Älykellon sensoridataan perustuva QWERTY-näppäimistön käytön päättely

Laura Paajanen

kandidaatintutkielma
HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

Helsinki, 31. tammikuuta 2018

HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta — Fakultet — Faculty	Laitos — Institution — Department
Matemaattis-luonnontieteellinen	Tietojenkäsittelytieteen laitos

Tekijä — Författare — Author
Laura Paajanen

Työn nimi — Arbetets titel — Title

Älykellon sensoridataan perustuva QWERTY-näppäimistön käytön päättely

Oppiaine — Läroämne — Subject
Tietojenkäsittelytiede

Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
kandidaatintutkielma	31. tammikuuta 2018	19

Tiivistelmä — Referat — Abstract

Älykellojen yleistyessä ja niiden erilaisten sensoreiden kehittyessä kellosta saattaa muodostua käyttäjän QWERTY-näppäimistön käytön päättelyyn käytettävä väline. Kellon liikesensoreiden tallentamasta sensoridatasta voidaan päätellä kirjoittajan ranteen liikkeet näppäimistöllä kirjoitettaessa, jolloin oikeanlaisella opetus- tai vertailudatalla näppäimistön käyttöä on mahdollista palauttaa sekä neuroverkkoihin että Bayes-mallinnukseen perustuvilla datan analysointimenetelmillä. Tarkastelun kohteena on, millä tavoin älykellojen sensoridatan avulla on mahdollista selvittää käyttäjän QWERTY-näppäimistön käyttöä, sekä millaisia uusia mahdollisuuksia älykellojen käyttö näppäimistön käytön päättelylle tarjoaa. Käytön päättelyä älykellon sensoridatan perusteella tutkittaessa on saatu onnistuneita tuloksia, vaikkakin todellisissa hyökkäystilanteissa muun muassa hyökkäyksen kohteiden erilaiset kirjoitustottumukset asettavat haasteita päättelyn onnistumiselle.

ACM Computing Classification System (CCS):
Security and privacy - *Systems security* - Information flow control

Avainsanat — Nyckelord — Keywords
tietoturva, älykello, näppäimistön käytön päättely, neuroverkot, Bayes-mallinnus

Säilytyspaikka — Förvaringsställe — Where deposited

Muita tietoja — Övriga uppgifter — Additional information

Sisältö

1 Johdanto

Älykellot ja muut ranteessa käytettävät älylaitteet sisältävät lähes aina erilaisia liikkeitä havainnoivia sensoreita. Näiden sensoreiden dataa käytetään esimerkiksi laitteen hallintaan ja käyttäjän aktiivisuuden mittaamiseen, mutta sensoreiden tuottamaa dataa on mahdollista käyttää myös väärin esimerkiksi käyttäjän käsien liikkeiden perusteella tehtävään näppäimistön käytön päättelyyn.

International Data Corporation on arvioinut älykellojen myynnin kasvavan vuoteen 2021 mennessä jopa 70 miljoonaan kappaleeseen vuodessa kaikkien älyasusteiden arvioidun myyntimäärän ollessa lähes 200 miljoonaa [5]. Älypuhelimissa, joissa mahdollisiin sivukanavahyökkäyksiin on jo osattu varautua, yksittäisen käyttäjän aktiivinen käyttöaika jäi vuonna 2013 keskimäärin 58 minuuttiin vuorokaudessa [10]. Vaikka puhelimien käyttöaika onkin varmasti viime vuosina kasvanut, on älykellojen aktiivinen käyttöaika tästä huolimatta suurempi laitteen ollessa ranteessa ja toiminnassa jatkuvasti, jopa vuorokauden ympäri. Tällöin hyökkäykseen tarvittavaa dataa on mahdollista saada käyttäjältä paljon.

Älykellojen ja niiden liikesensorien tuottaman datan turvallisuutta on viime aikoina herätty tutkimaan enemmän, ja mahdollisia menetelmiä joilla tunnistaa sensoridatan perusteella QWERTY-näppäimistöllä näppäiltyä tekstiä on löydetty useita. Näiden tutkimusten perusteella mahdolliselle hyökkääjälle riittää päästä käsiksi älykellon lähettämään sensoridataan, jonka avulla on mahdollista palauttaa korkealla onnistumisprosentilla käyttäjän kirjoittama teksti.

Tutkielmassa perehdytään siihen, mitä uusia mahdollisuuksia älykellojen liikesensoridata tarjoaa QWERTY-näppäimistön käytön päättelyyn, sekä millä menetelmillä liikesensoridatasta on mahdollista päätellä käyttäjän näppäimistön käyttöä. Asiaan perehdytään kolmen toisistaan toteutustapojen osalta poikkeavan älykellon liikesensoridataan perustuvan tutkimuksen kautta, joissa sensoridatan avulla on pyritty palauttamaan käyttäjien näppäimistön käyttöä neuroverkkojen sekä todennäköisyysmallinnuksen avulla.

Luvussa 2 käsitellään yleisesti QWERTY-näppäimistön käytön päättelytapojen lähtökohtia, sekä tarkastellaan aiemmin käytettyjen menetelmien heikkouksia älykellon tarjoamien, käytön päättelyä helpottavien tekijöiden näkökulmasta. Lisäksi luvussa määritellään tutkimuskysymykset. Luvussa 3 esitellään kerätyn ääni- ja liikesensoridatan mahdollisia analysointimenetelmiä. Luvussa 4 syvennytään aiempiin QWERTY-näppäimistön käytön päättelyyn tähtääviin menetelmiin, joissa hyökkäykseen on käytetty mikrofonien sekä älypuhelimen liikesensorien tuottamaa dataa. Älykellon käyttämistä hyökkäyskanavana käsitellään luvussa 5, jossa tarkastellaan kolmen eri tavoin toteutetun tutkimuksen tuloksia käytön päättelyn menetelmistä älykellon liikesensoridatan perusteella. Tuloksien lisäksi perehdytään tutkimusmenetelmiin, tehokkuuteen sekä mahdollisiin heikkouksiin ja vahvuuksiin aiempiin

menetelmiin verrattuna. Luvussa 6 kootaan tehdyt havainnot sekä pyritään niiden avulla vastaamaan esitettyihin tutkimuskysymyksiin, esitellään mahdollinen suojautumismenetelmä älykellojen avulla tehtävää näppäimistön käytön päättelyä vastaan sekä pohditaan sen käyttöönoton mahdollisuuksia.

2 Näppäimistön käytön päättely

Näppäimistön käytön päättelyllä tarkoitetaan tilannetta, jossa ulkopuolisella henkilöllä on mahdollisuus saada tietoonsa hyökkäyksen kohteen näppäimistön painallukset. Käyttäjän näppäimistön käytön selvittäminen on erittäin vahingollista tiedon päätyessä hyökkääjän käsiin, sillä hyökkääjällä on tällöin pääsy esimerkiksi kaikkiin kirjoitettuihin sähköposteihin, käyttäjätunnuksiin ja salasanoihin. Tietokoneelle päätyvien näppäimistön käyttöä suoraan lukevien vakoiluohjelmien lisäksi näppäimistön käyttöä on mahdollista selvittää menestyksellisesti myös akustisten vuotojen [6] [17] [2], videon ja heijastuvien kuvien [3], näppäimistön alla olevan pöydän värähtelyn [15] sekä jopa wifi-signaalin muutosten avulla [1].

Monissa edellä mainituissa menetelmissä ongelmallista on ulkoisen datankerääjän, esimerkiksi mikrofonin, älypuhelimen tai kameran, sijainnin vaikutus kerättyyn dataan sekä mahdolliset kerääjään kohdistuvat häiriötekijät kerätyssä datassa [6]. Puhelimen mikrofonin tai liikesensoreiden keräämään dataan vaikuttaa muun muassa puhelimen vaihtaminen näppäimistön oikealta puolelta vasemmalle puolelle [15]. Äänidataan perustuva näppäimistön käytön päättely edellyttää muutoin kohtalaisen hiljaista käyttöympäristöä, jotta ympäröivät äänet eivät häiritsisi saatua äänidataa, ja kuvaan perustuvissa menetelmissä kameran tulee olla suunnattuna näppäimistöön tai sitä heijastaviin pintoihin, eikä edessä saa olla näköesteitä. Näitä häiriötekijöitä on saatu onnistuneesti vähennettyä käyttämällä datan keräämiseen älykelloa [13] [14] [16]. Aiempiin menetelmiin verrattuna älykellon käytössä datan keräämiseen on hyvänä puolena se, että kelloa käytetään lähtökohtaisesti samassa ranteessa, jolloin se on lähellä ja jatkuvasti lähes samalla etäisyydellä näppäimistöstä. Näin dataa kerättäessä virheellisiä tuloksia saadaan vähennettyä poistamalla sijainninvaihtelun aiheuttamat muutokset.

Tutkimuskysymyksiksi on valikoitunut, millä tavoin älykellojen sensoridatan avulla on mahdollista selvittää käyttäjän QWERTY-näppäimistön käyttöä, sekä millaisia uusia mahdollisuuksia älykellojen käyttö näppäimistön käytön päättelylle tarjoaa. Älykellojen liikesensoridataa näppäimistön käytön päättelyyn käyttäviä tutkimuksia arvioidaan niiden tulosten sekä todellisiin hyökkäystilanteisiin kohdistuvien rajoitusten kautta. Aiemmista tutkimuksista käsitellään näppäimistön äänen tallentamista sekä puhelimen liikesensoridataa hyödyntäneitä näppäimistön käytön päättelymenetelmiä. Sekä äänidatan että liikesensoreiden tuottaman datan analysointitavat ovat samankaltaisia, ja useissa tutkimuksissa tutkimusasetelmat vastaavat hyvin

toisiaan. Aiemmissa tutkimuksissa käytettyjen datan analysointimenetelmien implementoinnin toimivuutta tarkastellaan liikesensoridatan analysoinnin kannalta, ja tutkimusasetelmien samankaltaisuuksia ja eroavaisuuksia pyritään hahmottamaan arvioimalla tuloksia sekä menetelmissä havaittuja heikkouksia.

3 Datan analysointimenetelmiä

Sekä ääni- että liikesensoridatan analysoinnissa saadusta datasta pyritään ensin päättelemään juuri näppäinten painalluksen aiheuttamat muutokset datassa. Äänidatasta pystytään erottamaan sekä näppäimen painalluksesta että sen vapauttamisesta aiheutuva ääni. Tutkimuksissa yksittäisen painalluksen pituudeksi on määritelty 100ms [6], ja tutkimusdatassa tapahtuneita muutoksia tutkitaan kyseisen ajanjakson sisällä. Liikesensoridatasta näppäimistön painallukset erotetaan z-akselilla tapahtuvien muutosten avulla, jolloin tällä akselilla tapahtuneen näppäilypiikin perusteella tutkimuksen kohteena on käden sijainti x- ja y-akseleilla painalluksen tapahtuessa. Kun sensoridatasta on saatu eroteltua näppäimien painalluskohdat, voidaan älykellon dataa tutkia esimerkiksi neuroverkkojen [14] [13] ja Bayes-mallinnuksen [16] avulla.

3.1 Neuroverkot

Näppäimistön käytön päättelyyn tähtäävässä sensoridatan analysoinnissa on mahdollista käyttää esimerkiksi neuroverkkoja. Neuroverkkojen toiminta perustuu yksittäisiin laskentayksiköihin, neuroneihin, jotka ovat yhteydessä toisiinsa [9]. Jokainen neuroni tekee oman laskentavaiheensa, ja neuroverkon rakenteesta riippuen antaa tuloksensa syötteenä eteenpäin joko yhdelle tai useammalle neuronille. Neuronit saavat syötteenään arvoja $x_1, ..., x_n$, ja neuroneiden arvoille ja niiden kaarien $w_1, ..., w_n$ painoille lasketaan pistetulo, joiden summan ja valitun aktivaatiofunäiktion f perusteella kyseinen neuroni tuottaa oman tulosteensa

$$f(\sum_{j=1}^{n} w_{ij}x_j).$$

Painokertoimien asettamiseksi oikein voidaan käyttää niin kutsuttua opetusdataa. Neuroverkon ohjatussa opetuksessa neuroverkolle annetaan ensin käsiteltäväksi valmiiksi luokiteltuja syötteitä, joiden haluttu tulos tiedetään. Neuroverkon painokertoimia muokataan syötteen avulla siten, että lopulta saadut tulosteet vastaavat odotettuja. Tämän jälkeen neuroverkolle voidaan antaa syötteenä tutkimusdataa, jonka luokittelu tapahtuu muokattujen painokertoimien avulla. Ohjaamattomassa neuroverkon opetuksessa neuroverkko saa opetussyötteenään dataa, josta se klusteroi samankaltaisimmat näytteet omiin luokkiinsa. Tällöin valmiita luokkia ei anneta suoraan, vaan luokat voidaan päätellä muodostettujen klustereiden avulla.

Yksinkertainen esimerkki neuroverkkoluokittimesta on perseptronialgoritmi, jolla opetussyötteen perusteella annettu syöte on jaettavissa kahteen eri luokkaan [9]. Luokittelu edellyttää että annettu opetusdata on lineaarisesti eroteltavissa. Muussa tapauksessa luokittelu määritetään loppumaan tietyn opetusaskelmäärän jälkeen.

3.2 Bayes-mallinnus

Sensoridatan analysoinnissa voidaan käyttää myös Bayes-mallinnusta, joka perustuu ehdolliseen eli posterioritodennäköisyyteen $P(W \mid O)$. Bayesin kaavalla

$$P(W \mid O) = \frac{P(O \mid W)\, P(W)}{P(O)}$$

saadaan laskettua ehdollinen todennäköisyys tapahtumalle $P(W \mid O)$ eli tapahtuman W todennäköisyys ehdolla O on tapahtunut [4].

Tutkimuksessa [16], jossa näppäimistön käytön päättelyyn on käytetty Bayes-mallinnusta, pyrittiin laskemaan posterioritodennäköisyys jokaiselle englanninkielisessä sanakirjassa esiintyvälle sanalle ehtona tapahtuneet liikesensoridatasta pääteltyjen kirjainten painallukset. Bayesin kaavan toimivuutta lisättiin huomioimalla mahdolliset kahden lähekkäisen merkin painallukset, joita sensoridatasta on vaikea havaita. Myös edellisen näppäillyn merkin sijainnin vaikutus ja kirjoitusnopeus huomioitiin tarkentamalla todennäköisyyden laskentakaavaa toimivammaksi. Todennäköisyyksien laskennan jälkeen algoritmi palautti sanakirjassa esiintyvät sanat ja niiden ehdolliset todennäköisyydet listana pareja <sana, todennäköisyys>.

4 Näppäimistön käytön päättely ääni- ja liikesensoridatan perusteella

Mikrofonilla tallennettua äänidataa on tutkimuksissa onnistuttu analysoimaan tehokkaasti, ja näppäimistön näppäimien painallusten yksilöllisistä äänistä on pystytty päättelemään käyttäjän kirjoittamaa tekstiä. Näissä näppäimistön lähelle on asetettu mikrofoni, jolla äänitetystä datasta on eroteltu kirjainten painallus- ja vapautusääni. Saatua äänidataa voidaan analysoida yksittäisten kirjainten, kirjainparien sekä ennalta määritettyjen sanakirjojen avulla. Liikesensoreiden avulla näppäimistön käyttöä on kyetty päättelemään esimerkiksi näppäimistön viereen asetetun puhelimen liikesensoridatan perusteella. Tällöin näppäilyn aiheuttama värähtely pöydän pinnassa on eroteltu merkeittäin, ja painallukset on jaoteltu näppäinten etäisyyden perusteella kirjainpareihin.

4.1 Käytön päättely kerätyn äänidatan perusteella

Äänidataan ja yksittäisten kirjainten sijaintiin perustuvassa tutkimuksessa [6] huomattiin, että sen lisäksi, että jokaisen näppäimen ääni on yksilöllinen, ääni myös korreloi näppäimen sijainnin kanssa. Näppäinten äänien samanlaisuus on suurinta muiden lähimpänä sijaitsevien näppäinten kanssa, ja pienimmät samanlaisuudet ääninäytteissä ovat toisistaan kauimpien näppäinten välillä. Näin jokaiselle kirjaimelle voidaan muodostaa taulukko, jossa määritellään kirjaimen vierusnäppäimet sekä muut, kauempana sijaitsevat näppäimet. Tutkimuksessa äänidatasta eroteltujen painallusäänien samankaltaisuutta tutkitaan signaalinkäsittelymenetelmillä, joilla tulokseksi saadaan yksittäisiä n pituisia sanoja, joiden kirjainten sijaintien korrelaatiot tiedetään. Tutkimuksessa käytetään yleisimmistä englanninkielisistä sanoista koostuvaa corncob-sanalistaa [7]. Äänidatasta erotellun sanan kirjainten sijaintikorrelaatiota verrataan kaikkien sanakirjassa esiintyvien n pituisten sanojen kirjainten kanssa, jolloin tulokseksi saadaan lista äänidataprofiliin parhaiten täsmäävistä sanakirjasanoista.

Edellä käsitellyssä tutkimuksessa käytön päättely perustuu kirjainten ääniin ja erityisesti sijaintiin suhteessa toisiinsa, minkä vuoksi erillistä opetusdataa ei käytön päättelyä varten tarvita. Neuroverkkoja äänidatan analysoinnin apuna käyttävissä tutkimuksissa opetusdatana on käytetty hyökkääjän näppäimistön käyttöä [2] sekä englanninkielisten sanojen ja kieliopin asettamia rajoituksia mahdollisten kirjainyhdisteiden ja sanojen rajaamiseksi [17]. Kuvitellun hyökkääjän syöttämään neuroverkon opetusdataan perustuvassa tutkimuksessa [2] opetusdatana käytetään yksittäisten kirjainten toistuvia painalluksia. Jokaista tutkittua kirjainta painetaan sata kertaa, ja saatu äänidata annetaan neuroverkolle opetusdatana. Neuroverkon luokitin luokittelee tutkittavista kirjaimista oikein keskimäärin 19/20, mutta siirryttäessä tilanteeseen, jossa neuroverkon tulee tunnistaa hyökkääjän kirjoitustyylistä poikkeavien henkilöiden näppäimistön käyttöä, luokittelun onnistumisprosentti laskee. Huomattava onnistumisprosentin lasku aiheutuu myös käytettäessä samaa opetettua neuroverkkoa muiden kuin neuroverkon opetusdatan keräämiseen käytetyn näppäimistön kanssa. Käyttämällä äänidatan analysoinnissa neuroverkon lisäksi puheentunnistuksesta tuttuja sana- ja lauserakenteita [17] saadaan eri näppäimistöjen käytöstä aiheutuvia ongelmia vähennettyä. Tutkimuksessa datan analysoinnissa käytössä on neuroverkko, jonka oppiminen on ohjaamatonta. Neuroverkko klusteroi datan, ja näppäiltyjen kirjainten päättelyyn käytetään kirjainklustereiden lisäksi esimerkiksi tietoa englannin kielessä todennäköisimmin esiintyvistä perättäisistä kirjaimista.

4.2 Käytön päättely puhelimen liikesensorin avulla

Käyttäjän QWERTY-näppäimistön käyttöä pääteltäessä ulkoisen ja erillisen datankerääjän, edellä käsitellyissä tapauksissa mikrofonin, käyttö asettaa

rajoituksia hyökkäyksen toteuttamiselle. Näppäimistön käytön päättelyyn on kuitenkin mahdollista käyttää myös älypuhelinta [15]. Tietokonetta käytettäessä asetetaan puhelin usein pöydälle näppäimistön lähistölle, jotta puhelin olisi mahdollisimman helposti saatavilla. Tällöin mahdollinen kanava hyökkäyksen toteuttamiselle tarjoutuu käyttäjän toimesta, eikä erillistä datankeräyslaitteistoa tarvita. Puhelimien mikrofonit eivät ole yhtä tehokkaita kuin näppäimistön käytön päättelyyn käytetyt erilliset mikrofonit, mutta näppäimistön käyttö voidaan havaita myös näppäimistön vieressä pöydällä olevan älypuhelimen kiihtyvyyssensorin avulla. Puhelimien kehittyessä myös niiden sensorit ovat entistä parempia.

Tutkimuksessa [15] oletetaan, että käyttäjä on ladannut puhelimeensa haittaohjelman, jolla on pääsy puhelimen kiihtyvyyssensoridataan. Näppäimistön käytön ja erityisesti yksittäisten näppäinten painalluksen erottaminen sensoridatasta on mahdollista myös puhelimen tarjoaman datan avulla. Kuitenkin aiemman analysointimenetelmän, jossa äänidatasta eroteltiin yksittäisten näppäinten painallukset [2], käyttäminen liikesensoridatan analysointiin epäonnistui puhelimen sensoridatan huomattavasti alemman näytteenottotaajuuden vuoksi.

Tutkimuksessa [15] sensoridatan analysoinnissa käytetäänkin yksittäisille kirjaimille määriteltyjä liikevektoreita, joista muodostetaan mahdollisia kirjainparivektoreita. Näppäimistön näppäimet jaetaan osiin jaon oikea - vasen sekä lähellä - kaukana mukaisesti. Tutkimuksessa käytetään kahta erillistä neuroverkkoa. Ensimmäisen neuroverkon opetusvaihetta varten kutakin näppäintä painetaan 150 kertaa, ja sensorin havainnoista muodostetut yksittäisten kirjainten vektorit P_i luokitellaan vasemman- ja oikeanpuoleisiin kirjaimiin. Toisen neuroverkon opetusdataa varten kirjainpareille muodostetaan yksittäisten kirjainten vektoreiden avulla kirjainparivektorit $dist(P_i, P_j)$, jotka luokitellaan P_i:n ja P_j:n sekä määritellyn kynnysetäisyyden mukaan joko luokkaan lähellä tai kaukana. Tulosten vertailu erillisellä mikrofonilla äänitetyn datan analysointituloksiin osoittaa, että corncob-sanakirjan [7] satunnaisten sanojen palauttaminen puhelimen liikesensoridatan avulla onnistuu lähes samalla todennäköisyydellä kuin äänidatasta pääteltyjen kirjainten ja niiden välisten sijaintirelaatioiden [6] avulla. Tulosten perusteella näppäimistön käytön päättely onnistuu myös todellista hyökkäystä jäljentävissä tilanteissa, joissa kirjoitetut sanat eivät ole yksittäisiä. Tutkimuksessa kuvitellut hyökkäyksen kohteet kirjoittivat lauseita artikkelista, kun viiden muun samaa aihetta käsitelleen artikkelin sanat oli annettu opetusdatana käytetyille neuroverkoille. Kontekstin rajaaminen vähentää samankaltaisten vektoriprofiilien esiintymistä verrattuna laajaan, noin 58 000 sanan corncob-sanakirjaan, jolloin virheellisten tulosten määrää saadaan laskettua.

5 Näppäimistön käytön päättely älykellon sensoridatan perusteella

Toisin kuin älypuhelimissa, älykelloissa sensorien datan kerääminen ja käyttö ei ole suojattua, eikä sensorien käytöstä näy käyttäjälle ilmoituskuvaketta [13]. Näin ollen sensoridataa voidaan tallentaa ilman erityistä ilmoitusta ja lupaa käyttäjältä esimerkiksi juuri näppäimistöä käytettäessä. Älykelloissa käyttäjän liikkeiden päättelyyn käytetään sekä kiihtyvyyssensoria että maan vetovoimaan perustuvaa gyroskooppia. Liikkeiden lisäksi näppäimistön käytön päättelyyn käytetään yleensä myös kellon mikrofonin äänidataa, jolla saadusta liikesensoridatasta saadaan erotettua näppäimistön käyttöön liittyvät käden liikkeet muista liikkeistä. Taulukossa 1 sivulla 7 esiteltävissä tutkimuksissa kerättyä dataa ja näppäimistön käyttöä analysoitiin kahdessa tutkimuksessa neuroverkkojen avulla [14] [13], ja yhdessä todennäköisyyslaskennan avulla [16].

Taulukko 1: Älykellon liikesensoridataa hyödyntävien tutkimusten koonti

tutkimus	näppäimistönjako	liikesensorit	mikrofoni	analysointimenetelmä	sanakirja	kellomalli
[14]	Näppäimistön ilmansuuntien mukainen jako	✓	✓	neuroverkko	suppea	Samsung Gear Live
[13]	Näppäimistön riveihin jako	✓	✓	neuroverkko	suppea	LG G WATCH
[16]	Yksittäisten näppäinten sijainti	✓	-	Bayes-mallinnus	koko sana-kirja	Samsung Gear Live

5.1 Tutkimusasetelmat

Käyttäjän QWERTY-näppäimistön käytön palauttamisen tehokkuutta on tutkittu kerätyn liikesensori- ja äänidatan perusteella [14] [13] [16]. Tutkimuksissa käytetään kahta eri älykellomallia, joissa kiihtyvyys- ja gyroskooppisensoreiden avulla liikettä mitataan x-, y- ja z-akseleiden muutoksina. Kaikissa tutkimuksissa on oletettu, että käyttäjä käyttää kelloaan vasemman käden ranteessa. Tutkimukseen osallistuvien henkilöiden oletettiin joko kirjoittavan ennalta määritetyn standardin kirjoitustavan mukaisesti [14] [13]

tai aloittaessaan kirjoittamaan pitävän käsiään tutkimuksessa määritetyssä aloitussijainnissa [16].

Molempien tutkimuksissa käytettyjen kellomallien näytteenottotaajus on lähes samalla tasolla, jolloin taajuudesta johtuvat eroavaisuudet datan analysointituloksissa eivät ole merkitseviä. Molemmissa neuroverkkoja hyödyntävissä tutkimuksessa [14] [13] käytössä on rajoitetulle määrälle englannin kielisiä sanoja ennalta määritellyt liikeprofiilit, joihin kiihtyvyyssensorin tuloksia verrattiin. Näppäimistön jakoa ilmansuuntien mukaan käyttävään tutkimukseen [14] osallistuneet henkilöt kirjoittivat saman 40 sanan osuuden lehtiartikkelista, kun liikemallisanakirjaan oli määritelty liikeprofiilit kuuden muun samaa aihetta käsitelleen artikkelin sanoista niiden esiintymisjärjestyksessä. Näppäimistön rivejä hyödyntävässä tutkimuksessa [13] testitapauksia oli kaksi. Ensimmäisessä tapauksessa pyrittiin viiden osallistujan kohdalla toistamaan aiemmassa tutkimuksessa toteutettu koe [6], jossa näppäimistön käyttöä oli pyritty päättelemään mikrofonin keräämän äänidatan perusteella. Näissä käytössä oli corncob-sanakirja, ja tarkoituksena palauttaa 35 testisanaa joiden pituudet vaihtelivat seitsemän ja 13 merkin välillä. Saman tutkimuksen [13] toisessa testitapauksessa vapaaehtoinen käyttäjää asensi kelloonsa haittaohjelman ja kirjoitti 20 satunnaisesti valittua lausetta ennalta määritetystä BBC:n uutisesta. Verrattavaan sanakirjaan oli määritelty mahdolliset liikemallit samaa aihepiiriä koskeville sanoille. Kuten aiemmassa älypuhelimen liikesensoridataan perustuvassa tutkimuksessa [15], tässäkin käytettiin vertailusanakirjana saman toimittajan muita samaa aihealuetta koskevia kirjoituksia.

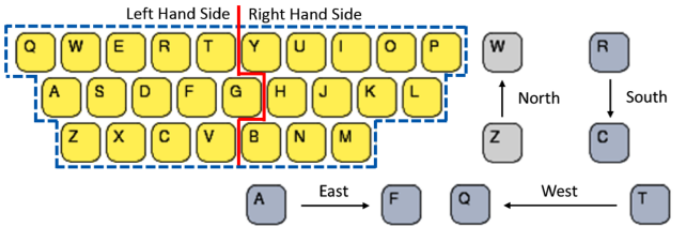
Liikesensorien tuottaman datan analysointiin posterioritodennäköisyyslaskentaa käyttävässä tutkimuksessa [16] tutkimukseen osallistuneet koehenkilöt kirjoittivat QWERTY-näppäimistöllä yhteensä 2400 yksittäistä sanaa. Vertailudatana käytettiin kuvitellun hyökkääjän syöttämää 500 sanan yksittäisten kirjainten painalluksia.

5.2 Liikesensoridatan analysointi

Koska yksittäisten kirjainten painamisen selvittäminen pelkän kiihtyvyyssensorin perusteella on vaikeaa, käytettiin molemmissa neuroverkkoja käyttävissä tutkimuksissa [14] [13] kirjoitettujen sanojen määrittämiseen kirjainnäppäinten fyysisen sijainnin ja liikkeen suunnan lisäksi älykellon mikrofonia. Äänidatan perusteella on mahdollista määrittää esimerkiksi kellottomalla kädellä tapahtuneet näppäinten painallukset tai välilyönnin painaminen sanojen erottamiseksi toisistaan. Todennäköisyyslaskentaan perustuvaa analyysiä käyttävässä tutkimuksessa [16] analyysimenetelmän toimivuus varmistettiin asettamalla puhelimen kamera siten, että näppäimistön todellinen käyttö oli tarvittaessa varmistettavissa kamerakuvan avulla.

Sensoridataa analysoitaessa ilmansuuntajakoon perustuvassa tutkimuksessa [14] datasta erotellut näppäilyt jaetaan kahden kirjaimen pareihin, ja

kaikki mahdolliset kirjainparit määritellään kuvan 1 relaationa fyysisen sijainnin sekä liikkeen suunnan, oikea - vasen (L - R) sekä pohjoinen - itä - etelä - länsi (N - W - S - E), välillä.



Kuva 1: Näppäimistön jako vasemman- ja oikeanpuoleisiin kirjaimiin neuroverkkoja käyttäneissä tutkimuksissa [14]

Kahden merkin pituisiksi kirjainpareiksi jaettuja merkkijonoja yhdistelemällä pyritään löytämään liikeratoja parhaiten vastaava sanakirjasana. Ennen varsinaista kirjainparien määrittämistä näppäimistö jaetaan kuvan 1 mukaisesti. Luokittelulla oikean ja vasemman välillä pyritään määrittelemään mitkä kirjainyhdistelmät on mahdollista selvittää vasemmassa kädessä pidetyn älykellon avulla. Tällöin sensoridatassa havaittuja liikkeitä voidaan käsitellä sijainnin $loc(Ki)$ ja ilmansuuntaliikkeiden $dir(Ki, Kj)$ avulla siten että näppäimen painalluksen tapahtuessa kellottomalla kädellä $rel(Ki, Kj) = loc(Ki)||X||loc(Kj)$ missä X on joku oikealle puolelle määritelty tuntematon merkki. Tämän jälkeen jokainen kirjain jaetaan joko luokkaan R tai L, ja kaikki kahden merkin parit niiden välisen liikeradan perusteella luokkiin N, W, S tai E. Neuroverkkojen opetusvaiheessa esimerkkisyötteenä käytettään tutkijan luomaa liikesensoridataa, joka sisältää 1000 englanninkielisen sanan liikeprofiilit. Käytössä on kaksi neuroverkkoa, joista ensimmäinen käyttää luokitteluperusteenaan oikea - vasen jakoa, ja toinen ilmansuuntiin perustuvaa jakoa.

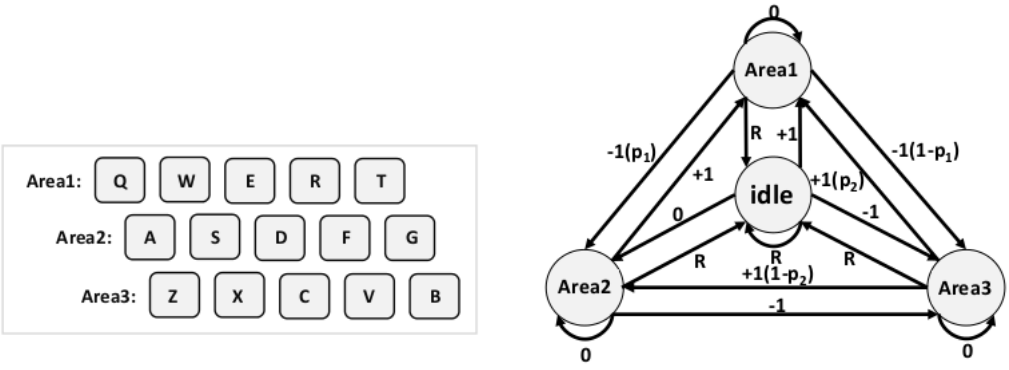
Oikealla kädellä tehdyt painallukset tunnistetaan älykellon mikrofonin avulla. Kaikki nappien painallukset yhdistetään liikesensoridatan kanssa, jolloin kellottoman käden painallukset on helppo erottaa vasemman käden painalluksista. Jos liikesensoridatassa ei havaita muutosta äänidatasta päätellyn painalluksen kohdalla, tiedetään painalluksen olevan joku näppäimistössä oikean käden puolella olevista kirjaimista. Sanoja erottavan välilyönnin painallus pystytään erottamaan muiden näppäinten painalluksesta myös älykellon heikkotehoisen mikrofonin avulla. Mikrofonin määrittelemän napinpainallusajan ja kiihtyvyyssensoridatan yhdistelmä annetaan syötteenä molemmille neuroverkoille, minkä jälkeen saatuja tuloksia verrataan sanakirjasanojen liikerataprofiileihin. Samanlaisuus pisteytetään, ja datasta erotetun

kirjoitetun sanan liikkeiden vastinpariksi saadaan korkeimman pistetuloksen saanut sanakirjasana.

Tutkimuksessa käytettävien neuroverkkoluokittimien oikeellisuutta tutkittiin foneettisesti tasapainoisten Harvard-lauseiden [11] avulla, joita käytetään yleisesti englannin kielen testaustapauksissa. Älykellon käyttäjä noudatti näppäillessään ennalta määrättyä oikea - vasen -jakoa, ja näppäimistöllä kirjoitettiin kymmenen lausetta, jotka kaikki löytyivät kokonaisina lauseina liikeprofiilisanakirjasta. Ilman kirjoitusvirheitä oikea - vasen -luokitin jakaa 100% tarkkuudella kirjoitetut lauseet oikeisiin luokkiin, ilmansuuntiin perustuva luokitin 95% tarkkuudella.

Myös toisessa neuroverkkoja käyttävässä tutkimuksessa, jossa näppäimistö on jaettu rivien mukaisesti [13], näppäimistön käytön liikeratoja ja äänidatan tietoja yhdistetään, ja saatuja tuloksia verrataan määriteltyihin liikeratamalleihin. Kuten ilmansuuntajakoon perustuvassa tutkimuksessa [14], näppäimistö on tässäkin luokiteltu kuvan 1 mukaisesti. Lisäksi näppäimistön rivit on numeroitu kuten kuvassa 2, ja rivinvaihdokset päätellään laitteen y-akselin suuntaisen liikkeen perusteella. Liikesensorin alhaisen otantanopeuden aiheuttamien virheiden vähentämiseksi kellon lähettämästä äänidatasta seurataan yksittäisten painallusten tapahtumahetkeä, jolloin liikkeet ovat paremmin suhteutettavissa todellisiin näippäimistön painalluksiin. Saatu data annetaan syötteenä optimointialgoritmille, joka palauttaa mahdollisten sanojen listan todennäköisyysjärjestyksessä.

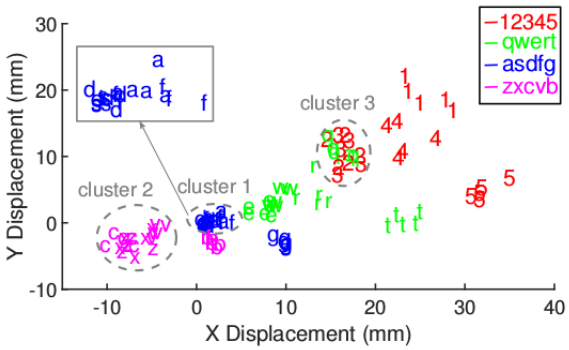
Kellon lähettämä data tallennetaan keräysvaiheessa laitteelle, josta se myöhemmin analysoidaan. Pääteltäessä käyttäjän näppäilemiä kirjaimia tutkimuksessa käytetään z-akselilla tapahtuvaa liikettä määrittelemään, onko äänidatasta havaittu painallus koskenut näppäimistön oikean (R) vai vasemman (L) puolen kirjaimia. Tämän jälkeen kellollisen käden puoleisten kirjainten yhteyksiä päätellään x- ja y-akselien liikkeiden perusteella. Tutkimuksessa riviltä ylöspäin tapahtunut liike saa arvon +1, alemmalle riville siirtyminen negatiivisen arvon -1 ja määritetyn kynnysarvon alle jäävä y-



Kuva 2: Näppäimistön jako riveittäin sekä luokittelutilakone

akselin muutos arvon 0. Englanninkielisille sanoille lasketaan liikemallit, jotka rakentuvat -1, 0, +1 ja R -merkeistä kuvan 2 luokittelutilakoneen avulla. Tilakoneessa merkkien luokat määritetään vertikaalisten liikkeiden perusteella. Tällöin mahdollisia luettuun liikerataan täsmääviä sanoja on useita, riippuen siitä miltä kohdalta näppäimistöä käden liike on alkanut. Ratkaisuna ongelmaan käytetään laskettuja todennäköisyyksiä käsien sijainnista mahdollisissa aloituskohdissa.

Posterioritodennäköisyyksiin perustuvassa tutkimuksessa [16] tutkimuksen opetusdatana käytetään kuvitellun hyökkääjän syöttämää erillisten 500 sanan yksittäisten kirjainten painalluksia. Painalluksista muodostetaan käden liikkeiden perusteella merkkien sijaintijoukko (character point cloud, CPC). Tutkimusdatan analysoinnissa oletetaan käyttäjän käsien lähtöasennon olevan keskellä näppäimistöä, kiintopisteinä vasemmalle kädelle merkki 'F' ja oikealle kädelle 'J' joiden kohdalla etusormien edellytetään lähtötilanteessa olevan. Hyökkääjän mallintamat liikkeet kutakin vasemmalla kädellä tapahtuvaa painallusta kohden tallennetaan, ja käyttäjän liikkeitä verrataan opetusdataan Bayesilaisen mallinnuksen ja sanakirjan avulla. Kirjaimet tunnistetaan kuuluviksi niiden sijainnin perusteella todennäköisimpään kuvan 3 kirjainklusteriin.



Kuva 3: Näppäinten painallusten klusterointi

Poiketen edellisistä hyökkäystavoista laskenta ei vaadi ennalta määriteltyjä liikeratoja sanakirjan sanoille, vaan sanoja käydään läpi kirjaimittain päätellen mahdollinen näppäilty sana suoraan kirjaimista ja niitä vastaavista hyökkääjän mallintamista liikeklustereista. Käyttäjältä saatu data käsitellään kolmessa eri vaiheessa. Ensimmäisessä moduulissa selvitetään 2D malli, jossa z-akselin muutoksina havaitut painallukset sijoitetaan koordinaatistoon. Tällöin näppäinten painalluksista saadaan muodostettuja <sijainti, aika> -pareja. Saatu luokittelemattomien sijaintien joukko (unlabeled point cloud, UPC) skaalataan pistejoukkojen yhteensovittamiseen tähtäävässä moduulissa hyökkääjän datasta tuotettuun merkkien sijaintijoukkoon. Uudelleen

skaalattu UPC toimii tämän jälkeen pohjana luokittelemattomissa sijainnissa olevien mahdollisten kirjainten selvittämisessä. Bayes-mallinnusta käyttävä moduuli saa syötteenä uudelleen skaalatun UPC:n, havaittujen näppäimistön painallusten sijainnit sekä 5000 yleisintä englanninkielistä sanaa sisältävän sanakirjan. Sanakirjan jokaiselle sanalle lasketaan todennäköisyys, jossa sanan kirjaimia ja saatuja painallusten sijainteja verrataan. Tuloksena moduuli palauttaa järjestetyn <sana, todennäköisyys> -listan.

5.3 Tulokset

Älykellon liikesensoridatan avulla tehdyissä tutkimuksissa [14] [13] [16] näppäilyn käytön päättelyn tulokset vaihtelevat taulukon 2 sivulla 12 mukaisesti riippuen analysointimenetelmästä sekä hyökkäyksen kohteen kirjoitustyylistä. Merkittäväksi tekijäksi kaikissa tutkimuksissa nousi kirjoittajan kirjoitustyylin samankaltaisuus hyökkäyksessä käytetyn vertailudatan tuottajan kanssa.

Taulukko 2: Tulokset

tutkimus	tutkimusasetelma	tulokset
[14]	Käytössä Harvard-lauseet, joista mukaan valittiin 48 kappaletta vähintään neljä merkkiä pitkiä sanoja	Parhaassa tapauksessa, jossa hyökkäyksen kohteen kirjoitustyyli lähimpänä opetusdataa, palautettiin täysin oikein 78%
[13]	1) Aiemmin toteutettu tutkimus, jossa corncob-sanakirja ja 35 testisanaa 2) Ennalta määritetystä uutisesta satunnaisesti valitut 20 lausetta (765 sanaa), kun vertailusanakirjassa saman toimittajan muita kirjoituksia	Testihenkilöistä riippuen 49-61% sanoista viiden todennäköisimmän sanan listalla, ja huomioitaessa 10 todennäköisintä sanaa tulokset välillä 58-69% Täysin oikein palautettiin 57%, ja kolmen todennäköisimmän joukossa 88%
[16]	2400 yksittäistä sanaa, opetusdatana hyökkääjän syöttämät 500 sanan yksittäisten kirjainten painallukset	30% syötetyistä sanoista viiden todennäköisimmän sanan joukossa. Jos kirjoitettaessa käsien aloituskohta oikea, niin sama 30% sanoista ensimmäinen tarjottu vaihtoehto

Erityisen alhaiseksi kirjoitetun sanan löytyminen jää posterioritodennäköisyyteen perustuvassa tutkimuksessa [16], jossa tutkimusasetelmasta poikkeavalla kirjoitustavalla todennäköisyys, että oikea sana on 24 korkeimman arvon joukossa saaneissa on 30%. Kirjoitettaessa käsien ollessa oletetussa sijainnissa samalla 30% todennäköisyydellä haettu sana on ensimmäinen löydetty vaihtoehto. Myös neuroverkkoja hyödyntävissä tutkimuksissa [14] [13] sanojen tunnistus lyhyiden 3-4 merkkiä pitkien sanojen kohdalla oli heikkoa, sillä niiden liikeprofiilit eivät eronneet merkittävästi toisistaan. Lyhyiden sanojen ollessa usein artikkeleita tai konjunktioita, oletetaan niiden olevan usein pääteltävissä kontekstista, ja arvioissa keskitytään pitkien sanojen tunnistustarkkuuteen. Ilmansuuntajakoa käyttävän tutkimuksen [14] sanatunnistukseen tähtäävässä testissä käytetään kymmentä Harvard-lausetta [11], joissa vähintään neljän merkin pituisia sanoja on 48 kappaletta. Tutkittaessa opetusdatan kirjoittaneen käyttäjän tuloksia näistä sanoista vain kolme tunnistettiin väärin onnistumisprosentin ollessa tällöin 93,75%. Kaikille 25:lle osallistujalle tehdyn kokeen sanojen tunnistusprosentti vaihteli laajasti osallistujien kesken. Korkeimmat tunnistusprosentit (21 oikein 27:stä) saavutettiin niillä testihenkilöillä, joiden kirjoitusnopeus oli lähimpänä neuroverkoille annetun opetusdatan kirjoittajan kirjoitusnopeutta.

Näppäimistön rivijakoon perustuvassa tutkimuksessa [13] ensimmäisen koeasetelman tapauksessa viiden testihenkilön kohdalla toistettiin aiemmassa tutkimuksessa toteutettu koe, jossa näppäimistön käyttöä pyrittiin päättelemään erillisellä mikrofonilla tallennetun äänidatan avulla [6]. Käytössä oli corncob-sanakirja [7], ja tarkoituksena palauttaa 35 testisanaa, joiden pituudet vaihtelivat seitsemän ja 13 merkin välillä. Alkuperäisessä tutkimuksessa [6] näppäimistön käyttöä pääteltiin äänidatan avulla. Tutkimuksessa tallennettiin näppäimistön ääntä erillisten sanojen osalta, ja äänidatan perusteella pyrittiin yhdistämään kirjoitettu sana sanakirjasta löytyvään sanaan. Verrattuna aiemman tutkimuksen tuloksiin oikeiden tulosten määrä älykellon sensoridataa, liikemalleja ja vertailualgoritmia käytettäessä oli selkeästi korkeampi. Älykellon datan perusteella etsitty sana oli kymmenen todennäköisimmän sanan joukossa 63% tapauksista pelkkään äänidataan perustuvan tutkimuksen tulosten jäädessä 43% tasolle. Älypuhelimen liikesensoridataa käyttäneessä tutkimuksessa [15] tulokset olivat taulukon 3 sivulla 14 mukaisesti samaa tasoa pelkkään äänidataan perustuvan alkuperäisen tutkimuksen [6] kanssa.

Saman liikeratamalleihin ja näppäimistöriveihin perustuvan tutkimuksen [13] toisessa testiasetelmassa, jossa käyttäjä kirjoitti 20 satunnaisesti valittua lausetta BBC:n uutisesta, päästiin myös hyviin tuloksiin. Vaikka sanakirjasanoja on yhteensä 765, onnistuu luokittelu siten että 615 sanan liikemallit olivat uniikkeja. Kokeessa onnistuttiin palauttamaan täysin oikein 57% kirjoitetuista 463 sanasta. Kun otetaan huomioon kolme todennäköisintä sanaa, on onnistumisprosentti 88. Vaikka erot eivät ole yhtä suuria kuin todennäköisyyslaskentaa käyttävässä tutkimuksessa [16], myös molemmissa

Taulukko 3: Näppäimistön rivijakoon perustuvan tutkimuksen [14] tulosten vertailu kahden aiemmin toteutetun puhelimen liikedataan ja äänidataan perustuvan tutkimuksen tuloksiin

tutkimushenkilöt [13]	top 5	top 10	top 25
henkilö 1	55%	64%	77%
henkilö 2	61%	69%	82%
henkilö 3	52%	60%	71%
henkilö 4	49%	58%	69%
henkilö 5	57%	64%	76%
keskiarvo	55%	63%	75%
puhelimen liikedata [6]	-	43%	61%
äänidata [15]	-	43%	50%

neuroverkkoja käyttäneissä tutkimuksissa kirjoittajan kirjoitusnopeudella ja -tavalla havaittiin olevan vaikutuksia sanatunnistuksen onnistumiseen. Näissä tutkimuksissa tunnistusta ja luokittelun onnistumista saattaa olla mahdollista parantaa käyttämällä opetussyötteenä eri nopeuksilla kirjoittavien henkilöiden dataa. Tutkimuksessa [14], jossa luokitteluun käytettiin ilmansuuntia, kirjainyhdistelmien jakaminen myös väli-ilmansuuntien mukaan todennäköisesti parantaisi tuloksia.

Tutkimuksessa, jossa liikesensoreiden tuottamaa dataa käsiteltiin todennäköisyyslaskennan avulla [16], tulokset olivat myös oletetulla kirjoitustavalla neuroverkkoja käyttäviä tutkimuksia heikompia. Tässä käyttämällä Bayesilaista mallinnusta tuloksen mediaaniksi saatiin 24. Käyttäjän kirjoittaessa näppäimistöllä on siis 50% todennäköisyys että oikea sana on luokiteltujen 24 todennäköisimmän vaihtoehdon joukossa, ja 30% todennäköisyydellä sana löytyy viiden korkeimmaksi luokitellun mahdollisuuden joukosta. Tutkimustavassa ongelmaksi nousi välilyönnin seurannan vaikeus, jolloin kokonaisten lauseiden erotteleminen erillisiksi sanoiksi on haastavaa. Myöskään kellottomalla kädellä tehtäviä painalluksia ei ollut mahdollista rekisteröidä, sillä kellon mikrofonia ei käytetty kuten kahdessa muussa tutkimuksessa. Muiden tutkimusten tapaan äänidatan käyttäminen todennäköisyysmenetelmän tukena todennäköisesti parantaisi tuloksia.

Lähtökohtaisesti kaikkien englanninkielisten sanojen sisältävän sanakirjan käyttäminen liikemalliin täsmäävän sanan löytämiseksi on haastavaa, sillä sanojen määrän kasvaessa myös niiden sanojen määrä joilla on sama liikeprofiili kasvaa. Molemmissa käsitellyissä tutkimuksissa [14] [13], joissa sanan tunnistus perustuu ennalta määritettyihin liikemalleihin, on käytetty tiettyjä sanoja sisältäviä, huomattavasti kokonaista sanakirjaa suppeampia sanao-

tantoja ja niille muodostettuja liikeratamalleja. Pohdinnassa [13] ongelmaan esitettiin kuitenkin mahdollisena ratkaisuna sanaston sitomista kontekstiin, jolloin todennäköisten sanojen määrä vähenee huomattavasti. Älykellojen ominaisuuksiin kuuluu käsiteltyjen liike- ja äänisensorien lisäksi myös esimerkiksi mahdollisuus GPS-seurantaan sekä muita käyttäjää identifioivia ominaisuuksia. Näiden pohjalta mahdollisen hyökkääjän voisi olla mahdollista päätellä missä kontekstissa käyttäjän kirjoittamat sanat esiintyvät, jolloin sanakirjan liikeratamalleja olisi mahdollista supistaa ja näin käytön päättelyn onnistumisprosenttia parantaa.

Todennäköisyyslaskentaan perustuvassa analysoinnissa [16] käytettiin sanan esiintymistodennäköisyytenä huomattavasti laajemman sanakirjan sanoilla samaa todennäköisyyttä. Tutkimuksista, joissa mahdollisten esiintyvien sanojen lukumäärää pienennettiin kontekstisidonnaisuudella [13] [15] ja näin sanan tunnistamisprosenttia saatiin nostettua, voidaan päätellä, että kontekstin päättely ja sanojen rajaaminen parantaisi tulosta todennäköisesti myös todennäköisyyslaskennan analysointimenetelmällä päättelyä tehtäessä.

Älykellot käyttävät tiedonsiirtoon Bluetoothia, ja erityisesti kellojen käyttämässä Bluetooth Low Energyssä (BLE) on löydetty tapoja identifioida käyttäjä laitteen lähettämien pakettien perusteella [8]. Tutkimuksessa BLE-tekniikka käyttävien aktiivisuusrannekkeiden todettiin säilyttävän BLE-osoitteensa. Tällöin vaikka lähetettävä data on salattua, on helppoa päätellä milloin tietty yksittäinen laite tietoa lähettää, jolloin käyttäjän yksilöinti suuremmasta joukosta on mahdollista. Näin ollen käyttäjän identifiointi ja kirjoitetun tekstin kontekstin rajaaminen saattaa olla mahdollista pelkän älykellon signaalien havainnoinnin perusteella.

Liikemalleihin perustuvien tutkimusten heikkoutena voitiin nähdä ennalta määriteltyjen liikeratojen ja sanakirjasanojen suuren määrän vaikutus siihen, miten monet sanat vastaavat samoja liikeratamalleja. Samaa ongelmaa ei esiinny Bayesilaiseen mallinnukseen pohjautuvassa näppäimistön käytön päättelyssä, sillä käytössä on jo valmiiksi koko sanakirja ja yksittäisiin kirjainpainalluksiin perustuvat liikkeet. Yksittäisiin painalluksiin pohjautuva menetelmä ei kuitenkaan poista kaikissa älykellon liikesensoridataa tutkineissa tutkimuksissa esiintyvää heikkoutta. Salasanojen ja käyttäjätunnusten voidaan olettaa toisinaan olevan pelkkiä kirjain- ja merkkiyhdistelmiä, jolloin niitä ei voida löytää sanakirjoista tai valmiiksi määritetyistä liikeratamalleista. Listoja suosituimmista vuodetuista salasanoista on kuitenkin saatavilla [12], jolloin salasanalistojen lisääminen käytettyyn sanakirjaan todennäköisesti parantaisi mahdollisuuksia myös salasanan selvittämiseen.

Kaikissa käsitellyissä liikesensoridataan perustuvissa tutkimuksissa näppäimistön käyttö pystyttiin päättelemään yllättävän korkealla onnistumisprosentilla. Koeasetelmissa yhteiseksi heikkoudeksi nousi kuitenkin päättelyn riippuvuus käyttäjän omasta kirjoitustavasta. Neuroverkkoihin ja ennaltamääriteltyihin sanojen liikemalleihin perustuvassa päättelyssä kirjoittajien oletettiin kirjoittavan määritellyllä standardilla kirjoitustavalla sujuvasti, ja

Bayes-mallinnukseen pohjautuvan tutkimuksen tutkimusasetelmassa käyttäjien oletettiin pitävän käsien niin sanottuna lähtötilanteena juuri tiettyä käsien sijaintia näppäimistöllä. Myös kirjoitusnopeuden vastaavuus hyökkääjän syöttämän opetusdatan kanssa oli merkittävä tekijä. Opetusdatan jakaminen erilaisiin kirjoitustyyppeihin ja näppäimistöllä kirjoitettujen sanojen vertaus erikseen näihin tyypiteltyihin opetusdatoihin voisi parantaa tuloksia, mutta toisaalta samalla myös monimutkaistaa selvitysprosessia tai pahimmassa tapauksessa vääristää tuloksia. Tulosten tarkkuutta kuitenkin lisäisi jokaisessa kokeessa, jos oletettu oppimis- tai vertausdata olisi mahdollista saada suoraan hyökkäyksen kohteeksi joutuvalta henkilöltä. Esimerkiksi lähetettyjen sähköpostien vuoto puhelimesta voisi olla tilanne, jossa QWERTY-näppäimistön käyttö pystyttäisiin ajallistesti yhdistämään yksittäisiin sähköposteihin, jolloin opetusdatana voisi olla mahdollista käyttää käyttäjän omia liikeratoja. Tällöin yksilölliset kirjoitustapaerot saataisiin vastaamaan määriteltyjä liikeratamalleja tai todennäköisyyksiin perustuvan päättelyn tapauksessa näppäinten painallussijainteja.

Tutkimustulokset sekä yksitellen että erityisesti yhdessä osoittavat vahvasti sen, että näppäimistön käytön päättely älykellojen sensoridatan perusteella on jo nyt mahdollista, ja esimerkiksi yhdistelemällä nyt käytettyjä metodeita ja hankkimalla tarvittava opetusdata suoraan käyttäjältä tuloksista voidaan saada erittäin paikkaansapitäviä.

6 Yhteenveto

Tutkimustulosten perusteella QWERTY-näppäimistön käytön päättely on mahdollista älykellon liikesensori- ja äänidatan avulla. Näppäimistön käytön päättely onnistuu sekä neuroverkkojen että todennäköisyysmallinnuksen avulla, ja kellon jatkuva käyttöaika antaa mahdolliselle hyökkääjälle keinon datankeräykseen ilman muita erillisiä datankerääjiä, kuten kameraa tai mikrofonia. Kun sensoridatan analysointiin käytetään hyviä analysointimenetelmiä, vaikuttaa käytön päättely älykellon avulla onnistuvan vähintään samalla tasolla kuin erillisiä kerääjiäkin käytettäessä. Älykellon käyttö hyökkäysvälineenä vähentää kuitenkin ulkoisten häiriöden vaikutuksia sekä datan keräämiseen vaadittavia laitteita.

Kaikissa älykellon sensoridataa analysoineissa tutkimuksissa lähtöoletuksena oli hyökkääjän pääsy kellon lähettämään liikesensoridataan esimerkiksi puhelimelle asennetun haittaohjelman kautta. Todellisissa hyökkäystapauksissa hyökkääjän tulee ensin saada pääsy älykelloa käyttävän henkilön puhelimeen. Ensisijainen suojautumiskeino älykellon liikesensoridataa käyttäviltä hyökkäyksiltä onkin estää hyökkääjän pääsy dataan, ja asentaa puhelimeen vain sovelluksia, joilla ei ole valtuuksia käyttää älykellon sensoridataa. Laitteistotasolla suojatumista voitaisiin helpottaa esimerkiksi älypuhelimen kaltaisilla notifikaatioilla sensoreiden käytöstä, sekä mahdolli-

suudella estää sensoridatan kerääminen hetkellisesti käyttäjän niin valitessa. Hyökkäysten toimiminen onnistuneesti todellisissa tilanteissa vaatii myös tutkimustapausten perusteella tietoa kirjoitetun tekstin kontekstista sekä hyökkäyksen kohteen kirjoitustottumuksista. Vaikka heikkouksia on olemassa, voidaan ongelmiin olettaa löytyvän ratkaisuja, joilla hyökkäyksistä saadaan todellisissa tilanteissa toimivampia. Kehittyneen hyökkäysohjelman avulla voi esimerkiksi olla mahdollista päästä käsiksi hyökkäyksen kohteen sähköposteihin, jolloin sekä konteksti että yksilöllistä kirjoitustapaa mukaileva opetusdata saattaa olla pääteltävissä.

Ilmansuutajakoon perustuvassa näppäimistön käytön tutkimuksessa [14] tietoturvaratkaisuksi esitetään kontekstitietoista sensorien toimintaa. Tutkimuksessa esitellään rTAD, jonka on mahdollista valvoa milloin älykellon käyttäjä käyttää näppäimistöä, ja estää sensoridatan kerääminen ja lähettäminen näissä tilanteissa. Näppäimistön käytön aiheuttamat muutokset liikesensoridatassa on helppo erottaa esimerkiksi liikunnan aiheuttamista datamuutoksista, sillä näppäilyn aiheuttamat muutokset ovat huomattavasti pienempiä kuin esimerkiksi askeleista johtuvat. Esitetyssä tietoturvaratkaisussa lähetettävä data kulkisi sensorivalvonnan kautta. Ehdotuksen kaltaiset ratkaisut vaativat muutoksia koko laitearkkitehtuuriin, jolloin kustannukset vähentävät varmasti valmistajien halukkuutta toteuttaa tietoturvaparannuksia. Tälläkin hetkellä esimerkiksi Bluetooth-tekniikkaa käyttävillä laitteiden on mahdollista vaihdella BLE-osoitetta, mikä vaikeuttaa yksittäisten laitteiden seurantaa ja yksilöimistä. Aktiivisuusrannekkeiden tietoturvaa tutkittaessa on kuitenkin osoitettu, ettei osoitteiden vaihtelua ole ainakaan tutkituissa laitteissa toteutettu [8]. Vaikka edellytyksiä parempaan tietoturvaan saattaa olla, ei valmistajien voida olettaa käyttävän parannuksia hyväkseen.

Ihmisten tietoturvan parantamiseen sekä omien tietojen hallinnointiin on viime aikoina kiinnitetty huomiota myös EU-tasolla, ja muun muassa evästeisiin sekä henkilötietorekistereihin on pyritty saamaan EU-alueiden asukkaille kattavat vaikutusmahdollisuudet. Laitevalmistajien sitouttaminen älykellojen käyttäjien tietoturvan varmistamiseen voisikin olla mahdollista esimerkiksi yleisten säädösten sekä lakien avulla.

Lähteet

[1] Ali, Kamran, Liu, Alex X., Wang, Wei ja Shahzad, Muhammad: *Keystroke Recognition Using WiFi Signals*. Teoksessa *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, MobiCom '15, sivut 90–102, New York, NY, USA, 2015. ACM, ISBN 978-1-4503-3619-2. http://doi.acm.org/10.1145/2789168.2790109.

[2] Asonov, Dimitri ja Agrawal, Rakesh: *Keyboard Acoustic Emanations*. Proceedings of the IEEE Symposium on Security and Privacy, sivut 3–11, 2004.

[3] Balzarotti, Davide, Cova, Marco ja Vigna, Giovanni: *ClearShot: Eavesdropping on Keyboard Input from Video*. Teoksessa *Proceedings of the 2008 IEEE Symposium on Security and Privacy*, SP '08, sivut 170–183, Washington, DC, USA, 2008. IEEE Computer Society, ISBN 978-0-7695-3168-7. http://dx.doi.org/10.1109/SP.2008.28.

[4] Barber, David: *Bayesian Reasoning and Machine Learning*. Cambridge University Press, New York, NY, USA, 2012, ISBN 0521518148, 9780521518147.

[5] Beaver, Laurie: *THE SMARTWATCH REPORT: Forecasts, adoption trends, and why the market isn't living up to the hype*. Teoksessa *Busines Insider*. http://tinyurl.com/zc7qusu.

[6] Berger, Yigael, Wool, Avishai ja Yeredor, Arie: *Dictionary Attacks Using Keyboard Acoustic Emanations*. Teoksessa *Proceedings of the 13th ACM Conference on Computer and Communications Security*, CCS '06, sivut 245–254, New York, NY, USA, 2006. ACM, ISBN 1-59593-518-5. http://doi.acm.org/10.1145/1180405.1180436.

[7] CornCob: *The corncob list*. http://www.mieliestronk.com/wordlist.html, vierailtu 2017-10-30 .

[8] Das, Aveek K., Pathak, Parth H., Chuah, Chen Nee ja Mohapatra, Prasant: *Uncovering Privacy Leakage in BLE Network Traffic of Wearable Fitness Trackers*. Teoksessa *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications*, HotMobile '16, sivut 99–104, New York, NY, USA, 2016. ACM, ISBN 978-1-4503-4145-5. http://doi.acm.org/10.1145/2873587.2873594.

[9] Ertel, Wolfgang: *Introduction to Artificial Intelligence*. Springer Publishing Company, Incorporated, 1st painos, 2011, ISBN 9780857292988.

[10] Fetto, John: *Simmons Connect Experian Marketing Services*, 2013. http://tinyurl.com/experiansmartphones, vierailtu 2017-03-13 .

[11] IEEE: *Recommended Practices for Speech Quality Measurements*, 1969. http://ieeexplore.ieee.org/document/7405210/, vierailtu 2017-10-30 .

[12] Keeper: *The Most Common Passwords of 2016*, 2017. http://tinyurl.com/kbhbr2n, vierailtu 2017-04-17 .

[13] Liu, Xiangyu, Zhou, Zhe, Diao, Wenrui, Li, Zhou ja Zhang, Kehuan: *When Good Becomes Evil: Keystroke Inference with Smartwatch*. Teoksessa *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15, sivut 1273–1285, New York, NY, USA, 2015. ACM, ISBN 978-1-4503-3832-5. http://doi.acm.org/10.1145/2810103.2813668.

[14] Maiti, Anindya, Armbruster, Oscar, Jadliwala, Murtuza ja He, Jibo: *Smartwatch-Based Keystroke Inference Attacks and Context-Aware Protection Mechanisms*. Teoksessa *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '16, sivut 795–806, New York, NY, USA, 2016. ACM, ISBN 978-1-4503-4233-9. http://doi.acm.org/10.1145/2897845.2897905.

[15] Marquardt, Philip, Verma, Arunabh, Carter, Henry ja Traynor, Patrick: *(Sp)iPhone: Decoding Vibrations from Nearby Keyboards Using Mobile Phone Accelerometers*. Teoksessa *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS '11, sivut 551–562, New York, NY, USA, 2011. ACM, ISBN 978-1-4503-0948-6. http://doi.acm.org/10.1145/2046707.2046771.

[16] Wang, He, Lai, Ted Tsung Te ja Roy Choudhury, Romit: *MoLe: Motion Leaks Through Smartwatch Sensors*. Teoksessa *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, MobiCom '15, sivut 155–166, New York, NY, USA, 2015. ACM, ISBN 978-1-4503-3619-2. http://doi.acm.org/10.1145/2789168.2790121.

[17] Zhuang, Li, Zhou, Feng ja Tygar, J. D.: *Keyboard Acoustic Emanations Revisited*. ACM Trans. Inf. Syst. Secur., 13(1):3:1–3:26, marraskuu 2009, ISSN 1094-9224. http://doi.acm.org/10.1145/1609956.1609959.