Aalto-yliopisto
Perustieteiden korkeakoulu
Tietotekniikan koulutusohjelma

Yksityisyydensuoja paikkatietoja hyödyntävissä palveluissa

Kandidaatintyö

24. huhtikuuta 2013

Janne Paalijärvi

Aalto-yliopisto
Perustieteiden korkeakoulu
Tietotekniikan koulutusohjelma

KANDIDAATINTYÖN
TIIVISTELMÄ

Tekijä:	Janne Paalijärvi
Työn nimi:	Yksityisyydensuoja paikkatietoja hyödyntävissä palveluissa
Päiväys:	24. huhtikuuta 2013
Sivumäärä:	24
Pääaine:	Tietoliikenneohjelmistot
Koodi:	T3005
Vastuuopettaja:	Prof. Tomi Janhunen
Työn ohjaaja(t):	TkL Sanna Suoranta (Tietotekniikan laitos)

Työssä tarkastellaan erilaisia teknisiä ratkaisuja, joilla voidaan parantaa käyttäjien yksityisyydensuojaa paikkatietoa hyödyntävissä palveluissa. Tyypillisesti käyttäjä joutuu luopumaan osasta yksityisyyttään käyttäessään tällaista palvelua. Kehitettyjen järjestelmien ja ratkaisujen avustuksella yksityisyyden menettäminen näissä tilanteissa ei kuitenkaan ole täydellistä, vaan käyttäjän yksityisyydensuoja voidaan pitää hyvänä palvelutason laadun säilyessä hyväksyttävänä.

Keskeisimmät työssä tutkitut järjestelmät ja ratkaisut sisältävät keskitetyn ja luotetun välityspalvelimen, jota kautta päätelaite viestii varsinaisen paikkatietoja hyödyntävän palvelun kanssa. Välityspalvelin muokkaa välitettäviä paikkatietoja siten, että päätelaitteen tunnistus vaikeutuu, mutta palvelu pysyy edelleen käyttökelpoisena.

Avainsanat:	paikkatieto, yksityisyys, yksityisyydensuoja
Kieli:	Suomi

Sisältö

Alkusanat

Haluan kiittää muutamia henkilöitä, jotka ovat suuresti myötävaikuttaneet tämän kandidaatintyön syntymiseen. Ensimmäisenä mieleeni tulee Lauri Kääriäinen, jonka lähes viikottaiset kannustavat kommentit olivat omiaan viemään projektia eteenpäin. Tahdon lisäksi kiittää Milla Sairasta. Psyykkasit juuri oikeina hetkinä musertavan työtaakan alla. Kiitos. Haluan myös lausua kiitokset ohjaajalleni Sanna Suorannalle. Hänen mainio ohjauksensa ja joustava suhtautuminen asioihin palautti suuresti uskoani akateemiseen maailmaan. Kiitos. Kiitos myös kaikille muille projektissa minua tukeneille ja tsemppaushuutoja huudelleille. Niin nimellisille kuin anonyymeillekin.

Espoossa 24. huhtikuuta 2013

Janne Paalijärvi

1 Johdanto

Tämä kandidaatintyö käsittelee yksityisyydensuojaa internetin paikkatietoa hyödyntävissä palveluissa. Aihe on tutkimisen arvoinen, sillä tällaista palvelua käyttääkseen joutuu yleensä luopumaan ainakin osasta yksityisyyttään, mikä luo mielenkiintoisen ristiriidan. Tyypillisesti huonompi yksityisyydensuoja on korreloinut paremman palvelun laadun kanssa.

Tutkimusongelmana on luoda katsaus erilaisiin yksityisyydensuojaa internetin paikkatietoa hyödyntävissä palveluissa parantaviin ratkaisuihin. Tutkimus on perusteltu, sillä kokoavaa ja ajantasaista suomenkielistä artikkelia aiheesta ei ole. Tässä työssä paneudutaan erilaisiin teknisiin ratkaisuihin, jotka auttavat yksityisyydensuojan säilyttämisessä paikkatietoja hyödyntävissä palveluissa. Ratkaisut voivat olla konkreettisia toteutuksia tai teoreettisia malleja. Ratkaisut voivat sisältää palvelu-, siirtotie- tai päätelaitekomponentteja.

Työn tavoite on listata useita erilaisia tekniikoita tutkimuksen aihealueelta ja kertoa niiden toimintatavoista. Juridiset kysymykset ovat tarkastelun ulkopuolella. Menetelmänä työssä toimii enimmäkseen kirjallisuuskatsaus alan artikkeleihin ja julkaisuihin.

Työn pääpaino keskittyy erilaisten suurempien kokonaisjärjestelmien tutkimiseen ja esittelyyn. Näitä käsitellään työn alkupuolella. Työn loppupuolella käsitellään arkisempia paikkatietoja hyödyntäviä palveluita ja yksityisyyden suojaamista niiden osalta. Lopuksi esitetään yhteenveto löydöksistä.

2 Yksityisyys ja paikkatiedot

2.1 Yksityisyyden määritelmä

Yksityisyys tarkoittaa oikeutta määritellä se, milloin ja ketkä saavat saada tietoja itsestämme, ominaisuuksistamme ja omistuksistamme. [1] Myös ihmisen sijaintitiedon voi rinnastaa kuuluvan yksityisyyden piiriin. Julkisessa ja kansoitetussa tilassa liikkuessaan ihminen voi tosin harvemmin salata oikean sijaintitietonsa; hän ei voi yhtäkkiä päättää, ettei olekaan fyysisesti paikalla. Hän voi kuitenkin - ainakin teoriassa - määritellä, minkälaisia paikkatietoja hänen käyttämänsä päätelaitteet viestivät ulkomaailmaan.

Oikeus yksityisyyteen on eräs länsimaalaisen sivistysyhteiskunnan kulmakiviä. Ihmisen yksityisyyden vähintään implisiittisestä loukkaamisesta ovat kiinnostuneita useat tahot. Valtiot pyrkivät valvomaan kansalaisiaan länsimaissakin, ja myös mainostajat ovat tuttu riesa jokaiselle internet-käyttäjälle. Ääritapauksessa rikolliset ja poliisi ovat kiinnostuneita kohteidensa liikkeistä. Yksityisyys on yksi niistä kansalaisoikeuksista, joiden olemassaolon

muistaa vasta siinä vaiheessa, kun se otetaan pois.

Paikkatietoja käyttävä palvelu tunkeutuu käyttäjän yksityisyydensuojan alueelle. Mitä tarkemmin palvelu tietää käyttäjän sijainnin, sitä paremmin palvelu tyypillisesti toimii. Käyttäjä vaihtaa palveluissa yksityisyyttään parantuneeseen palvelun laatuun [2]. Tämä tasapainottaminen on luonteeltaan nollasummapeliä. Ääritapauksessa käyttäjä voi olla luovuttamatta paikkatietojaan kokonaan, jolloin paikkatietoja hyödyntävän palvelun käyttö muuttuu todennäköisesti mahdottomaksi tai ainakin suurimmaksi osaksi hyödyttömäksi. Käyttäjä ei ehkä halua edellä mainittua, mutta ei myöskään päätelaitteen jatkuvaa ja äärimmäisen tarkkojen sijaintitietojen lähettämistä palveluihin. Toisin sanoen näiden kahden ääripään väliltä on löydettävä jonkinlainen sopuratkaisu tyydyttämään sekä yksityisyydensuojan tarpeet että takaamaan jonkinlainen palvelun laatu.

Paikkatietojen hyödyntävien palvelujen suhteen yksityisyydensuojan parantamista voidaan toteuttaa rikkomalla yhteyttä henkilön tai päätelaitteen ja koordinaattitiedon välillä joko osittain tai kokonaan. Haluttu palvelutaso sanelee käytetyn metodiikan ja sen asteen.

2.2 K-anonymiteetti

K-anonymiteetti on eräs keskeinen parametri yksityisyydensuojaa käsittelevässä tutkimuskirjallisuudessa. Jos jokin palvelu toteuttaa k-anonymiteetin, se tarkoittaa, että palvelun yksittäistä käyttäjää ei voida tunnistaa k-1 muun käyttäjän joukosta. K-anonymiteetti kehitettiin alun perin tietokanta-aineistojen anonymisointiin.

Latanya Sweeneyn [3] mukaan tietokannan arvo on monesti kiinni siitä, millaisin edellytyksin se on anonyymisti hyödynnettävissä. Anonyymiyttä tarvitaan siksi, että usein tietokannat sisältävät sellaista salassa pidettävää tietoa, joka saattaa kiinnostaa esimerkiksi henkilön lähipiiriä, työnantajaa tai vakuutusyhtiötä. Toisinaan tietokannoilla voi olla suurta arvoa myös vieraiden valtioiden edustajille. Laajemman sovellusalueen ongelmien pohtiminen on johtanut k-anonymiteetin nostamiseen perusparametriksi yksityisyydensuojaa käsittelevissä tutkimusaineistoissa.

3 Paikkatietojen anonymisointijärjestelmät

3.1 Yleistä

Tutkijat ovat kehittäneet useita erilaisia järjestelmiä ja menetelmiä, joiden avustuksella voidaan parantaa käyttäjien yksityisyydensuojaa paikkatietoja hyödyntävissä palveluissa. Kehitetyillä järjestelmillä voidaan päästä vakuuttaviin tuloksiin yksityisyyden säilyttä-

misessä palvelutason pysyessä siedettävänä. Järjestelmiä on kahta eri tyyppiä, niitä jotka vaativat jonkinlaisen kolmannen osapuolen komponentteja toimiakseen, ja niitä, jotka toimivat ilman. Ensiksi mainittuja on olemassa enemmän kuin viimeksi mainittuja.

Seuraavassa kehitettyjä ratkaisuja esitellään lähtien yksinkertaisista ja päätyen kompleksisempiin. Jokainen kuvatuista järjestelmistä on sellainen, että sen päätelaitekomponenttina voi toimia GPS-kykyinen matkapuhelin, johon voidaan asentaa tietoliikenneominaisuuksia ja verkkoa sekä paikannusominaisuuksia käyttävä sovellus.

3.2 Paikka- ja aikasumennus

Marco Gruteser ja Dirk Grunwald kehittivät paikka- ja aikasumennusta (spatial and temporal cloaking) hyväksikäyttävän anonymisointijärjestelmän paikkatietopalveluja varten [4]. Järjestelmän lähtöoletuksiin kuuluu päätelaitteen tietämä tarkka sijaintitieto joko GPS:n, verkon kolmiokartoituksen tai hybridiratkaisujen kautta. Järjestelmässä toimii luotettu välityspalvelin, jota kautta tarkat paikkatiedot kulkeutuvat varsinaiseen paikkatietoja hyödyntävään palveluun. Järjestelmän kehittäjien suurin huoli on ollut tunnistetietojen kerääntyminen paikkatietopalveluihin. Nämä tunnisteet voivat myötävaikuttaa murtautumistilanteissa henkilöiden yksilöityjen paikkatietojen selviämiseen. Moni myöhempi anonymisointikonsepti on saanut paljon vaikutteita Gruteserin ja Grunwaldin järjestelmästä.

Gruteser ja Grunwald tunnistavat sovellusalueella olevan kahdentyyppisiä yksityisyydensuojaongelmia. Ne liittyvät joko viestinvälitykseen tai itse paikkatietoihin. Rajatun tilan tunnistamisessa hyökkääjä käyttää hyväkseen tietoa siitä, että vain yksi käyttäjä sijaitsee jollakin tietyllä alueella. Tästä voidaan päätellä, että kaikki alueelta lähetetyt viestit kuuluvat tietylle käyttäjälle. Toinen ongelmatyyppi on tarkkailuun perustuva tunnistus. Mikäli käyttäjä on aikaisemmin lähettänyt paikkatietonsa ja tunnistautumistietonsa, ja haluaisi kommunikoida myöhemmissä viesteissä anonyymisti palvelimien kanssa, hänet voidaan tunnistaa, mikäli uusien viestien paikkatiedot ovat samat. Sijaintiseurannassa hyökkääjä saa selville yhden tai useamman paikkatieto-tunnistamistieto-parin ja pystyy tämän perusteella päättelemään historiallisten ja tulevien paikkatietojen liittyvän tiettyyn käyttäjään.

Guteserin ja Grunwaldin järjestelmässä [4] päätelaitteet ottavat aluksi yhteyttä luotettuun anonymisointipalvelimeen. Yhteys on salattu ja autentikoitu. Päätelaitteen lähettämien paikkatietojen salaus puretaan ja prosessoidaan anonymisointipalvelimessa. Ylimääräiset tunnistetiedot poistetaan. Tämän jälkeen paikkatiedot sumennetaan ja lähetetään varsinaiseen paikkatietoja hyödyntävään palveluun. Estääkseen edellä kuvattuja hyökkäysvektoreita anonymisointipalvelu voi myös muuttaa viestien järjestystä. Tällöin hyökkäysmielessä tapahtuva viestien yhdistäminen käyttäjiin tulee vaikeammaksi.

Paikkatietoalkiota järjestelmässä kuvataan kolmiulotteisella avaruudella, jonka akselit ovat x-koordinaatti, y-koordinaatti ja aikakoordinaatti. Parametrit rajaavat tästä avaruudesta kuution tarkoittaen, että jollakin tietyllä aikavälillä päätelaite on sijainnut jonkin tietyn maantieteellisen alueen sisäpuolella. Mikäli k-1 muuta päätelaitetta projisoituu saman kuution sisään, on alkio k-anonyymi. Järjestelmässä käyttäjä asettaa minimivaatimuksen k-parametrille. Jos minimivaatimukset k-anonymiteetille eivät täyty paikkatietoalkiossa, voidaan aluekoordinaattien osalta kasvattaa tarkasteltavan alueen kokoa, kunnes alueella on k-1 muutakin päätelaitetta. Vastaavasti aikakoordinaattien kanssa voidaan suorittaa lavennusta siten, että alueelle saadaan k-1 muuta päätelaitetta yhtä aikaa. Näin saavutetun k-anonymiteetin jälkeen parametrit voidaan palauttaa. Tarpeen vaatiessa voidaan siis kasvattaa jomman kumman, aikaparametrien tai aluekoordinaattien, tarkkuutta toisen kustannuksella. Tätä "vaihtokauppaa" operoidessa on kiinnitettävä huomiota siihen, missä sovelluskontekstissa tietoja käytetään.

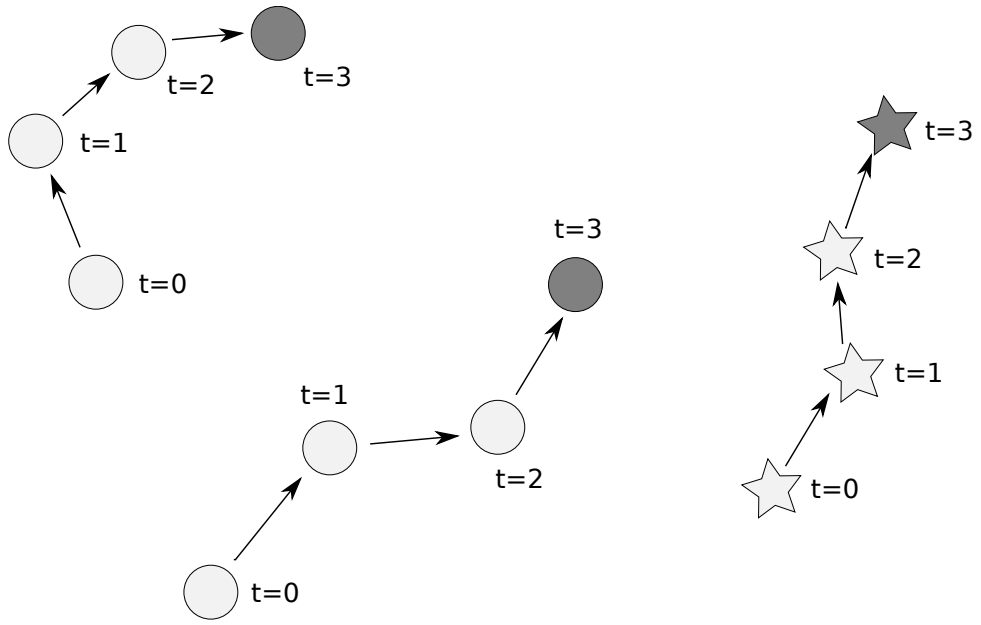
3.3 Valetietojen lähettäminen

Eräs mielenkiintoinen ratkaisu anonymiteetin kasvattamiseen paikkatietoja hyödyntävien palveluiden osalta on valetietojen käyttäminen. Hidetoshi Kido, Yutaka Yanagisawa ja Tetsuji Satoh ovat tutkineet aihetta [5]. Monista muista alan tutkimusongelman ratkaisusta ilahduttavasti poiketen nyt käsiteltävässä ratkaisumallissa avainkomponenttina ei ole luotettu välityspalvelin, vaan kaikki tiedonvälitys tapahtuu suoraan paikkatietoja hyödyntävän palvelun ja päätelaitteen välillä.

Tutkijat muistuttavat artikkelissaan, että kerran anonymisoimatta lähetettyjä paikkatietoja ei periaatteessa koskaan voi tuhota, vaan ne säilyvät tietokannoissa hamaan tulevaisuuteen saakka. Mikään ei estä paikkatietoja hyödyntävän palvelun tietojärjestelmiä analysoimasta tästä datasta esimerkiksi käyttäjien liikkeitä ja toteuttamasta mahdollisesti sellaista toiminnetta, joka näkyvästi rikkoo käyttäjän määrittelemää yksityisyydensuojaa.

Tutkijat paneutuvat työssään erityisesti realistiselta näyttävän liikkumista kuvaavien valetietojen generointiin. [5] Kido ja kumppanit muistuttavat monien kollegoidensa tavoin, että vaikka pseudonyymit tunnukset olisivat käytössä, ja vaikka ainoa yhteys henkilön ja paikkatietojärjestelmän loogisessa kommunikaatioketjussa olisi pseudonyymin tunnuksen kuvautuminen paikkatietoihin, henkilön pitkäaikaisten oleskelutietojen avulla voidaan tehdä tarkkoja arvauksia siitä, ketkä henkilöt vastaavat mitäkin koordinaatteja. Tutkijat puntaroivat, että ylimääräisen satunnaisuuteen perustuvan paikkatiedon lähettämisessä on ongelmia siinä tapauksessa, mikäli tiedot saava palvelu tekee niistä analyysin; tällöin suoraviivaiset kulkureitit erottuvat havaintoaineistosta selvästi.

Edellä mainitun ongelman ratkaistakseen tutkijat kehittivät kaksi algoritmia. Ensimmäi-



Kuva 1: Oikeiden sijaintitietojen lähettäminen koherenttien valetietojen kera paikkatietoa hyödyntävään palveluun.

sessä algoritmissa päätelaite lähettää paikkatietoja hyödyntävään palveluun valetietoja myös keksittyjen päätelaitteiden sijainnista. Päätelaite pitää kirjaa lähetettyjen valheellisista sijaintitiedoistaan ja tekee niiden perusteella päätöksiä, mitä valetietoja lähetetään seuraavaksi siten, että reittien koherenttius säilytetään. [5] Kuvassa 1 on nähtävillä paikkatietoa hyödyntävään palveluun lähetettävä sijaintitietoaineisto. Mukana on oikeita paikkatietoja kuvattuna tähdellä ja valetietoja, jotka on kuvattu ympyrällä.

Toinen algoritmi on tarkoitettu tilanteisiin, joissa alueella on jo ennestään liikennettä. Tällöin uusien valetietojen sijaintiin otetaan huomioon muiden päätelaitteiden paikkatiedot siten, että päätelaitteiden sijainteja levitetään väljemmille alueille. Päätelaitteen lähetettyä useita eri laitteita koskevat päivityksen paikkatietoja hyödyntävään palveluun, se saa vastauksena haluamansa palvelun, esimerkiksi tiedon lähimmästä ravintolasta. Se saa tiedon jokaista päätelaitepyyntöä kohti, joten lopuksi päätelaitteen on osattava käyttää juuri sitä koskevan vastauksen tietoja.

3.4 Seka-alueet ja pseudonymiteetti

Alastair Beresford ja Frank Stajano pohtivat anonyymiyden ja paikkatietoa hyödyntävien palvelujen ongelmaa. [6] Heidän teeseissään keskeinen uhkakuvaidea on globaali. Periaatteessa mihinkään palveluun ei voida luottaa, vaan kaikkia palveluja käsitellään yhtenä vihamielisenä joukkona. Tutkijoiden lähestymistapa ongelmaan on pseudonyymien käyttö. Heidän järjestelmässään keskeisenä komponenttina on anonyymi välityspalvelin, joka

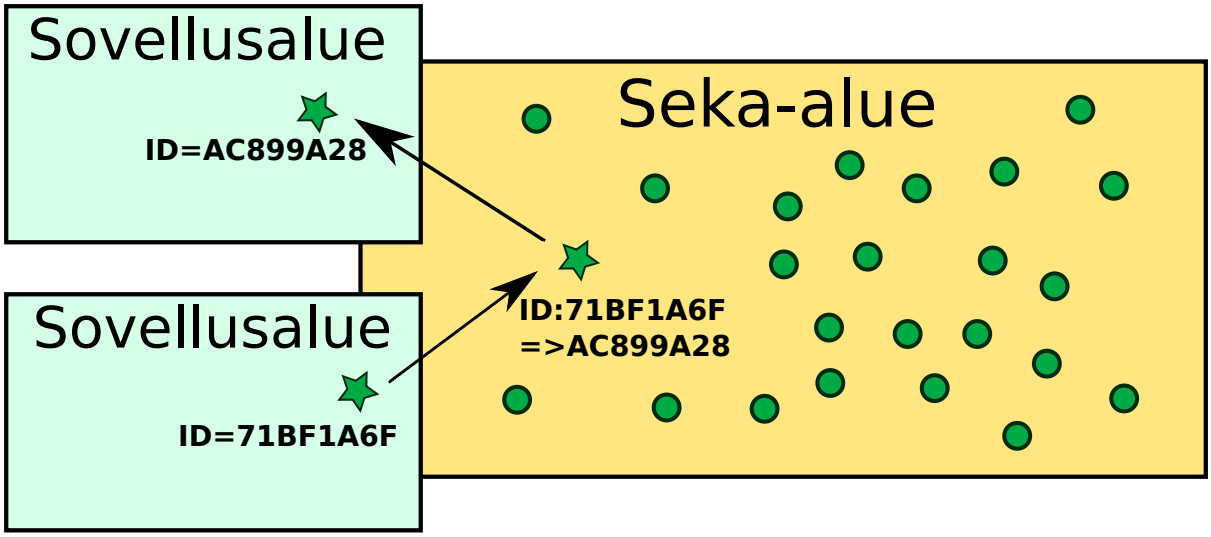
vastaanottaa päätelaitteiden paikkatietopäivityksiä ja avustaa palveluihin rekisteröidyttäessä. Toimintamallissa päätelaitteisiin ei lähetetä automaattisesti palvelutietoja, vaan jokaiseen palveluun täytyy rekisteröityä erikseen. Kun käyttäjä saapuu tällaisen rekisteröimänsä palvelun vaikutusalueelle, hän saa haluamansa palvelukokemuksen välityspalvelun toimiessa päätelaitteen ja palvelun välissä.

Esimerkkitapauksena voidaan tarkastella kahvilan tuotetarjouksista kertovaa palvelua. Käyttäjä rekisteröityy palveluun itse käyttäen apuna välityspalvelinta. Rekisteröityminen voidaan esimerkiksi Internetissä www-sivulla. Rekisteröityminen määrittelee välityspalvelimelle käyttäjän olevan kiinnostunut esimerkiksi kahvilan hintatiedoista aina kahvilan läheisyydessä sijaitessaan. Pelkkien pseudonyymien palvelukohtaisten tunnusten käytössä on kuitenkin ongelmansa, joita käsitellään seuraavaksi.

Pitkät oleskeluajat tunnetussa paikassa voivat luoda korrelaation pseudonyymin tunnuksen ja päätelaitteen välille. Tutkijat todensivat ongelman myös käytännössä toimistotiloihin suunnatun paikkatietoja hyödyntävän palvelun suhteen. He onnistuivat tunnistamaan oleskeluaikojen perusteella jokaisen järjestelmän käyttäjän [6]. Eräs ratkaisumalli on käyttää pysyvien pseudonyymien tunnusten sijaan vaihtuvia tunnuksia. Valitettavasti kuitenkin tällainen tunnuksen vaihtaminen ei ole riittävä suojautumiskeino, mikäli vaihto tapahtuu ajallisesti ja maantieteellisesti rajatulla alueella.

Tutkijoiden varsinainen ratkaisu ongelmaan ovat niinkutsutut seka-alueet. Seka-alue on järjestelmän kontekstissa alue, joka yhdistää varsinaisia sovellusalueita toisiinsa. Sovellusalueet tarkoittavat alueita, joissa varsinainen paikkatietoja hyödyntävä palvelu sijaitsee ja palvelee päätelaitteita. Seka-alueella ollessaan palvelut eivät saa päätelaitteilta minkäänlaisia paikkatietoja välityspalvelimen kautta tai muutenkaan. Seka-alueilla ollessaan päätelaite voi valita itselleen uuden pseudonyymin tunnuksen, jota käyttää seuraavalla sovellusalueella. Kuvassa 2 on esimerkki tilanteesta, jossa päätelaite liikkuu sovellusalueelta toiselle seka-alueen kautta vaihtaen tunnusta. [6]

Tunnusta voi ja kannattaa vaihtaa joka kerta, kun päätelaite palaa seka-alueelle. Mikäli seka-alueella on tarpeeksi muita järjestelmää käyttäviä päätelaitteita, käyttäjän pseudonyymiä tunnusta ei voida yhdistää varsinaiseen käyttäjään. Sama pätee myös toisin päin: mikäli seka-alueella on vain yksi käyttäjä, tunnuksen vaihtamisesta ei ole juurikaan iloa, mitä käyttäjän anonyymiyteen tulee. Järjestelmässä käyttäjä pystyy lähettämään välityspalvelimelle kyselyn eri seka-alueiden käyttäjien lukumäärästä. Mikäli käyttäjä katsoo lukumäärän liian pieneksi, ja näin siis anonymiteettinsä liian heikosti, hän voi lopettaa päätelaitteensa sijaintitietojen lähettämisen, kunnes tilanne on parantunut uusien käyttäjien saapumisen myötä.



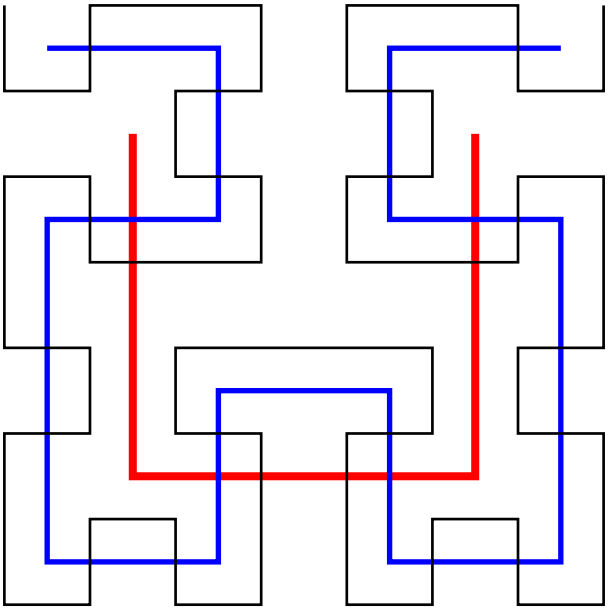
Kuva 2: Käyttäjän liikkuminen sovellusalueelta toiselle seka-alueen kautta.

3.5 Mobihide

Mobihide on vertaisverkkoarkkitehtuuria käyttävä yksityisyyssuojaratkaisu paikkatietoja hyödyntäviä palveluita varten lähialuekyselyiden kontekstissa. Kehittäjinä ovat toimineet Gabriel Panos Kalnis ja Spiros Skiadopoulos [7]. Järjestelmässä on useita päätelaitteita, jotka muodostavat DHT-tyylisen (Distributed Hash Tables, jaetut hajautustaulut) vertaisverkon. Ennen verkkoon liittymistä päätelaite autentikoituu varmennepalvelimelle, minkä jälkeen viestintä vertaisverkkoon sallitaan. Vertaisverkon solmut koostuvat muutaman käyttäjän ryppäistä. Solmussa on tiedot myös edeltävästä ja seuraavasta solmusta, redundantti lista seuraavista solmuista ja taulukko osoitetiedoista solmuihin, jotka sijaitsevat 2^i etäisyydellä tästä solmusta. Verkkoon liittymistä varten uusi päätelaite saa aloitustiedot mahdollisista liittymissolmuista varmennepalvelimelta.

Solmujen järjestys DHT-vertaisverkossa on itse asiassa maantieteellisen sijaintitiedon kuvaus fraktaalimaisella Hilbertin käyrällä. Sopivanasteisella Hilbertin käyrällä voidaan täyttää halutulla tarkkuudella jokainen neliömäinen maantieteellinen alue. Valitsemalla piste käyrältä valitaan samalla jokin sijaintitieto. Mobihide käyttää operoidessaan hyväksi tietoa, jonka mukaan Hilbertin käyrällä lähellä olevat pisteet kuvautuvat lähellä oleviksi pisteiksi myös maantieteellisesti. Hilbertin käyriä on esitetty tarkemmin kuvassa 3.

Mobihiden päätelaiteryppäät ovat adaptiivisia pystyen jakautumaan ja yhdistymään muiden ryppäiden kanssa, mikäli ryppääseen tulee liikaa tai liian vähän päätelaitteita. [7] Rypäsratkaisuun on päädytty tehokkuussyistä, jotta vältettäisiin suurten DHT-vertaisverkon linkkiketjujen läpikäyminen. Varsinainen paikkatieto-operointi tapahtuu siten, että jokin päätelaite muodostaa sopivalla k-anonymiteetillä Hilbertin käyrällä naa-



Kuva 3: Ensimmäisen, toisen ja kolmannen asteen Hilbertin käyrät piirrettynä punaisella, sinisellä ja mustalla. Asteluvun kasvaessa murtoviiva peittää yhä suuremman osan alueesta. [8]

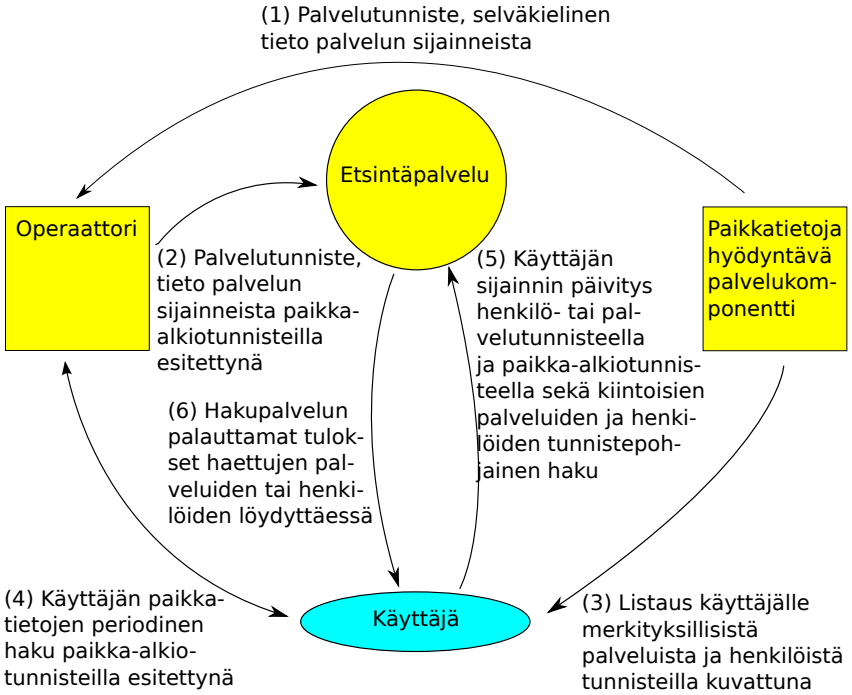
purustossa olevien solmujen maantieteellisten sijaintitietojen avulla sumennetun nelikulmion, jonka alueelta lähialuetietoja tullaan kysymään. Aktiivinen päätelaite lähettää nelikulmioalueen pseudonymisoivan (ei välttämättä järjestelmänlaajuisesti aina saman) palvelimen välityksellä varsinaiseen paikkatietoja hyödyntävään palveluun. Palvelu vastaa palauttamalla lähialueen kiintoisat pisteet, jotka välitetään takaisin aktiiviselle päätelaitteelle. Lopuksi päätelaite valitsee palautetusta tietomassasta itselleen tarpeelliset hakutulokset.

3.6 Trust No One

Trust No One on hajautettu hakujärjestelmä paikkatietoja hyödyntäviä palveluita varten. [9] Järjestelmä keskittyy yksityisyydensuojan parantamiseen operointikontekstissa ja sen ovat kehittäneet Sharad Jaiswal sekä Animseh Nandi. Siinä missä moni muu yksityisyyttä parantava järjestelmä tarvitsee luotetun ja keskitetyn välityspalveluratkaisun, Trust No One on kehitetty autonomiseksi tästä tarpeesta.

Jaiswal ja Nandi ovat tehneet havaintoja henkilöiden tietojen subjektiivisesta suojaustarpeesta paikkatietoja hyödyntävissä palveluissa sekä pohdintoja luotetun osapuolen problematiikasta. Tutkijoiden mielestä tärkeimmät suojeltavat tiedot ovat paikkatietokoordinaatit, sijainnilliset mielenkiinnonkohteet, sekä sosiaaliset verkostot, jotka järjestelmistä on mahdollista generoida. Tutkijat miettivät luotetun osapuolen suhteen, mikä

taho olisi sopiva tällaiseen “valtaan ja vastuuseen”. Olisiko se välityspalvelin vai operaattori? Huomioitavaa on, että vaikka esimerkiksi operaattori olisi juridisesti velvoitettu tietämään käyttäjien paikkatiedot, operaattorien ei tarvitse tietää sosiaalisista verkostoista tai käyttäjien mielenkiinnon kohteista. Toisin sanoen myös operaattoreita vastaan käyttäjällä on suojattavaa. Tämän takia tutkijoiden mukaan luotetusta välityspalvelinratkaisusta ei ole yksistään turvallisen järjestelmän perustaksi.



Kuva 4: Trust No One -järjestelmän keskeiset toimijat ja niiden välinen vuorovaikutus. [9]

Trust No One -järjestelmän toimintaperiaate on vastaavuuksien tai parien löytäminen paikkatietojen ja alueen palvelujen tai ihmisten suhteen hajauttamalla tarpeellisten tietojen käsittely kolmelle peruskomponentille [9]. Tätä etsintää varten jokainen tarkastelualueen paikka-alkio koodataan jollakin tunnisteella. Samoin tehdään palveluille/ihmisille. Esimerkiksi pizzapaikalla voi olla palvelutunnus B465 ja sushi-ravintolalla B380 sekä jollakin tietyllä henkilöllä vaikkapa B89121. Järjestelmän etsintäpalvelu vertaa keskenään paikka-alkiotunnisteita ja palvelutunnisteita ja palauttaa löydetyt parit.

Järjestelmässä paikka-alkiotunnisteiden hallinnasta päättää operaattori. Paikkatietoja hyödyntävä palvelukomponentti toimii palvelu/henkilötunnisteiden hallinnoinnista. Se rekisteröi palveluiden tunnistenumerot ja lähettää ne oikeiden palvelujen paikkatietojen kanssa operaattorille. Operaattori vaihtaa paikkatiedot paikka-alkiotunnisteisiin ja lähettää ne etsintäpalvelulle. Voidaan sanoa, että tässä vaiheessa infrastruktuurisen paikkatietojen osalta järjestelmän alustus on saatu suoritettua.

Kun varsinainen käyttäjä saapuu järjestelmään, tapahtuu seuraavaa. Käyttäjä pyytää paikkatietoja hyödyntävältä palvelukomponentilta tietoja siitä, millä tunnisteilla sitä kiinnostava palvelut tai ihmiset on osoitettu. Se saa myös tiedon omasta tunnisteestaan. Tämän jälkeen käyttäjä kysyy operaattorilta periodisesti tietoja omasta sijainnistaan ja lähettää etsintäpalveluun kyselyitä, joissa on käyttäjän oma tunniste, henkilön sijaintitiedon paikka-alkiotunniste ja lista paikka- ja henkilötunnisteina niistä henkilöistä tai palveluista, joista käyttäjä on kiinnostunut. Kun tällainen mielenkiintoinen paikka löydetään, etsintäpalvelu palauttaa käyttäjälle tiedon asiasta [9]. Kuvassa 4 on kuvattu järjestelmän toimintaperiaate.

Etsintäpalvelun sisäinen toteutus on tehty DHT-tyyppisellä vertaisverkkomallilla. On huomattava, että etsintäpalvelu ei missään vaiheessa tiedä tarkasti henkilöiden/palveluiden ja paikkatietojen vastaavuutta vaan ainoastaan näiden tunnisteet. Palvelun suojausominaisuus on juuri tämäntyyppisessä oivaltavassa “vallan hajauttamisessa”.

3.7 CliqueCloak

CliqueCloak on anonymisointikonsepti, joka tukee k-anonymiteetin lisäksi vapaasti valittavia sijainnin ja aikaikkunan tarkkuusparametreja. Järjestelmän tekijöiden Bugra Gedikin ja Ling Liun mielestä aikaisemman samoja parametreja käyttävän toteutuksen [4] ongelma on mm. k:n staattisuus ja järjestelmän huono palvelutaso. CliqueCloakissa k-parametri on viestikohtainen. [3]

Järjestelmä toimii siten, että se olettaa joukon luotettuja ja turvallisia anonymisointipalvelimia. Päätelaite ottaa palvelimeen salatun yhteyden ja lähettää sijaintitietonsa. Anonymisointipalvelin poistaa tiedoista mahdollisimman paljon päätelaitetta yksilöivää tietoa, minkä jälkeen se suorittaa paikkatiedon ja siihen liittyvän aikatiedon sumentamisen CliqueCloak-algoritmilla. Tämän jälkeen anonymisoitu tieto välitetään varsinaiseen paikkatietoja hyödyntävään palveluun. K-anonymiteetin saavuttaakseen voidaan siis käyttää kahta eri parametria tietojen häivytykseen. Nämä tiedot ovat aikatieto ja paikkatieto. Aikatiedolla ei ole sovelluksen kannalta suurempaa auktoriteettiasemaa, vaan se toimii koordinaattiavaruuden yhtenä lisäulottuvuutena.

CliqueCloakin perimmäinen idea pohjautuu erilaisiin aika-avaruuden ryhmiin tai klikkeihin (josta englanninkielinen nimikin tulee). [3]. Järjestelmässä jokaisen paikkatietoviestin sumentamisen jälkeen aika-avaruudesta etsitään niiden viestien ryhmiä, jotka täyttävät vaaditut k-anonymiteettivaatimukset. Jokaisesta paikkatietoviestistä tulee avaruuteen oma kuutionsa, jota geometrisesti rajaavat tiedot x- ja y-koordinaateista ja aikaparametrista. Algoritmi vertailee näitä kuutioita keskenään ja yrittää löytää joukosta kolmiulotteisen alueen, jonka kaikki paikkatietoviestialueet tunnuslukuineen sisältävät. Tällaisen ryhmän löydyttyä kaikki ryhmään kuuluvat viestit lähetetään eteenpäin varsi-

naiseen paikkatietosovellukseen. Ennen lähettämistä jokainen viesti saa tunnusluvuikseen löydetyn ryhmän parametrit, eikä omia varsinaisia paikka- tai aikatietoja. Ne viestit, joita ei kelpuutettu, jäävät odottamaan uusia viestejä, joiden kanssa sopivia ryhmiä voisi muodostua. Kaikista vanhimmat viestit poistetaan vanhentuneina järjestelmästä, kun tarpeeksi aikaa on kulunut.

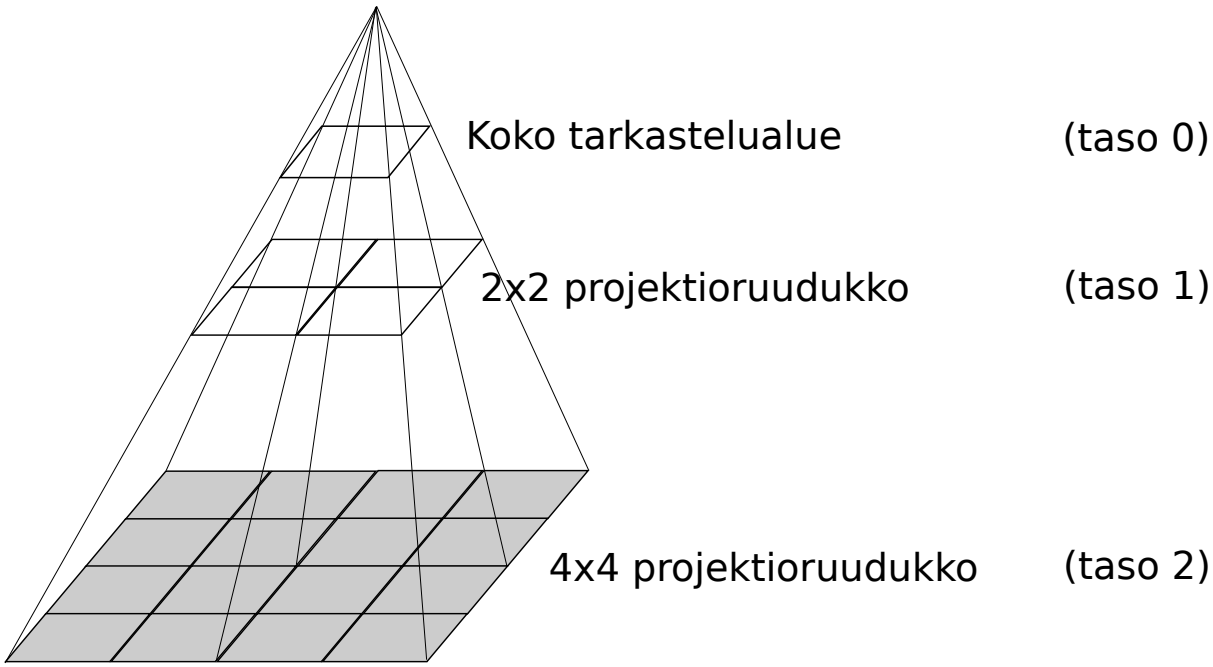
3.8 Casper

Casper on mobiilipäätelaitteita varten kehitetty yksityisyydensuojaa parantava järjestelmä. [2]. Järjestelmä on kehitetty vuonna 2006, jolloin paikkatietopalvelujen kasvu oli "jo" räjähdysmäistä. Casper koostuu kahdesta pääkomponentista, jotka ovat paikkatiedon anonymisoija ja tätä tukeva pyyntökäsittelijä. Casper lupaa tarjota korkeatasoisen paikkatietopalvelukokemuksen ja säilyttävänsä samalla käyttäjän yksityisyyden. Järjestelmän kehittäjät Mokbel, Chow ja Aref tunnistavat pseudonymiteettiin pohjautuvien järjestelmien vaara-alttiuden esimerkiksi tilanteessa, jossa pseudonyymi käyttäjä haluaa etsiä lähimmän ravintolan. Casper on kehittäjiensä mukaan myös huomattavasti parempi järjestelmä kuin alan aikaisemmat toteutukset aika- ja paikkatietojen sumennus (spatial and temporal cloaking) ja CliqueCloak [2]. Järjestelmä tukee erilaisia kyselytyyppejä: yksityiset kyselyt julkisesta datasta, julkiset kyselyt yksityisestä datasta ja yksityiset kyselyt yksityisestä datasta. Anonymisoinnin takia järjestelmä ei pysty palauttamaan käyttäjälle eksakteihin paikkatietoihin perustuvia vastauksia kyselyihin. Sen sijaan palvelu palauttaa kandidaattilistan mahdollisista vastauksista. Näiden vastausten lomasta päätelaite pystyy valitsemaan haluamansa tiedon.

Casperin yksinkertaisen paikkatiedon anonymisoijan tietorakenne on pyramidimainen tasoruudukko, jossa pidetään kirjaa kunkin ruudun tunnisteesta ja ruudun alueella olevien päätelaitteiden määrästä. Tasoja on useita, ja niistä korkein (nollataso) tarkoittaa koko maantieteellistä tarkastelualuetta. Kaikki käyttäjät pystyvät sijoittumaan tämän tasoruudun alueelle. Mentäessä tasoille 1 ja eteenpäin aluetta kuvaavan tasoruudukon ruutujen määrä kasvaa (2x2, 4x4, 8x8 jne.). Samalla käyttäjän sijaintitarkkuus paranee. Kuvassa 5 kyseinen idea on esitetty visuaalisesti.

Erillisessä hajautustaulussa on tietoalkiona käyttäjän tunniste, käyttäjän määrittelemä yksityisyysprofiili ja pyramiditasoruudun numero. Käyttäjä kertoo päätelaitteensa avustuksella yksityisyysprofiilinsa, jonka perusteella anonymisoija tekee työnsä. Profiilin parametrit ovat k-anonyymiys ja A_{min}. [2]. A_{min} on parametri, joka tarkoittaa tarkoittaa sitä, että käyttäjä on havaittavissa minimissään A_{min} kokoisen maantieteellisen karttaruudun (oikean tai jollain tavalla projisoidun) alueella.

Anonymisoija laskee käyttäjän koordinaateista hajautusfunktiolla arvon, joka kuvaa koordinaatin tasoruudukon alimpaan osaan. Arvo on uusi ruutunumero. Tämän jälkeen teh-



Kuva 5: Casper-järjestelmän tietorakenteen pyramidimalli. [2]

dään yksityisyysprofiilin perusteella käyttäjän sijaintitarkkuuden sumentaminen siten, että palautettava ruutunumero on joko ruutu itse, ruutupari naapurin kanssa, tai jokin ruudun isäruudusta tietopyramidin huippua kohti (huippua kohdenhan tarkkuus heikentyi). [2]

Casper sisältää myös edistyneemmän anonymisoijan, joka toimii perusversiota nopeammin. Toiminta on muuten samanlaista, mutta siinä missä perusversiossa operointi aloitetaan pyramiditasoruudukon alimmasta kerroksesta, edistyneemmässä versiossa käytetään vain niitä osia tietorakenteesta, jotka on yksityisyysprofiilien nojalla sallittu. Voi ilmentyä esimerkiksi tilanne, jossa sumentamistarkkuus on kaikilla päätelaitteilla sellainen, ettei sitä voida sitoa tarkimman tasoruudukon resoluutioon. Tällöin kyseistä tasoa ei käytetä ollenkaan. Seurauksena on operaatioiden nopeutuminen.

Casperin pyyntökäsittelijä käyttää tietokannassa kahdentyyppisiä tietoalkioita, julkisia ja yksityisiä. Yksityinen paikkatieto on tallennettuna summittaisena, julkinen taas tarkasti. [2] Tietokannasta tehtävät haut perustuvat tasoruudun ja sen lähialueiden (tarkkojen tai summittaisten) paikkatietojen geometrisiin suodatuksiin ja hakukandidaattilistan palauttamiseen. Lopuksi päätelaite valitsee kandidaateista oman tarkan sijaintitietonsa avulla halutun vastauksen.

4 Arkiset paikkatietoa hyväksikäyttävät palvelut ja suojautuminen

4.1 Yleistä

Edellä käsiteltyjen, ehkä hieman teoreettisten järjestelmien ja mallien lisäksi voidaan löytää myös arkisia paikkatietopalveluita, joissa käyttäjä saattaa haluta nostaa yksityisyydensuojaansa joko ideologisista syistä tai saavuttaakseen jotain muuta hyötyä kuten uusiin mediasisältöihin pääsemistä menettämättä yksityisyyttään. Seuraavaksi käsitellään paria tällaista arkipäiväisempää tilannetta ja suojautumista niissä.

4.2 Näkökulmana IP-osoite paikkatietona

Erilaisia Internetin medianjakelukanavia voidaan pitää paikkatietoja hyödyntävinä palveluina. Näkyvin esimerkki näistä peruskäyttäjälle ovat mainospalvelut, mutta myös erilaiset audiovisuaaliseen sisältöön liittyvät viihdepalvelut ovat yleistymässä. Palvelut tunnistavat käyttäjän paikkatiedon IP-osoitteesta käyttämällä erillisiä ns. GeoIP-tietokantoja, joihin on listattu IP-osoitteiden maantieteellisiä vastaavuuksia eri alueisiin ja toisinaan jopa kaupunginosiin. [10]

Mainostajien osalta paikkatietojen hyödyntämisen tarve on selkeä: Käyttäjille halutaan tarjota mainoksia sellaisiin tuotteisiin ja palveluihin, joita hän voi helposti ostaa ja kuluttaa vailla maantieteellisiä esteitä. Mainostaja voi pyrkiä vaikuttamaan positiivisesti ostopäätökseen myös käyttämällä käyttäjän oletettua äidinkieltä.

Mediapalveluissa käyttäjän paikkatietojen kaksi suurinta sovellusaluetta ovat maantieteellinen markkinasegmentointi ja sisällönvälitys. Segmentoinnissa pyritään siihen, että mikään markkina-alue ei pääse käsiksi mediasisältöön ennen kyseisen alueen virallista julkaisuajankohtaa. Esimerkiksi juuri USA:ssa julkaistun televisiosarjan osaa ei välttämättä voida katsoa kuin USA:ssa sijaitsevien IP-osoitteiden kautta. Toisinaan segmentoinnissa mediasisältöä ei haluta julkaista jollekin markkina-alueelle lainkaan. Käyttäjällä voi olla tarve saada haltuunsa mediasisältöä ennen kansallisia julkaisuajankohtia myös oman markkina-alueensa ulkopuolelta. [11]

Mediasisällönvälitys on toinen merkittävä aihe. Saamalla tieto siitä, missä käyttäjä sijaitsee, voidaan valita hänen kannaltaan optimaalisin väylä median välitykseen. Esimerkiksi monien suoratoistovideopalveluiden saattaa olla kannattavaa pitää paikallisia medianvälityspalvelimia korkealaatuisen mediasisällön lähettämisen mahdollistamiseksi, sen sijaan että käytettäisiin hitaampia ja korkealatenssisempia ulkomaanyhteyksiä keskuspalvelimiin. Sisällönvälityspalvelinten hajasijoitustoiminnan “kylkiäisenä” tulee helppo mahdol-

lisuus soveltaa järjestelmää myös markkina-aluesegmentointiin.

Edellä mainittuja ongelmia voidaan ratkaista häivyttämällä käyttäjän IP-osoitetietoja mainos- ja medianvälityspalvelimilta. Tämä voi tapahtua esimerkiksi käyttämällä välityspalvelimia (proxyt) tai virtuaalisia erillisverkkoja (VPN). Molempien tekniikoiden toimintaperiaate on se, että käyttäjä ottaa kyseisiin palveluihin yhteyttä ja käyttää niiden kautta varsinaista sisältöpalvelua. Tässä sovelluskontekstissa virtuaalisen erillisverkkoyhteyden päätepisteen tai välityspalvelimen täytyy sijaita sellaisella maantieteellisellä alueella, jossa palvelun suuntaan tapahtuvalla anonymiteetin kasvulla on hyötyä. Esimerkiksi mainospalveluissa mainokset eivät sinänsä ehkä häviä minnekään, vaan korvautuvat kyseisten alueiden "räätälöidyillä" mainoksilla. Näin ollen mainostajalla ei kuitenkaan ole tietoa loppukäyttäjän oikeasta sijainnista, eikä hänestä pystytä tekemään paikkansapitävää kuluttajaprofilointia. On muistettava, että IP-osoite ei ole välttämättä ainoa käyttäjän tunnistava tekijä mainospalvelinten suuntaan, vaan päätelaitteet voivat viestiä niille myös meta-tietojen (kuten www-selainten cookieiden) avulla. [11]

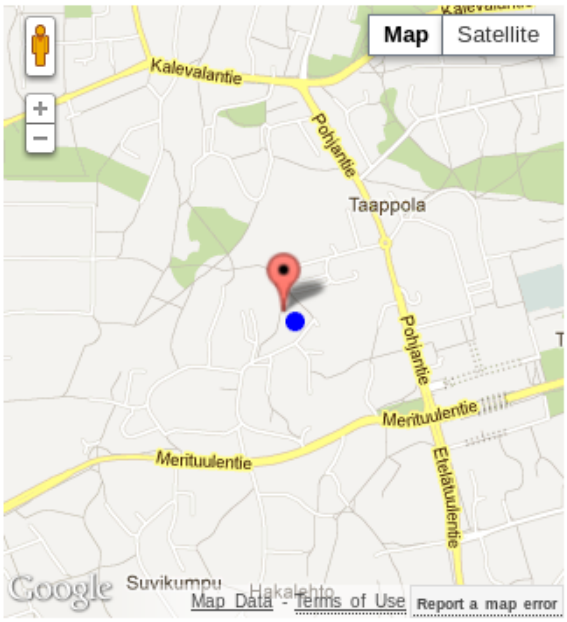
Mediapalveluissa edellä mainittujen ratkaisun käyttämisellä voidaan saavuttaa tyypillisesti kaksi asiaa. Nämä ovat pääsy erilaiseen mediasisältöön ja palvelun laadun muutos. Koska virtuaalisten erillisverkkojen ja välityspalvelinten käyttö saa yhteyden mediapalveluun näyttämään tulevan uudelta markkina-alueelta, päätelaitteelle voidaan tarjoilla erilaista mediasisältöä. Esimerkiksi USA:ssa sijaitseva välityspalvelin voi antaa suomalaisen päätelaitteen näytettäväksi sellaisia vasta julkaistuja elokuvia, jotka näytettäisiin Suomessa vasta useiden kuukausien viiveellä. Samaisen esimerkin voimin voidaan miettiä myös palvelun laadun muutosta. Koska uusi järjestely ohittaa kansallisen medianvälityspalvelimen kokonaan, verkkolatenssit kasvavat ja tyypillisesti myös käytettävissä oleva kaista kutistuun. Nämä muutokset voivat joskus laskea dramaattisesti välitetyn mediasisällön laatua.

4.3 Www-selainpohjaiset paikkatietopalvelut

Kehittyneet www-selaimet sisältävät nykyään mahdollisuuden paikkatietoa hyödyntävien www-palvelujen kanssa toimimiseen. Mozilla-säätiön Firefox-selain on eräs näistä. Firefox käyttää paikkatiedon löytämiseen tietokoneen IP-osoitetta ja tietoa läheisistä langattomista verkoista [12] sekä uniikkia tunnistetta, joka vaihtuu määräajoin. Mielenkiintoisin tekniikka näistä on langattomien verkkojen käyttö.

Tässä mallissa selaimen käyttäjän paikkatiedot saadaan selville lähettämällä tieto käyttäjän koneen lähistön WLAN-verkoista paikkatietopalveluun, esimerkiksi Googlelle. Paluuviestinä saadaan paikkakoordinaatit. Allekirjoittaneen Google onnistui paikantamaan suorastaan pelottavalla tarkkuudella, kuten kuvasta 6 nähdään. Paikannus osuu kohdalle noin 20 metrin tarkkuudella sinisen pallon edustaessa oikeaa sijaintia.

Here is a live example of using geoPosition.js to attempt to get your location and display a map of your immediate surroundings:

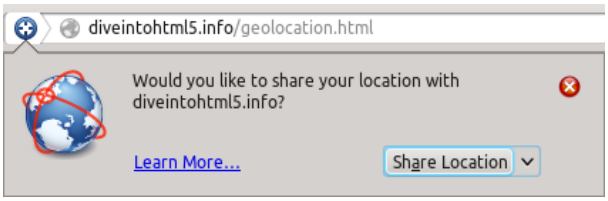


Kuva 6: Firefox-selaimen paikkatunnistustarkkuus taajama-alueella. [13]

Google kerää paikkatietoja paikkatietokantaansa Android-alustansa kautta. Tekniikkaa valotetaan Wall Street Journalin artikkelissa [14]. Päätelaitteet lähettävät palveluntarjoajalle tiedot lähistöllä näkemistään WLAN-verkoista ja GPS-koordinaateista. Tämä luo linkin WLAN-verkkojen tunnistetietojen ja maantieteellisen sijainnin välille. Aikaisemmin Google keräsi tietoja myös StreetView-kartoituksen aikana, mutta lopetti kertomansa mukaan käytännön, kun kerättyyn tietomassaan tuli vahingossa mukaan sivullisten käyttäjätunnuksia, salasanoja ja sähköpostiosoitteita. Wall Street Journalin mukaan paikkatietoja päätelaitteiden avustuksella kerää myös Apple, mutta olisi todella outoa, jos millään muulla alustalla näin ei tapahtuisi. Teknisesti asia olisi ainakin helppo toteuttaa.

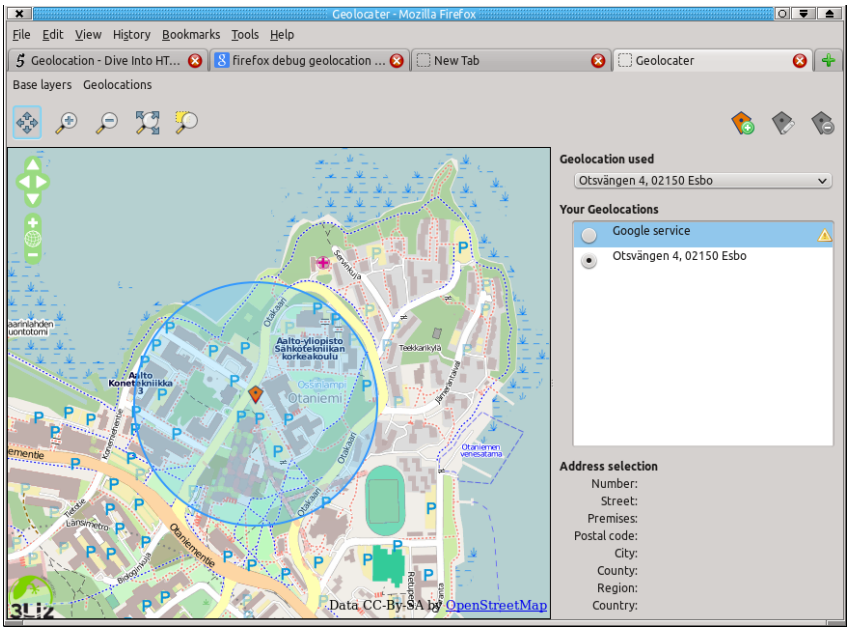
Kuten jo työn alkuluvuissa kerrottiin, periaatteessa paikkatieto hyödyntävissä palveluissa on aina mahdollisuus kytkeä paikkatiedon lähettäminen pois päältä. Tämä on eritoten totta W3C:n sijaintipaikannusmäärittelyssä, joka eksplisiittisesti kieltää käyttäjän paikannuksen ilman tämän nimenomaista lupaa [15]. Mozillan Firefox-selain toteuttaa ainakin määrittelyä tarkasti, eikä anna tehdä paikannusta ilman käyttäjän lupaa, kuten oheisesta kuvasta 7 voidaan nähdä.

Mikäli käyttäjä haluaa suojata tarkan sijaintinsa palveluilta, hän voi lähettää palveluihin



Kuva 7: Firefox-selaimen paikkatunnistuspyynnön kyselyikkuna.

paikkatietoa, joka on eksplisiittisesti kiinnitetty johonkin tiettyyn paikkaan jollakin tarkkuudella. Firefox-selaimelle on jo olemassa lisäosa, jossa selaimen sijainnin voi asettaa staattisesti. Tätä työtä varten tehtiin koe, jossa Firefox-selaimeen ladattiin Geolocater-lisäosa [16]. Lisäosan avustuksella allekirjoittaneen sijainti "siirrettiin" Espoon Tapiolasta Otaniemen kampusalueelle kuvan 8 osoittamalla tavalla.

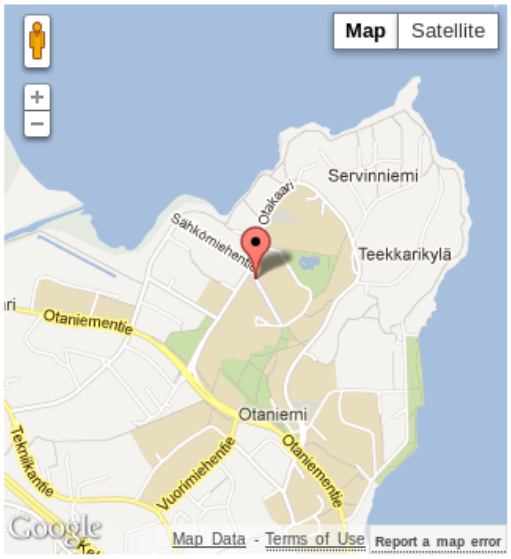


Kuva 8: Staattisesti Otaniemen kampusalueelle kiinnitetty paikkatietoasetus.

Asetuksen käyttöönoton jälkeen aikaisemman kuvan 6 osoittamassa tapauksessa selain myös oikeasti paikansi itsensä halutusti Otaniemeen eikä Tapiolaan, kuten kuvasta 9 voidaan havaita.

Haluttaessa suojata yksityisyyttä edellä mainitun Geolocater-lisäosan avustuksella, ongelmana on se, että paikkatietojen sumentamisen joutuu tekemään jokaisessa fyysisessä sijainnissa erikseen. Toisaalta, mikään ei estä sellaisen oman lisäosan tekemistä, joka hoitaisi sumentamisen automaattisesti. Tällainen lisäosa voisi toimia siten, että käyttäjä määrittelee ensin yksityisyysprofiilin, jonka pohjalla sumennuksia tehdään. Profiilissa voitaisiin esimerkiksi kieltää päätelaitteen uniikkitunnisteen lähettäminen ja määrittää,

Here is a live example of using geoPosition.js to attempt to get your location and display a map of your immediate surroundings:



Kuva 9: Otaniemen kampusalueelle osoittava paikannus.

mitä WLAN-verkkojen tunnisteita lähetetään paikkatietopalveluun ja millä tarkkuudella. Palvelu palauttaisi koordinaatit, jotka sijaitsevat lähellä käyttäjän sijaintia kohtalaisen palvelun laadun takaamiseksi, muttei kuitenkaan kertoisi käyttäjän tarkkaa sijaintia.

5 Yhteenveto

Työssä havaittiin, että moni yksityisyydensuojaa paikkatietopalveluissa parantava järjestelmä vaatii luotetun komponentin, joka vastaa oikeiden paikkatietojen sumentamisesta pienemmälle tarkkuudelle. Usein tämä komponentti sijaitsee läheisesti itse paikkatietotietokannan yhteydessä, jolloin voidaankin jossain määrin kyseenalaistaa yksityisyydensuojan toteutuminen palvelun tuottajan suuntaan. Tämä siksi, että mikään ei periaatteessa estä tuottajaa kaappaamasta tarkkaa paikkatietoa ja sen hyödyntämistä esimerkiksi mainostustarkoituksiin.

Rohkeita poikkeuksiakin keskitetyn välityspalvelimen käytöstä on, erityisesti Jaiswalin ja Nandin “Trust No One”-järjestelmä, jossa tietojenkäsittely hajautettiin kolmelle eri komponentille [2] oli yksinkertaisuudestaan huolimatta vaikuttava.

Monissa tutkituissa järjestelmissä luotetaan “joukkovoimaan”. Tietoryhmiä liikutellaan käyttäjäjoukkoina, jolloin tietyn käyttäjän yksilöinti tästä joukosta vaikeutuu. Malli vaatii sen, että näitä yksittäisiä käyttäjiä on tarpeeksi järjestelmässä. Joissakin ratkaisuista

käyttäjät tai päätelaitteet avustavat suoraan toisiaan esimerkiksi osoitteistuksessa järjestelmän sisällä.

Monet järjestelmät myös painottavat valinnanvapautta käyttäjän omasta yksityisyydestä. Valitsemalla sopiva yksityisyysprofiili tai -asetuskokonaisuus käyttäjä voi tasapainoilla siinä, kuinka paljon yksityisyyttään hän "uhraa" palvelunlaatunsa eteen.

Suurin osa käsitellyistä järjestelmistä on siinä määrin akateemishenkisiä, ettei niiden yleistymistä voi tai kannata odottaa. Niistä voi kuitenkin olla suurempien tietojärjestelmien implementoijille suurta hyötyä joissakin erityiskäyttökohteissa, esimerkiksi jos jokin eettinen tai juridinen seikka vahvasti puoltaa yksityisyyden suojaa parantavan palvelukomponentin käyttöönottoa.

Käyttäjän kannalta turvallisin paikkatiedon anonymisointi tapahtuu päätelaitteessa, jolloin palvelun tuottajalla on pienemmät mahdollisuudet saada selville tarkat tiedot, joskin tässäkin tapauksessa joudutaan luottamaan palvelua käyttävän asiakasohjelman hyviin tarkoitusperiin. Todennäköisesti useimpia tyydyttävässä ratkaisussa tämä asiakasohjelma olisi avointa lähdekoodia tai muuten auditoitavissa.

Lähteet

[1] Richard B Parker. Definition of privacy, a. *Rutgers L. Rev.*, 27:275, 1973.

[2] M.F. Mokbel, C.Y. Chow ja W.G. Aref. The new casper: query processing for location services without compromising privacy. *Proceedings of the 32nd international conference on Very large data bases*, sivut 763–774. VLDB Endowment, 2006.

[3] Latanya Sweeney. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05):557–570, 2002.

[4] Marco Gruteser ja Dirk Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. *Proceedings of the 1st international conference on Mobile systems, applications and services*, sivut 31–42. ACM, 2003.

[5] Hidetoshi Kido, Yutaka Yanagisawa ja Tetsuji Satoh. An anonymous communication technique using dummies for location-based services. *Pervasive Services, 2005. ICPS'05. Proceedings. International Conference on*, sivut 88–97. IEEE, 2005.

[6] Alastair R Beresford ja Frank Stajano. Location privacy in pervasive computing. *Pervasive Computing, IEEE*, 2(1):46–55, 2003.

[7] Gabriel Ghinita, Panos Kalnis ja Spiros Skiadopoulos. Mobihide: a mobilea peer-to-peer system for anonymous location-based queries. *Advances in Spatial and Temporal Databases*, sivut 221–238, 2007.

[8] Richards Geoff. Hilbert curves. `http://en.wikipedia.org/wiki/File:Hilbert_curve_3.svg`, 7 2008. [Haettu 23.3.2013].

[9] Sharad Jaiswal ja Animesh Nandi. Trust no one: a decentralized matching service for privacy in location based services. *Proceedings of the second ACM SIGCOMM workshop on Networking, systems, and applications on mobile handhelds*, sivut 51–56. ACM, 2010.

[10] Brian Eriksson, Paul Barford, Joel Sommers ja Robert Nowak. A learning-based approach for ip geolocation. *Passive and Active Measurement*, sivut 171–180. Springer, 2010.

[11] Carlos Filipe Zambujo Lopes Pereira. Security on over the top tv services. Pro gradu, University of Lisbon, 2012.

[12] Mozilla Foundation. Location-aware browsing. `http://www.mozilla.org/en-US/firefox/geolocation/`. [Haettu 20.3.2013].

[13] Mark Pilgrim. Dive into html 5: You are not here (and so is everybody else). http://diveintohtml5.info/geolocation.html, 2011. [Haettu 20.3.2013].

[14] Julia Angwin ja Valentino-Devries Jennifer. Apple, google collect user data. http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html. [Haettu 20.3.2013].

[15] Andre Popescu. W3c proposed recommendation on geolocation api specification. http://www.w3.org/TR/geolocation-API/, 5 2012. [Haettu 21.3.2013].

[16] ReLuc. Geolocater add-on for mozilla firefox 1.6. https://addons.mozilla.org/en-us/firefox/addon/geolocater/, 3 2012. [Haettu 21.3.2013].