų dalis. Norint apibūdinti objektą, galima išvardinti jam priklausančius požymius arba nurodyti užklausą pagal požymius.

Erdvinė rolė yra pagrindinis Geo-RBAC terminas, kuris apibrėžiamas kaip pora < *r*, *e* >, kur *r* yra rolės pavadinimas, o *e* yra erdvinė rolės apimtis (trumpiau apimtis). Rolės apimtis apibrėžia erdvines ribas, kuriose vartotojas gali prisiimti rolę. Priimama, kad rolės apimtys modeliuojamos kaip požymiai, kurie gali būti įvairių tipų. Tas pats rolės pavadinimas gali būti skirtingose erdvinėse rolėse. Pavyzdžiui, rolė *Daktaras* gali būti susieta su skirtingomis apimtimis, tarkim, ligoninėmis, formuojant atskiras erdvines roles.

Geo-RBAC modelyje priimama, kad vartotojai turi vietą, kuri gali keistis laikui bėgant. Vieta gali būti tikra arba loginė. Tikra vieta atitinka vartotojo vietą Žemėje. Ji gali būti nustatyta naudojant tokius mobilius įrenginius kaip GPS transporto priemonės sekimo įtaisas arba mobilusis telefonas. Tikros vietos gali būti išreikštos skirtingų tipų geometrijomis, priklausomai nuo pasirinktos technologijos ir pageidaujamo tikslumo, jos gali atitikti taškus arba daugiakampius. Loginė vieta modeliuojama kaip erdvinis požymis. Pavyzdžiui, transporto priemonės loginė vieta gali būti daugiakampis požymis, kurio tipas yra *miestas*. Loginė vieta gali būti išskaičiuota pagal tikrą vietą naudojant tam tikras sulyginimo funkcijas.

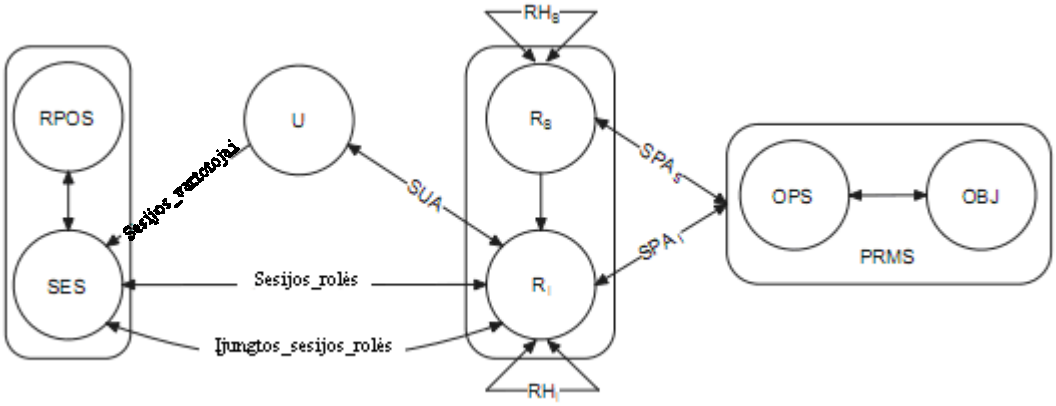
Pagrindinė Geo-RBAC idėja yra rolės schemos ir rolės egzemplioriaus koncepcijų atskyrimas. Rolės schema ne tik apibrėžia vieną pavadinimą erdvinių rolių rinkiniui, bet ir apriboja erdvę, kur gali veikti rolės. Be to rolės schema specifikuoja loginių vietų tipą ir vietos, kurioje vartotojas gali atlikti rolę, dydį. Rolės egzempliorius yra rolė, išpildanti apribojimus, apibrėžtus schemos lygmenyje. Taigi erdvinė rolė turi tokį patį pavadinimą kaip ir schemos rolė, o rolės erdvės ribos yra erdvinis požymis su tikslia semantika. Reikia paminėti, kad visos erdvinės rolės, būdamos rolės schemos egzemplioriais, yra pilnai identifikuojamos rolės apimties (požymio) pavadinimu. Kita svarbi rolės schemos savybė yra ta, kad jai gali būti priskirti leidimai. Tie leidimai yra paveldimi visų schemos egzempliorių. Vartotojams yra priskiriamos erdvinės rolės, kitaip sakant, tam tikros rolės schemos egzemplioriai , kurie gali būti aktyvuoti sesijos metu. Kitaip nei RBAC modelyje, rolės veikia tik tada, kai vartotojo vieta yra rolės apimtyje. Autoriai naudoja iš RBAC paimtą grafinį atvaizdavimą (žr. 10 pav.). R_i ir R_s vaizduoja atitinkamai rolių egzempliorių ir rolių schemų aibes. *RPOS* yra tikrų vietų aibė, *U, SES, OPS* ir *OBJ* atitinkamai vartotojų, sesijų, operacijų ir objektų aibės.



10 pav. Geo-RBAC branduolys

Rolės schema apibrėžia bendrą rolių rinkinio pavadinimą, rolės apimties požymio tipą, loginės vietos požymio tipą ir sulyginimo funkciją, susiejančią tikrąsias vietas su loginėmis vietomis. Rolės schema yra ketvertas < *r*, *ext*, *loc*, m_{loc} >, kur *r* yra rolės pavadinimas, *ext* – rolės apimties požymio tipas, *loc* – loginės vietos požymio tipas, m_{loc} – vietos sulyginimo funkcija požymio tipui *loc*. Priimama, kad turinti rolės pavadinimą *r* rolės schema yra unikali visoje aibėje R_s. Rolės schemos pavyzdys yra ketvertas < *Daktaras*, *Ligoninė*, *Sektorius*, $m_{Sektorius}$ >, kuriame Daktaras yra rolės pavadinimas, Ligoninė yra rolės apimties požymio tipas (kartu ir objekto, kuris apriboja rolę erdvėje, rūšis), Sektorius yra loginės vietos požymio tipas (tariama, kad ligoninės erdvė yra padalinta į sektorius), $m_{Sektorius}$ – sujungimo funkcija, kuri tikrąją vietą sujungia su logine. Skirtingos schemos tai pačiai rolei, pavyzdžiui, < *Daktaras*, *Ligoninė*, *Sektorius*, $m_{Sektorius}$ > ir < *Daktaras*, *Departamentas*, *Kambarys*, $m_{Kambarys}$ >, yra neleidžiamos. Turint rolės schemą r_s, r_s egzempliorius r_i yra pora < *r*, *e* >, kur $r=r_s.r$ ir *e* yra toks požymis, kurio tipas sutampa su $r_s.ext$.

Geo-RBAC modelyje leidimai gali būti susieti su rolės schema ir paveldėti visų rolės egzempliorių arba tiesiogiai susieti su rolės egzemplioriumi. Kai vartotojas prisijungia, aktyvuojama sesija ir išrenkamos tai sesijai skirtos rolės, tačiau, kad sesijos rolė veiktų, vartotojo loginė vieta turi būti rolės apimtyje. Prieigos užklausa gali būti išreikšta ketvertu < *s*, *rp*, *p*, *o* >, kuris reiškia, kad sesijos *s* vartotojas esantis tikroje vietoje *rp* nori atlikti operaciją *p* su objektu *o*. Prieigos užklausa gali būti patenkinta tikroje vietoje *rp*, jei leidimas (*p*, *o*) priklauso rinkiniui leidimų, susietų su šioje sesijoje *s* veikiančiomis rolėmis, kai vartotojas yra *rp* vietoje.



11 pav. Geo-HRBAC

M. L. Damiani ir kiti [18] apibrėžia hierarchinį Geo-RBAC modelį (Geo-HRBAC), kuris pavaizduotas paveikslėlyje 11. Priimama, kad rolių schemų hierarchinis išrikiavimas gali būti apibrėžtas tik tada, kai tarp rolės schemų apimčių ir vietos tipų yra buvimo dalimi ryšys. Pavyzdžiui, turint dvi schemas:

Dakt = < *Daktaras*, *Ligoninė*, *Sektorius*, $m_{Sektorius}$ >

Ped = < *Pediatras*, *Departamentas*, *Kambarys*, $m_{Kambarys}$ >

Dakt $\prec_s$ *Ped* reiškia, kad pediatras mažiausiai turi tokius pat leidimus kaip ir daktaras. Požymio tipas *Departamentas* yra *Ligoninėje*, o požymio tipas *Kambarys* yra *Sektoriuje*. Hierarchinis išrikiavimas $\prec_i$ apibrėžtas ir rolių egzemplioriams. Rolių egzemplioriai paveldi savo rolės schemai paskirtus leidimus ir leidimus, paskirtus paveldėtoms rolėms. Pagal tik ką apibrėžtas schemas *Dakt* $\prec_s$ *Ped* rolės egzempliorius *Pediatras*(Dep_1) paveldės ir Pediatro ir Daktaro rolių schemų leidimus. Be to *Pediatras*(Dep_1) paveldės ne tik *Dakt* schemos leidimus, bet ir atskirai egzemplioriui *Daktaras*($Ligon_1$) priskirtus leidimus. Tarkime, turime rolės schemą r_s ir rolės egzempliorius r_s (e_1) ir r_s (e_2) tokius, kad e_2 geometrija yra e_1 viduje. Kadangi atrodo prasminga, kad vartotojas, turintis rolę r_s (e_2), turėtų ir rolę r_s (e_1) su didesniu e_1, tokia hierarchija apibrėžta tarp egzempliorių. Rolės schemų hierarchinis išrikiavimas atitinka vietovės dydį: kuo tiksliau specifikuota rolė ir jos apimtis mažesnė, tuo vieta tampa tikslesnė. Kitaip galima pasakyti, kad „galingesnės“ rolės veikia mažesniuose regionuose. Hierarchinis egzempliorių išrikiavimas apibrėžiamas pagal buvimo dalimi ryšius tarp jų apimčių. Pagal prieš tai apibrėžtą modelį rolė *r* yra aktyvuojama sesijoje *s*, kai *r* priklauso sesijai *s* išrinktų rolių rinkiniui. Rolė yra įjungiama vietoje *rp*, kai *rp* yra rolės *r* erdvinėje apimtyje. Kad prieigos valdymo funkcija veiktų su Geo-HRBAC modeliu, priimama, kad kai *r* aktyvuojama, visi rolės *r* protėviai hierarchijoje yra taip pat aktyvuojami toje sesijoje.

3.2.6 LBAC politikų administravimas

R. Bhatti ir kiti [14] aptaria valdymo mechanizmą egzistuojančiam LBAC modeliui, Geo-RBAC, kuris yra RBAC modelio plėtinys. Straipsnio autoriai nagrinėja prieigos valdymo konceptualų (galimybes natūraliai išreikšti vietos informacija pagrįstus apribojimus) ir loginį (vietos informacija paremtų apribojimų interpretavimą ir pritaikymą sistemoms) lygius. Konceptualusis lygis yra pagrįstas Geo-RBAC vietos informacija paremtų apribojimų žodynu, o loginis lygis pagrįstas X-GTRBAC politikos specifikavimo kalba. Autoriai formaliai apibrėžia Geo-RBAC ir X-GTRBAC administravimo komandų jungimą. Konceptualiojo lygio politika ir Geo-RBAC išreikštos administravimo komandos yra išverčiamos į X-GTRBAC politiką ir administravimo komandas. Politikos sujungiamos naudojant Sąsajos apibrėžimo kalbą (angl. *Interface Definition Language*).

3.2.7 Kiti darbai, nagrinėjantys vietos informacijos įvedimą į saugos politiką

Nemažai yra darbų, kurie pristato vietos informacijos privatumo klausimo sprendimus, vieni iš jų yra [7, 8, 10, 12]. [15, 16] pristato LBAC politikų užrašymo kalbas.

3.3 Vietos informacijos įvedimo poveikis autentifikacijos, autorizacijos ir prieigos valdymo procesams

Prieigos valdymo mechanizmai yra paremti prielaida, kad vartotoją apibūdinančių savybių, dažniausiai nusakomų prisijungimo duomenimis, užtenka priimti sprendimui, kuriuos veiksmus vartotojas yra autorizuotas atlikti su ištekliais, tačiau standartiniai vartotojo prisijungimo duomenys nėra vienintelė informacija, kurią reiktų įvertinti, priiminėjant prieigos valdymo sprendimus. Kaip teigiama ir 2.2 skyrelyje nagrinėtuose literatūros šaltiniuose, vietos informacija taip pat atlieka svarbų vaidmenį suteikiant prieigos teises. Ji suteikia galimybę leisti prieigą pagal vietos informacija pagrįstus požymius (pavyzdžiui, tai, kurioje vietoje yra vartotojas ar objektas). Vietos informacija pagrįsta autentifikacija gali būti naudojama vietoje standartinių nelabai patogių vartotojui metodų. Tokia autentifikacija gali būti įvykdoma automatiškai vartotojui atėjus į tam tikrą tam skirtą vietą, tokiu atveju vartotojui nereikėtų įvesti slaptažodžio ar kitų prisijungimo duomenų. Taip pat vietos informacija gali papildyti standartinius nevisai saugius autentifikacijos metodus, kad teisingo autentifikavimo tikimybė būtų didesnė. Pavyzdžiui, jei dėl fizinės apsaugos į tam tikras vietas, pavyzdžiui pastato kabinetus, gali patekti tik legalūs sistemos vartotojai, vietos informacijos įvertinimas autentifikacijos metu gali padidinti prieigos prie sistemos saugą.

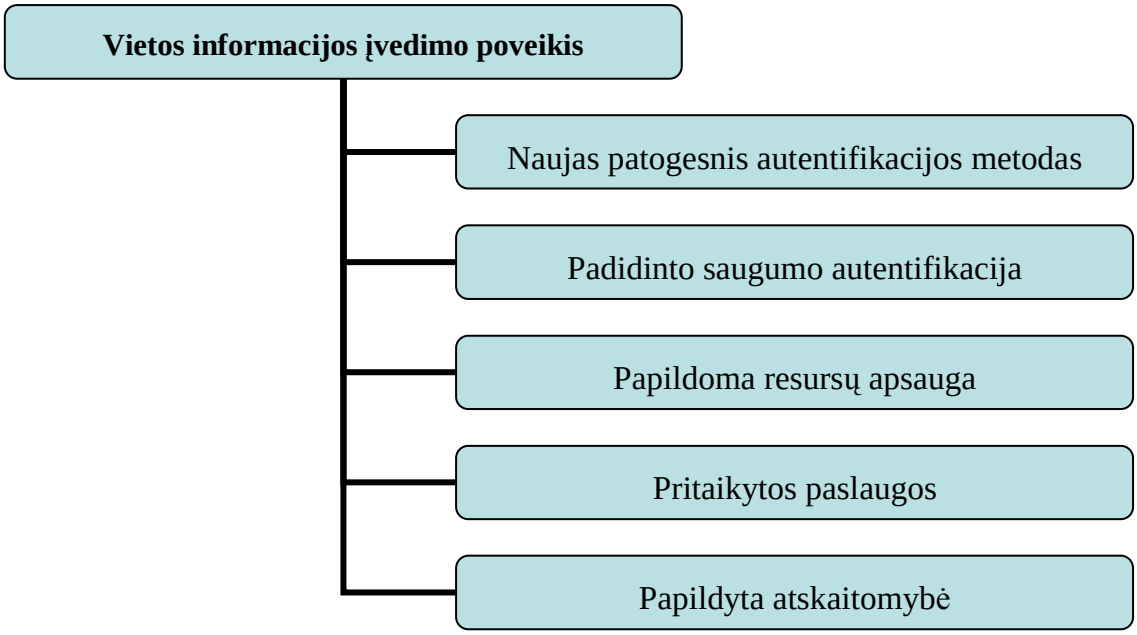
Naudojant vietos informaciją prieigos valdymui, gali būti formuojama vietos informacija pagrįsta saugos politika. Galima išskirti tokias vietos informacija pagrįstos saugos politikos kryptys:

- Resursai gali būti prieinami tik „saugioje“ vietos informacija paremtoje būsenoje;
- Resursai gali būti prieinami tik tose būsenose, kuriose jie reikalingi / aktualūs.

Pirmosios krypties saugos politika neleistų vartotojui prieiti prie resurso tokioje vietos informacija paremtoje būsenoje, kuri laikoma nesaugi naudotis tuo resursu (pavyzdžiui, ten, kur kiti neautorizuoti vartotojai gali nužiūrėti slaptus duomenis) arba nesaugi tuo, kad joje gali bandyti prieiti prie resurso nelegalūs vartotojai (saugios vietos galėtų būti, pavyzdžiui, kameromis stebimi kabinetai, nuo kurių raktus turi tik legalūs vartotojai, o visos kitos vietos – nesaugios). Antrosios krypties saugos politika apribotų naudojimąsi resursu taip, kad jis būtų prieinamas tik vartotojui esant toje vietos informacija pagrįstoje būsenoje, kurioje legaliems vartotojams juo reikia naudotis (pavyzdžiui, daktarui paciento medicininė kortelė reikalinga tik darbo vietoje). Tokie apribojimai gali būti įvedami saugos tikslais – kuo mažesnėje teritorijoje prie resurso galima prieiti, tuo nelegaliam vartotojui bus sunkiau tai padaryti, net jei ir jis įveiks standartinį autentifikacijos mechanizmą, kuris derinamas su vietos informacija. Taigi autentifikacijos ir prieigos valdymo papildymas vietos informacija gali padidinti teisingos autentifikacijos tikimybę ir geriau apsaugoti resursus nuo pašalinių tuo metu, kai jais naudojasi autorizuoti vartotojai.

Vietos informacija leidžia ne tik lanksčiau valdyti prieigą prie resursų, ji gali būti panaudota teikti vartotojams pagal vietos informaciją pritaikytas paslaugas, tokias kaip vartotojo vietos atvaizdavimas žemėlapyje, kelio suradimas, vartotojo priminimų valdymas pagal vietą, vartotojo vietų registravimas ir peržiūra ir t.t. [7, 18]. Paslaugos gali būti įvertinančios ne tik vartotojo vietos informaciją (VI), bet ir kitų objektų ar subjektų VI, ir, pavyzdžiui, padėti vartotojui rasti kitą vartotoją [12].

Be minėtų panaudojimo atvejų nustačius vartotojo vietos informaciją, ji gali būti panaudota registruojant vartotojo atliktus veiksmus (žurnaluose užregistruojami ne tik veiksmai, bet ir kuriose vietose, jie buvo atlikti) arba vartotojui pasirašant dokumentus (vietos informacija pridedama prie vartotojo parašo). Išskirti vietos informacijos įvedimo į autentifikacijos, prieigos valdymo ir atskaitomybės procesus privalumai parodyti 12 paveikslėlyje.



12 pav. Vietos informacijos įvedimo privalumai

3.4 Skyriaus apibendrinimas

Šiame skyriuje pristatyti vietos informacijos nustatymo būdai. WiFi tinkluose vietos informacija gali būti nustatoma dviem būdais: matuojant laiką, per kurį duomenų paketas bevieliu tinklu nukeliauja nuo vieno įrenginio iki kito, arba įvertinant įrenginio signalų stiprumus. Šiais būdais gali būti pasiekiamas 1-3 m tikslumas, jais negali būti įvertintos visos vietos informacija pagrįstos būsenos, tačiau jie gali būti naudojami nustatyti, kurioje zonoje yra vartotojas.

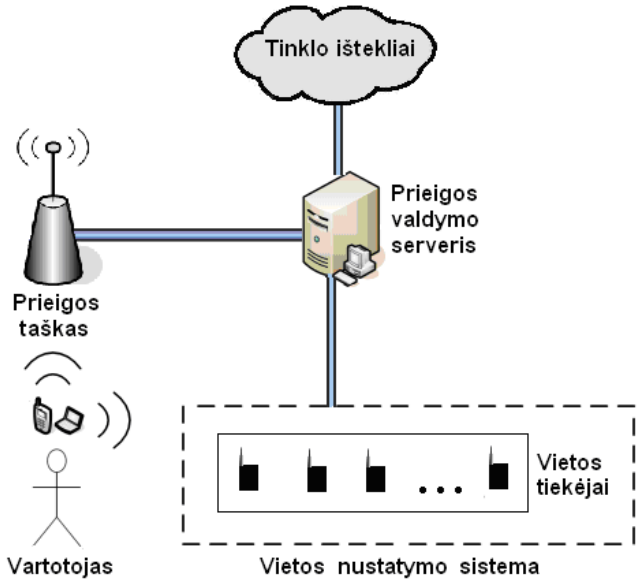
2.2 skyrelyje pristatyti keli darbai, nagrinėjantys vietos informacijos panaudojimą autentifikacijai ir prieigos valdymui. Darbuose parodoma, kaip vietos informacija gali būti panaudota pakeisti arba papildyti standartinius autentifikacijos metodus, kokia yra vietos informacija pagrįsto prieigos valdymo architektūra ir kokios gali būti naudojamos vietos informacija pagrįstos būsenos. 2.2.5 ir 2.2.4 skyreliuose išnagrinėti darbai, pateikiantys sprendimus, kaip vietos informacija gali būti įvesta į standartinius MAC ir RBAC modelius. Sprendimai nėra pritaikyti būtent bevielio tinklo prieigos valdymui, jie yra bendri ir dėl to pakankamai sudėtingi. Juose nenurodyti vietos informacijos nustatymo ir panaudojimo algoritmas, vartotojo realios ir loginės vietos susiejimo funkcijos, vartotojo loginės vietos ir rolės apimties susiejimo Geo-RBAC modelyje arba subjektų / objektų vietų ir leistinų subjekto / objekto vietų susiejimo MAC modelyje funkcijos. Į sprendimus įtraukta tik viena vietos informacija pagrįsta būsena. Iš 2.2 skyrelyje nagrinėtų literatūros šaltinių matosi, kad plačiausiai ir daugiausiai naudojama nurodanti, ar vartotojas yra tam tikroje zonoje, vietos informacija pagrįsta būsena, tačiau gali būti panaudotos ir kitos, tokios kaip greitis, nuotolis,

vietinis tankis ir tankis. Kitų būsenų nustatymas yra sudėtingesnis ir kitos būsenos daugeliu atvejų nėra reikalingos. Egzistuojančių sprendimų analizės metu nustatyta, kad nėra bendro modelio / būdo siūlančio, kaip projektuojant pasirinkti sistemos, prieigos prie bevielio tinklo išteklių valdymui naudojančios vietos informaciją, architektūrą, vietos informacija pagrįstus požymius, jų tipus bei įvertinimo būdą ir leidimų priskyrimo periodiškumo strategiją.

2.3 skyrelis nurodo, kokia yra vietos informacijos panaudojimo autentifikacijos, prieigos valdymo ir atskaitomybės procesuose nauda. Vietos informacija paremta autentifikacija gali būti panaudota vietoje standartinių autentifikavimo būdų kaip patogesnis būdas, taip pat gali būti derinama su standartiniais autentifikacijos metodais bei fiziniais saugos metodais, kad padidintų saugumą ir teisingos autentifikacijos tikimybę. Vietos informacija leidžia teikti vartotojams pritaikytas paslaugas, taip pat gali būti panaudota vartotojo parašui dokumentuose papildyti ar registracijos žurnaluose.

4 PRIEIGOS PRIE BEVIELIO TINKLO RESURSŲ VALDYMO, GRĮSTO VIETOS INFORMACIJA, PROJETAVIMAS

4.1 Prieigos prie bevielio tinklo resursų valdymo grįsto vietos informacija modelis

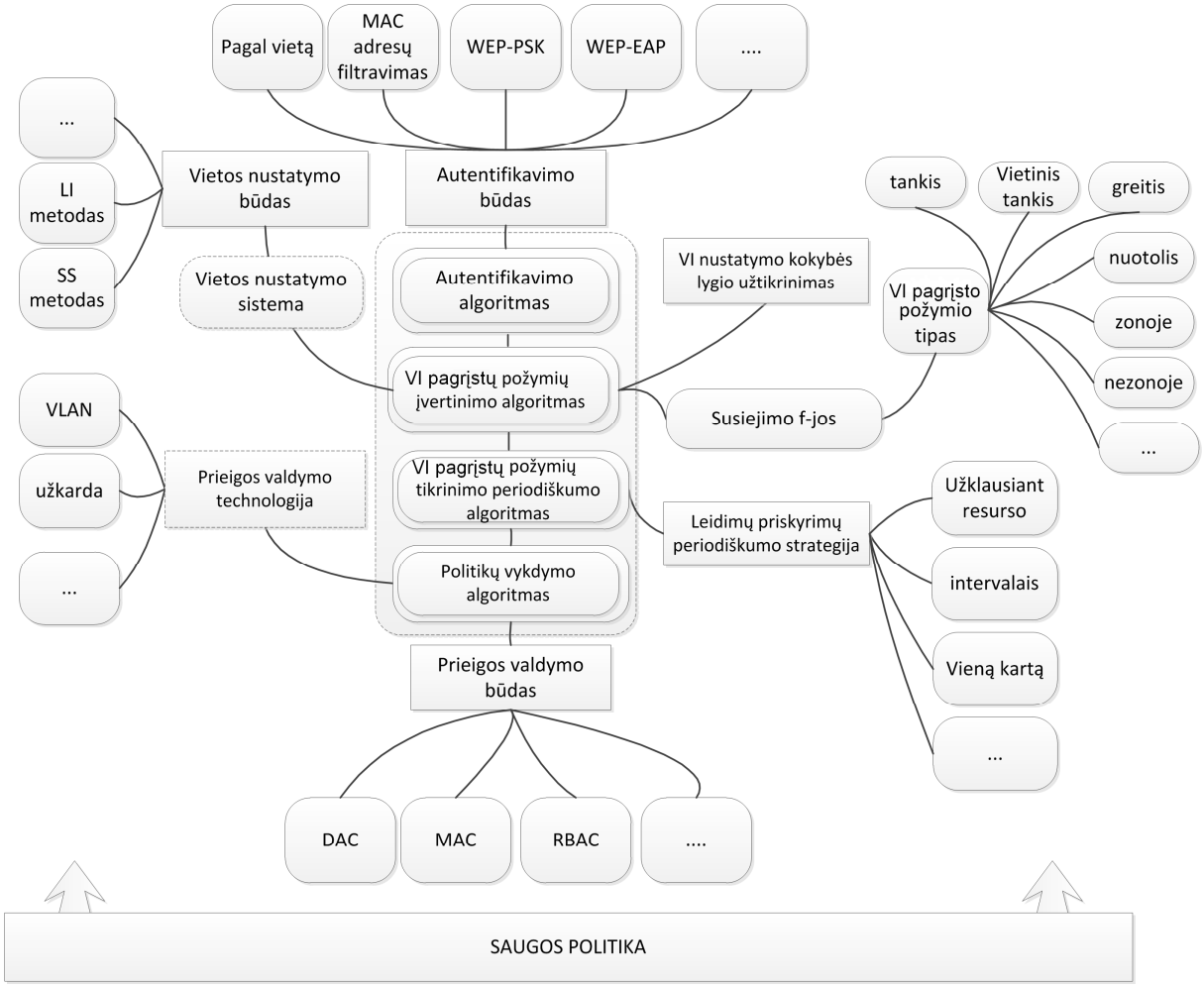


13 pav. Vietos informacija pagrįsto prieigos valdymo infrastruktūra

Remiantis atlikta autentifikacijos ir prieigos valdymo mechanizmų bei jų derinimo su vietos informacija galimybių analize galima sudaryti bendrą vietos informacija paremto prieigos prie bevielio tinklo resursų valdymo sistemos infrastruktūros schemą, kuri pateikta 13 paveikslėlyje. Kaip matyti iš paveikslėlio, į prieigos valdymą įvedant vietos informaciją infrastruktūra turi būti papildyta vietos nustatymo sistema. Vartotojas, norėdamas prieiti prie tinklo išteklių, turi gauti leidimą iš prieigos valdymo serverio (PVS). Prieigos taškas veikia tik kaip tarpininkas tarp vartotojo ir PVS. PVS turi įvertinti, ar vartotojui leisti prieigą. Kad tą padarytų, PVS turi žinoti vartotojo vietos informaciją, todėl kreipiasi į vietos informacijos nustatymo sistemą (VNS), kuri analizuoja iš jutiklių (angl. *sniffers*) gautus duomenis, nustato vartotojo vietą ir grąžina atsakymą. Atskirais atvejais prieigos valdymo serveris gali veikti prieigos taške, nebūtinai atskirai nuo jo, taip pat PVS gali reikti komunikuoti su keliais prieigos taškais, kaip siūlo [9] ir [10] (2.3.1 ir 2.3.2 skyreliai), o ne su vienu, tačiau ir tokiais atvejais prieigos valdymo sistemos architektūra gali būti pavaizduota apibendrinta 13 paveikslėlyje pateikta schema. Priklausomai nuo prieigos valdymo technologijos tam tikrais atvejais dalis prieigos valdymo (užklausų filtravimas, leidimas / blokavimas) gali būti

atliekama prieigos taške arba kokiame nors kitame objekte (pavyzdžiui, objekte, kuriame yra resursai) ir tinklo ištekliai tuomet gali būti pavaizduoti ne už prieigos valdymo serverio.

Remiantis atlikta autentifikacijos ir prieigos valdymo mechanizmų bei jų derinimo su vietos informacija galimybių analize siūlomas 14 pav. pateiktas prieigos prie tinklo resursų valdymo panaudojant vietos informaciją modelis.



14 pav. Prieigos prie tinklo resursų valdymo panaudojant vietos informaciją modelis

Iš 14 paveikslėlio matosi, kad vietos informacija gali būti nustatoma skirtingais būdais. Jos nustatymą atlieka vietos nustatymo sistema (VNS), kuri gali būti laikoma visos prieigos valdymo sistemos dalimi. Vietos informacija gali būti derinama su skirtingais prieigos valdymo ir autentifikacijos būdais. Vietos informacijai prieigos valdyme apibūdinti pasirinkta naudoti vietos informacija pagrįsto požymio sąvoką, kuri suderinama su Geo-RBAC modelyje [18] naudojama ir iš OGC (angl. *Open GeoSpatial Consortium*) [31] paveldėta požymio sąvoka. Požymiai turi nuo taikymo priklausomą semantiką, kurią išreiškia požymio tipo koncepcija. Susiejimo funkcijos susieja VNS pateikiamą vietos informaciją su prieigos

valdymui naudojamais VI požymiais. Kiekvienam VI požymio tipui gali būti naudojama skirtinga susiejimo funkcija. Naudojant vietos informaciją prieigos valdymui reikia užtikrinti pakankamą vietos informacijos nustatymo kokybės lygį. Projektuojant prieigos valdymo sistemą, svarbu parinkti ir leidimų priskyrimo periodiškumo strategiją. Projektuojant prieigos valdymo sistemą turi būti pasirinkta tinkama prieigos valdymo technologija.

Aptartas prieigos prie tinklo resursų modelis tinka prieigos prie bet kokio tipo tinklo resursų valdymui, tačiau 14 paveiksle pavaizduoti autentifikacijos būdai ir vietos nustatymo būdai yra skirti būtent bevielio tinklo vartotojams. Modelio dalys, kurios buvo įtrauktos į tipinio prieigos valdymo modelį papildant jį vietos informacija, yra vietos nustatymo sistema, naudojanti kokį nors vietos nustatymo būdą, vietos nustatymo kokybės lygio užtikrinimas, susiejimo funkcijos, VI pagrįsti požymiai ir jų tipai bei leidimų priskyrimo periodiškumo strategija. Prieigos prie tinklo resursų valdymo panaudojant vietos informaciją modelis apima sekančiuose skyreliuose aptartus aspektus.

4.1.1 Autentifikacijos būdo parinkimas.

Projektuojant prieigos prie bevielio tinklo resursų valdymo sistemą būtina parinkti labiausiai tinkamą autentifikavimo būdą. Kaip parodyta 14 paveikslėlyje su vietos informacija gali būti derinami šie standartiniai bevielio tinklo autentifikacijos būdai: a) atvira autentifikacija; b) WPA; c) MAC adresų filtravimas d) WEP-PSK; e) WEP-EAP. 1.1 skyrelyje pateikti detalesni skirtingų būdų aprašymai. Naudojant standartinius WiFi autentifikacijos metodus, tokius kaip WEP arba WPA-PSK, autentifikacijos serveris yra nereikalingas. Norint šiuos metodus derinti su vietos informacija, reiktų, kad visas prieigos valdymo serverio funkcijas atliktų prieigos taškas. Tai įgyvendinti būtų sudėtinga dėl prieigos taško ribotų galimybių, todėl paprasčiau naudoti atskirą prieigos valdymo serverį, kuris naudojamas WPA-EAP atveju. Reikia atkreipti dėmesį, kad vieni autentifikacijos būdai yra lengviau pažeidžiami, kiti gana saugūs, pavyzdžiui, WEP-EAP. Autentifikacija tik pagal vietos informaciją (atviros autentifikacijos ir vietos informacijos derinimas) gali būti patogesnė vartotojui, tačiau reikia atsižvelgti į tai, kad tokiu atveju prieigos apsauga tiesiogiai susijusi su fizine tam tikrų vietų sauga ir toks būdas gali nepakankamai apsaugoti resursus. Vienu metu galima naudoti kelis autentifikacijos būdus, pavyzdžiui, WEP ir MAC adresų filtravimą. Pasirinkus standartinį prieigos prie bevielio tinklo autentifikacijos būdą, jį galima dar papildyti VI požymių įvertinimu arba kokia nors kita autentifikacijos technologija, kaip kad USB raktai ar PIN kodų generatoriai. Standartinį būdą papildant vietos informacija gali būti pasiekta didesnė teisingo autentifikavimo tikimybė, taigi ir aukštesnis saugos lygis. Nuo pasirinkto autentifikacijos būdo priklauso autentifikacijos algoritmas.

Projektuojama sistema vykdo vartotojų autentifikaciją pagal vietą ir gali būti papildyta standartiniais autentifikacijos bevieliame tinkle būdais.

4.1.2 Vietos informacija pagrįstų požymių ir jų tipų parinkimas.

Ardagna ir kiti [7, 8, 13] nurodo kelias vietos informacija pagrįstas (iš vietos informacijos išverstas) būsenas (žr. 9 lentelę), kurias gali įvertinti prieigos valdymo sistema. Nurodytų būsenų prasmė bent iš dalies atitinka požymių tipų koncepciją, todėl vietos informacija pagrįstas būsenas vadinsime vietos informacija (VI) pagrįstų požymių tipais. 9 lentelėje pateiktas tokių požymių tipų sąrašas su paaiškinimais.

9 lentelė. Vietos informacija pagrįstų požymių tipai

VI požymių tipas	**Paaiškinimas**
zonoje(vartotojas, zona)	Įvertina, ar vartotojas zonos ribose.
nezonoje(vartotojas, zona)	Įvertina, ar vartotojas už zonos ribų.
nuotolis(vartotojas, objektas, min_atstumas, max_atstumas)	Įvertina, ar atstumas nuo vartotojo iki objekto yra intervale [min_atstumas, max_atstumas].
greitis(vartotojas, min_greitis, max_greitis)	Įvertina, ar vartotojo greitis yra intervale [min_greitis, max_greitis]
tankis(zona, min_kiekis, max_kiekis)	Įvertina, ar vartotojų kiekis tam tikroje zonoje yra ne didesnis už max_kiekis ir ne mažesnis už min_kiekis.
vietinis_tankis(vartotojas, zona, min_kiekis, max_kiekis)	Įvertina, ar vartotojų tankis zonoje aplink vartotoją yra intervale [min_kiekis, max_kiekis]

Kaip bebūtų, skirtingų VI požymių tipų gali būti žymiai daugiau priimant, kad skirtingos paskirties zonos atitinka skirtingus VI požymių tipus. Tokia požymių tipų semantika pasiskolinta iš Geo-RBAC modelio. Taigi erdvinių požymių tipų sąrašas gali būti papildytas tokiais tipais kaip *miestas*, *kaimas*, *pastatas*, *kabinetas*, *ežeras* ir panašiai. Geo-RBAC modelyje požymiai gali būti erdviniai arba neerdviniai priklausomai nuo to, ar esybėms gali būti priskirta kažkokia vieta erdvėje. Pavyzdžiui, požymis *Drūkšių ežeras* yra erdvinis, tuo tarpu mašina, identifikuojama numeriu *FBC234*, yra neerdvinis požymis, nes mašinos vieta keičiasi. Galime daryti išvadą, kad visi požymio tipai nurodantys tam tikrą zoną, yra erdvinių požymių tipai. Erdviniams požymiams ir jų tipams gali būti apibrėžta hierarchija pagal esybių apimtį. Jei viena esybė yra kitos dalis, tai pirmoji yra hierarchijoje aukščiau. Tokios hierarchijos sudarymas gali būti panaudojamas sudarant vietos informacija pagrįsto prieigos valdymo modelį. Pagal minėtą apibrėžimą tokių tipų kaip *nuotolis*, *greitis*, *tankis*, *vietinis tankis* požymiai gali būti laikomi neerdviniais. Kaip bebūtų, šių tipų požymiai yra išvesti iš vietos informacijos, nes jų nustatymui turi būti įvertinama vietos informacija. Neerdviniams požymiams negalima apibrėžti hierarchijos. Dar reikia pastebėti, kad *tankis* tipo požymiai nėra susiję su vartotoju, neapibūdina vartotojo, tačiau jie gali būti susieti su tam

tikrais leidimais ir gali būti naudojami kaip sąlyga leidimo suteikimui. Reikia pastebėti, kad toks požymis beveik nepriklauso nuo vartotojo.

Projektuojant sistemą reikia parinkti, kurie požymiai bus naudojami prieigai valdyti. Kaip jau minėta, be nurodytų požymių tipų į sistemą galima įtraukti ir daugiau požymių tipų, tokių kaip *miestas*, *departamentas* ir t.t., kurie sąraše apibūdinti vienu pavadinimu *zonoje*, tačiau skiriasi vienas nuo kito pritaikymu. Prie kiekvieno požymio tipo skliausteliuose nurodyti parametrai, naudojami požymio nustatymui. Pavyzdžiui, išraiška *kabinete(Aldona, laboratorija1)* nusako požymį, kuris nurodo, kad vartotojas Aldona yra *laboratija1* kabinete, *įstaiga(Algis, KTU)* nurodo, kad vartotojas Algis yra įstaigoje, kuri vienareikšmiškai identifikuojama pavadinimu *KTU*, *greitis(Aldona, 0, 3)* nurodo, kad Aldona juda ne didesniu kaip 3 km/val. greičiu. Minėtų tipų požymiai gali būti taikomi ne tik vartotojams (subjektams), bet ir objektams (resursams), kai objektų vietos informacija taip pat gali būti nustatyta. Tokiu būdu per rolės, saugos lygio ar kitą koncepciją leidimai gali būti suteikiami vartotojui tik tuomet, kai patvirtinami visi su tuo leidimu susieti požymiai (požymiai gali būti suprantami kaip sąlygos, kurioms esant galima gauti leidimą). Reikia pastebėti, kad tokie požymiai kaip vartotojo *bilietas*, *greitis* ar *kabinetas*, kuriame jis yra, priklauso nuo vartotojo, o tokie požymiai kaip vartotojų *tankis* tam tikroje auditorijoje arba *kabinetas*, kuriame yra resursas, nuo vartotojo nepriklauso. Pagal prieigos valdymo politikas prieš suteikiant vartotojui leidimą reikia patikrinti ir patvirtinti visus požymius, kurie numatyti kaip sąlygos to leidimo suteikimui.

Projektuojamoje sistemoje apsiribojama naudoti požymių tipus išreiškiančius, kurioje zonoje yra vartotojas. Šis sprendimas priimtas atsižvelgiant į tai, kad sistema turi būti pritaikyta bevieliam tinklui ir kitų tipų, tokių kaip, greitis, kryptis, tankis požymių įvertinimui reikalingos papildomos sudėtingesnės technologijos ir įranga nei vien tik bevielio tinklo eteris. Taip pat atsižvelgta į tai, kad greičio ar nuotolio įvertinimas tokioje sistemoje nėra aktualus. Žinoma, nustatyti, pavyzdžiui, ar dekano kabinete nėra kitų darbuotojų, nuo kurių turi būti slepiamas tam tikras resursas, galbūt ir būtų naudinga. Priede Nr. 1 nagrinėjama, kaip sistema galėtų būti papildyta kitų tipų požymiais. Projektuojamoje sistemoje įvertintinami tik subjektų (t.y. tų, kurie naudojasi resursais) VI požymiai, nes universiteto bevielio tinklo resursai nėra susieti su objektais, kurių vietos informacija galėtų būti nustatyta.

4.1.3 Susiejimo funkcijų parinkimas.

Vietos informacija pagrįsto prieigos valdymo sistemose naudojamos susiejimo funkcijos. Jos nurodo, kaip VNS atsiųstus duomenis PVS susieja su naudojamais VI pagrįstais požymiais. Skirtingiems požymių tipams gali būti taikomos skirtingos susiejimo funkcijos.

Jei, pavyzdžiui, VNS teikiama vietos informacija yra tik santykinės vartotojo koordinatės, tai tam, kad galėtų būti įvertintas greičio tipo erdvinis požymis, PVS gautiems duomenims turės pritaikyti tam skirtą susiejimo funkciją. Tokia funkcija, pavyzdžiui, galėtų užklausti vartotojo koordinačių kelis kartus ir pagal gautus duomenis bei laiko išmatavimus apskaičiuoti vartotojo greitį, t.y. nustatyti VI požymį. Aišku, kad tai užtrukti (PVS turi užklausti vietos informacijos dar kartą), todėl geriau, kad šias susiejimo funkcijas taikytų pati VNS ir prieigos valdymo serveriui atsakinėtų į tokias užklausas kaip, ar vartotojo greitis yra tarp vienos ir kitos reikšmės, ar vartotojas yra tam tikroje zonoje, ir panašiai. Reikia pastebėti, kad erdvinio požymio nustatymui PVS užtektų kreiptis į VNS ir gauti vartotojo koordinates vieną kartą, todėl nebūtų didelio skirtumo, ar susiejimo funkciją taiko pats VNS ar PVS. Nuotolio tipo požymiams įvertinti reiktų užklausti ne tik vartotojo koordinačių, bet ir kito objekto, iki kurio matuojamas atstumas, koordinačių. Tankio ir vietinio tankio tipo požymius nustatyti tik iš vartotojų koordinačių būtų žymiai sunkiau, nes reiktų tikrinti visų įmanomų vartotojų koordinates. Šiuos požymius turėtų nustatyti pati VNS. Kai susiejimo funkcijos veikia PVS, jos yra VI pagrįstų požymių įvertinimo algoritmo dalis.

Skirtingiems erdvinių požymių tipams gali būti taikomos skirtingos susiejimo funkcijos, tačiau projektuojamoje sistemoje užtenka apibrėžti vieną susiejimo funkciją visiems požymių tipams, kurie nurodo, kurioje zonoje yra vartotojas (erdviniams požymiams). Taip yra dėl to, kad visos universiteto zonos susideda iš stačiakampio formos zonų.

4.1.4 Vietos informacijos nustatymo kokybės lygio užtikrinimas.

Kadangi paprastai VNS yra atskirta nuo prieigos valdymo sistemos, o ne jos dalis, prieigos valdymo sistema kažkokiu būdu turi užtikrinti, kad vietos informacija nustatoma pakankamai tiksliai ir tinkamu būdu, t.y. turi užtikrinti pakankamą šios paslaugos kokybės lygį. Šis aspektas priklauso nuo pasirinktos VNS. Prieš gaunant vietos informaciją tarp PVS ir VNS gali būti atliekamas susitarimas dėl vietos nustatymo paslaugos kokybės lygio. Toks žingsnis reikalingas, jei VNS teikia įvairaus lygio paslaugas ir iš anksto nėra suderintas reikalingas paslaugos kokybės lygis. Be minėto susitarimo kiekvieną kartą nustatant vietos informaciją VNS gali nustatyti ir jos patikimumo lygį arba paklaidą. Paklaida nurodo, kokiu didžiausiu atstumu tikroji vieta gali skirtis nuo nustatytosios, o patikimumas – tikimybę, kad galinis įrenginys yra būtent toje vietoje. Patikimumas gali būti vertinamas procentais ir pagal jo reikšmę PVS nusprendžia, ar vietos informaciją gali naudoti, ar jos užklausti dar kartą ar vietos informacija negali būti naudojama prieigos valdymui. Patikimumas priklauso nuo tokių aspektų kaip tikslumas, aplinkos ir oro sąlygos, užklaustos vietos smulkumas, matavimui naudojamos technologijos. Patikimumo reikšmės įvertinimui gali būti panaudota [13]

pasiūlyta metodika, aprašyta 2.2.3.3 skyrelyje. Kaip parodyta 14 paveikslėlyje, nuo pasirinkto vietos informacijos nustatymo kokybės lygio užtikrinimo priklauso Erdvinių požymių įvertinimo algoritmas.

Projektuojamoje sistemoje vietos informacijos nustatymo kokybės lygis valdomas įvertinant kiekvienos gautos vietos informacijos patikimumo reikšmę, išreikštą procentais. Įvertinimas atliekamas pagal [13] pasiūlytą metodiką. Toks variantas buvo pasirinktas dėl planuojamos naudoti VNS savybių.

4.1.5 Leidimų priskyrimo periodiškumo strategija.

Paprastai prieigos valdymo sistemose vartotojas yra vieną kartą autentifikuojamas ir jam suteikiama prieiga prie visų resursų, kuriuos jis yra autorizuotas prieiti. Kadangi laikoma, kad vartotojai yra mobilūs ir jų vietos informacija gali kisti laike, vietos informaciją įvertinančioje prieigos valdymo sistemoje po vartotojo autentifikacijos ji gali pasikeisti ir turėtų būti nustatyta dar kartą. Pasikeitus vartotojo vietos informacijai turėtų keistis ir prieigos leidimai, kuriuos vartotojas yra autorizuotas turėti. Dėl šios priežasties vietos informacija gali būti įvertinama dažniau nei, pavyzdžiui, slaptažodis, ne tik prisijungimo prie sistemos ar autentifikacijos metu, bet ir po to. VI pagrįstų požymių tikrinimo ir leidimų priskyrimo periodiškumo strategija apibrėžia, kada ir kaip bus įvykdomos politikos keičiantis vietos informacijai. Kaip parodyta 14 paveikslėlyje nuo pasirinktos strategijos priklauso VI pagrįstų požymių tikrinimo periodiškumo algoritmas. Galima išskirti 3 skirtingas strategijos:

a) Vieną kartą. VI pagrįsti požymiai ir kiti požymiai gali būti patikrinami ir leidimai vartotojui nustatomi tik vieną kartą – autentifikacijos metu. Toks požiūris yra paveldėtas iš standartinio prieigos valdymo modelio, kuriame vietos informacija iš vis nenaudojama. Vietos informacijos tikrinimas atliekamas vartotojo prisijungimo prie tinklo metu, t.y. tada, kai vartotojas siunčia prisijungimo užklausą, todėl galima sakyti, kad vartotojas pats gali pakartotinai inicijuoti vietos informacijos nustatymą. Prie šio atvejo priskiriama ir strategija, pagal kurią numatyta galimybė vartotojui pačiam inicijuoti pakartotinį vietos informacijos nustatymą ir leidimų priskyrimą, (tai vartotojas gali atlikti, pavyzdžiui, tada, kai neleidžiama jo prieiga prie tam tikro resurso). Kai kuriose prieigos valdymo sistemose gali nebūti vieno prisijungimo (autentifikacijos) prie sistemos, vartotojo kredencialai gali būti tikrinami kiekvienąkart, kai vartotojas siunčia užklausą, kad gautų prieigą prie tam tikro resurso. Tokiu atveju galime sakyti, kad vartotojas prisijungia ne prie sistemos, bet kiekvienąkart atskirai prisijungia prie kiekvieno resurso. Vartotojų prieigos (prisijungimo prie sistemos arba resurso) pobūdis priklauso nuo prieigos valdymo technologijos. Taikoma technologija ir prieigos pobūdis priklauso nuo to, kokie yra tinklo resursai.

b) Intervalais. Pagal šią strategiją vietos informacija ir / arba erdviniai požymiai tikrinami tam tikrais pastoviais laiko intervalais arba tuomet, kai praeina galiojimo reikšme nurodytas laiko tarpas. Galiojimo reikšmė gali būti atsiunčiama iš vietos nustatymo sistemos kartu su vietos informacija arba ją gali parinkti pats prieigos valdymo serveris. Kaip bebūtų, galiojimo reikšmė nusako, po kokio laiko tarpo reikės vėl patikrinti subjekto ar objekto vietos informaciją. Norint pasiekti aukštesnį prieigos valdymo saugumo ir kokybės lygį, VI požymius įvertinti ir leidimų sąrašus atnaujinti reikia dažniau, t.y. kuo mažesniais intervalais. Jei tikrinimo intervalai dideli, gali atsitikti taip, kad vartotojas atėjęs į vietą, iš kurio prieiga jam turi būti suteikta, negalės prieiti prie resurso dėl to, kad dar bus nenustatyta jo nauja vieta ir nesuteikta prieiga pagal kitą VI pagrįstą požymį. Gali atsitikti ir taip, kad gavęs prieigą prie resurso iš vienos vietos vartotojas pereis į kitą ir kurį laiką dar vis galės naudotis resursu vietoje, iš kurios prieiga prie resurso neturėtų būti teikiama. Žinoma, dažnas VI pagrįstų požymių tikrinimas ir leidimų priskyrimas gali apkrauti prieigos valdymo serverį arba vietos nustatymo sistemą.

c) Užklausiant resurso. Vietos informacija gali būti tikrinama kiekvienąkart, kai vartotojas užklausia tam tikro resurso. Tokiu atveju, reikia, kad VI pagrįsti požymiai būtų įvertinami labai greitai. Toks atvejis labiau tinka privalomojo prieigos valdymo modelio sistemoms, nes jose kiekvienas leidimas, arba operacija, kurią subjektas (vartotojas) gali atlikti su objektu (resursu), yra tiesiogiai susietas su leistinomis subjektų ir objektų vietomis, o ne su rolėmis ar rolių schemomis. Tokia strategija saugumo prasme yra geresnė už dvi pirmąsias, tačiau ją taikant reikalinga greita ir tiksli vietos nustatymo sistema, greita komunikacija tarp PVS ir VNS, o tai pasiekti bevieliuose tinkluose naudojamais vietos nustatymo būdais yra gan sudėtinga. Paprastesnis tokios strategijos variantas gali būti vietos informaciją tikrinti periodiškai (pastoviais laiko intervalais arba pagal galiojimo reikšmę), o kai vartotojas užklausia resurso, pagal prieš tai jau nustatytą vietos informaciją tik patikrinti, ar leidimas subjektui gali būti suteiktas. Galbūt tokį periodinį vietos informacijos nustatymą VNS galėtų atlikti automatiškai visiems prisijungusiems vartotojams be PVS užklausų. Apibūdinta strategija be reikalo neapkrauna prieigos valdymo serverio (nes leidimai tikrinami, tik tada, kai vartotojas užklausia resurso), tačiau ji negali apriboti vartotojui prieigos prie resurso po to, kai jis tą prieigą jau gavo. Gali atsitikti taip, kad vienoje vietoje gavęs prieigą prie resurso vartotojas, besinaudodamas resursu, nueis į kitą vietą, kur resursas turėtų būti neprieinamas. Tokiu atveju sistema veiks nevisai pagal prieigos politikas, nes neblokuos prieigos prie resurso tol, kol vartotojas nesikreips į resursą iš naujo. Leidimų priskyrimo strategija užklausiant resurso tinka sistemoms, kuriose prieigos valdymo technologija nėra

atskirta nuo prieigos valdymo serverio, PVS gali stebėti vartotojų užklausas ir greitai leisti arba drausti prieigą prie resursų.

Strategiją reikia pasirinkti pagal tai, kam yra skirta prieigos valdymo sistema, kokie saugomi resursai, kokį saugos lygį ji turi užtikrinti, kokios yra vietos nustatymo sistemos savybės. Reikia pastebėti, kad strategija priskirti leidimus užklausiant resurso yra gerai pritaikoma vietos informacija pagrįstoms prieigos valdymo sistemoms, bet kai kuriais atvejais ją geriau derinti su leidimų priskyrimo intervalais strategija. Vartotojui atsiuntus užklausą ir gavus priėjimą prie resurso pagal trečiąją strategija, jis gali naudotis resursu, kiek nori, nepaisant to, kad jo vietos informacija gali pasikeisti. Tai gali būti laikoma trūkumu, nes mobilus vartotojas gavęs prieigą „saugioje“ vietoje ir išėjęs į „nesaugią“ vietą sudaro terpę saugos pažeidimams. Jei pagal saugos politiką resursas turi būti prieinamas tik iš tam tikros vietos, kuri laikoma saugi, tai yra tikslinga vartotojui besinaudojant resursu papildomai tikrinti jo vietos informaciją tam tikrais laiko tarpais, kaip numatyta pagal antrąją strategiją.

Projektuojamoje sistemoje pasirinkta leidimų priskyrimo intervalais strategiją derinti su leidimų priskyrimo užklausiant resurso metu strategija, nes toks variantas geriausiai užtikrintų resursų apsaugą ir geriau apsaugotų nuo nelegalių vartotojų įsilaužimo į sistemą. Projektuojamoje sistemoje VNS yra atskirta nuo PVS ir vietos informacijos užklausimas bei gavimas iš VNS gali užtrukti. Tokiu atveju vienos iš strategijų reiktų atsisakyti, kad sistema veiktų greičiau. Kadangi planuojama naudoti VNS nenustato vietos informacijos galiojimo reikšmės, pasirinkta leidimus priskirti kas 3 minutes.

4.1.6 Vietos informacija pagrįsto prieigos valdymo būdas.

Vietos informacija gali būti derinama su standartiniais prieigos valdymo būdais, tokiais kaip RBAC, MAC, DAC. Prieigos valdymo būdas pasirenkamas pagal tai, kokio reikia saugumo lygio, kokio pobūdžio organizacijai yra skirtas prieigos valdymas, pavyzdžiui, ar joje vartotojams gali būti priskirtos griežtai apibrėžtos rolės, ar teises patogiau suteikti kiekvienam vartotojui atskirai, ar sistemai reikalingos įvairios taisyklės (kaip kad kuriuo metu kurie objektai gali būti prieinami), ar sistemoje reikalinga galimybė vartotojams patiems valdyti prieigą prie resursų, ar geriau, kai prieiga valdoma centraliai. Sistemoms, kurioms saugumas yra svarbiausias, pvz., karinėms sistemoms, labiau tinka privalomasis prieigos valdymas. MAC modelis užtikrina didesnį saugumo lygį. Kita vertus savarankiškas prieigos mechanizmas yra lankstesnis, reikalauja mažiau resursų, valdymo ir palaikymo. Role pagrįstas prieigos valdymas labiausiai tinka tokioms sistemos, kur rolės tiksliai apibrėžtos ir nėra jokių papildomų taisyklių, tačiau šis modelis yra ribotas, kai prieigos sprendimui yra

svarbus kontekstas, pavyzdžiui, ar dabar naktis ar diena, ar karas ar taika. Role pagrįstą prieigos valdymą taip pat sunku pritaikyti kelias sritis apimančiai sistemai.

Priklausomai nuo pasirinkto būdo, į prieigos valdymo modelį gali būti įtrauktos atitinkamos esybės, tokios kaip rolė, rolės schema, saugos lygis. Šios esybės turėtų sietis su į modelį jau įtrauktomis požymio ir požymio tipo esybėmis. Nuo pasirinkto prieigos valdymo būdo priklauso politikų vykdymo algoritmas.

Projektuojamoje sistemoje pasirinktas role pagrįstas prieigos valdymas dėl to, kad jis gali lengvai būti pritaikomas tokioms organizacijoms kaip universitetas. Universiteto vartotojams, kurie yra studentai, dėstytojai ir kiti darbuotojai, nesunkiai gali būti apibrėžtos rolės. Role pagrįstas prieigos valdymo modelis papildomas vietos informacija pagal Geo-HRBAC modelį [18] įtraukiant į jį [7, 8, 13] pasiūlytas vietos informacija pagrįstas būsenas kaip erdvinių požymių tipus.

4.1.7 Prieigos valdymo technologija.

Nuo prieigos valdymo technologijos priklauso Politikų vykdymo algoritmas. Prieigos valdymo technologija reiškia tam tikrą mechanizmą riboti / leisti vartotojų prieigą prie resursų pagal prieigos politikas. Ji priklauso nuo to, kokie tinklo resursai, kur ir kokiu būdu prieinami. Prieigos valdymo technologija susijusi su leidimų priskyrimo periodiškumo strategija. Ji gali būti realizuota įvairiai. Priklausomai nuo to ji gali būti daugiau ar mažiau atskirta nuo prieigos valdymo serverio. Ji gali veikti prieigos valdymo serveryje, kitame serveryje arba prieigos taške. Jei tinklo ištekliai pasiekiami per prieigos valdymo serverį, jame kaip prieigos valdymo technologija gali veikti universali užkarda filtruojanti vartotojų srautus / užklausas pagal jiems suteiktus leidimus. PVS tokiu atveju turi identifikuoti vartotojus ir resursus užkardai tinkamu būdu. Užkarda filtruotų į tinklą ir atgal einantį srautą pagal PVS nurodymus. Vietoje užkardos gali būti panaudotas prieigos valdymas virtualių tinklų (angl. VLAN) pagalba: prieigos taškas galėtų žymėti vartotojų siunčiamus paketus tam tikro VLAN žyme pagal PVS nurodymus. Skirtingi VLAN galėtų atitikti, pavyzdžiui, skirtingas vartotojų roles ir leistų prieigą pagal tam tikrą leidimų rinkinį. Skirtingose prieigos valdymo technologijose gali būti naudojami skirtingi parametrai, pavyzdžiui, VLAN žymė, aktyvios rolės, vartotojams suteikti leidimai (vartotojų, resursų ir operacijų identifikatoriai).

Projektuojama sistema gali būti pritaikyta veikti su įvairiomis prieigos valdymo technologijomis.

4.1.8 Vietos nustatymo būdas ir sistema.

Projektuojant prieigos valdymo sistemą, reikia numatyti, kokia bus naudojama vietos informacijos nustatymo sistema ir kokiais būdais bus nustatinėjama vietos informacija. VNS

turi nustatyti vietos informaciją pagal PVS užklausą. Gali būti ir tokių VNS, kurios gali nustatinėti vietos informaciją ir be PVS užklausų iš anksto numatytu būdu pačios. Vietos informacijos nustatymo sistemos gali skirtis tikslumu ir veikimo būdu. 3.1 skyrelyje pateikta vietos informacijos nustatymo būdų apžvalga. WiFi tinkluose vartotojo vieta nustatoma matuojant vartotojų galinių įrenginių siunčiamų signalų stiprius (tai atlieka tam skirti jutikliai) (14 paveiksle šis būdas pažymėtas SS) [1, 2, 3, 4] arba matuojant paketo siuntimo vartotojui trukmę (14 paveiksle šis būdas pažymėtas LI) [4, 5, 6]. Projektuojant prieigos valdymo sistemą svarbu įvertinti, kokią vietos informaciją teikia VNS. Pavyzdžiui, ar VNS gali nustatinėti vartotojo x, y, z koordinates, ar gali atsakyti į užklausą apie tam tikrą erdvinį požymį. Taip pat svarbu įvertinti, ar VNS gali su vietos informacija nurodyti ir jos patikimumą (paprastai išreikštą procentais), arba galbūt paklaidą (gali būti išreiškiama absoliučiais dydžiais), ar prieš nustatant vietos informaciją tarp prieigos valdymo ir vietos nustatymo sistemų gali būti atliekamas susitarimas dėl vietos nustatymo paslaugos kokybės lygio (toks žingsnis reikalingas, jei VNS teikia įvairaus lygio paslaugas ir iš anksto nėra suderintas reikalingas paslaugos kokybės lygis). Vietos informacijos galiojimo reikšmė taip pat svarbus dalykas, kurio gali prireikti vietos informacija grįstam prieigos valdymui. Galiojimo reikšmė nurodo, kiek laiko galioja nustatyta vietos informacija, arba kiek laiko tokia informacija galima pasitikėti pagal nurodytą patikimumo reikšmę arba iš anksto sutartą paslaugos kokybės lygį.

Projektuojama sistema pritaikoma veikti su vietos informaciją nustatančia pagal vartotojų galinių įrenginių siunčiamų signalų stiprius VNS. Pasirinkta naudoti VNS, kuri nustato vietos informacijos patikimumą atsakydama į kiekvieną PVS užklausą. VNS nustatoma vietos informacija yra galinio įrenginio, su kurio MAC adresu buvo atsiųsta užklausa, santykinės koordinatės x, y, z, kur z atitinka pastato aukšto numerį.

4.2 Vietos informacija grįsto prieigos valdymo pažeidžiamumai

Vietos informacija grįsto prieigos valdymo mechanizmas gali būti pažeidžiamas neapsaugojus PVS komunikacijos su prieigos tašku, VNS ar objektu, kuriame realizuota prieigos valdymo technologija, jei ji yra atskirta nuo PVS. Kai autentifikacijai naudojama tik vietos informacija, o vartotojai identifikuojami MAC adresais, yra pavojus, kad legalūs ar arba nelegalūs vartotojai pasikeis įrenginio MAC adresą sistema juos klaidingai identifikuos. Jei vietos informacija derinama su naujais autentifikacijos metodais, tokiais kaip WPA-EAP, sistema yra apsaugota nuo vartotojų prisijungimo duomenų perėmimo ir klastojimo, tačiau tai neapsaugo nuo vartotojų MAC adresų perėmimo ir klastojimo. Valdymo mechanizmas gali būti pažeidžiamos DoS (angl. *Denial of Service*) atakomis, kai piktavalis pasirenka MAC

adresą tokį, kokį turi prisijungęs vartotojas, tada VNS klaidingai nustato prisijungusio vartotojo vietą ir dėl to blokuoja jam prieigą prie resursų. Dar daugiau žalos galėtų padaryti kirmino skylės (angl. *warmhole*) ataka, kai du piktavaliai pasirenka vienodus MAC adresus ir bando gauti prieigą iš tos vietos, kur ji yra neleidžiama. Atakos metu vienas atakuotojas yra vienoje išorinėje zonos, kur prieiga leidžiama, pusėje, o kitas kitoje – taip bandoma apsimesti vienu vartotoju, kuris yra zonos viduje. Apsauga nuo tokių atakų turėtų būti įdiegta vietos nustatymo sistemoje.

4.3 Reikalavimų projektuojamai sistemai specifikacija

Sistemos paskirtis yra pagal organizacijos saugos politiką autentifikuoti bevielio tinklo vartotojus ir valdyti jų prieigą prie bevielio tinklo resursų.

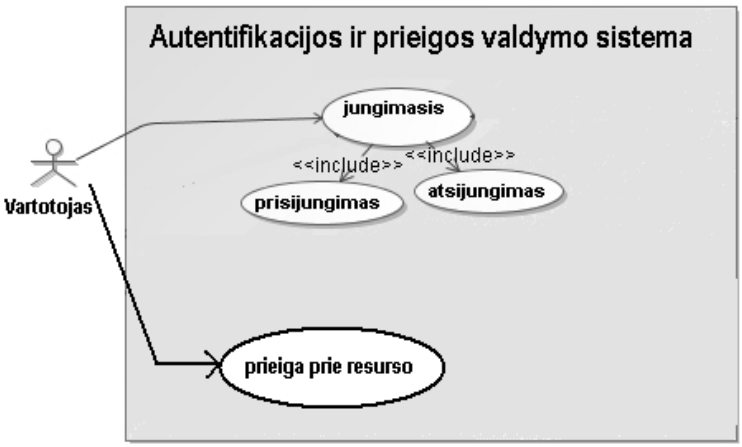
4.3.1 Vartotojai

10 lentelė. Sistemos vartotojai

Sistemos vartotojai	**Sistemos administratoriai**	**Galutiniai vartotojai bevieliame tinkle**
Sprendžiami uždaviniai	diegia ir administruoja sistemą	prisijungia prie bevielio tinklo nešiojamų įrenginių pagalba, naudojasi bevielio tinklo resursais
Patirtis dalykinėje srityje	specialistai	naujokai, pažengę vartotojai
Patirtis informacinėse technologijose	specialistai	naujokai, pažengę vartotojai

10 lentelėje yra apibūdinti sistemos vartotojai. Lentelėje jie suskirstyti į dvi grupes – sistemos administratoriai ir galutiniai vartotojai, besinaudojantys bevieliu tinklu. Numatoma, kad sistemos galutiniai vartotojai bus dėstytojai, studentai ir kiti universiteto darbuotojai.

15 paveikslėlyje parodyta panaudos atvejų diagrama. Paveikslėlyje pažymėtas vartotojas yra galutinis vartotojas.



15 pav. Panaudos atvejų diagrama

4.3.2 Apribojimai sprendimui

- Programos kūrimui ir funkcionavimui turi visiškai pakakti atviro kodo programinės įrangos (teksto redaktoriai, kompiliatoriai, duomenų bazės ir t.t.), išskyrus tą programinę įrangą, kuri įsigyjama kartu su aparatine įranga ir be kurios aparatinė įranga negali veikti (tvarkyklės, įmontuotoji programinė įranga (angl. *firmware*), operacinė sistema ir t.t.).
- Serverio programinė įranga turi veikti UNIX/Linux operacinėje sistemoje.
- Sistema, kiek įmanoma, turi būti pritaikyta komunikuoti su vartotoju per prieigos tašką, t. y. turėtų veikti panašiai į RADIUS serverį, arba būti pritaikyta integravimui į RADIUS ar panašų bevielio tinklo autentifikaciją atliekantį serverį.
- Sistemoje numatomuose naudoti prieigos taškuose, jei jie numatomi, turi veikti EAP-LEAP autentifikacija, jie turi palaikyti Cisco VPN paslaugos adapterius (angl. *VPN Service Adapter* – VSA).
- Prieigos valdymo serveris, kiek įmanoma, turi būti pritaikytas gauti vartotojo vietos informaciją iš vietos informacijos nustatymo sistemos, kuri pagal MAC adresą, nustato užklausto galinio įrenginio santykines koordinates x, y, z, kur z – pastato aukšto numeris, ir nustatytų koordinačių patikimumo reikšmę.
- Prieigos valdymo serveris turi turėti galimybę atlikti vartotojų autentifikaciją pagal vietos informaciją arba pagal standartinį autentifikacijos metodą, papildytą vietos informacija.

4.3.3 Diegimo aplinka

- Sistema veiks IEEE 803.11a/b/g standarto bevieliuose tinkluose.
- Prieigos valdymo serverio programinė įranga veiks UNIX/Linux operacinėje sistemoje.
- Programos kūrimui ir funkcionavimui naudojamos atviro kodo programinės įrangos, išskyrus tą programinę įrangą, kuri įsigyjama kartu su aparatine įranga ir be kurios aparatinė įranga negali veikti (tvarkyklės, įmontuotoji programinė įranga (angl. *firmware*), operacinė sistema ir t.t.).
- Naudojama duomenų bazių valdymo sistema - MySQL (5 versija).
- Sistema veiks pastatų viduje.
- Duomenų apsikeitimui su vietos informacijos nustatymo sistema numatomas naudoti SOAP protokolas.

4.3.4 Numatoma darbo vietos aplinka

- Galutiniai sistemos vartotojai naudosis nešiojamais įrenginiais (nešiojamaisiais kompiuteriais, delninukais, mobiliaisiais telefonais).
- Sistema galima naudotis kelių aukštų pastatų viduje.

4.3.5 Bendradarbiaujančios sistemos

Vietos informacija bus gaunama iš vietos informacijos nustatymo sistemos, įdiegtos KTU Informatikos fakultete, ir nustatančios vartotojo vietą apytiksliai vieno metro tikslumu. Sistemoje naudojamas vietos informacijos nustatymo pagal vartotojų galinių įrenginių siunčiamų signalų stiprius būdas. VNS skirtose užklausose nurodomas MAC adresas to įrenginio, kurio vietos informacijos klausiama. Atsakydama į užklausą VNS grąžina santykines įrenginio koordinates x, y, z, kur z atitinka pastato aukšto numerį, ir jų patikimumo reikšmę, išreikštą procentais.

4.3.6 Funkciniai ir nefunkciniai reikalavimai

Reikalavimai saugos politikai:

1. Saugos politika turi numatyti KTU Informatikos fakulteto bevielio tinklo vartotojų aptarnavimo tvarką;
2. Saugos politika turi numatyti KTU Informatikos fakulteto bevielio tinklo vartotojų prieigą prie informacinės sistemos išteklių;
3. Saugos politika turi numatyti bent šias keturias skirtingas vartotojų kategorijas: dėstytojai, darbuotojai, studentai ir svečiai;
4. Saugos politikoje turi būti nurodyta, kad autentifikacijai ir prieigos valdymui naudojama vartotojo vietos informacija;
5. Saugos politika turi numatyti, kokie KTU Informatikos fakulteto informacinės sistemos resursai yra prieinami, kuriems vartotojams ir kuriose pastato vietose kabineto tikslumu;
6. Saugos politikoje turi būti nurodyta, kad paskyros vartotojams suteikiamos, uždaromos ir keičiamos turi būti centraliai administratoriaus;
7. Saugos politikoje turi būti nurodyta, koks vietos informacijos nustatymo tikslumas arba patikimumas yra reikalaujamas;
8. Saugos politikoje turi būti nurodyta, kad vartotojų prisijungimo duomenys ir vietos informacija turi būti saugomi ir neprieinami pašaliniams asmenims (ne sistemos administratoriams).

Reikalavimai vietos informacija pagrįsto prieigos prie bevielio tinklo resursų valdymo sistemai:

9. Prieigos valdymo sistema turi valdyti prieigą prie bevielio tinklo resursų pagal saugos politikos nustatytus reikalavimus;
10. Sistema turi veikti Prieigos valdymo serveryje;
11. Sistema, kiek įmanoma, turi būti pritaikyta kreiptis į KTU Informatikos fakultete įdiegtą vietos informacijos nustatymo sistemą, kad gautų vartotojų koordinates;
12. Sistema bendravimas su Vietos informacijos nustatymo sistema turi būti vykdomas SOAP (angl. *Simple Object Access Protocol*) protokolu per žiniatinklį, per žiniatinklį teikiama paslauga aprašyta žiniatinklio paslaugų aprašymo kalba (angl. *Web Service Definition Language*);
13. Sistema, kreipdamasi į vietos informacijos tiekėją, turi nurodyti vartotojo, kurio vietos informacijos užklausia, fizinį adresą MAC ir autentifikavimosi vietos nustatymo sistemoje duomenis (ID ir slaptažodį);
14. Sistema turi įvertinti gautos vartotojo vietos informacijos patikimumą (vietos nustatymo sistema vietą gali nustatyti metro tikslumu) bei koordinates ir pagal šiuos duomenis priimti sprendimą autentifikacijai/prieigai;
15. Sistemos komponentų veikimo stebėjimas turi būti automatizuotas, kur įmanoma, sistema turi būti pati save atstatanti;
16. Sistema turi priimti sprendimą, ar autentifikuoti ar ne prie IEEE 803.11a/b/g bevielio tinklo bandančius prisijungti klientus pagal jų ID, slaptažodį (nebūtinai) ir vietos informaciją;
17. Sistema turi paruošti prieigos taškui atsakymą, ar vartotojas gali prisijungti prie bevielio tinklo;
18. Sistema turi vykdyti autentifikaciją pagal vietos informaciją, ir, kiek įmanoma, būti paruošta papildyta kitu standartiniu bevielio tinklo autentifikacijos metodu;
19. Sistema turi kreiptis į vietos nustatymo sistemą, įvertinti gautą vartotojų vietos informaciją ir atnaujinti prieigos nustatymus ne rečiau kaip kas 5 min.;
20. Sistema turi veikti pagal rolėmis pagrįstą prieigos valdymo modelį papildant jį vietos informacija.

4.4 Duomenų struktūros

Prieigos valdymo sistemos darbui reikalingi tokie duomenys: informacija apie vartotoją (jo vardas, slaptažodis, vietos informacija ir pan.), informacija apie išteklius (duomenų ir paslaugų identifikatoriai) ir informacija apie veiksmus, kuriuos vartotojai gali atlikti su ištekliais. Prieigos valdymo politikos gali būti išreiškiamos taisyklėmis, kuriose nurodomi šie trys elementai: subjektai (vartotojai), objektai (ištekliai) ir veiksmai.

Sistemos objektai yra bevielio tinklo ištekliai ir turi būti kaip nors identifikuojami. Objektai gali būti atskiriami ir nusakomi šiomis savybėmis: objekto IP adresas, naudojamo prievado nr., objekto ar paslaugos/programos pavadinimas.

Veiksmai, kuriuos vartotojai gali atlikti su objektu, gali būti tokie: skaityti, rašyti, spausdinti, kopijuoti, vykdyti ir pan. Vieno objekto ir veiksmo, kurį galima atlikti su tuo objektu, kombinacija gali būti pavadinta leidimu. Norint realizuoti prieigos valdymą, tokį leidimą ar analogiškų leidimų sąrašą galima priskirti vartotojui. Objektų ir veiksmų, kuriuos galima su jais atlikti analizavimas nėra šio darbo dalis, todėl detaliau analizuojami subjektų duomenys ir vietos informacija.

Duomenys, susiję su vartotoju, gali priklausyti nuo prieigos valdymo modelio, autentifikacijos metodo, vietos nustatymo ir įvertinimo būdo. Projektuojamoje sistemoje pasirinkta naudoti rolėmis pagrįstą prieigos valdymą, papildytą vietos informacija. Vietos informacija apie vartotoją gali būti nusakoma įvairiai, priklausomai nuo vietos nustatymo sistemos (VNS) ir saugos politikos. VNS vietos informacija gali būti nusakyta koordinatėmis arba požymio reikšme, paklaida arba patikimumo reikšme bei galiojimo reikšme. Koordinatės paprastai būna santykinės x, y, z vartotojo galinio įrenginio koordinatės. Požymis nusako, ar vartotojas yra tam tikroje būsenoje (pvz., tam tikrame kabinete, tam tikru atstumu nuo ko nors arba juda tam tikru greičiu) ar ne. Pagal sukurtą prieigos prie bevielio tinklo resursų valdymo panaudojant vietos informaciją modelį, be minėtų gali būti nustatyti ir kitų tipų erdviniai požymiai, tokie kaip vartotojo judėjimo greitis, atstumas tarp vartotojo ir kito objekto, vartotojų tam tikroje erdvėje tankis. Kaip rašo Ardagna ir kiti [13] vietos informacija gali būti nusakyta keliais vietos informacija pagrįstais predikatais (predikatas išreiškia erdvinį požymį, kuris gali būti siejamas su vartotoju), kurie išvardyti ir apibūdinti 9 lentelėje. Šiame darbe sistema įvertins tik vieną požymių tipų aibę, kuri nusako, ar vartotojas yra tam tikroje zonoje. Tyrimui naudojama VNS nustato vartotojo santykines koordinates x, y, aukšto, kuriame jis yra, numerį, ir patikimumą. Kadangi vietos nustatymo sistema iš tikro nustato ne pačio vartotojo, bet jo mobiliojo įrenginio vietą, turi būti susiejami vartotojo ID ir jo naudojamo įrenginio MAC adresas. Tokie ir panašūs duomenys gali būti išreikšti per vartotojo profilį, kuris gali būti vienareikšmiškai identifikuojamas vartotojo ID. Vartotojo MAC adresas, vietos informacija ir jos paklaida laikui bėgant gali keistis. Projektuojamai sistemai reikalingi šie duomenys apie subjektą:

- ID;
- slaptažodis;
- rolė;

- MAC adresas;
- koordinatės x, y;
- aukšto, kuriame jis yra, numeris;
- vietos informacijos paklaida.

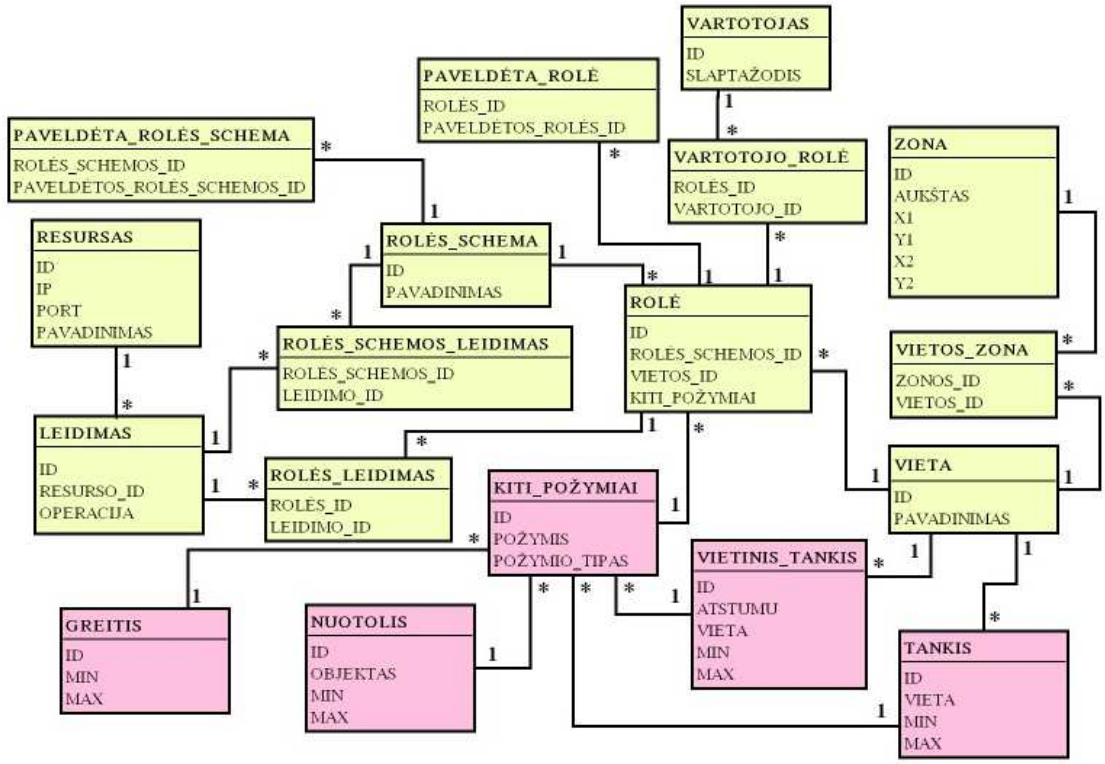
Kaip jau minėta, prieigą sistemoje pasirinkta valdyti pagal rolėmis pagrįstą prieigos valdymo modelį, papildytą vietos informacija. Projektuojant prieigos valdymo sistemą remiamasi [18] pasiūlytu Geo-RBAC modeliu. Kaip specifikuota reikalavimuose, prieiga turi būti valdoma įvertinant tai, kuriame kabinete yra sistemos vartotojas, ir prieigos valdymas turi būti pritaikytas veikti kelių aukštų universiteto pastato viduje. Dėl šių priežasčių Geo-RBAC modelis yra šiek tiek pakeičiamas pagal minėtus reikalavimus. Kadangi Geo-RBAC modelyje egzistuoja tik daugiakampio formos esybės, jis papildomas įvertinimu, kuriame pastato aukšte yra pasaulio esybė, ir truputį supaprastinamas laikant, kad erdvinės pasaulio esybės gali būti tik stačiakampio arba iš stačiakampių sudarytos formos. Kadangi prieigos valdymas turi veikti kabineto tikslumu tarp tokių esybių, kurios atitinka universiteto patalpas apibrėžiamas vienintelis buvimo dalimi ryšys. Dėl šios priežasties tarp esybių, atitinkančių universiteto kabinetus ir kitas patalpas, nesunkiai gali būti įvesta hierarchija numatyta Geo-HRBAC (Geo-RBAC hierarchinis modelis) modelyje.

Kadangi prieigos valdymo sistemoje naudojami erdviniai požymiai nusako, kurioje taisyklingos formos zonoje yra vartotojas, į projektuojamą sistemą užtenka įtraukti vieną realios vietos (santykinių koordinačių x, y, z, kur z atitinka pastato aukšto numerį) susiejimo su erdviniu požymiu (pavyzdžiui, kabineto nr.) funkciją, kuri tikrina, ar vartotojo x, y koordinatės yra tam tikros zonos viduje ir ar sutampa vartotojo ir zonos aukšto numeris. Pagal Geo-RBAC modelį vartotojams yra priskiriamos rolės, veikiančios tik su tam tikrais erdviniais požymiais. Vienai erdvinei rolei nurodytas tik vienas erdvinis požymis. Projektuojamoje sistemoje šie požymiai nusako, kurioje universiteto patalpoje ar patalpų rinkinyje yra vartotojas. Rolės gali būti nusakomos rolės pavadinimu ir vietos informacija paremtu erdviniu požymiu (dar kitaip galima vadinti rolės apimtimi arba zona), kurį turintis vartotojas galės atlikti rolę. Taigi į saugos politiką įtraukiami leidimai ir apribojimai vartotojams pagal tai, kurioje rolės zonoje jie tuo metu yra. Zonos, pavyzdžiui, gali būti universiteto laboratorijos. Visoje zonoje tam tikrą rolę atliekantis vartotojas turi tuos pačius leidimus.

M. L. Damiani ir kiti [18], kaip pristatyta 2.2.5. skyrelyje, į prieigos valdymo modelį įtraukia ir rolių schemas, kurios nurodo leidimus, kuriuos gauna visi to paties pavadinimo rolę atliekantys vartotojai, nepriklausomai nuo to, kurioje vietoje jie tuo metu yra. Vadinasi, tam

tikrą rolę atliekantis vartotojas turi ne tik jo rolei priskirtus leidimus, bet ir tos rolės schemai priskirtus leidimus. Autoriai taip pat siūlo tarp rolių ir rolių schemų įvesti hierarchiją, arba paveldėjamumo ryšius. Tai reiškia, kad tam tikrą rolę atliekantis vartotojas turės ne tik tai rolei priskirtus leidimus, bet ir visus protėvinių rolių leidimus, taip pat tos rolės schemos leidimus ir visus tos schemos protėvių leidimus. Hierarchija tarp rolių turi būti nustatyta atsižvelgiant į zonas, kuriose jos veikia. Rolė gali turėti tik tokį protėvį, kuris veikia visoje jos zonoje arba dar daugiau apimančioje zonoje. Rolės schema nurodo rolės pavadinimą ir tipą, arba stambumą, zonų, kuriose veikia to pavadinimo rolės. M. L. Damiani ir kiti [18] į rolės schemą įtraukia tikros vietos, kurioje vartotojas gali būti, ir loginės vartotojo vietos susiejimo funkciją bei nurodo loginės vartotojo vietos tipą. Susiejimo funkcija pagal vartotojo tikrą vietą nustato, kurioje loginėje vietoje jis yra, o kadangi tarp loginių vietų yra apibrėžta tiksli hierarchija, tada nesunkiai gali būti nustatyta ir ar vartotojo loginė vieta yra rolė apimtyje. Kadangi projektuojamoje sistemoje erdvinius požymius atitinkančios esybės yra primityvios ir jas lengva nusakyti koordinatėmis, galima naudoti vieną susiejimo funkciją, kuri iš karto susietų vartotojo tikrąją vietą, (VNS nustatytas koordinates) su erdvinės rolės apimtimi (pavyzdžiui, kabineto numeriu). Dėl šios priežasties nėra prasmės rolės schemoje nurodyti susiejimo funkcijos bei loginės vietos.

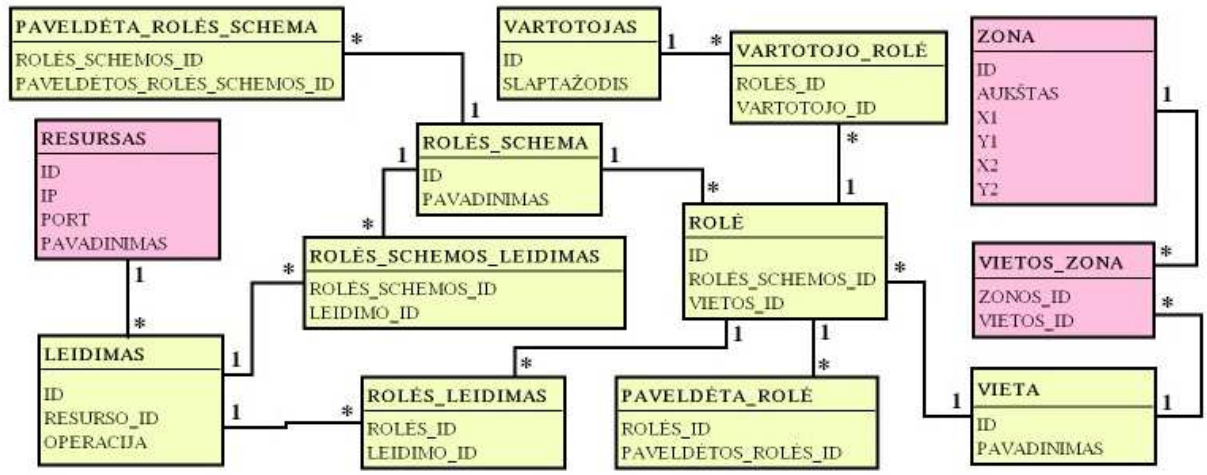
Geo-RBAC modelis, neįvertina kitų VI pagrįstų požymių, tokių kaip greitis, atstumas. Jis gali būti papildytais kitais požymiais toliau aprašytu būdu. Prie rolės, kuri susideda iš pavadinimo, apibrėžiančio jos schemą, ir apimties, nurodančios erdvinį požymį, pridedamas papildomų VI pagrįstų požymių sąrašas. Tokį trejetą galima pažymėti atitinkamai <r, e, p>. Tokiu būdu rolė nurodoma pavadinimu, erdvinių požymiu (kurioje vietoje veikia) ir kitų VI pagrįstų požymių sąrašu, kuris yra kaip papildomi apribojimai. Be apribojimo, kurioje vietoje rolė veikia, nurodomos papildomos sąlygos tokios kaip, kokiu greičiu judantis (*greitis*), kokiu atstumu nutolęs nuo tam tikro objekto (*nuotolis*), tarp kiek kitų vartotojų esantis (*vietinis tankis*) vartotojas ją gali atlikti. Sąraše gali net būti nurodyta, koks vartotojų tankis turi būti tam tikroje zonoje (*tankis*). Kitų požymių sąrašas gali būti tuščias arba jame gali būti nurodyta bet koks skaičius bet kurių kitų VI pagrįstų požymių, tokių kaip greitis, nuotolis ir panašiai. Erdvinių požymių tame sąraše jau nebus, nes kiekviena erdvinė rolė identifikuojama tik vienu erdviniu požymiu. 16 paveikslėlyje parodyta esybių ryšių diagrama, įtraukus į ją kitus VI pagrįstų požymių tipus. Rausva spalva pažymėtos esybės, kurių nebūtų prieigos valdymo sistemoje, įvertinančioje tik erdvinius požymius.



16 pav. Vietos informacija pagrįsto prieigos valdymo sistemos esybių ryšių diagrama

Svarbu apibrėžti, kaip dėl naujai atsiradusių VI pagrįstų požymių turi būti sudaryta hierarchija tarp rolių, nes rolė gali skirtis nuo kitos rolės ne tik apimtimi, bet ir papildomais požymiais. Tai gali būti išsprendžiama dviem būdais. Galima įvesti apribojimą, kad viena erdvinė (vienos apimties) rolė gali būti papildyta tik vienu papildomu požymių sąrašu. Tai reiškia, kad erdvinės rolės išliks tos pačios (identifikuojamos pavadinimu ir apimtimi) kaip ir tuo atveju, kai kiti požymiai nevertinami, tik bus nurodyta papildomų sąlygų (apribojimų), kuriomis erdvinė rolė gali būti atliekama. Jei pavyzdžiui, dekanas gali atlikti savo erdvinę rolę atėjęs į savo kabinetą, tai įvedus kitus požymius jo rolei atsirastų daugiau apribojimų. Kad jis galėtų atlikti tą rolę, reikėtų ne tik, kad jis būtų savo kabinete, bet ir, pavyzdžiui, kad jo kabinete nebūtų jokių kitų subjektų. Apibūdintu atveju rolių hierarchija nesikeičia, nes rolės lieka tos pačios, tik labiau jas galima apriboti.

Kitas sprendimas gali būti kitų požymių pagrindu sukurti naujas erdvines roles. Tokiu būdu galėtų egzistuoti dvi skirtingos rolės $<r_1, e_1, p_1>$ ir $<r_1, e_1, p_2>$, kurios skiriasi tik kitais požymiais, bet atliekamos toje pačioje zonoje. Hierarchija tarp rolių turėtų išlikti tokia, kokia apibrėžta pagal erdvinius požymius, o toms rolėms, kurios skiriasi tik kitais požymiais galima taikyti tokią taisyklę: kuo daugiau kitų VI požymių rolė turi tuo ji yra aukščiau hierarchijoje. Rolė $<r_1, e_1, p_1>$ gali paveldėti rolės $<r_1, e_1, p_2>$ leidimus tik tada, kai p_2 požymių sąraše yra visi p_1 kitų požymių sąraše esantys požymiai.



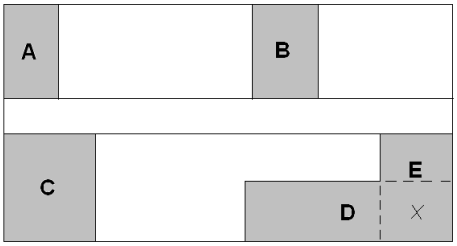
17 pav. Vietos informacija pagrįsto prieigos valdymo sistemos esybių ryšių diagrama

Kadangi bevieliame tinkle gali būti įvertinti tik zoną nurodantys erdviniai požymiai, visoms aptartoms duomenų struktūroms ir ryšiams tarp jų atvaizduoti buvo suprojektuota 17 paveikslėlyje parodyta esybių ryšių diagrama. Esybės ZONA ir VIETOS_ZONA pažymėtos kita spalva, nes jų galima būtų atsisakyti tuo atveju, jei VNS grąžintų ne vartotojo tikrąją vietą (koordinates), bet atsakytų į užklausą, ar vartotojui būdingas tam tikras erdvinis požymis (pvz., ar vartotojas yra tam tikrame kabinete). Esybė RESURSAS yra nereikalinga tuo atveju, kai PVS pagal prieigos valdymo technologiją nustato tik aktyvuotas vartotojų roles arba leidimų sąrašą, o patys resursai identifikuojami ir valdomi pagal tam tikrą prieigos valdymo technologiją kitame objekte. Duomenų bazės lentelės PAVELDĖTA_ROLĖS_SCHEMA ir PAVELDĖTA_ROLĖ saugomi duomenys parodo paveldėjamumo ryšius tarp rolių ir rolių schemų. Lentelėje VIETA saugoma informacija apie visus įmanomus erdvinius požymius (kitaip galima sakyti rolių apimtis), su kuriais vartotojai gali atlikti įvairias roles. Lentelėje Vieta gali būti specifikuoti tokie erdviniai požymiai, kaip Informatikos fakulteto raštinė arba Kompiuterių tinklų katedra. Tokie erdviniai požymiai nusako visą erdvę (rolės apimtį), kurioje vartotojas gali atlikti vieną savo rolę. Kadangi tokia vieta gali būti netaisyklingos formos arba susidėti iš kelių atskirų ne šalia viena kitos esančių zonų, požymiai susiejami su juos nusakančiomis mažesnės apimties ir stačiakampio gretasienio formos zonomis, iš kurių ir susideda erdviniai požymiai. Taigi duomenys apie atskiras zonas atskirti lentelėje ZONA, o lentelė VIETOS_ZONA nurodo, kurios zonos, kuriuos požymius sudaro.

Kaip jau minėta, projektuojant sistemą priimama, kad patalpos, kuriose veiks sistema yra stačiakampio formos. Todėl zonos taip pat laikomos stačiakampio gretasienio formos. 18 paveikslėlyje parodytas pavyzdys zonų (jos pažymėtos pilka spalva ir sužymėtos raidėmis), kurios sudaro vieną loginę vietą, pavyzdžiui, Kompiuterių tinklų katedrą. Kompiuterių tinklų

katedrai gali priklausyti keli ne šalia vienas kito esantys kabinetai. Kabinetus gali skirti koridorius ar kitos patalpos. D ir E raidėmis pažymėtas plotas yra ne stačiakampio formos. Tokiu atveju laikoma, kad tame plote yra dvi stačiakampio formos zonos, dalinant plotą į dvi dalis. 18 paveikslėlyje nubrėžtos dvi punktyrinės linijos, kurios galėtų padalinti pilką plotą į du stačiakampius. Ne stačiakampio formos plotas dalinamas į dvi zonas taip, kad abi zonos būtų stačiakampio formos, užimtų kuo didesnį plotą ir persidengtų viena su kita. Taip daroma dėl to, kad nėra svarbu nustatyti, ar vartotojas yra vienoje ar kitoje zonoje, svarbu nustatyti ar vartotojas yra bent vienoje iš zonų, o tai atlikti lengviau kai zona yra didesnio ploto.

Tokiu būdu pateiktame pavyzdyje Kompiuterių tinklų katedrai priklausytų zonos A, B, C, D ir E tokios, kad D ir E iš dalies sutaptų. D ir E zonų persidengimo plotas pažymėtas x ženklu.



18 pav. Loginių vietų skirstymas į zonas

Kadangi Vietos nustatymo sistema nustato vartotojo santykines koordinates ir, kuriame aukšte jis yra, norint nustatyti, ar vartotojas yra tam tikroje zonoje, reikia žinoti, kuriame aukšte yra zona, bei , pavyzdžiui, zonos (darant vieno aukšto pjūvį ir projektuojant vaizdą iš viršaus) kairiojo apatinio ir dešiniojo viršutinio kampų koordinates x1, y1 ir x2, y2. Būtent tokios esybės ir atvaizduotos 17 paveikslėlyje.

4.5 Saugos politika

Šiame skyrelyje aptarta projektuojamai vietos informacija pagrįsto prieigos prie bevielio tinklo išteklių valdymo sistemai skirta saugos politika, pagal kurią ir veiks sistema.

Norint sukurti saugos politiką, reikia identifikuoti visas reikalingas sistemos veikimui rolių schemas ir roles, nurodyti, kuriose zonose jos veikia, ir nustatyti tarp jų paveldėjamumo ryšius. Skirtingoms rolėms ir rolių schemoms reikia priskirti skirtingus leidimų sąrašus.

Lentelė 11. Rolių schemos

Rolės pavadinimas	Zonų, kuriose veikia rolė, tipas
Dekanas	Kabinetas
Prodekanas	Kabinetas
Darbuotojas	Katedra
Dėstytojas	Sektorius
Laborantas	Kabinetas
Studentas	Katedra
Klausytojas	Sektorius
Svečias	Universitetas

KTU Informatikos fakulteto bevielio tinklo vartotojams bus skirtos 11 lentelėje surašytos rolių schemos. Laikoma, kad tipas `kabinetas` nurodo, kad požymis bus ne didesnis už vieną kabinetą, katedra gali būti keli kabinetai, priklausantys vienai iš universiteto katedrų arba raštinė (šioje prieigos valdymo sistemoje Informatikos fakulteto raštinė laikoma Katedros tipo požymiu). Universiteto erdvėje galima išskirti tokius du sektorius: vienas – didžiosios auditorijos, kitas –kiti mokymui skirti kabinetai ir laboratorijos. Visa likusi universiteto erdvė (koridoriai, poilsio vietos, biblioteka ir panašiai) sektoriumi nelaikoma. Universitetu laikomos visos universiteto patalpos.

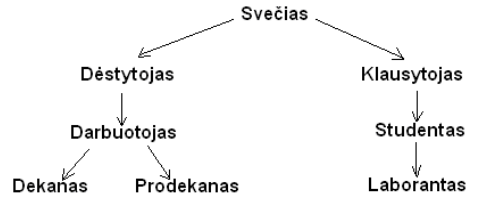
Lentelė 12. Erdvinės rolės

Pavadinimas	Apimtis (erdvinis požymis)	Žymėjimas
Dekanas	Informatikos fakulteto dekanato kabinetas	Dekanas(Z1)
Prodekanas	Prodekano kabinetas raštinėje	Prodek(Z9)
Prodekanas	Prodekano kabinetas Kompiuterių tinklų katedroje	Prodek(Z10)
Darbuotojas	Informatikos fakulteto raštinė	Darb(Z2)
Dėstytojas	Kompiuterių tinklų katedra	Dėst (Z4)
Dėstytojas	Multimedijos katedra	Dėst (Z5)
Dėstytojas	Kiti kabinetai ir laboratorijos	Dėst(Z3)
Dėstytojas	Didžiosios auditorijos	Dėst(Z8)
Studentas	Multimedijos katedra	Stud(Z5)
Studentas	Kompiuterių tinklų katedra	Stud(Z4)
Laborantas	Kompiuterių tinklų katedros laboratorija nr. 1	Labor(Z6)
Klausytojas	Kiti kabinetai ir laboratorijos	Klausyt(Z3)
Klausytojas	Didžiosios auditorijos	Klausyt(Z8)
Svečias	Kauno technologijos universitetas 7	Svečias(Z7)

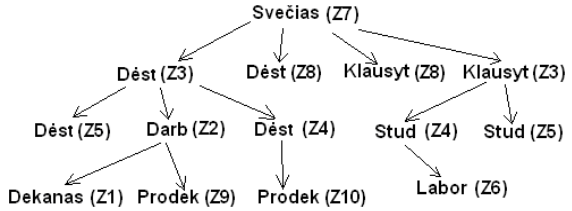
Saugos politikai įgyvendinti reikalingos 12 lentelėje surašytos erdvinės rolės.

Požymio *Multimedijos katedra* tipas nėra *sektorius*, nes Multimedijos katedra tik vieno universiteto sektoriaus dalis. Erdvinėse rolėse turi būti nurodytos ne didesnės zonos požymiai nei nurodyta tų rolių schemoje. Erdvinės rolės gali veikti tik dalyje schemoje nurodytos

zonos, bet svarbu, kad neišeitų už to tipo zonos ribų. Pavyzdžiui, erdvinė rolė <Studentas, Koridorius1> neatitiktų Studento rolės schemos. Iš 12 lentelės galime matyti, kad yra 10 skirtingų erdvinių požymių, su kuriais susieti vartotojai gali atlikti kokią nors rolę: Kauno technologijos universitetas (Z7), kiti kabinetai ir laboratorijos (Z3), Multimedijos katedra (Z5), Kompiuterių tinklų katedra (Z4), Kompiuterių tinklų katedros laboratorija nr. 1 (Z6), Informatikos fakulteto raštinė (Z2), Didžiosios auditorijos (Z8), Prodekano kabinetas raštinėje (Z9), Prodekano kabinetas Kompiuterių tinklų katedroje (Z10) ir Informatikos fakulteto dekano kabinetas (Z1).



19 pav. Rolių schemų hierarchija



20 pav. Erdvinių rolių hierarchija

Hierarchija tarp rolių ir rolių schemų turi būti nustatyta atsižvelgiant į tai, ar vienos rolės/schemos zona yra kitos rolės/schemos zonos dalis. Pavyzdžiui, jei Didžiosios auditorijos yra KTU universiteto dalis, erdvinė rolė < Svečias , Kauno technologijos universitetas >gali būti erdvinės rolės < Studentas, Didžiosios auditorijos > protėvis. Jei yra dvi skirtingos to paties pavadinimo rolės ir vienos jų zona yra kitos dalis, pirmoji turi paveldėti antrosios leidimus. Pavyzdžiui, < Studentas, Kompiuterių tinklų katedros laboratorija nr. 1 > turėtų paveldėti visus rolės < Studentas, Kompiuterių tinklų katedra > leidimus. Pagal šiuos principus sukurta hierarchija tarp rolių ir rolių schemų pavaizduota atitinkamai 19 ir 20 paveikslėliuose. Rodyklė rodo tą rolę ar rolės schemą, kuri paveldi leidimus iš tos rolės ar rolės schemos, iš kurios išvesta rodyklė.

13 lentelė. Rolėms ir rolių schemoms priskirti leidimai

Rolės pavadinimas	**Schemos leidimai**	**Leidimai, skirti erdviniai rolei tam tikroje apimtyje**									
		Z1	**Z2**	**Z3**	**Z4**	**Z5**	**Z6**	**Z7**	**Z8**	**Z9**	**Z10**
Dekanas	-	L10	-	-	-	-	-	-	-	-	-
Prodekanas	L14	-		-	-	-	-	-		L15	L16
Darbuotojas	L8	-	L13	-		-	-	-	-	-	-
Dėstytojas	L3, L9, L11	-	-	L5	L6, L7	L4	-	L12	-	-	-
Laborantas	-	-	-	-	-	-	-	-	-	-	-
Studentas	L2	-	-	-	-	-	-	L6	L4	L7	-
Klausytojas	-	-	-	L3	-	-	-	-	-	-	-
Svečias	-	--	-	-	-	-	-	L1	-	-	-

Lentelėje 13 surašyti, kurie leidimai, kurioms rolių schemoms ir erdvinėms rolėms, yra priskirti. 14 lentelėje leidimai detalizuoti nurodant, kokią operaciją ir su kuriuo tinklo resursu (objektu) vartotojas gali atlikti.

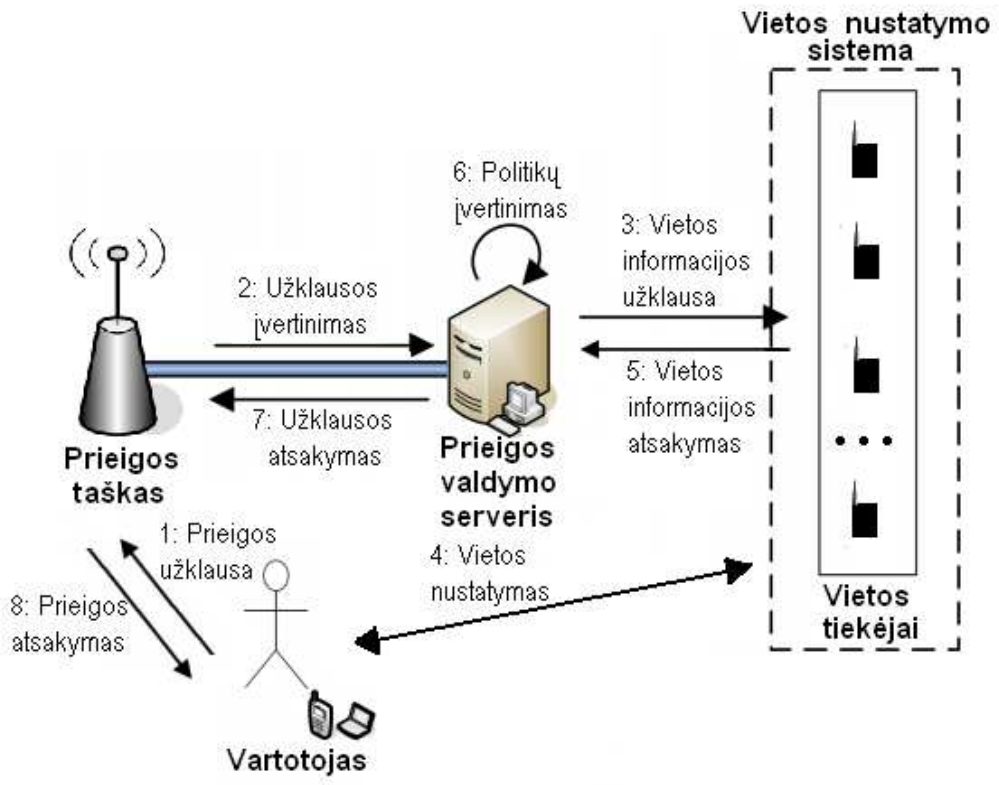
14 lentelė. Leidimai

Leidimas	**Objektas**	**Operacija**
L1	Internetas	Skaityti/Rašyti
L2	Paskaitų medžiaga	Skaityti
L3	Spausdintuvas studentams	Vykdyti
L4	Multimedijos laboratoriniai darbai	Vykdyti
L5	Laboratorinių darbų kūrimo programa	Vykdyti
L6	Tinklų katedros laboratoriniai darbai	Vykdyti
L7	Laboratorinis darbas „Bevielių tinklų saugumo tyrimas“	Vykdyti
L8	Programa „Raštvedyba“	Vykdyti
L9	Žurnalas	Rašyti
L10	Dokumentų tvarkymo ir pasirašymo programa	Vykdyti
L11	Paskaitų medžiaga	Rašyti
L12	Spausdintuvas darbuotojams	Vykdyti
L13	Spausdintuvas Informatikos fakulteto raštinėje	Vykdyti
L14	Informatikos fakulteto failai	Skaityti
L15	Informatikos fakulteto failai	Rašyti
L16	Failai susiję su studentų dalyvavimu mainų programose	Rašyti

4.6 Projektuojamos sistemos architektūra

21 paveikslėlyje pavaizduota projektuojamos sistemos architektūra. Kaip parodyta, vartotojas norėdamas prieiti prie bevielio tinklo išteklių, turi gauti leidimą iš prieigos valdymo serverio (PVS). Prieigos taškas veikia tik kaip tarpininkas tarp vartotojo ir PVS. PVS turi įvertinti, ar vartotojui leisti prieigą. Kad tą padarytų, PVS turi žinoti vartotojo vietą, todėl kreipiasi į vietos nustatymo sistemą (VNS), kuri analizuoja iš jutiklių (angl. *sniffers*) gautus duomenis, nustato vartotojo vietą ir grąžina atsakymą. Tarp trečio ir ketvirto žingsnio gali būti įterptas dar vienas žingsnis – susitarimas tarp prieigos valdymo ir vietos nustatymo sistemų dėl vietos nustatymo paslaugos kokybės lygio. Toks žingsnis reikalingas, jei VNS teikia įvairaus lygio paslaugas ir iš anksto nėra suderintas reikalingas paslaugos kokybė lygis. Kaip bebūtų šiame darbe šis žingsnis praleidžiamas.

Autentifikacijos metu prieigos valdymo serveris bendru atveju gali patikrinti ir kitus vartotojo naudojamus kredencialus ne tik VI pagrįstus požymius. Viską įvertinęs pagal saugos politikas, prieigos valdymo serveris priima sprendimą dėl prieigos ir grąžina vartotojui atsakymą.



21 pav. Vietos informacija pagrįsto prieigos valdymo architektūra

Prieigos valdymo serveris autentifikuoja vartotoją tuomet, kai vartotojas pareiškia norą prisijungti prie bevielio tinklo ir atjungia vartotoją, kai jis baigia naudotis bevielio tinklo ištekliais. Kadangi vartotojo vieta gali keistis, prieigos valdymo serveris turi vis patikrinti vietos informaciją ir priskirti vartotojui tų rolių, kurias vartotojas gali atlikti toje vietoje, leidimus.

Taigi galima išskirti tokias tris prieigos valdymo serverio funkcijas:

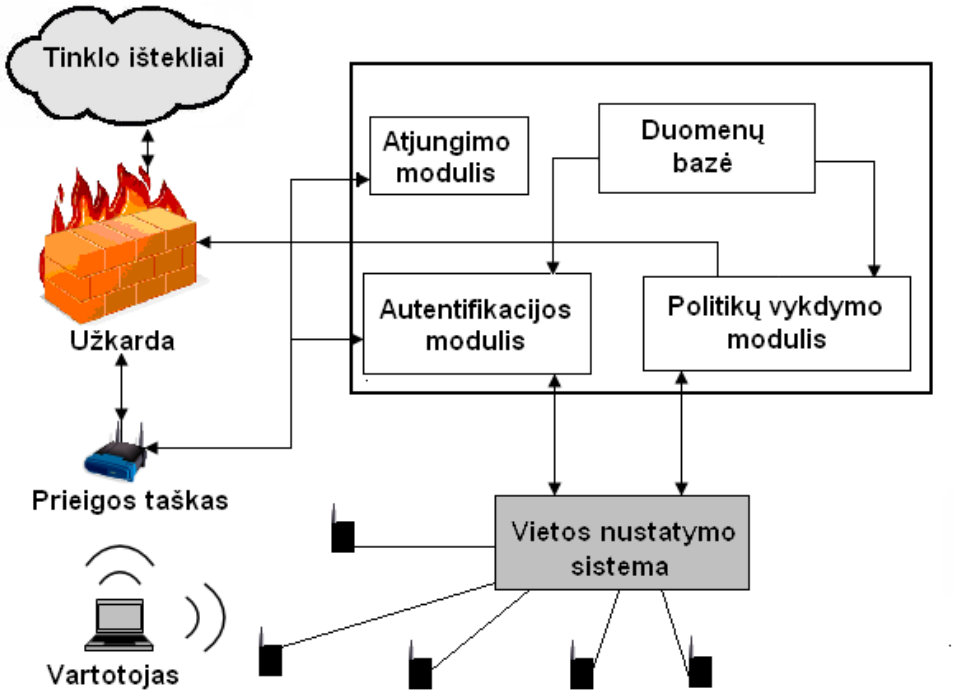
1. autentifikacija (patikrinimas, ar vartotojo kredencialai ir erdviniai požymiai yra tinkami leisti prieiti prie bevielio tinklo resurso (-ų), erdvinių rolių priskyrimas ir prieigos leidimas / blokavimas),
2. atjungimas nuo tinklo ir prieigos prie tinklo resursų blokavimas
3. politikų vykdymo algoritmas (kas kažkiek laiko atliekamas atnaujinimas vartotojui priskirtų rolių ir leidimų pagal erdvinius požymius).

19 paveikslėlyje šios trys skirtingos funkcijos pavadintos atitinkamai Autentifikacijos, Atjungimo ir Politikų vykdymo moduliais. Kad vartotojas galėtų pasiekti tik tuos resursus, kuriuos jis yra autorizuotas pasiekti, prieigos valdymo sistema turi tikrinti kiekvieną autentifikuoto vartotojo užklausą ir ją atmesti arba leisti pagal vartotojo atliekamoms rolėms priskirtus leidimus. Ši sistemos funkcija / dalis 21 paveikslėlyje pavaizduota kaip užkarda.

Visos vartotojų užklausos turėtų eiti pro tam tikrą užkardą ar būti kitaip apdorojamos pasirinkta prieigos valdymo technologija, kuri užtikrina prieigos valdymą.

Politikų vykdymo modulis kas tam tikrą laiko tarpą nustato, kurie leidimai turi būti priskirti, kuriems vartotojams ir atitinkamai pakeičia užkardos nuostatas. Tai atliekama dėl to, kad prisijungęs vartotojas gali judėti ir jo vietos informacija gali laikui bėgant keistis. Pagal gautą informaciją, vartotojui uždraudžiama arba leidžiama prieiga prie tam tikrų resursų, pavyzdžiui, vartotojui išėjus iš savo darbo kabineto į kitas patalpas, panaikinama galimybė naudotis tais resursais, kurie turi būti prieinami tik iš darbo kabineto. Sesija naikinama tuomet, kai vartotojo galinis įrenginys atsijungia nuo prieigos taško (apie tai PVS praneša prieigos taškas) arba atsiranda už teritorijos, kur teikiama prieiga prie tinklo, ribų (tai PVS apskaičiuoja iš vartotojo vietos informacijos).

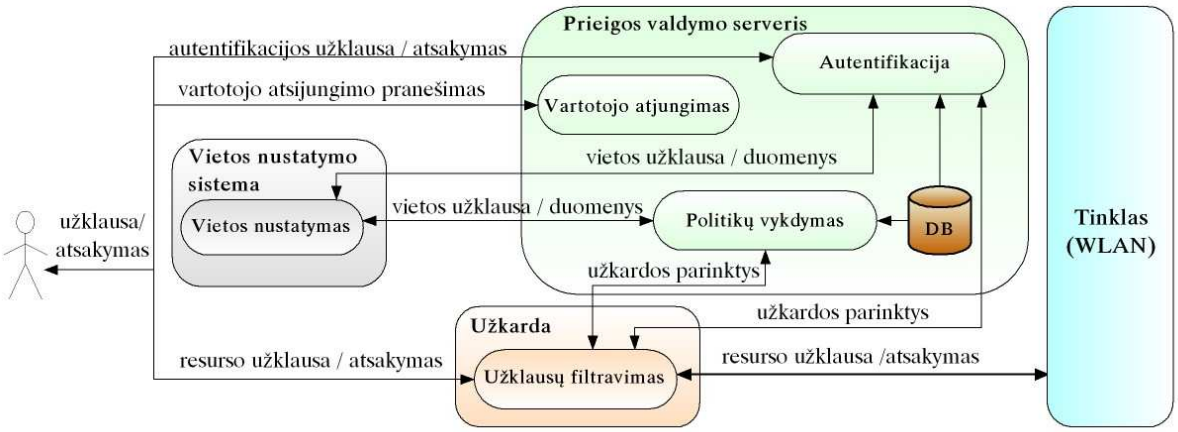
Autentifikacijos ir politikų vykdymo moduliai skaito duomenis iš duomenų bazės, kurioje saugoma informacija apie visus vartotojus, erdvinius požymius ir roles bei leidimus, kuriuos vartotojai gali gauti (žr. pav. 22).



22 pav. Tyrimo sistemos elementai ir jų komunikacija

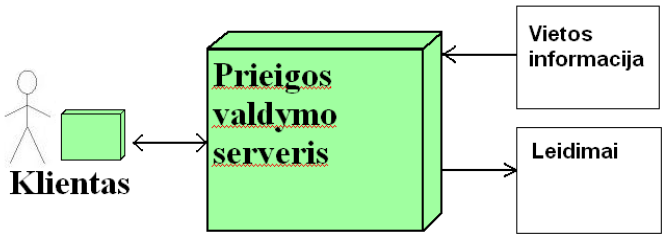
Politikų vykdymo modulis tam tikrais pastoviais laiko intervalais turi atnaujinti vartotojams suteiktus leidimus pagal erdvinius požymius ir veikti nepriklausomai nuo autentifikacijos modulio. Autentifikacijos metu pagal erdvinius požymius vartotojui parenkama rolė ir suteikiama prieiga prie resurso (-ų). 22 paveikslėlyje pavaizduoti trys prieigos valdymo sistemos moduliai: „Vartotojo atjungimas“, „Autentifikacija“ bei „Politikų

vykdymas“. 23 paveikslėlyje taip pat pavaizduoti duomenų srautai tarp PVS, VNS, Užkardos, WLAN ir prieigos taško.



23 pav. Vietos informacija grįsto prieigos valdymo sistemos duomenų srautų diagrama

Kadangi prieigos valdymo sistema projektuojama tyrimo tikslais, į ją nebūtina įtraukti konkrečios prieigos valdymo technologijos. Prieigos valdymo sistema gali būti ištirta vartotojams priskirtus leidimus arba atitinkamus prieigos valdymo technologijos parametrus įrašant į failą. Kad darbas nebūtų per didelės apimties, pasirinktas 24 paveikslėlyje atvaizduotas sistemos veikimas. Kaip parodyta paveikslėlyje, vietos informaciją prieigos valdymo serverio programa skaito iš failo, o ne iš vietos nustatymo sistemos. VNS veikimas simuliuojamas skaitant iš failo įrašus, susidedančius iš MAC adreso, santykinių z, y, z koordinačių ir vietos informacijos patikimumo reikšmių, ir pagal vartotojo MAC adreso reikšmę išrenkant vietos informacijos bei patikimumo reikšmes. Sąsajai su vartotoju arba prieigos tašku naudojama kliento programa. Kliento programos pagalba vartotojas gali prisijungti ir atsijungti nuo bevielio tinklo arba siųsti užklausą priėjimui prie tam tikro resurso. Vartotojas klieno programos pagalba gali pasirinkti, ar turi būti vykdomas prisijungimas prie tinklo ar atsijungimas nuo tinklo, nurodyti savo vardą, slaptažodį ir MAC adresą arba su kliento programa vartotojas nurodo resursą, prie kurio prieigos reikalauja. Pasirinkus ir įvedus reikalingus duomenis kliento programa kreipiasi į serverio programą, kuri įvykdo autentifikacijos, atsijungimo nuo tinklo arba prieigos prie tam tikro resurso modulį ir grąžina vartotojui atsakymą (atsakyme nurodoma, ar vartotojas buvo atjungtas nuo tinklo, ar jam buvo suteikta prieiga ar ne).

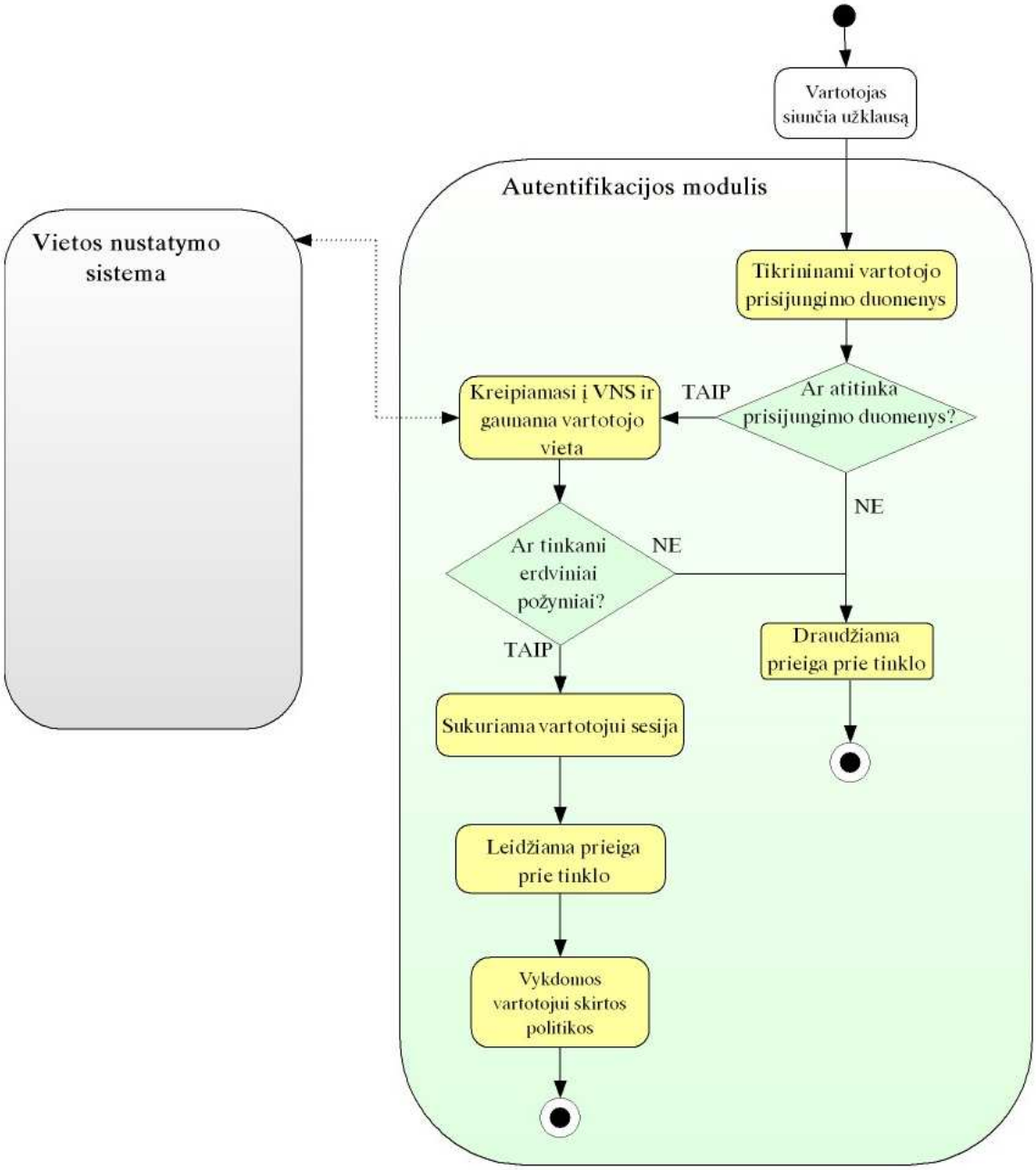


24 pav. Projektuojamos sistemos veikimo schema

4.7 Programinių modulių ar objektų specifikacijos

Duomenų srautų diagramoje (žr. 23 paveikslėlį) pažymėtas autentifikacijos modulis įvykdo autentifikaciją ir prieigos pagal jo atliekamą rolę suteikimą. Šio modulio vykdymo metu atnaujinami užkardos nustatymai ir vartotojui suteikiama prieiga prie tinklo resursų. 25 paveikslėlyje pavaizduotas autentifikacijos algoritmas. Šis algoritmas pradedamas vykdyti vartotojui atsiuntus autentifikacijos užklausą.

Pagal 25 paveikslėlyje parodytą vykdymo seką visų pirma tikrinami tokie vartotojo prisijungimo duomenys kaip slaptažodis, sertifikatas ir panašiai. Jei duomenys tinkami, kreipiamasi į VNS ir užsakoma VI pagrįstiems požymiams įvertinti reikalinga vietos informacija. Tuomet patvirtinami erdviniai požymiai, kurie reikalingi vartotojo autentifikacijai. Bendru atveju tai gali būti, pavyzdžiui, tokie požymiai kaip, ar vartotojas juda ne didesniu, kaip 3 km/val. greičiu, ar jis yra savo kabinete ir ar kabinete nėra daugiau nei 10 kitų klientų. Jei patvirtinami visi šie požymiai, vartotojui sukuriama sesija (jo MAC ir vardas įrašomi į prisijungusių vartotojų sąrašą), leidžiama prieiga prie tinklo ir vykdomos vartotojui skirtos politikos. Autentifikacijai naudojant slaptažodžius, ar kitus autentifikacijos mechanizmus turi būti užtikrinamas saugus jų perdavimas nuo kliento iki PVS. Tas gali būti užtikrinta naudojant RADIUS protokolą, kaip tai daroma WPA-EAP autentifikacijos metodo atveju.



25 pav. Autentifikacijos ir pradinio politikų vykdymo seka

26 paveikslėlyje detaliau išnagrinėtas saugaus WPA-EAP autentifikacijos metodo algoritmo seka, papildyta VI požymių įvertinimu. 26 paveikslėlyje pavaizduota, koks duomenų apsikeitimas vyksta tarp kliento, prieigos taško, PVS ir VNS, klientui bandant prisijungti prie bevielio tinklo. Kadangi vaizduojamas autentifikacijos procesas, Prieigos valdymo sistema paveikslėlyje vadinama Autentifikacijos serveriu. Ties komunikacijų rodyklėmis 26 paveikslėlyje skliausteliuose parašyta, kokie duomenys siunčiami iš vieno taško į kitą:

ID – vartotojo vardas;

MAC – vartotojo fizinis adresas;

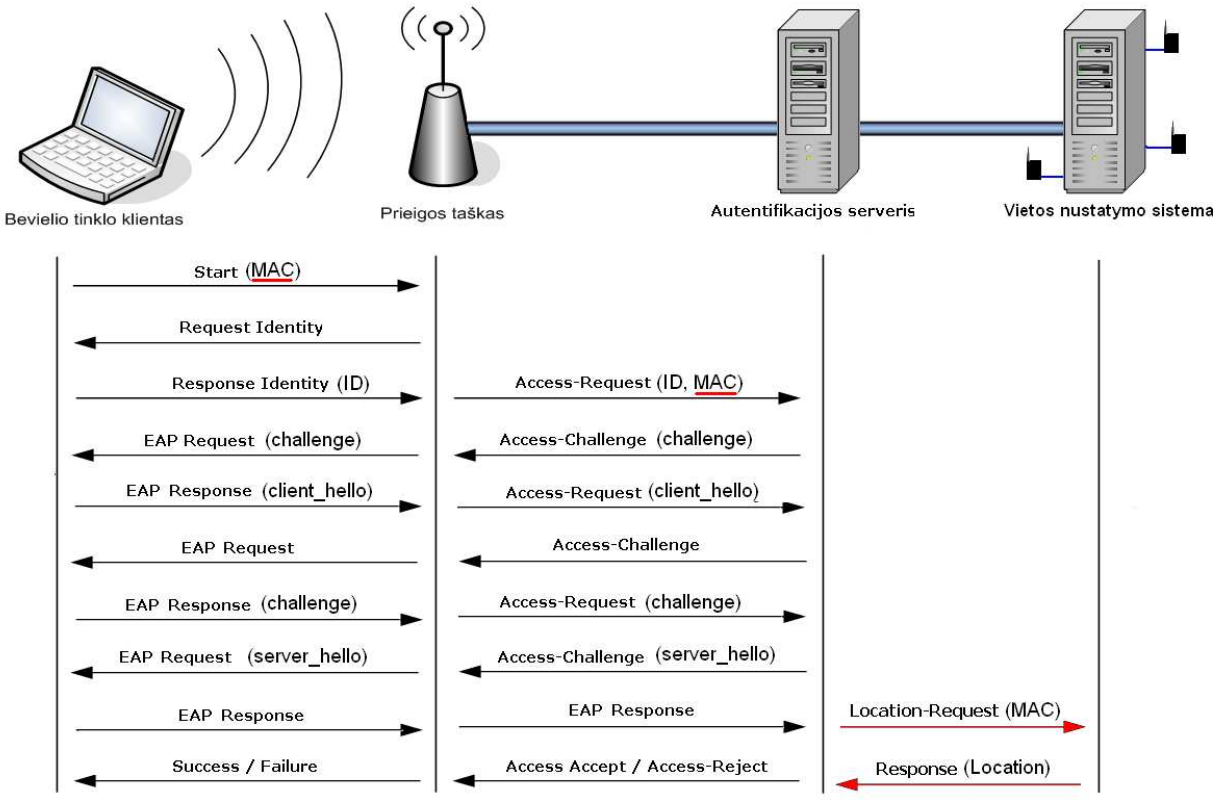
challenge – iššūkio reikšmė;

client_hello – nuo iššūkio priklausomas vartotojo įrodymas, kad jis žino slaptažodį ir turi privatųjį raktą (tai galėtų būti tik slaptažodžio su iššūkio reikšme santrauka);

server_hello – serverio įrodymas, kad jis žino slaptažodį ir savo privatųjį raktą (reikšmė priklauso nuo vartotojo atsiųsto iššūkio);

Location – vartotojo vietos informacija (koordinatės ir paklaida).

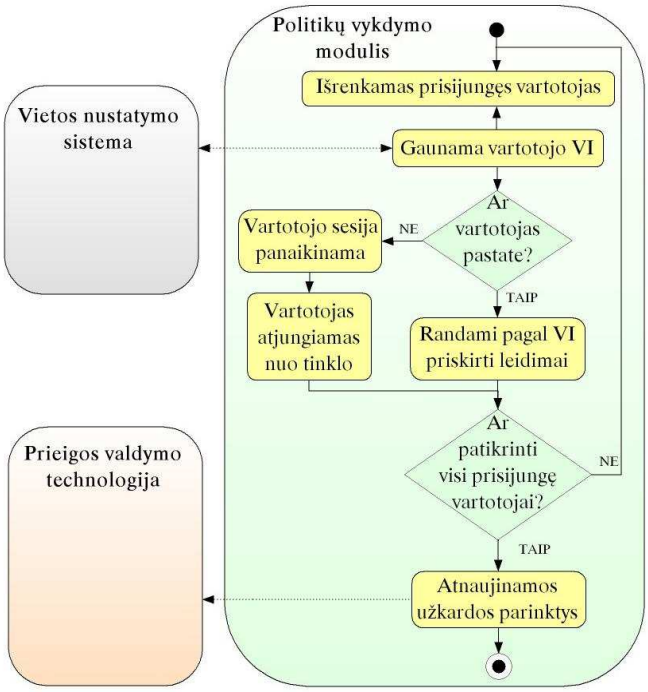
Kaip parodyta paveikslėlyje, iš pradžių prieigos taškas paprašo, kad vartotojas atsiųstų savo identifikacijos duomenis, ir nuo to momento veikia tik kaip tarpininkas tarp vartotojo galinio įrenginio ir autentifikacijos serverio. Visus iš vartotojo gautus paketus jis įpakuoja ir siunčia Autentifikacijos serveriui pagal AAA protokolą saugiu kanalu. Kanalas tarp vartotojo (paveikslėlyje vadinamas Bevielio tinklo klientu) laikomas nesaugiu. Po to, kai Autentifikacijos serveris įsitikina, kad vartotojui galima suteikti prieigą, jis apskaičiuoja raktus, kurių pagalba vartotojas ir prieigos taškas galės saugiau komunikuoti, tam galės bus naudojamas saugus protokolas, pavyzdžiui, IKE (angl. *Internet Key Exchange*) protokolas. Autentifikacijos serveris raktą nusiunčia prieigos taškui, o vartotojas pats apsiskaičiuoja raktą (raktas išvedamas iš vartotojui ir autentifikacijos serveriui žinomų duomenų). 23 paveikslėlyje pavaizduoti ne visi duomenų srautai. Prieš pradedant abipusę autentifikaciją, Autentifikacijos serveris susitaria su vartotoju dėl naudojamo EAP autentifikacijos metodo.



26 pav. Autentifikacijos pagal vietą duomenų srautų diagrama

Kaip pavaizduota 26 paveikslėlyje, naudojamas autentifikacijos metodas nuo standartinio EAP-LEAP metodo skiriasi tik tuo, kad prieš grąžindamas vartotojui pranešimą apie sėkmingą autentifikaciją autentifikacijos serveris kreipiasi į vietos nustatymo sistemą, gauna vartotojo vietos informaciją ir pagal ją patikrina VI pagrįstus požymius, kurie turi būti patvirtinti (paveikslėlyje pažymėta raudonai). Pavyzdžiui, gali būti patikrinamas erdvinis požymis, ar vartotojas yra universiteto pastate, arba, ar jis yra savo darbo kabinete. Patvirtinus, leistinus erdvinius požymius, vartotojui pranešama apie sėkmingą autentifikaciją ir jis prijungiamas prie bevielio tinklo.

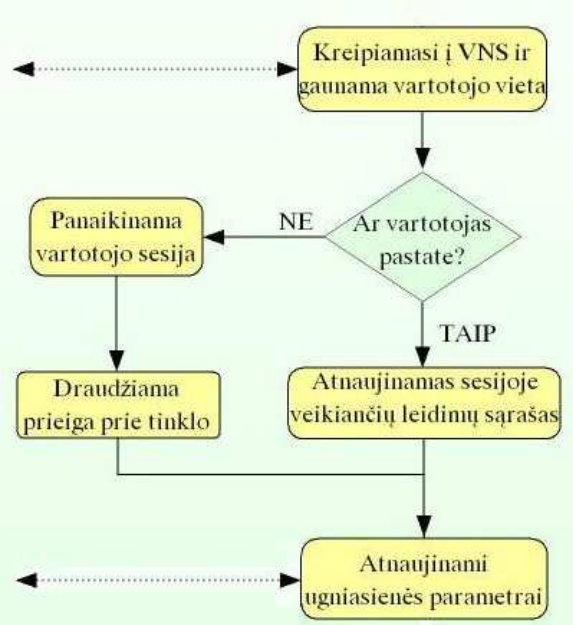
27 paveikslėlyje pavaizduotas politikų vykdymo algoritmas. Jis vykdomas nustatytais laiko intervalais, pavyzdžiui kas 3 minutes. Kaip parodyta, prieš atnaujinant vartotojui priskirtų leidimų sąrašą, patikrinama, ar vartotojas yra pastato viduje. Kadangi vartotojas už pastato ribų negalės atlikti nei vieno erdvinės rolės, šis požymis patikrinamas prieš visus kitus.



27 pav. Politikų vykdymo seka

Po autentifikacijos algoritmo iškart turi būti atliekamas ir prieigos valdymo algoritmas, skirtas vienam vartotojui, nes autentifikuotas vartotojas turi būti kuo greičiau autorizuotas ir užkarda turi būti atnaujinta taip, kad leistų vartotojui naudotis jam skirtais bevielio tinko resursais. Kad taip įvyktų po autentifikacijos turi būti atliekami keli svarbūs veiksmai:

suteiktų leidimų nustatymas ir priskyrimas vartotojui pagal jo atliekamas erdvines roles. Šie veiksmai išskirti 28 paveikslėlyje.



28 pav. Prieigos valdymo algoritmo seka

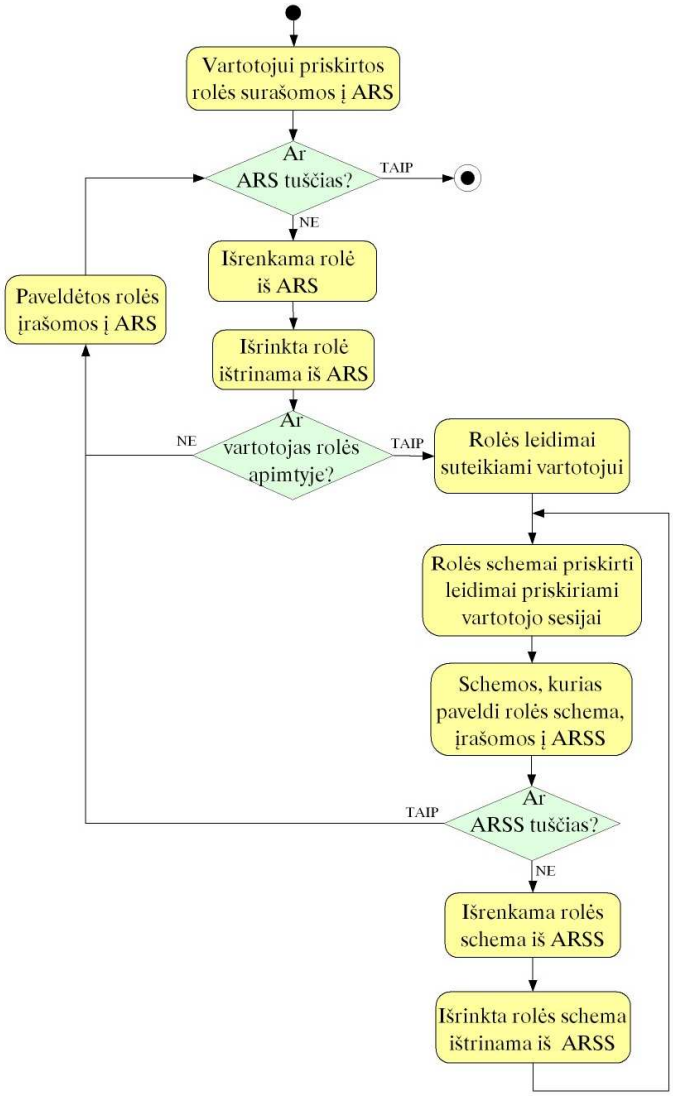
Iš visų 28 paveikslėlyje pavaizduotų autorizacijos veiksmų sudėtingesnis yra sesijoje veikiančių leidimų sąrašo atnaujinimas, nes šio veiksmo metu nustatoma, kokias roles vartotojas gali atlikti. 29 paveikslėlyje šis veiksmas yra pavaizduotas detaliau.

Kaip parodyta, iš pradžių sudaromas vartotojui priskirtų rolių (jos identifikuojamos pagal rolės ID) sąrašas (aktyvių rolių sąrašas – ARS), kuris vėliau papildomas įrašant paveldėtas roles, bet kartu iš sąrašo patikrintos rolės ir trinamos. Rolė iš sąrašo ištrinama prieš įrašant į sąrašą jos paveldėtas roles ir prieš patikrinant ar vartotojas, ją gali atlikti (ar vartotojui būdingi erdviniai požymiai, kurie priskirti tai rolei).

Jei nustatoma, kad vartotojas tą erdvinę rolę gali atlikti, rolei priskirti leidimai priskiriami vartotojo sesijai (kitaip dar galime sakyti, vartotojui). Tada analizuojamos rolių schemos. Pasirinktosios veikiančios rolės schemai priskirti leidimai priskiriami vartotojo sesijai. Schemos paveldėtos schemos surašomos į aktyvių rolių schemų sąrašą (ARSS). Jei sąrašas ne tuščias, schemos iš eilės yra renkamos ir trinamos iš sąrašo, priskiriant jų leidimus vartotojo sesijai ir tikrinant, ar nėra daugiau paveldėjamų schemų, kurias galima būtų įrašyti į ARSS.

Toks tikrinimas nutraukiamas tada, kai ARSS nebelieka įrašytų schemų (visos būna jau patikrintos ir ištrintos), tada toliau nagrinėjamos rolės iš ARS, kol visos patikrinamos ir ištrinamos.

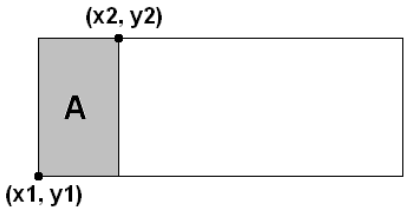
Aprašytas algoritmas užtikrina, kad būtų įvertinta vartotojo vieta, jam priskirtos rolės ir rolių bei rolių schemų hierarchija. Tik įvertinus visus šiuos dalykus gali būti priskirtas teisingas leidimų sąrašas vartotojo sesijai. Kaip pavaizduota Politikų vykdymo algoritmo sekoje, tik sudarius / atnaujinus leidimų sąrašus visų aktyvių vartotojų sesijoms, atnaujinami užkardos parametrai.



29 pav. Leidimų išrinkimas pagal erdvinius požymius

Iš visų 29 paveikslėlyje pateiktų veiksmų detaliau aptarsime, kaip nustatoma, ar vartotojas yra rolės apimtyje. Kaip jau minėta 3.3 ir 3.4 skyreliuose, kiekviena rolė, kuri gali būti priskirta vartotojui, turi savo apimtį – erdvinį požymį. Vartotojas gali atlikti tą rolę tik tada, kai patvirtinamas tas erdvinis požymis, pavyzdžiui, nustatoma, kad vartotojas yra Kompiuterių tinklų katedroje. Kadangi projektuojamoje sistemoje kiekvienas požymis yra stačiakampė arba iš stačiakampio formos zonų (praktiškai patalpų ar patalpų dalių) sudaryta

zona, naudojama tik viena VNS pateikiamos vietos informacijos ir erdvinio požymio susiejimo funkcija. Duomenų bazėje saugomi šie duomenys apie zonas: aukštas – kuriame aukšte zona yra, X1 – apatinio kairio kampo x koordinatė, Y1 – apatinio kairio kampo y koordinatė, X2 – viršutinio dešinio kampo x koordinatė, Y2 – viršutinio dešinio kampo y koordinatė (žr. pav. 30).



30 pav. Duomenys apie zonas

Užklausus vartotojo vietos informacijos, vietos nustatymo sistema grąžina vartotojo galinio įrenginio koordinates (x, y) ir aukšto numerį, kuriame yra vartotojas. (x, y) yra tokios pat santykinės koordinatės, kuriomis žymimos zonos. Taigi norint nustatyti, ar vartotojas yra rolės zonoje, turi būti patikrinta ši sąlyga: $(a0=a1) \wedge (x0>x1) \wedge (y0>y1) \wedge (x0<x2) \wedge (y0<y2)$. a0 yra aukšto, kuriame yra vartotojas, nr., a1 – aukšto, kuriame yra zona, nr., (x0, y0) – vartotojo santykinės koordinatės. Jei sąlyga tenkinama, vartotojas yra nagrinėjamoje zonoje. Taip patikrinamos visos rolės erdvinį požymį sudarančios zonos. Jei vartotojas nėra nei vienoje iš jų, laikoma, kad vartotojas nėra rolės apimtyje ir tos rolės atlikti negali. Tokiu atveju 29 paveikslėlyje parodytos algoritmo sekos elementas „Ar vartotojas rolės apimtyje?“ pateiks atsakymą **NE**.

4.8 Panaudotos techninės ir programinės įrangos specifikacija

Tyrimo sistemos kūrimui buvo panaudota atviro kodo programinė įranga. Buvo suprojektuotas prieigos valdymo serveris ir paleistas kompiuteryje su Linux Ubuntu operacine sistema. Serverio ir kliento programa parašytos C programavimo kalba. Serveris sukonfigūruotas taip, kad reikalingus duomenis apie vartotoją, roles ir erdvinius požymius gautų iš MySQL duomenų bazės. Serverio programai buvo panaudota libevent biblioteka, leidžianti serveriui paleisti metodus įvykus tokiems įvykiams, kaip rašymas į tam tikrą prievadą (`event` tipo įvykis, kuris įvyksta, kai kliento programa kreipiasi į serverio programą) ir tam tikro laiko tarpo praėjimas (`evtimer` tipo įvykis, kuris įvyksta po nustatyto laiko tarpo) Taip pat buvo parašytos kelios programos, skirtos sistemos testavimui.

Suprojektuotą sistemą sudaro prieigos valdymo serverio funkcijas imituojanti programa ir sąsajai su vartotoju skirta kliento programa. Sistema buvo išbandyta tokiu būdu: paleidžiama kliento programa, kuri paprašo įvesti vartotojo prisijungimo duomenis: ar vartotojas nori prisijungti, ar atsijungti, vardą, slaptažodį ir MAC adresą. Jei buvo nurodyta,

kad vartotojas nori jungtis prie tinklo, kliento programa kreipiasi į serverį, kuris patikrina vartotojo duomenis; jei jie tinka, nuskaito iš failo (jis atitiktų modelyje pažymėtą VNS) vietos informaciją pagal gautą MAC adresą. Pagal nuskaitytos vietos informacijos patikimumo reikšmę nustatoma, ar vietos informacija negali būti nustatyta, ar ji nustatyta pakankamai gerai, ar reikia nuskaityti vietos informaciją dar kartą. Jei vietos informacija yra patikima, pritaikant susiejimo funkciją, patikrinami erdviniai požymiai ir pagal tai išrenkamos veikiančios rolės. Rolės arba leidimai yra įrašomi į vartotojo sesiją. Priskirti vartotojui leidimai yra surašomi į kitą failą (jis atitinka modelyje pavaizduotą Užkardą). Serverio programa kiekvieno prisijungimo bandymo metu atsiunčia kliento programai atsakymą, ar klientui prieiga buvo leista, ar ne. Vartotojo sesija naikinama tada, kai vartotojas nurodo kliento programai, kad nori atsijungti nuo tinklo ir ši perduoda informaciją serverio programai. Kadangi pagal saugos politiką vartotojas gali naudotis tinklo resursais tik būdamas universiteto pastate, sesija naikinama ir tada, kai nepatvirtinamas buvimo universiteto pastate požymis *KTU*. Testavimo metu nustatyta, kad serverio ir kliento programa veikia tinkamai, vartotojai teisingai autentifikuojami pagal prisijungimo duomenis ir vietos informaciją, jiems teisingai priskiriami leidimai. Kliento programos pagalba vartotojas gali imituoti kreipimąsi į tam tikrą resursą, tuomet PVS pagal VI pagrįstus požymius leidžia arba draudžia prieigą.

4.9 Skyriaus apibendrinimas

Buvo pasiūlytas prieigos prie tinklo resursų valdymo panaudojant vietos informaciją modelis. Modelis apima aspektus, kurie įvertinami modeliuojant prieigos prie bevielio tinklo resursų valdymo sistemą, kurioje naudojama vietos informacija. Pasiūlytas modelis skiriasi nuo standartinio vietos informacijos neįvertinančio modelio tuo, kad yra papildytas vietos nustatymo sistema, vietos informacijos nustatymo kokybės lygio užtikrinimu, susiejimo funkcijomis, kurios yra skirtos skirtingų tipų erdviniams požymiams įvertinti, ir leidimų priskyrimo strategija. Taip pat į modelį buvo įtrauktas autentifikavimo pagal vietą būdas, o prieigos valdymo būdai papildyti vietos informacija. Pagal pasiūlytą modelį buvo suprojektuota prieigos prie bevielio tinklo resursų valdymo sistema. Pagal vietos informacijos nustatymo kokybės lygio užtikrinimo būdą buvo sudarytas erdvinių požymių įvertinimo algoritmas, kuriame naudojamos pasirinktos susiejimo funkcijos. Pagal leidimų priskyrimo periodiškumo strategiją buvo sudarytas erdvinių požymių tikrinimo periodiškumo algoritmas. Pagal pasirinktą prieigos valdymo modelį derinant jį su vietos informacija buvo sudarytas prieigos valdymo algoritmas. Taip pat buvo sudarytas autentifikacijos pagal vietą algoritmas.
Suprojektuota sistema buvo išbandyta sukūrus kliento ir serverio programas, imituojančias vartotoją arba prieigos tašką (nes jis yra tarpininkas tarp vartotojo ir PVS) ir prieigos valdymo

serverį. Bandymo metu nustatyta, kad prieigos valdymo serveris veikia gerai, teisingai įvertina erdvinius požymius ir priskiria vartotojui leidimus. Bandymo metu vietoj VNS sistemos vietos informacija buvo nuskaitoma iš failo, o leidimai rašomi taip pat į failą, kuris naudojamas imituoti objektą, naudojamą tam tikros prieigos valdymo technologijos įgyvendinimui.

5 SISTEMOS TESTAVIMAS IR EKSPERIMENTINIAI TYRIMAI

5.1 Eksperimentų aplinka

Testavimas ir eksperimentiniai tyrimai buvo atliekami Pentium (R Dual-Core) 2 GHz CPU, 512 MB RAM virtualiu kompiuteriu (įdiegtas naudojant VirtualBox virtualizacijos programą) su Linux Ubuntu OS. Eksperimentinių tyrimų metu buvo paleidžiama serverio ir kliento programos, taip pat eksperimentiniams tyrimams specialiai parašytos programos, padedančios geriau valdyti serverio veikimą ir apdoroti eksperimentinių tyrimų rezultatus. Eksperimento metu faile, iš kurio nuskaitoma vietos informacija buvo 20 įrašų ir kiekvieno kreipimosi metu buvo patikrinama vidutiniškai 10 įrašų. Duomenų bazėje be saugos politikoje specifikuotų duomenų buvo įvesta 30 skirtingų vartotojų, kuriems buvo priskirtos įvairios saugos politikoje numatytos erdvinės rolės.

5.2 Eksperimentų eiga

Pirmo eksperimento metu buvo tiriama, per kiek laiko aptarnaujamos vienu metu priimtos vartotojų užklausos (užklausa gali būti autentifikacijos arba prieigos prie tam tikro resurso užklausos). Kliento programa buvo paleidžiama daug kartų vienu metu (tai atliekama komanda `./klientas & ./klientas & ./klientas` ...), tai turėtų atitikti vienu metu į prieigos valdymo serverį besikreipiančius vartotojus. Buvo tiriama, kiek vartotojų vienu metu gali kreiptis į serverį ir per kiek laiko jie bus aptarnaujami kiekvienu atveju. Tyrimo metu išmatuotas autentifikacijos modulio veikimo laikas. Prieigos prie tam tikro resurso užklausa iš esmės yra tolygi autentifikacijos užklausai ir tyrimo metu gauti rezultatai parodo ir prieigos prie resurso modulio veikimo laiką.

15 lentelė. Klientų užklausų aptarnavimo greitis

Užklausų skaičius	**Aptarnavimo trukmė**	
	Visi klientai	**1 klientas**
1	1	<1s
10	1	<1s
50	3	<1s
100	5	<1s
300	15	<1s
400	20	<1s
500	25	<1s
600	30	<1s
700	35	<1s
800	42	<1s
900	45	<1s
1000	50	<1s
1200	60	<1s
1500	75	<1s

Tyrimo rezultatai surašyti 15 lentelėje. Lentelėje surašyta per kiek laiko, kiek vienu metu besikreipiančių klientų yra aptarnaujami. Stulpelyje „visi klientai“ surašytas bendras laikas, per kurį buvo aptarnauti visi klientai. „1 klientas“ stulpelyje nurodytas laikas, per kurį buvo aptarnaujamas kiekvienas klientas atskirai. Iš šios lentelės galima pamatyti, kiek laiko ilgiausiai gali užtrukti vartotojo autentifikacija, priklausomai nuo vienu metu besijungiančių vartotojų skaičiaus.

Antro tyrimo metu buvo tiriamas kompiuterio resursų išnaudojimas prieigos valdymą atliekant su skirtingu skaičiumi prisijungusių vartotojų. Buvo tiriama modulio „Politikų vykdymas“ veikimo trukmė. Rezultatai surašyti į 16 lentelę. RES stulpelyje surašyti fizinės atminties kiekiai, skirti skirtingoms užduotims (kodui ir duomenims saugoti). VIRT stulpelyje surašyti, kiek tam tikra užduotis naudoja virtualios atminties. RAM stulpelyje – RAM atminties naudojimas. „Vykdymo laikas“ stulpelyje nurodyti atitinkamai vidutinė (gauta iš 8 reikšmių) ir maksimali politikų įvykdymo visiems vartotojams trukmės. Bandymai buvo atlikti su Pentium (R Dual-Core) 2 GHz CPU, 512 MB RAM kompiuteriu, kuriame įdiegta Linux Ubuntu operacinė sistema. Iš 15 lentelės galima matyti, kokių resursų reikia, kad pakartotinė autorizacija veiktų gautu greičiu.

16 lentelė. Politikų vykdymo išnaudojami resursai

Vartotojų kiekis	**Vidutinis vykdymo laikas, s**	**Maksimalus vykdymo laikas, s**	**RES, kb**	**VIRT, kb**	**RAM, %**
10	0,2	0,2	1652	4512	0,3
100	1,4;	1,8	1668	4512	0,3
200	3,9;	4,2	1692	4612	0,3
300	4,6;	6,0	1704	4612	0,3
500	6,5;	7.0	1740	4616	0,3
1000	13,5;	15,2	1844	4732	0,4
1500	19,8;	20,8	35,7	4782	0,4
2000	27,5	28,5	1996	4832	0,4
4000	51,5;	52,0	2316	5252	0,5
8000	110,5;	117,3	3016	5892	0,6
12000	154,6;	159,5	3622	6492	0,7
20000	260,2;	268,7	4928	7848	1,0
30000	379,7;	394,0	6564	9468	1,3

Trečio eksperimento metu buvo bandoma ištirti su kokiu procesoriumi, kiek truktų politikų vykdymas tam tikram vartotojų skaičiui. Tyrimas galėtų parodyti, ar serveris galėtų sėkmingai veikti prieigos taške, kur resursai yra riboti. Tyrimo rezultatai surašyti 17 ir 18 lentelėse. Rezultatai parodo, kiek laiko su kokiu prisijungusių vartotojų skaičiumi veikia

modulis “Politikų vykdymas”. Skirtinguose stulpeliuose surašyta, iki kiek procentų buvo apribotas CPU naudojimas atitinkamo bandymo metu serverio programos procesui. Rezultatai parodo, su kokiu CPU pajėgumu kokias politikų vykdymo trukmes galima pasiekti skirtingam vartotojų skaičiui. Lentelėse nurodytos vidutinės ir maksimalios vykdymo trukmės, apskaičiuotos iš 10 bandymų metu gautų reikšmių. Galime matyti, kad esant iki 300 prisijungusių vartotojų ir apribojus CPU iki 30 %, modulio vykdymo laikas praktiškai išlieka tas pats. Esant didesniam prisijungusių vartotojų skaičiui, vykdymo laikas praktiškai nesikeičia CPU apribojus iki 50 %.

17 lentelė. Politikų vykdymo trukmė mažam vartotojų skaičiui

Vartotojų skaičius	**5% CPU**	**10% CPU**	**20% CPU**	**30% CPU**	**40% CPU**	**50% CPU**	**70% CPU**	**100% CPU**
10	0,2	0,2	0,2	0,2	0,2	0,2	0,2	0,2
50	6,1 7,7	2,3;2,5	0,8; 0,9	0,7; 0,8	0,7; 0,8	0,7; 0,8	0,7; 0,8	0,7; 0,8
100		8,2; 9,2		1,9; 1,9	1,5; 1,6	1,4; 1,4		1,4; 1,8
300		25,0; 31,5		7,4; 9,0	4,7; 4,8	4,3; 4,4		4,6; 6,0

18 lentelė. Politikų vykdymo trukmė didesniam vartotojų skaičiui

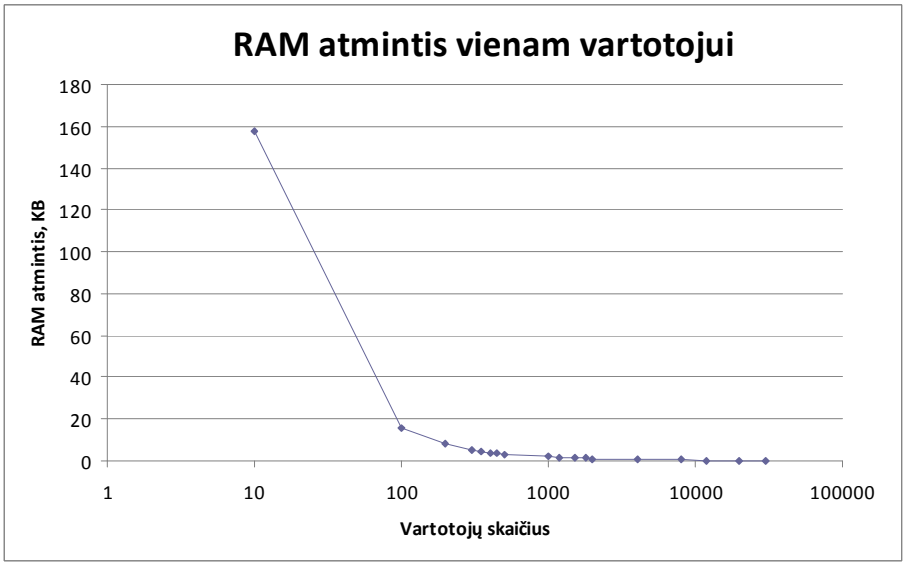
Vartotojų skaičius	**10% CPU**	**30% CPU**	**50% CPU**	**100% CPU**
500	47,3; 53,6	12,5; 14,5	6,7; 7,4	6,5; 7.0
1000	68,2; 76,7	21,6; 23,4	12,9; 13,2	13,5; 15,2
1500	157,7; 160,4	35,5; 42,2	19,8; 20,0	19,8; 20,8
2000	150,6; 207,9;	54,5; 58,6	29,6; 35,4	27,5; 28,5
4000	383,9; 408,7	111,4; 117, 7	53,5; 56,6	51,5; 52,0
8000	630,8; 648,2	252,3; 229,2	105,3; 107,1	110,5; 117,3
12000	1191,6; 1325,3;	351,8; 344,7	155,5; 158,7	154,6; 159,5

5.3 Eksperimentų rezultatai

Iš pirmo eksperimentinio tyrimo gautų rezultatų galima pastebėti, kad matuojant vieno kliento aptarnavimo laiką, gauta, kad klientas aptarnaujamas greičiau nei per 1s, nepriklausomai nuo vienu metu aptarnaujamų klientų skaičiaus (žr. 15 lentelę). Tuo tarpu matuojant visų klientų aptarnavimo trukmę (žr. 15 lentelę stulpelį „Visi klientai“), gauta, kad paskutinis klientas baigiamas aptarnauti vėliau nei po 1 min. nuo pirmo kliento aptarnavimo pradžios. Ir pirmas ir paskutinis klientas (visi klientai), atliekant eksperimentą, iš tikro užklausas pateikia vienu metu. Vadinasi, galime sakyti, kad iš tikro jų aptarnavimo pradžia sutampa, bet skiriasi tik pabaigos laikas. Tokiu būdu galime daryti išvadą, kad paskutiniam

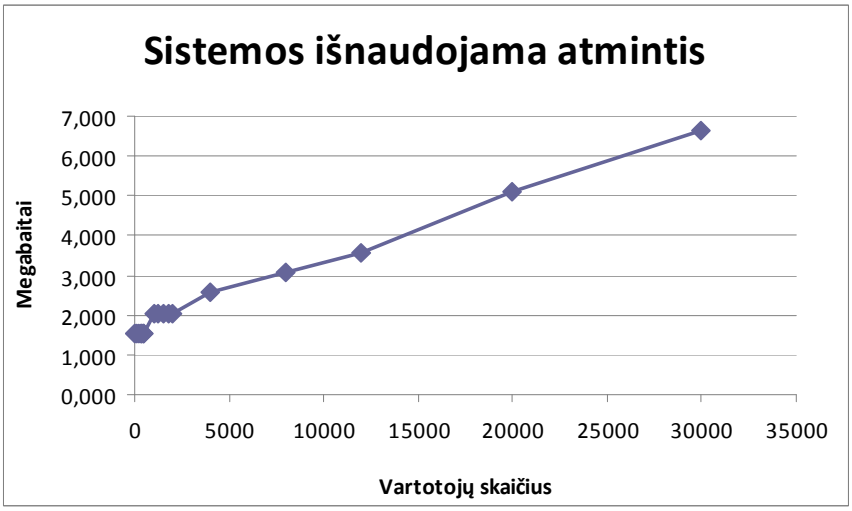
klientui, gali reikti laukti ilgiau nei vieną minutę nuo užklausos pateikimo, jei tuo pačiu metu užklausas pateikia iš viso 1500 klientų. Iš 15 lentelės matosi, kad jei užklausas vienu metu pateikia 500 klientų, jų aptarnavimas baigiamas po 30s. Tai reiškia, kad bent vienam klientui teko laukti 30 s, kol jo užklausa bus aptarnauta. Iš to matosi, kad „Visi klientai“ ir „1 klientas“ stulpeliuose gauti rezultatai prieštarauja vienas kitam. Toks rezultatų neatitikimas gali būti paaiškinamas tuo, kad net ir vienu metu visiems klientams pradėjus vykdyti užklausą, vis dėl to kompiuteris jas priima ne visai tuo pačiu metu. Nors klientų užklausos pateikiamos vienu metu ir turėtų veikti lygiagrečiai, jos pradedamos viena po kitos ir anksčiau pradėtos užklausos baigiamos anksčiau, o vėliau pradėtos – vėliau. Tai galima paaiškinti tuo, kad eksperimento metu klientų užklausų paleidimui naudojamas tik vienas procesorius, todėl jos vykdomos tik iš dalies lygiagrečiai. Antrasis bandymas yra tikslesnis ir atskleidžia tikresnius rezultatus tiriant vartotojų užklausų aptarnavimo trukmę. Iš antro bandymo metu gautų rezultatų matome, kad vartotojų užklausų aptarnavimo trukmė tiesiogiai priklauso nuo vartotojų užklausų skaičiaus Apskaičiuota vieno kliento užklausos aptarnavimo (nuo užklausos pateikimo iki prieigos suteikimo) trukmė yra 0,05 s. Per 7 s serveris gali atsakyti į atsakyti į 500 klientų prieigos užklausas.

Iš antro ir trečio eksperimentinių tyrimų metu gautų rezultatų galima nubrėžti 31-35 paveikslėliuose pateiktas diagramas.

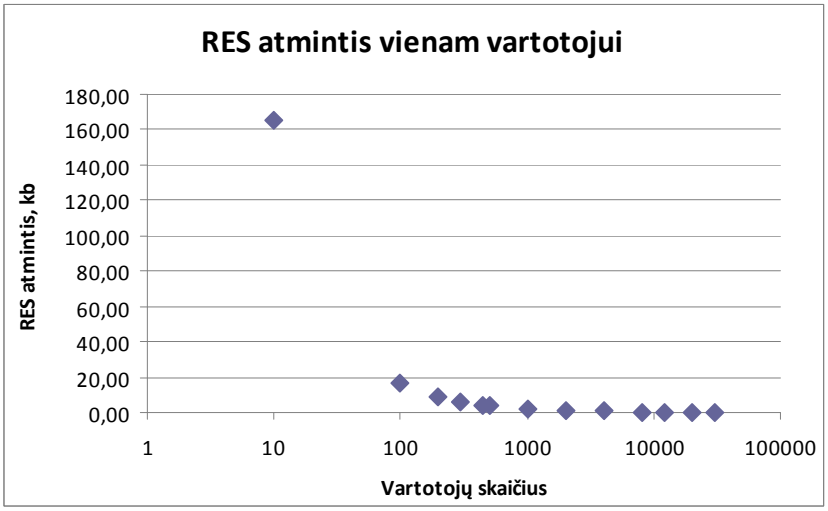


31 pav. RAM ištekliai vieno kliento aptarnavimui

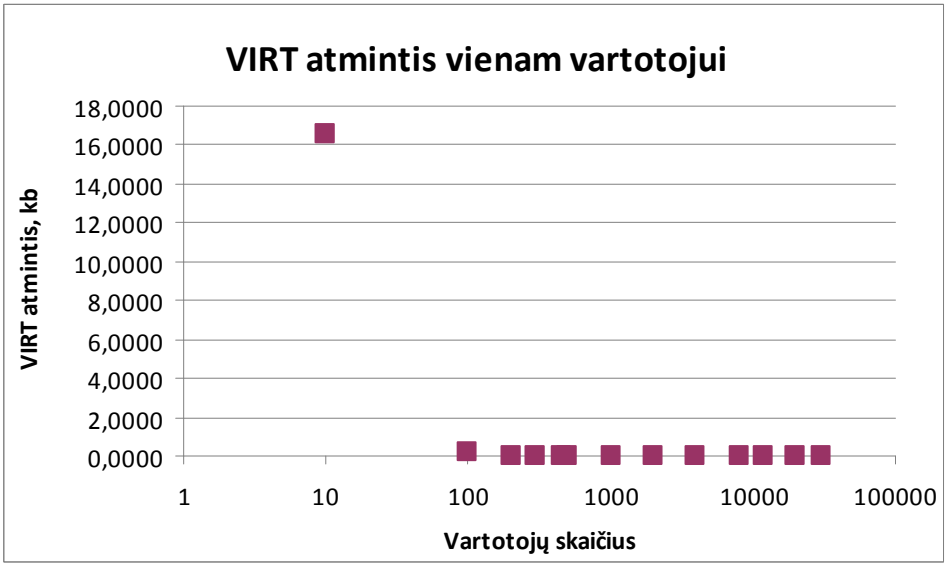
31 paveiksle pavaizduota vienam klientui skirtų RAM išteklių priklausomybė nuo aptarnaujamų vartotojų skaičiaus. Iš brėžinio matosi, kad atminties kiekis, reikalingas aptarnauti vieną klientą didėja nežymiai.



32 pav. Politikų vykdymui naudojama atmintis



33 pav. Rezervuotos atminties kiekis, tenkantis vienam klientui



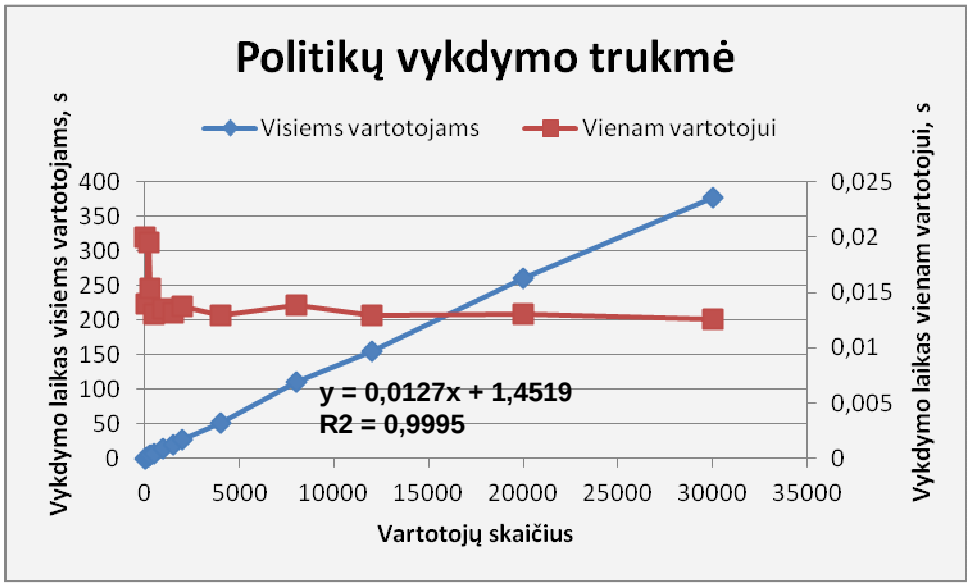
34 pav. Virtualios atminties kiekis, tenkantis vienam klientui

32 paveikslėlyje pavaizduota politikų vykdymui skiriamos atminties priklausomybė nuo vartotojų skaičiaus. Iš grafiko matosi, kad sistemos atminties išnaudojimas tiesiškai priklauso nuo vartotojų skaičiaus. Atlikus eksperimentą su 30 tūkstančių vartotojų nustatytas 6,656 MB atminties išnaudojimas. Lyginant net su šiuolaikinių mobiliųjų įrenginių resursais tai yra labai mažas reikalingos atminties kiekis.

33 ir 34 paveikslėliuose pavaizduota skirtingų rūšių atminties kiekio, tenkančio vienam vartotojui, priklausomybės nuo aptarnaujamų vartotojų kiekio. Galima daryti išvadą, kad kuo daugiau vartotojų reikia aptarnauti, tuo mažiau atminties sunaudojama kiekvieno iš vartotojų.

35 paveikslėlyje pavaizduota politikų vykdymo trukmė esant skirtingam vartotojų skaičiui. Grafike matosi, kad politikų vykdymo (leidimų atnaujinimo pagal erdvinius požymius) laikas tiesiškai priklauso nuo vartotojų skaičiaus, ir augant vartotojų skaičiui vieno vartotojo aptarnavimo laikas išlieka pastovus –apie 120 - 130 milisekundžių. Ištirtas Politikų vykdymo modulis projektuojamoje sistemoje yra skirtas patikrinti VI pagrįstus požymius ir pagal juos iš naujo priskirti leidimus visiems prisijungusiems vartotojams. Šis modulis vykdomas periodiškai, numatoma, jį vykdyti kas 3 min. Reikia paminėti, kad sistemoje yra numatytas vartotojų užklausų kiekvienam atskiram resursui priėmimas ir VI požymių įvertinimas prieigos leidimui suteikti. Kitaip sakant, sistemoje yra atskiras mechanizmas priimantis vartotojų užklausas ir nustatantis leidimą kiekvienai užklausai, todėl nuo šio modulio nepriklauso tai, ar vartotojui bus laiku suteikta prieiga prie resurso, prie kurio pagal VI pagrįstus požymius ji turi jam būti suteikta. Nuo šio modulio priklauso tik tai, ar vartotojui bus laiku blokuota prieiga prie tam tikrų resursų pasikeitus VI pagrįstiems požymiams. Dėl minėtų priežasčių nėra labai svarbu, kad tirtas politikų vykdymo modulis, įsijungiantis kas 3 min., veiktų labai greitai. Svarbu yra tai, kad jis netrukdytų klientų užklausų aptarnavimui. Prieigos valdymo sistema buvo realizuota taip, kad minėtas modulis ir užklausų aptarnavimo modulis vykdomi vienas po kito, o ne lygiagrečiai. Tokiu atveju politikų vykdymas turi veikti ne ilgiau kaip kokias 7 s, kad klientams nereiktų ilgai laukti, kol jų užklausos bus vėl aptarnaujamos. Galima daryti išvadą, kad sistema kokybiškai gali aptarnauti iki 500 vartotojų. Jei vartotojų skaičius didesnis, vidutinis politikų vykdymo laikas, o kartu ir klientų neaptarnavimo laikas, išauga. Norint sistemą naudoti 1000 ar daugiau prisijungusių vartotojų prieigos valdymui, reikėtų didinti sistemos skaičiavimo pajėgumus (CPU) arba optimizuoti prieigos valdymo algoritmus. Kad politikų vykdymo modulis netrukdytų užklausų aptarnavimui, reiktų jį paleisti kaip atskirą procesą ir serverio resursus visų pirma skirti klientų užklausų aptarnavimui, o minėtą modulį vykdyti tik tada, kai resursų nereikia klientų

užklausų aptarnavimui. Serverio darbui naudojant du procesus reikėtų papildomai spręsti, kaip išsaugoti tų duomenų, kuriuos abu procesai gali keisti vienu metu, vientisumą.



35 pav. Politikų vykdymo trukmė.

5.4 Skyriaus apibendrinimas

Buvo atlikti trys eksperimentai, kurių metu ištirta klientų užklausų (autentifikacijos arba prieigos prie resursų) aptarnavimo trukmė, „Politikų vykdymas“ modulio vykdymo trukmė ir išnaudojami kompiuterio resursai. Gauti rezultatai parodė, kad suprojektuota sistema, veikianti Pentium (R Dual-Core) 2 GHz CPU, 512 MB RAM serveryje gali kokybiškai aptarnauti iki 500 vienu metu prisijungusių klientų. Klientų užklausų aptarnavimas veikia pakankamai greitai ir vienas klientas aptarnaujamas per maždaug 0,05 s, jei tuo metu nevykdomas kas 3 min. atliekamas politikų vykdymo modulis. Kad politikų vykdymo modulis netrukdytų klientų aptarnavimui jį reikėtų paleisti atskirame procese ir skirti likusius nuo užklausų aptarnavimo serverio resursus. Kaip bebūtų gauti rezultatai neparodo, kaip greitai veiktų sistema, jei vietos informaciją skaitytų ne iš failo, o gautų iš vietos nustatymo sistemos. Tokiu atveju prie gautų užklausų aptarnavimo ir politikų vykdymo trukmių prisidėtų ir vietos nustatymo bei komunikacijos tarp PVS ir VNS trukmės.

Prieigos valdymo sistemos veikimo sparta galėtų dar būti ištirta su didesniu duomenų bazėje įvestų duomenų skaičiumi. Galima būtų atlikti tuos pačius bandymus su žymiai didesniu vietos informacijos įrašų skaičiumi faile ir nustatyti įrašų perrinkimo trukmę.

6 IŠVADOS

1. Atlikta autentifikacijos mechanizmų bevieliuose tinkluose analizė parodė, kad patikimiausias autentifikavimo būdas yra paremtas EAP protokolu. WEP algoritmo autentifikacija yra pažeidžiama dėl silpno slapto rakto. VPN gali užtikrinti saugią autentifikaciją, tačiau nėra bevieliams tinklams taikytinas sprendimas.
2. Atlikta prieigos valdymo mechanizmų analizė parodė, kad bevieliam tinklui, kaip ir kitos rūšies tinklams, gali būti pritaikomas bet koks prieigos valdymo modelis. Prieigos valdymo modelis pasirenkamas pagal informacinės sistemos paskirtį, dydį, struktūrą, vartotojų veiklos pobūdį, reikalingą saugumo lygį. Projektuojamai KTU Informatikos fakulteto prieigos prie bevielio tinklo resursų valdymo sistemai parinktas role pagrįstas prieigos valdymas.
3. Atlikta autentifikavimo ir prieigos prie bevielio tinklo resursų valdymo būdų derinimo su vietos informacija galimybių analizė parodė, kad vietos informacija gali būti panaudota pakeisti arba papildyti standartinius autentifikacijos ir prieigos valdymo metodus taip padidinant saugumą ir teisingos autentifikacijos tikimybę. Projektuojant ir realizuojant šiuos sprendimus, reikalingi architektūriniai projektuojamos sistemos papildymai, vietos informacija pagrįstų požymių įvertinimas.
4. Atlikus prieigos prie bevielio tinklo resursų valdymo būdų, grįstų vietos informacija, analizę, nustatyta, kad nėra bendro modelio / būdo siūlančio, kaip projektuojant pasirinkti sistemos, prieigos prie bevielio tinklo išteklių valdymui naudojančios vietos informaciją, architektūrą, vietos informacija pagrįstus požymius, jų tipus bei įvertinimo būdą ir leidimų priskyrimo periodiškumo strategiją.
5. Darbe pasiūlytas apibendrintas prieigos prie tinklo resursų valdymo, grįsto vietos informacija, modelis, leidžiantis derinti įprastinius autentifikavimo ir prieigos prie bevielio tinklo išteklių valdymo mechanizmus su vietos informacija.
6. Pasiūlyto modelio pagrindu suprojektuotas erdviniais požymiais ir rolėmis pagrįsto prieigos prie bevielio tinklo resursų valdymo kelių aukštų pastato viduje sistemos prototipas, apibrėžiantis rolėmis bei erdviniais požymiais pagrįstą prieigos valdymą, autentifikaciją pagal vietos informaciją, leidimų priskyrimą pastoviais laiko intervalais ir erdvinių zonos tipo požymių įvertinimą
7. Darbe pristatyti prieigos valdymo, naudojančio vietos informaciją, išplėtimai: autentifikacijos ir politikų vykdymo algoritmų papildymai, erdvinių požymių tikrinimo periodiškumo algoritmas, erdvinių požymių įvertinimo algoritmas ir reikalingos duomenų

struktūros. Sudaryta vietos informacija pagrįsto prieigos prie bevielio tinklo išteklių valdymo sistemai skirta saugos politika.

8. Pasiūlyta prieigos prie bevielio tinklo resursų valdymo sistema ištestuota. Gauti rezultatai parodė, kad ji veikia teisingai. Jos savybės ištirtos eksperimentiniu būdu. Tyrimais nustatyta, kad sistema, veikianti Pentium (R Dual-Core) 2 GHz CPU, 512 MB RAM kompiuteryje, gali kokybiškai ir greitai aptarnauti iki 500 prisijungusių prie tinklo klientų. Taip pat nustatyta, kad klientai būtų aptarnaujami greičiau, jei politikų vykdymo modulis ir užklausų aptarnavimas veiktų atskiruose procesuose ir klientų užklausų aptarnavimui būtų suteikta pirmenybė naudotis serverio resursais.
9. Modelį galima būtų praplėsti įtraukiant į jį ir kitokius VI pagrįstų požymių tipus, tokius kaip vietinis tankis, atstumas, zonos tankis. Ateities darbai galėtų būti tam tikro WPA-EAP autentifikacijos metodo, prieigos valdymo technologijos realizacijos ar tam tikros vietos nustatymo sistemos integravimo / suderinimo su pasiūlytu modeliu tyrimai.

LITERATŪRA

[1] Test attack WPA-PSK and WPA2-PSK by using pyrit. *Tech.Viewz.org* – [žiūrėta 2009-12-10]. Prieiga per internetą: <http://techviewz.org/2009/04/test-attack-wpa-psk-and-wpa2-psk-by.html>

[2] 802.1x White Paper. *Allied Telesi*, 2006.

[3] **R. S. Turnbull, R. Gedge**. (WO/2006/103387) Location Based Authentication. *PATENTSCOPE*, 2006.

[4] Galileo - What do we want to achieve. *European Commission Enterprise and Industry* – [žiūrėta 2009-12-10]. Prieiga per internetą: <http://ec.europa.eu/enterprise/policies/space/galileo/index_en.htm>

[5] **J. Vollbrecht, R. Moskowitz**, Wireless LAN Access Control and Authentication. *Interlink Networks Inc.*, 2002.

[6] **O. Cheikhrouhou, M. Laurent, A. B. Abdallah, M. B. Jemaa**. An EAP-EHash authentication method adapted to resource constrained terminals. *Institut TELECOM and Springer-Verlag*, 2009.

[7] **C. A. Ardagna, M. Cremonini, S. De Capitani di Vimercati, P. Samarati**. Access Control in Location-Based Services. *Privacy in Location-Based Applications: Research Issues and Emerging Trends, Springer-Verlag*, 2009, 106 – 126 psl.

[8] **C. A. Ardagna, M. Cremonini, S. De Capitani di Vimercati, P. Samarati**. Privacy-enhanced Location-based Access Control. *The Hand-book of Database Security: Applications and Trends, Springer-Verlag*, 2007.

[9] **A. Mishra, S. Banerjee**. Secure Spaces: Location-based Secure Wireless Group Communication. *POSTER SESSION: Special feature on MobiCom 2002 posters, ACM*, 2003, 68 – 70 psl.

[10] **Y. S. Cho, L. Bao, M. Goodrich**. Secure Access Control for Location-Based Applications in WLAN Systems. *Proceedings of the 3rd IEEE International Conference on Mobile Adhoc and Sensor Systems*, 2006.

[11] **M. Kappes, S. Garg, M. Mani** US Patent 7403773 - Location-based access control for wireless local area networks. 2008.

[12] **I. Ray, M. Kumar**. Towards a Location-Based Mandatory Access Control Model. *Computers & Security*, 25(1), 2006.

[13] **C. A. Ardagna, M. Cremonini, E. Damiani, S. De Capitanidi Vimercati, P. Samarati**. Supporting Location-Based Conditions in Access Control Policies. *Proceedings of the 2006 ACM Symposium on Information, Computer and Communication Security*, 2006.

[14] **R. Bhatti, M. L. Damiani, D. W. Bettis, E. Bertino.** Policy Mapper: Administering Location-Based Access-Control Policies. ***IEEE Internet Computing***, 2008.

[15] **V. Kolovski, J. Hendler, B. Parsia**. Analyzing Web Access Control Policies. *Proceedings of the 16th International Conference on World Wide Web*, 2007, 677 – 686 psl.

[16] **J. Ligatti, B. Rickey, N. Saigal**. LoPSiL: A Location-based Policy-specification Language. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering , Volume 17, Springer Berlin Heidelberg*, 2009.

[17] [žiūrėta 2009-12-10]. Prieiga per internetą: <http://www.flickr.com/photos/redhatmagazine/481929076/sizes/o/>

[18] **M. L. Damiani, E. Bertino, B. Catania, P. Perlasca**. GEO-RBAC: A Spatially Aware RBAC. *ACM Transactions on Information Systems and Security*, 2006.

[19] Fingerprint recognition and mobile security. ***A Farpoint Group White Paper***, 2008, Document FPG 2008-435.1.

[20] **R. Plėštys, D. Rimkus, I. Lagzdinytė, N. Sarafinienė**. Tinklų sauga. *Mokomoji knyga*, 2008.

[21] **R. Plėštys, D. Rimkus, I. Lagzdinytė, N. Sarafinienė**. Kompiuterių tinklų sauga. *Mokomoji knyga*, 2008.

[22] **N. Sastry, U. Shankarand, D. Wagner**. Secure Verification of Location Claims. *Proceedings of ACM Workshop on Wireless Security*, 2003.

[23] **Y. Zhang, W. Liu, W. Lou, Y. Fang**. Securing Sensor Networks with Location-Based Keys. *IEEE Wireless Communications and Networking Conference*, 2005.

[24] **B. Watersand, E. Felten**. Proving the Location of Tamper Resistant Devices. *Technical report, Princeton University*, 2003.

[25] **M. Beck, E. Tews**. Practical attacks against WEP and WPA. *Proceedings of the second ACM conference on Wireless network security*, 2009.

[26] **C. Rigney, S. Willens, Livingston, A. Rubens, Merit, W. Simpson, Daydreamer.** Remote Authentication Dial In User Service (RADIUS). *The Internet Engineering Task Force (IETF), Request for Comments: 2865*, 2000 [žiūrėta 2010-03-10]. Prieiga per internetą: http://www.flickr.com/photos/redhatmagazine/481929076/sizes/o/

[27] **S. Ganu, A. S. Krishnakumar, P. Krishnan**. Infrastructure-based location estimation in WLAN networks. *IEEE Wireless Communications and Networking Conference*. 2004.

[28] **M. Youssef, A. Agrawala**. Continuous Space Estimation for WLAN Location Determination Systems. *Proceedings of the 13th International Conference on Computer Communications and Networks*, 2004.

[28] **M. Youssef, A. Agrawala**. Continuous Space Estimation for WLAN Location Determination Systems. *Proceedings of the 13th International Conference on Computer Communications and Networks*, 2004.

[29] **A. H. Karp**. Authorization-Based Access Control for the Services Oriented Architecture. *Proceedings of the Fourth International Conference on Creating, Connecting, and Collaborating through Computing (C5)*, 2006.

[30] **D. Gollmann.** Computer Security, 3-as leidimas. *Wiley Publishing*, 2011

[31] **A. Jøsang, D. Gollmann, R. Au.** A Method for Access Authorisation Through Delegation Networks. *Proceedings of the Australasian Information Security Workshop (AISW'06), Hobart*, 2006.

[31] **OPEN GIS CONSORTIUM** Open GIS simple features specification for SQL. 1999.

[32] Lietuvos respublikos elektroninių ryšių įstatymas, 3 ir 65 straipsniai.

WIRELESS LAN LOCATION-BASED ACCESS CONTROL

Summary

Location-based Access Control LBAC techniques allow taking users' physical location into account when determining their access privileges. The analysis of possibilities of integrating location information into access control and authentication is provided. I show the advantages of using location information for authentication and access control. I present location-based access control model that can increase the probability of correct authentication. I design wireless LAN location-based access control system that is used in building of several floors. The model is compliant with OGC (Open GeoSpatial Consortium) and Geo-RBAC (the extent of RBAC model); it integrates other types of location-based features and uses the hierarchy of spatial roles. I describe the periodicity algorithm of location-based access control and design the policy enforcement algorithm that uses location mapping functions and the evaluation of confidence. The model is evaluated by testing the speed of the system and computer resources used by the system. The vulnerabilities of location-based access control are discussed in the context of sniffing, highjacking, DoS and warmhole attacks.

PRIEDAI

1 Priedas. Publikacija paskelbta „Informacinės technologijos 2011“ magistrantų ir doktorantų konferencijoje

PRIEIGOS PRIE BEVIELIO TINKLO RESURSŲ VALDYMAS, PAGRĮSTAS VIETOS INFORMACIJA

Ingrida Lagzdinytė-Budnikė[1], Rasa Petrauskienė[2]

Kauno technologijos universitetas, Kompiuterių tinklų katedra, Studentų g.50 , Kaunas,
[1]ingrida.lagzdinyte@ktu.lt, [2]rasa.petrauskiene@stud.ktu.lt

Santrauka (abstract). Šiame darbe pagrindžiamas vietos informacijos naudojimas autentifikavimo ir prieigos prie bevielio tinklo išteklių valdyme. Pristatomas pasiūlytas autentifikavimo ir prieigos valdymo modelis, pagrįstas vietos informacija. Aptariami įprastinių ir pasiūlyto autentifikavimo ir prieigos prie išteklių valdymo mechanizmų pažeidžiamumai vykdant tokias atakas kaip autentifikavimo duomenų ar MAC adreso perėmimas ir suklastojimas, kirmino skylės (angl. *Warmhole*) ir DoS atakos.

Raktiniai žodžiai: vietos informacija, autentifikacija, prieigos valdymas, bevielis tinklas, vietos informacija pagrįsta autentifikacija, vietos informacija pagrįstas prieigos valdymas, Geo-RBAC.

1 Įvadas

Autentifikacija ir prieigos prie bevielio tinklo resursų valdymas yra vienas svarbiausių dalykų užtikrinant sėkmingą bevielio tinklo naudojimą. Vartotojų autentifikacija paprastai užtikrinama šiais autentifikavimo mechanizmais:

1. paremtais žinoma informacija (pavyzdžiui, slaptažodžiai, PIN kodai);
2. priklausomais nuo turimų priemonių (pvz., kriptografinės kortelės, skaitmeniniai sertifikatai);
3. paremtais informacija, išvesta remiantis vartotojo individualiosiomis savybėmis (pvz., įvairūs biometriniai metodai - atpažinimas pagal piršto antspaudus, akies rainelę, net DNR seką).

Kiekvienas iš šių metodų yra pažeidžiamas. Derinant šiuos standartinius autentifikavimo mechanizmus su vietos informacija, galima pasiekti didesnį saugumą. Autentifikacija, paremta vien vietos informacija, gali būti patogesnė už minėtus mechanizmus, vartotojui nereiktų įvedinėti slaptažodžio ar pateikti biometrinių duomenų, užtektų būti tam tikroje vietoje, kuri paprastai yra įprasta vartotojo darbo vieta.

Moksliniuose darbuose [1, 2, 3, 4, 5, 6] yra aprašyta keletas būdų, kaip galima nustatyti mobilaus vartotojo vietą. Tobulėjant mobilioms technologijoms vietos informacija tapo svarbi prieigos valdymui ir atsiranda vis daugiau mokslinių darbų šia tema. Ardagna ir kiti [7, 8] nagrinėja, kaip į tradicinį bendrąjį prieigos valdymo mechanizmą gali būti integruojamos vietos informacija pagrįstos sąlygos, kaip jos įvertinamos ir pritaikomos. I. Ray ir M. Kumar [9] rašo, kaip formalizuoti vietos informaciją, kaip standartinio privalomojo prieigos valdymo (angl. *Mandatory Access Control*) modelio komponentus susieti su vietos informacija ir kaip vietos informacija gali būti panaudojama nustatyti, ar subjektas turi prieigą prie tam tikro objekto. Autorių siūlomas modelis yra tinkamas karinėms programoms, į kurias įeina statiniai bei dinaminiai objektai ir kuriose suteikiant prieigą turi būti įvertinta subjektų ir objektų vietos informacija. M. L. Damiani ir kiti [10] pristato Geo-RBAC – role pagrįsto prieigos valdymo (angl. *Role-based Access Control*) modelio išplėtimą įvedant į jį vietos informaciją.

Šiame darbe aiškinami vietos informacija pagrįsto prieigos valdymo privalumai, architektūra. Pristatomas rolėmis pagrįstas prieigos valdymo modelis, papildytas vietos informacija ir pritaikytas prieigos prie bevielio tinklo resursų valdymui pastato viduje. Aptariami vietos informacija grįstų prieigos valdymo sistemų pažeidžiamumai, taip pat modelio pritaikymo ir išplėtimo galimybės.

2 Autentifikavimo ir prieigos valdymo būdų derinimo su vietos informacija privalumai

Pagal [11] vietos informacija – tai elektroninių ryšių tinkluose tvarkomi duomenys, nurodantys elektroninių ryšių paslaugų naudotojo galinių įrenginių geografinę padėtį. Vietos informacija gali nurodyti bevielio tinklo vartotojo galinio įrenginio geografinę platumą bei ilgumą, aukštį, kryptį, vietos nustatymo informacijos tikslumo lygį, tinklo elementą, prie kurio galinis įrenginys yra prisijungęs ir panašiai. Naudojant vietos informaciją autentifikacijai ir prieigos valdymui, gali būti formuojama vietos informacija pagrįsta saugos politika. Žemiau pateiktos dvi saugos politikos kryptys:

- Resursai prieinami tik saugioje vietos informacija paremtoje būsenoje;

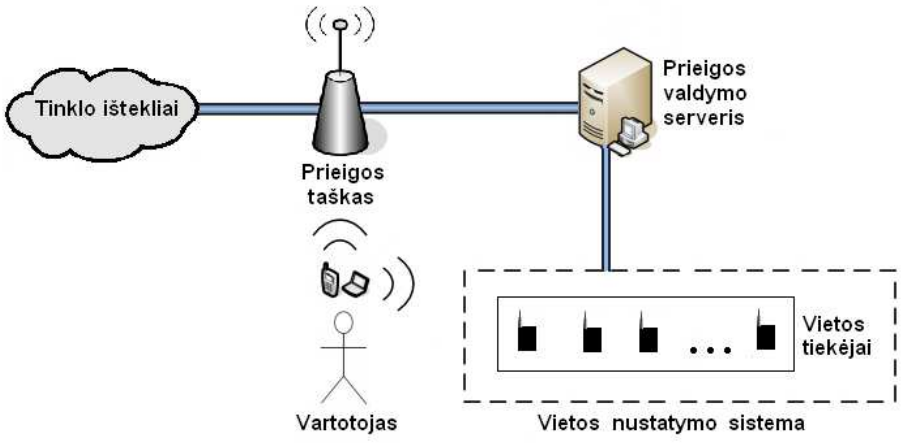
- Resursai prieinami tik tose būsenose, kuriose jie reikalingi / aktualūs.

Pirmosios krypties saugos politika neleidžia vartotojui prieiti prie resurso tokioje vietos informacija paremtoje būsenoje, kuri laikoma nesaugi naudotis tuo resursu (pavyzdžiui, ten, kur kiti neautorizuoti vartotojai gali nužiūrėti slaptus duomenis) arba nesaugi tuo, kad joje gali bandyti prieiti prie resurso nelegalūs vartotojai (saugios vietos, pavyzdžiui, gali būti kameromis stebimi kabinetai, nuo kurių raktus turi tik legalūs vartotojai, o visos kitos vietos – nesaugios). Antrosios krypties saugos politika apriboja naudojimąsi resursu taip, kad jis prieinamas tik vartotojui esant toje vietos informacija pagrįstoje būsenoje, kurioje legaliems vartotojams reikia juo naudotis. Tai gali būti daroma saugos tikslais – kuo mažesnėje teritorijoje prie resurso galima prieiti, tuo nelegaliam vartotojui bus sunkiau tai padaryti, net jei ir jis įveiks standartinį autentifikacijos mechanizmą, kuris derinamas su vietos informacija. Taigi autentifikacijos ir prieigos valdymo papildymas vietos informacija gali padidinti saugą ir tai yra susiję su prieigos vietų fizine sauga.

3 Vietos informacija pagrįsto prieigos prie bevielio tinklo resursų valdymo architektūra

Prieigos prie bevielio tinklo resursų architektūra pavaizduota 1 paveiksle. Mobilus vartotojas jungiasi prie WiFi tinklo per prieigos tašką, kuris komunikuoja su prieigos valdymo serveriu. Prieigos valdymo serveris (PVS) patikrina vartotojo prisijungimo duomenis bei vietos informaciją ir pagal tai praneša prieigos taškui, ar vartotojui leista jungtis prie tinklo išteklių, ar ne. PVS gauna vartotojo vietos informaciją iš vietos nustatymo sistemos (VNS). VNS vartotojo vietą WiFi tinkluose nustato matuojant vartotojų galinių įrenginių siunčiamų signalų stiprius (tai atlieka vietos tiekėjai) [1, 2, 3, 4] arba paketo siuntimo vartotojui trukmę [4, 5, 6].

Naudojant standartinius WiFi autentifikacijos metodus, tokius kaip WEP arba WPA-PSK, autentifikacijos serveris yra nereikalingas. Norint šiuos metodus derinti su vietos informacija, reiktų, kad visas prieigos valdymo serverio funkcijas atliktų prieigos taškas. Tai įgyvendinti būtų sudėtinga dėl prieigos taško ribotų galimybių, todėl paprasčiau naudoti atskirą prieigos valdymo serverį, kuris naudojamas WPA-EAP atveju.



1 pav. Vietos informacija pagrįsto prieigos valdymo architektūra

4 Vietos informacija pagrįstos būsenos ir jų įvertinimas

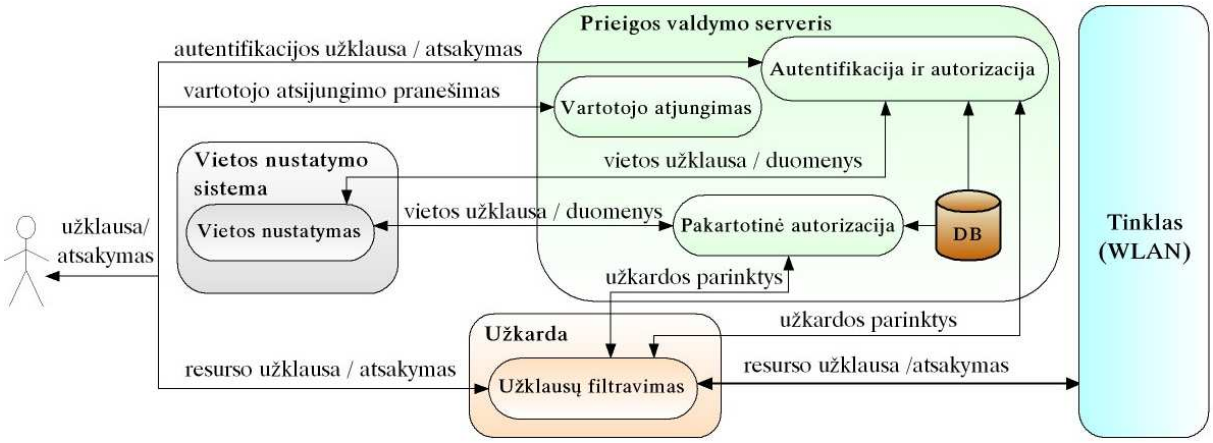
Gali būti keletas vietos informacija pagrįstų būsenų, pagal kurias gali būti valdoma prieiga [7, 8]. Šiame darbe įvertinama tik viena – nusakanti, ar vartotojas yra tam tikroje zonoje, pavyzdžiui, tam tikrame kabinete. Kitų būsenų, tokių kaip vartotojo greitis, nuotolis ar subjektų tankis tam tikroje zonoje, įvertinimas prieigos prie bevielio tinklo resursų valdymui nereikalingas. Kaip bebūtų, jas įtraukti į modelį būtų nesudėtinga, reiktų tik pridėti papildomų esybių ir algoritmų tokios informacijos įvertinimui.

Vietos informacija pagrįstų būsenų įvertinimas priklauso nuo to, kokius duomenis pateikia VNS. VNS gali grąžinti ne tik būsenos reikšmę, bet ir patikimumo bei galiojimo reikšmes [7, 8]. Patikimumas gali būti vertinamas procentais (toks variantas pasirinktas šiame darbe) ir pagal tai PVS gali nuspręsti, ar galima pasitikėti gauta vietos informacija, ar ji turėtų būti užklausta dar kartą. Pagal galiojimo reikšmę PVS gali nuspręsti, kada reikės pakartoti vietos informacijos užklausą. Jei VNS galiojimo reikšmės nenustato, PVS gali užklausti vietos informacijos kiekvienąkart, kai vartotojas nori prieiti prie resurso, arba periodiškai kas kažkiek laiko. PVS gali nenaudoti galiojimo reikšmės ir dėl kokių nors kitų priežasčių. Jei VNS grąžina ne būsenos reikšmę, o tik vartotojo koordinates, būsenos reikšmę nustato PVS (tai įgyvendinta siūlomame prieigos valdymo mechanizme).

5 Vietos informacija grįsto prieigos valdymo modelis

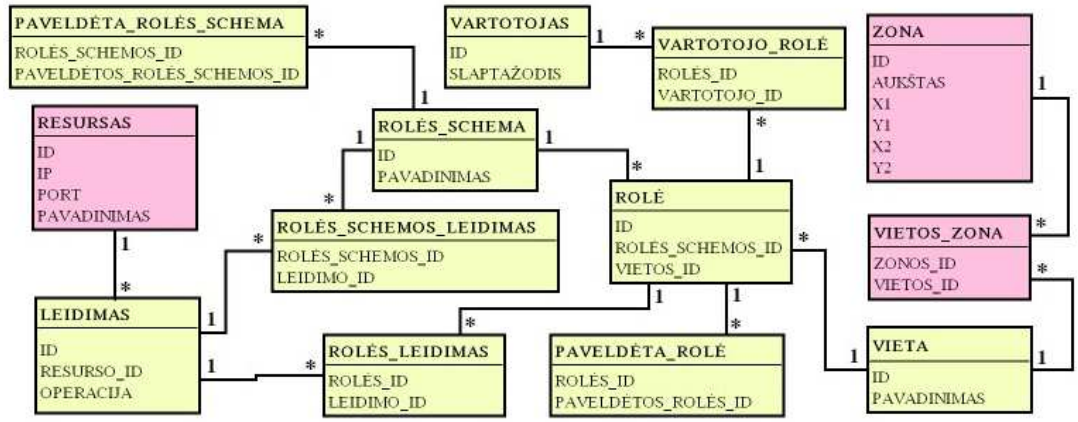
Vartotojui norint prisijungti prie bevielio tinklo, WPA-EAP autentifikacijos atveju prieigos taškas kreipiasi į PVS, tai paprastai atliekama [12] RADIUS protokolu. Pagal pasiūlytą prieigos valdymo mechanizmą (žr. 2 pav.) PVS sutikrina vartotojo prisijungimo duomenis bei vietos informaciją ir praneša prieigos taškui, ar

vartotojas autentifikuotas. Autentifikavus, vartotojui sukuriama sesija ir leidžiama prieiga prie bevielio tinklo resursų. Vartotojui naudojantis tinklu, jo vardo ar kitų prisijungimo duomenų nebeklausiama, tačiau periodiškai, pavyzdžiui, kas 5 min., PVS užklausia vietos informacijos, kurią patikrina ir grąžina VNS. Tai atliekama dėl to, kad prisijungęs vartotojas gali judėti ir jo vietos informacija gali keistis. Pagal gautą informaciją, vartotojui uždraudžiama arba leidžiama prieiga prie tam tikrų resursų, pavyzdžiui, vartotojui išėjus iš savo darbo kabineto į kitas patalpas, panaikinama galimybė naudotis tais resursais, kurie turi būti prieinami tik iš darbo kabineto. Sesija naikinama tuomet, kai vartotojo galinis įrenginys atsijungia nuo prieigos taško (apie tai PVS praneša prieigos taškas) arba atsiranda už teritorijos, kur teikiama prieiga prie tinklo, ribų (tai PVS apskaičiuoja iš vartotojo vietos informacijos).



2 pav. Vietos informacija grįsto prieigos valdymo sistemos duomenų srautų diagrama

2 pav. pavaizduota užkarda reiškia tam tikrą būdą riboti / leisti vartotojų prieigą prie tam tikrų resursų. Tai gali būti realizuota įvairiai. Užkarda gali būti prieigos valdymo serveryje ir filtruoti visą į tinklą einantį srautą, ji gali būti kitame serveryje arba prieigos taške. Vietoje užkardos gali būti panaudotas prieigos valdymas virtualių tinklų (angl. VLAN) pagalba: prieigos taškas galėtų žymėti vartotojų siunčiamus paketus tam tikro VLAN žyme pagal PVS nurodymus. Srautas „užkardos parinktys“ priklausomai nuo užkardos realizacijos, gali būti tik VLAN žymė, aktyvių rolių pavadinimai arba vartotojams suteikti leidimai.



3 pav. Vietos informacija pagrįsto prieigos valdymo sistemos esybių ryšių diagrama

Paprastai organizacijose, kur nereikalingas ypatingo lygio saugumas, naudojamas rolėmis pagrįstas prieigos valdymas, todėl pasiūlytame prieigos valdymo mechanizme pasirinkta naudoti [10] Geo-RBAC modelį. Mechanizmas turi būtų pritaikytas veikti kelių aukštų pastato viduje ir įvertinti vartotojo būseną stačiakampio gretasienio formos patalpų esančių pastate atžvilgiu. Kadangi Geo-RBAC modelyje egzistuoja tik daugiakampio formos esybės, jis papildomas įvertinimu, kuriame pastato aukšte yra pasaulio esybė, ir truputį supaprastinamas laikant, kad erdvinės pasaulio esybės gali būti tik stačiakampio arba iš stačiakampių sudarytos formos. Tarp tokių esybių egzistuoja vienintelis buvimo dalimi ryšys. Dėl šių priežasčių į pasiūlytą mechanizmą užtenka įtraukti vieną realios vietos (santykinių koordinačių x, y, z, kur z atitinka pastato aukšto numerį) vertimo į loginę vietą (pavyzdžiui, kabineto nr.) funkciją, kuri tikrina, ar vartotojo x, y koordinatės yra tam tikros zonos viduje ir ar sutampa vartotojo ir zonos aukšto numeris. 3 paveiksle pavaizduota tokio modelio esybių ryšių diagrama. Esybės ZONA ir VIETOS_ZONA pažymėtos kita spalva, nes jų galima būtų atsisakyti tuo atveju, jei VNS

grąžintų ne vartotojo koordinates, bet loginės vietos, kurioje jis yra, ID. Esybė RESURSAS yra nereikalinga tuo atveju, kai PVS elementui „Užkarda“ perduoda tik aktyvuotas vartotojų roles arba leidimų sąrašą.

Pasiūlytas mechanizmas buvo išbandytas iš failų (jie atitiktų modelyje pažymėtus prieigos tašką ir VNS) skaitant vartotojų prisijungimo duomenis (vardą ir slaptažodį) ir vietos informaciją bei įrašant suteiktus leidimus į išvesties failą (jis atitinka modelyje „Užkardą“). Į kitą išvesties failą, kuris modelyje atitinka prieigos tašką, rašoma, kurie vartotojai autentifikuojami, kurie ne ir kurie vartotojai turi būti atjungti dėl to, kad išėjo iš pastato. Modulis „Vartotojo atjungimas“ skaito iš įvesties failo, atitinkančio prieigos tašką, vartotojų vardus ir panaikina atitinkamų vartotojų sesijas. Tyrimo metu nustatyta, kad mechanizmas veikia tinkamai, vartotojai teisingai autentifikuojami pagal prisijungimo duomenis ir vietos informaciją, jiems teisingai priskiriami leidimai.

6 Vietos informacija grįsto prieigos valdymo pažeidžiamumai

Vietos informacija grįsto prieigos valdymo mechanizmas gali būti pažeidžiamas neapsaugojus PRS komunikacijos su prieigos tašku, VNS ar „Užkarda“. Jei vietos informacija derinama su naujais autentifikacijos metodais, tokiais kaip WPA-EAP, sistema yra apsaugota nuo vartotojų prisijungimo duomenų perėmimo ir klastojimo, tačiau tai neapsaugo nuo vartotojų MAC adresų perėmimo ir klastojimo. Valdymo mechanizmas gali būti pažeidžiamos DoS (angl. *Denial of Service*) atakomis, kai piktavalis pasirenka MAC adresą tokį, kokį turi prisijungęs vartotojas, tada VNS klaidingai nustato prisijungusio vartotojo vietą ir dėl to blokuoja jam prieigą prie resursų. Dar daugiau žalos galėtų padaryti kirmino skylės (angl. *warmhole*) ataka, kai du piktavaliai pasirenka vienodus MAC adresus ir bando gauti prieigą iš tos vietos, kur ji yra neleidžiama. Atakos metu vienas atakuotojas yra vienoje išorinėje zonos, kur prieiga leidžiama, pusėje, o kitas kitoje – taip bandoma apsimesti vienu vartotoju, kuris yra zonos viduje. Apsauga nuo tokių atakų turėtų būti įdiegta vietos nustatymo sistemoje.

7 Išvados ir ateities darbai

Pasiūlytame prieigos valdymo mechanizme naudojamas Geo-RBAC modelis, pritaikytas prieigos prie bevielio tinklo resursų valdymui kelių aukštų pastato viduje. Pasiūlytas prieigos valdymo algoritmas periodiškai tikrina vartotojų vietos informaciją, o kiti vartotojų prisijungimo duomenys tikrinami tik kartą. Mechanizmas gali būti įgyvendintas derinant vietos informaciją su WPA autentifikacijos metodais ir naudojantis vietos nustatymo sistemomis, nustatančiomis vartotojų santykines x, y, z koordinates ir duomenų patikimumą, kur z – pastato aukšto numeris. Modelį galima būtų praplėsti įtraukiant į jį ir kitas vietos informacija pagrįstas būsenas. Ateities darbai galėtų būti tam tikro WPA-EAP autentifikacijos metodo, „Užkardos“ dalies realizacijos ar tam tikros vietos nustatymo sistemos suderinimo su pasiūlytu modeliu tyrimai.

8 Literatūros sąrašas

[1] **S. Ganu, A. S. Krishnakumar, P. Krishnan**. Infrastructure-based location estimation in WLAN networks. *IEEE Wireless Communications and Networking Conference.* 2004.

[2] **A. Mishra, S. Banerjee**. Secure Spaces: Location-based Secure Wireless Group Communication. *POSTER SESSION: Special feature on MobiCom 2002 posters, ACM*, 2003, 68 – 70 psl.

[3] **M. Kappes, S. Garg, M. Mani** US Patent 7403773 - Location-based access control for wireless local area networks. 2008.

[4] **M. Youssef, A. Agrawala**. Continuous Space Estimation for WLAN Location Determination Systems. *Proceedings of the 13th International Conference on Computer Communications and Networks*, 2004.

[5] **N. Sastry, U. Shankarand, D. Wagner**. Secure Verification of Location Claims. *Proceedings of ACM Workshop on Wireless Security*, 2003.

[6] **B. Watersand, E. Felten**. Proving the Location of Tamper Resistant Devices. *Technical report, Princeton University*, 2003.

[7] **C. A. Ardagna, M. Cremonini, S. De Capitani di Vimercati, P. Samarati**. Access Control in Location-Based Services. *Privacy in Location-Based Applications: Research Issues and Emerging Trends*, *Springer-Verlag.* 2009, 106 – 126 psl.

[8] **C. A. Ardagna, M. Cremonini, S. De Capitani di Vimercati, P. Samarati**. Privacy-enhanced Location-based Access Control. *The Hand-book of Database Security: Applications and Trends, Springer-Verlag.* 2007.

[9] **I. Ray, M. Kumar**. Towards a Location-Based Mandatory Access Control Model. *Computers & Security*. 2006.

[10] **M. L. Damiani, E. Bertino, B. Catania, P. Perlasca**. GEO-RBAC: A Spatially Aware RBAC. *ACM Transactions on Information Systems and Security.* 2006.

[11] Lietuvos respublikos elektroninių ryšių įstatymas, 3 ir 65 straipsniai.

[12] **C. Rigney, S. Willens, Livingston, A. Rubens, Merit, W. Simpson, Daydreamer.** Remote Authentication Dial In User Service (RADIUS). *The Internet Engineering Task Force (IETF), Request for Comments: 2865.* 2000.

Wireless LAN Location-based Access Control

We show the advantages of using location information for wireless LAN authentication and access control in this work. We present location-based authentication and access control model. We describe the vulnerabilities of standart authentication and access control methods as well as of those evaluating location information. The vulnerabilities are dicussed in the context of sniffing, highjacking, DoS and warmhole attacks.