Sistema de prevenció d'epidèmies en comportaments de risc mitjançant smartphones.

Josep Ribó Ferriz[*1], Dr. Antoni Pérez Navarro*[*2]*
[1] Universitat Oberta de Catalunya, Rambla Poblenou 156, Barcelona, Spain
[2] Estudis d'Informàtica, Multimèdia i Telecomunicació,Universitat Oberta de Catalunya, Rambla Poblenou 156, Barcelona, Spain

Email: Josep Ribó Ferriz - jribof@uoc.edu; Antoni Pérez Navarro* - aperezn@uoc.edu*
** Correspon a l'autor*

PARAULES CLAU:
Risc, mòbil, prevenció, epidèmia, amistat, GPS, WIFI, Access Point

ABSTRACT
Rerefons:
Els *smartphones* faciliten els contactes entre persones i, en alguns casos, aquests contactes deriven en relacions sexuals sense les adequades mesures preventives. La conseqüència d'aquest fet és l'augment de les malalties de transmissió sexual (*MTS*).
L'objectiu d'aquest projecte és desenvolupar una *App* per *Android OS,* capaç de prevenir a l'usuari de conductes de risc, tenint en compte els senyals *WIFI* captats pels diversos *smartphones*, així com les hipotètiques relacions d'amistat existents entre els contactes de l'agenda.

Mètode:
La metodologia que es farà servir és la *Design and Creation*, per desenvolupar un artefacte *App* per *Android OS*.
L'experiment consistirà en identificar una hipotètica coincidència física entre dos usuaris, utilitzant els *WIFI Access Points* travessats. I per identificar les hipotètiques relacions d'amistat entre els usuaris, es cercaran els contactes comuns entre les agendes dels seus telèfons mòbils (amb diversos nivells de distància) utilitzant la teoria de les 6 baules.

Resultats:
Els resultats obtinguts per l'inventari de posicions mostren variabilitat en els senyals i temps de permanència identificats per cada usuari. Després d'analitzar les posicions, hem definit quatre tipus de posicionament, amb diferents nivells de risc associat: residència, treball, desplaçament i oci.
Pel que fa a les coincidències entre les agendes, l'experiment ha permès establir l'indicador *Friendship Probability* tenint en compte la relació entre les agendes de contactes dels usuaris caracteritzada pels nivells de distància entre dos contactes, tenint en compte tres tipus de creuaments: la relació bidireccional entre usuaris de primer nivell, la relació bidireccional entre usuaris d'n nivells i la relació unidireccional entre usuaris.

Conclusions:
L'estudi demostra que tot i no disposar de les coordenades *GPS,* ni dels usuaris, ni dels *WIFI Access Points*, podem identificar situacions i/o zones de risc tenint en compte la proximitat física entre persones que l'anàlisi de la cobertura *WIFI* pot oferir.
En l'àmbit de l'anàlisi de la relació entre usuaris, hem quantificat el nivell de risc entre contactes, tenint en compte la distància de la baula de coincidència entre els telèfons de les agendes de dues persones.
Una tasca futura és la implementació, a nivell de servidor, d'un sistema expert (intel·ligència artificial), que permeti analitzar, raonar i adquirir nous coneixements, segons situacions ja viscudes, i d'aquesta forma millorar la detecció de conductes de risc per part dels usuaris.

Rerefons:

La proliferació dels *LBS* (serveis basats en localització) en els *smartphones,* introdueix una nova dimensió dins del pla virtual: la posició física de cada individu.
La publicació per part de l'usuari d'una informació tan sensible com és la posició, facilitarà la proliferació de relacions entre humans, utilitzant criteris tan subjectius com són la proximitat entre dispositius, i l'interès d'assolir el que es coneix com a "cita exprés".
El risc de contagi de malalties de transmissió sexual en el context de mal ús de la tecnologia és important, i el principal inconvenient és la dificultat d'identificar aquest tipus de situacions.
Tot i la potència de càlcul, connectivitat, i sensors dels *smartphones*, aquests no poden predir una conducta de risc desenvolupada pel seu usuari *[8]*, però poden oferir les característiques de la computació ubiqua, disciplina que integra la informàtica dins de l'entorn de la persona, de forma que els ordinadors ja no són percebuts com objectes diferenciats.
L'objectiu d'aquest projecte és potenciar les mesures preventives mitjançant la recepció, de forma voluntària, d'avisos preventius als *smartphones* dels usuaris, cada cop que el sistema identifica una conducta de risc.
Per identificar una conducta de risc el sistema s'utilitzarà dos mecanismes independents. El primer calcularà les relacions existents entre els contactes de les agendes dels *smartphones* dels usuaris registrats, utilitzant una estructura de dades arborescent, de fins a sis nivells d'alçada (entre l'usuari arrel i el darrer usuari fulla). El sistema realitzarà aquest procés de forma transparent, segura i automàtica, i sense que l'*App* enviï informació confidencial fora de l'*smartphone*.
El segon mecanisme consistirà a detectar la coincidència d'usuaris dins del radi de cobertura d'un mateix *WIFI Access Point*, i cada cop que el servidor detecti aquest tipus de coincidència, utilitzarà les deduccions del primer mecanisme per descobrir l'existència d'alguna relació entre les agendes d'ambdós usuaris.
En aquest punt es considera que existeix un lligam que diferencia una relació en les xarxes socials d'una en la vida real, i és el valor afegit de posseir el número de telèfon mòbil d'una persona.
El sistema no alertarà als usuaris que coincideixin en un mateix *WIFI Access Point*, si prèviament no ha detectat cap tipus de relació d'agenda entre ells.

Mètode:

Per tal de desenvolupar l'artefacte *App*, hem utilitzat la metodologia *Design and Creation [4]* (disseny i creació), que permet elaborar el prototipus durant el procés de recerca, mitjançant els experiments realitzats, que en aquest projecte han estat dividits en cinc fases:
- Fase 1. Realització de proves:
• Verificar l'accés en consulta que el sistema operatiu *Android OS* permet al servei d'agenda de contactes de l'*smartphone* per obtenir les dades dels contactes: Nom, cognom i número de telèfon mòbil.
• Assegurar la confidencialitat de la informació que es transmetrà a la base de dades centralitzada d'aquest sistema d'informació. Hem previst la creació, mitjançant l'algorisme criptogràfic *MD5* (acrònim de *Message-Digest Algorithm 5*) *[6],* d'una signatura o resum característic per cada número de telèfon de l'agenda de l'usuari. El resum o *hash MD5* s'expressarà com una seqüència de 32 dígits hexadecimals, que no permetrà reconstruir el número de telèfon original.
• Analitzar la informació que els diferents sensors d'un s*martphone* podem facilitar: servei *WIFI, s*ervei *3G i s*ervei *GPS*.
• Prioritzar l'ús dels serveis *WIFI [3]* per posicionar (amb o sense coordenades *GPS*) l'*smartphone*, tenint en compte la predisposició natural dels usuaris a deixar el servei *WIFI* actiu, respecte l'ús poc habitual del servei *GPS.* Cal destacar que tot i que existeix la possibilitat de localitzar i posicionar persones mitjançant *WIFI Access Points* en entorns *indoor/outdoor*, l'objectiu d'aquest projecte és únicament trobar coincidències d'usuaris sota un mateix senyal *WIFI*.

Figura 1: Esquema de l'arquitectura tecnològica del projecte.

• Sincronitzar l'*App* i el servidor: Connexió, registre, publicació de les signatures dels contactes de l'agenda, publicació de la posició i consulta d'alertes de risc.
- Fase 2. Disseny del nou sistema d'informació. Les entitats identificades en aquest sistema d'informació són l'usuari, l'agenda de contactes i els *WIFI Access Points*. Les relacions entre les entitats són:
• L'usuari amb els codis *hash* que representen a cadascun dels usuaris de la seva agenda.
• L'històric de les posicions de cada usuari, tenint en compte que el sistema analitzarà les posicions dels darrers minuts.
Com a atribut dels *WIFI Access Point,* identificarem la seva posició *GPS*. És una informació que no utilitzarem en el procés d'identificació de risc, però que volem recollir per analitzar si hi ha relació entre la situació geogràfica d'un *WIFI Access Point*, i la concurrència i coincidència d'usuaris.
- Fase 3. Implementació del sistema d'informació, tenint en compte les conclusions dels experiments realitzats durant les fases 1 i 2, i tenint en compte els dos entorns que integren l'arquitectura a implementar (figura 1):
• *Web server*: Dispositiu que publicarà els *Web Services* responsables de la lògica de negoci i que executarà el motor de base de dades que centralitzarà les dades recollides per les *Apps.* Implementarem una arquitectura *LAMP (Línux, Apache, MySQL, PHP)*, integrada per un sistema operatiu *Linux*, en el que desplegarem un servidor web *Apache*, configurat amb el paquet *PHP* i una base de dades *MySql*.
Smartphone App: Programari que té la missió d'identificar a l'usuari i recollir les seves dades (signatura dels contactes de l'agenda, senyals *WIFI* i geoposició). També serà el responsable de rebre les alertes de risc. Desenvoluparem l'*App* en llenguatge *Java*. El sistema operatiu *host* dels *smartphones* en què desplegarem l'*App serà Android OS (*versió 2.2 o superior).
Per realitzar l'intercanvi de dades entre l'*App* i el servidor, hem utilitzat la filosofia *Web Service RESTful* (*Representational State Transfer*) mitjançant l'estàndard *JSON* (*JavaScript Object Notation*), per la seva lleugeresa i facilitat d'implementació sense eines específiques.
- Fase 4. Prova pilot amb tres *smartphones* que permetran realitzar:
• L'estudi del rendiment (consum de *RAM/CPU*).
• L'estudi del consum *WIFI/3G*.
• L'estudi del consum de bateria.
• L'anàlisi de les dades recollides.
- Fase 5. Publicació i publicitació del projecte mitjançant la plataforma de distribució d'aplicacions per a *smartphones*, *Google Play [5]*.

Procés de recollida i anàlisi de dades.

Un cop l'usuari hagi instal·lat l'*App* (figura 2), i autoritzi l'accés als telèfons que conformen la seva agenda, s'iniciarà el procés que codificarà i enviarà els resultats (les signatures dels números de telèfon de l'agenda) al servidor central.
El servidor utilitzarà el mètode d'anàlisis quantitatiu, habitual en investigacions positivistes, per obtenir el coeficient de correlació *Friendship probability [2]*.

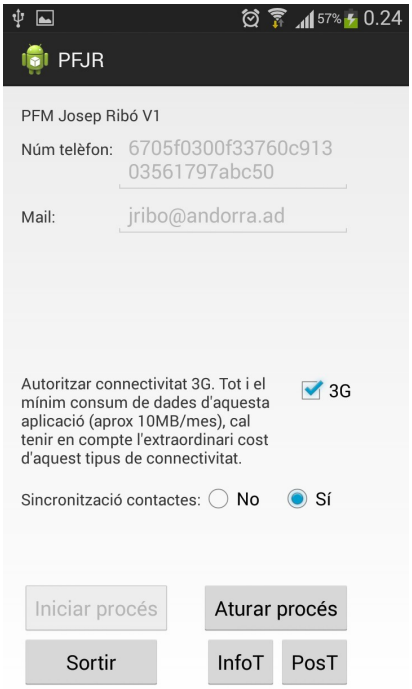

Figura 2: Interfície de l'App.

Aquest estadístic mostrarà la relació existent entre dues persones utilitzant una estructura de dades arborescent de fins a sis nivells d'alçada (entre l'usuari arrel i el darrer usuari fulla) amb tres tipus de lligams:
- Relació bidireccional entre usuaris de primer nivell:

L'agenda de l'usuari A té registrat el número de telèfon mòbil de l'usuari B, i l'agenda del telèfon de l'usuari B té registrat el número de telèfon mòbil de l'usuari A.
- Relació bidireccional entre usuaris d'n nivell:

L'agenda de l'usuari A té registrat el número de telèfon mòbil dels usuaris B i C, i l'agenda del telèfon de l'usuari B no té registrat el número de telèfon mòbil de l'usuari A, però sí de l'usuari C. L'agenda de l'usuari C té registrat els telèfons mòbils de l'usuari A i B.
Tenint en compte la teoria de les 6 baules *[2]*, considerarem una distància màxima de 6 salts entre usuaris de diferents nivells.
– Relació unidireccional entre usuaris:

L'agenda de l'usuari A té registrat el número de telèfon mòbil de l'usuari B, però l'agenda de l'usuari B no té registrat el telèfon mòbil de l'usuari A.

Cal dir que el procés que relaciona els contactes de les agendes dels *smartphones* és independent del procés que identifica les coincidències entre usuaris en un *WIFI Access Point*, i per tant, no és necessària la coincidència dels usuaris A, B i C en un mateix *WIFI Access Point* per utilitzar les relacions entre les tres agendes.

Tenint en compte el grau (baula) de relació entre dos contactes, els hi assignarem un nivell de risc proporcional a la distància entre ambdós, tenint en compte que una relació (d'agenda) propera disposa de més confiança que una relació entre baules allunyades.
Els usuaris amb relacions unidireccionals responen a un nivell de risc extrem, donat que ni gaudeixen de prou confiança i/o informació de l'usuari objectiu, ni hi ha identificats contactes intermedis als quals consultar informació complementària.

Un cop el servidor ha calculat les relacions entre els contactes del sistema, l'*App* inventariarà els *WIFI Access Points* travessats per l'usuari, i el temps de permanència sota cadascun dels senyals. El procediment de sincronització entre l'*smartphone* i el servidor no necessita connectivitat *WIFI*, donat que el dispositiu pot enviar informació al servidor central mitjançant el servei *3G*, o qualsevol altre tipus de connexió. En cas de no disposar de cap tipus de cobertura de dades, el dispositiu registrarà les posicions dins de la base de dades local de l'*smartphone*, i un cop restablerta la connectivitat, es sincronitzarà amb el servidor central.
Cal dir que tot i no disposar de cobertura de dades, el servidor podria enviar alertes de perill als *smartphones* mitjançant missatges *SMS*, això sí, tenint en compte l'històric de les darreres posicions (senyals *WIFI* i temps de permanència) que l'*smartphone* hagi enviat al servidor abans de perdre la connexió.
Cada cop que el servidor rebi les posicions dels usuaris enviades per les *Apps*, cercarà si per un mateix instant (o amb pocs minuts de diferència),

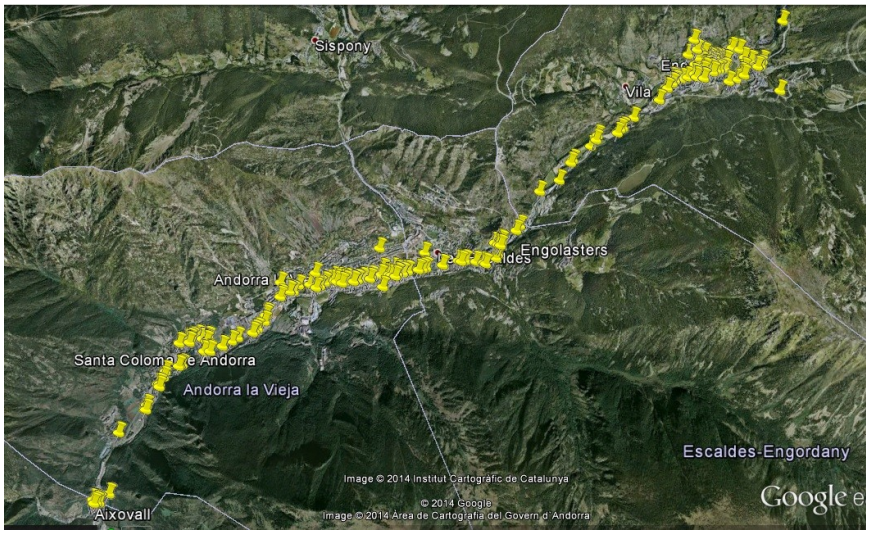

Figura 3: L'usuari travessa 725 WIFI Access Points en un trajecte de 12 Km. entre els lloc de residència i treball.

existeixen altres usuaris registrats, amb algun nivell *Friendship Probability*, sota els mateixos senyals dels *WIFI Access Points*.
Tenint en compte el radi de cobertura del senyal *WIFI*, l'usuari rebrà l'alerta de risc tot i tenir a l'usuari objectiu a desenes o centenars de metres.
Considerem que és un bon moment per prevenir a l'usuari del possible contacte físic que pot succeir.
Per diferenciar tècnicament els *WIFI Access Points,* l'*smartphone* utilitzarà l'identificador de xarxa *BSSID (Basic Service Set Identifier),* únic i irrepetible.
Cada cop que el servidor detecti coincidències en una mateixa posició (lloc i moment) entre els contactes pels que la base de dades del servidor té identificat algun *Friendhip Probability*, el servidor enviarà una alerta de risc als usuaris implicats.

Limitacions del projecte.
Les limitacions detectades durant el procés de recerca han estat:
– Existeix un bloqueig tècnic, en l'àmbit dels drets del sistema operatiu, que impedeix analitzar els processos, esdeveniments i/o contactes de cadascuna de les *Apps* actives en un *smartphone*. La gestió de recursos efectuada pel sistema operatiu del dispositiu *Android OS* no permet l'accés a programaris o processos de tercers *[4]*. Per aquest motiu es descarten les línies de recerca relacionades amb l'anàlisi d'*Apps*.
– Les diferents casuístiques de connectivitat característiques de les *Apps*. Tot i que el procés d'identificació de xarxes *WIFI* es realitza de forma contínua (mitjançant un servei *Android OS*), cal tenint en compte que el dispositiu pot perdre connectivitat amb la xarxa.

Resultats:

Hem analitzat el comportament d'aquest nou sistema d'informació al Principat d'Andorra (Europa), amb una superfície de 468 km², i amb una elevada densitat de població en les zones poblades, situació que ha permès identificar i geoposicionar una gran quantitat de *WIFI Access Points,* i de forma natural, s'han identificat diferents coincidències entre contactes.
Hem realitzat l'estudi sobre una mostra de divuit col·laboradors. Dos dels divuit col·laboradors no van activar el servei que envia (al servidor) la informació dels senyals *WIFI* amb què han tingut contacte, i per tant, no podran beneficiar-se del mecanisme d'avís de situació de risc, però en haver compartit les signatures dels contactes de les seves agendes, participaran del mecanisme d'identificació de relacions entre les agendes dels usuaris.
Cal remarcar que només un dels divuit col·laboradors mantenia activat el servei *GPS* dels seu *smartphone*. L'important consum de bateria d'aquest servei de geoposicionament, lligat a la poca utilitat en espais *indoor* fa que sigui un servei només utilitzat durant períodes concrets.
Tot i que l'objectiu d'aquest projecte no era geoposicionar els *WIFI Access Points*, hem demanat a dos col·laboradors de mantenir actiu el

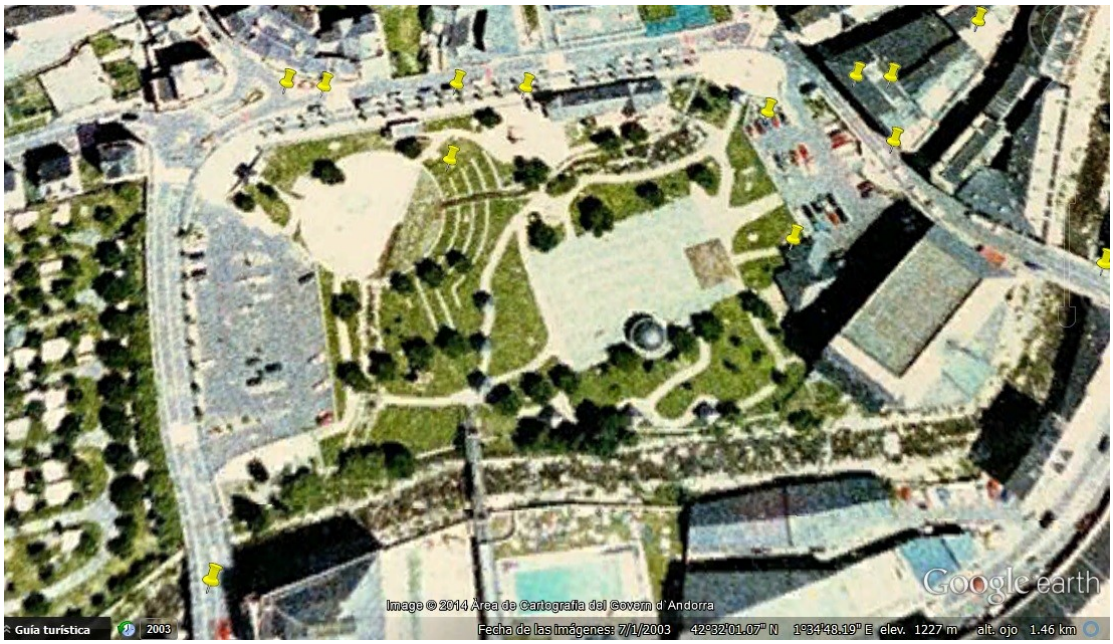

Figura 4: WIFI Access Points que envolten la zona d'esbarjo Prat Gran d'Encamp, identificats per 4 dels 16 col·laboradors, amb una permanència aproximada de 10h setmanals.

servei *GPS* per permetre, a més de l'anàlisi dels temps i els senyals *WIFI,* la seva posició geogràfica. La longitud i latitud dels *WIFI Access Points* són atributs prescindibles segons el disseny de l'aplicació, però que permeten analitzar la quantitat i temps de cobertura dels usuaris, tenint en compte la geoposició dels *WIFI Access Points*.

L'experiment d'identificació de la posició dels usuaris mitjançant les xarxes *WIFI* travessades, l'han realitzat setze col·laboradors entre el 03/04/2014 i el 25/04/2014, que han identificat 18.092 *WIFI Access Points (AP)*, dels que 6.269 *AP* no han estat geoposicionats i 11.823 *AP* sí ho han estat.
En aquest àmbit s'han identificat 55.822 posicions durant unes 1.713 hores d'experiment, 37.750 posicions no han estat inicialment geoposicionades, 18.072 posicions s'han geolocalitzat en viu, i aprofitant la geolocalització dels *WIFI Access Points* (identificades pels usuaris amb el servei *GPS* actiu), el sistema ha geoposicionat en diferit 24.487 posicions.

El temps d'activitat de cada usuari han estat variables (entre l'hora i les 512 hores) i l'inventariat de les posicions també ho ha estat (entre les 52 posicions i les 27.358 posicions).
Un cop analitzades les posicions obtingudes pels usuaris, i tenint en compte les coincidències d'usuaris en aquests *WIFI Access Points,* els hem catalogat en quatre famílies, amb els nivells de risc associats:
1.- Residència. Caracteritzada per extensos períodes de cobertura (12 hores/dia de mitjana), la major part en horari nocturn, en el que s'experimenten poques coincidències amb altres usuaris en els *WIFI Access Points*. Detectem repeticions en els grups de persones que es connecten. Associarem un coeficient de risc moderat, donat que és el lloc de convivència amb la família.
Per exemple, dos dels setze col·laboradors acumulaven més de 20 hores/dia en una posició d'aquest tipus. Vam deduir (i posteriorment confirmar) que es tractava d'un matrimoni.
2.- Treball. Caracteritzada per extensos períodes de cobertura (un mínim de 7 hores/dia de mitjana), habitualment en horari diürn, en el que intervenen un nombre variable d'usuaris en els *WIFI Access Point* propers. Detectem repeticions en els grups de persones que es connecten. Associem un risc moderat, tenint en compte que és l'entorn en què es desenvolupa una tasca professional.
Per exemple, dos dels setze col·laboradors acumulaven més de 28 hores/dia durant tres dies, en posicions d'aquest tipus. Vam deduir (i

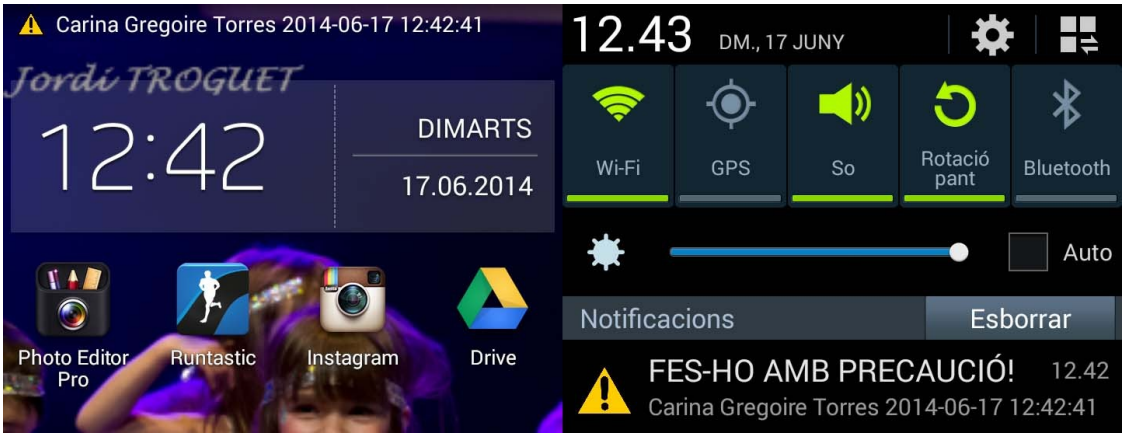

Figura 5: Alerta de proximitat física tenint en compte l'agenda de contactes del propi smartphone.

posteriorment confirmar) que es tractava de companys de feina.
3.- Desplaçament. Caracteritzada per temps de connexió mínims, de l'ordre de segons. Intervenen molts usuaris en els *WIFI Access Points* propers. Associem un risc mínim, donat que són zones de pas, habitualment amb vehicles (figura 3). Són fàcils d'identificar, donat que l'usuari travessa desenes de senyals *WIFI* per minut.
4.- Oci. Caracteritzada per temps de connexió mig d'entre trenta minuts i dues hores, en el que coincideixen molts usuaris en un conjunt de *WIFI Access Points* propers. Són zones de risc elevat, donat que podem coincidir físicament amb un nombre elevat de persones. Són centres de negocis, superfícies comercials, zones verdes, discoteques...

D'altra banda, i analitzant les dades obtingudes, hem verificat un cas de 8 coincidències (de les 16 possibles) en un mateix *WIFI Access Point.* Hem comprovat que els temps de permanència en aquest punt sempre estan per sota del minut, i per tant, hem deduït que es tracta d'un senyal *WIFI* de trànsit. No hi ha cap coincidència física ni temporal entre els seus usuaris. Podem concloure que no respon a un lloc de risc, per molt que les activitats que es realitzin en aquest punt responguin a un potencial risc de contreure malalties de transmissió sexual.
Alhora, hem detectat un *WIFI Access Point* travessat per quatre dels setze col·laboradors durant llargs períodes de temps, d'entre trenta minuts i dues hores. Pot ser considerat un senyal de risc, en tractar-se d'una zona d'oci (figura 4), en la que coincideixen força persones.

Els resultats de l'anàlisi de les relacions entre els contactes de les agendes dels *smartphones* determina que onze dels divuit col·laboradors han permès l'accés als contactes de la seva agenda, mentre que set no han autoritzat l'accés. D'aquests onze col·laboradors, hem codificat i compartit 1.707 contactes, amb una mitjana de 155,2 contactes per agenda.
Els resultats obtinguts per cadascun dels tres tipus de relació són:
- 29 casos de relació bidireccional entre usuaris de primer nivell.
- 4 casos de relació bidireccional entre usuaris de segon nivell. Cap relació en nivells més allunyats.
- 3 dels 11 usuaris participants no tenen cap relació bidireccional entre ells.
- 112 casos de relació unidireccional.

Conclusions:

L'objectiu del projecte ha estat desenvolupar una *App* per *Android OS,* capaç de prevenir a l'usuari de conductes de risc, mitjançant la recepció, de forma voluntària, d'avisos preventius als seus *smartphones*.
Per identificar una conducta de risc el sistema s'utilitzarà dos mecanismes independents. El primer calcularà les relacions existents entre els contactes de les agendes dels *smartphones* dels usuaris registrats, utilitzant una estructura de dades arborescent de fins a sis nivells d'alçada (entre l'usuari arrel i el darrer usuari fulla). El sistema realitzarà aquest procés de forma transparent, segura i automàtica, i sense que l'*App* enviï informació confidencial fora de l'*smartphone*.

El segon mecanisme consistirà a detectar la coincidència d'usuaris dins del radi de cobertura d'un mateix *WIFI Access Point*, i cada cop que el servidor detecti aquest tipus de coincidència, utilitzarà les deduccions del primer mecanisme per descobrir l'existència d'alguna relació entre les agendes d'ambdós usuaris.
En tot cas, no resulta trivial identificar les situacions i/o posicions de risc. Les malalties de transmissió sexual a les que fem referència no responen a cap patró concret d'activitat, moviment o zona geogràfica.
L'estudi mostra que tot i no disposar de les coordenades *GPS,* ni dels usuaris, ni dels *WIFI Access Points*, podem identificar situacions i/o zones de risc tenint en compte la proximitat física que l'anàlisi de la cobertura *WIFI* pot oferir.
També hem demostrat que podem establir diferents nivell de risc, tenint en compte les relacions existents entre les agendes de contactes dels *smartphones* dels usuaris.
Arribat aquest punt, i després de creuar ambdues fons de dades, hem estat capaços de detectar quins contactes de l'agenda formaven part de la família de l'usuari i quins eren companys de treball, tenint en compte els patrons de cobertura *WIFI* (llocs i períodes).
Els membres d'una família comparteixen durant més de vuit hores/dia una mateixa zona de cobertura, i que de forma esporàdica coincidiran en desplaçaments a diferents localitzacions, incloses les zones d'esbarjo, o les grans superfícies. D'altra banda, podem identificar com a companys de feina, contactes que comparteixen durant més de set hores/dia localitzacions amb pocs desplaçaments.
En aquest sentit, el sistema podria identificar posicions de risc (figura 5), detectant situacions fora de context, com podria ser un company de feina en una zona d'oci (proper a l'usuari objectiu), durant el mateix període de temps. Un cop detectada una hipotètica situació de risc, el servidor alertarà a l'*App*.
En l'àmbit de l'anàlisi de la relació entre usuaris, considerarem que els contactes amb relacions de primera baula poden considera-se contactes de baix nivell de risc, vist que hi ha prou confiança entre ambdós per facilitat-se els números de telèfon mòbil, situació poc habitual en tractar-se de desconeguts.
Pel que fa als contactes amb relació d'n baula, hem considerat un nivell de risc elevat, tenint en compte que l'usuari no disposa de prou confiança per correspondre aquesta relació.
Els usuaris amb relacions unidireccionals responen a un nivell de risc extrem, donat que ni gaudeixen de prou confiança i/o informació de l'usuari objectiu, ni hi ha identificats contactes intermedis als que consultar informació complementària.
En tots tres casos el sistema podria proposar als usuaris l'opció de validar les hipòtesis generades pel servidor, amb l'objectiu de millorar la qualitat de les alertes.
Una tasca futura és la implementació, a nivell de servidor, d'un sistema expert (intel·ligència artificial), que li permeti analitzar, raonar i adquirir nous coneixements, segons situacions ja viscudes, i d'aquesta forma, millorar la detecció de conductes de risc, tenint en compte la informació recopilada per l'*App* que hem desenvolupat.

Referències:

1. ***Preventive medicine for epidemic outbreaks and risky behavior through mobile devices and ubiquitous computing*** *Felipe Besoaın-Pino i Antoni Perez-Navarro; Màster tesis en format web, 06/12 Universitat Oberta de Catalunya, Rambla Poblenou 156, Barcelona, Spain.*

2. ***Six Degrees of Separation in Online Society****, Lei Zhang, Tsinghua-Southampton Joint Lab on Web Science Graduate School in Shenzhen, Tsinghua University, Shenzhen, Guangdong Province, P.R.China, i Wanqing Tu, Department of Computer Science, University College Cork, Cork, Ireland, article de recerca en la pàgina web WebSci'09: Society On-Line, 18-20, Athens, Greece, any 2009.*

3. ***A Smart-Phone Indoor/Outdoor Localization System****, Carlos Pereira, Ludimar Guenda and Nuno Borges Carvalho, Instituto de Telecomunicações, Dep. Electrónica, Telecomunicações e Informática, Universidade de Aveiro, ponència en la International Conference on Indoor Positioning and Indoor Navigation*

(IPIN), Guimarães, Portugal, setembre de 2011.
4. ***Researching Information Systems and Computing****, Briony J. Oates, 2008. ISBN: 978-1-4129-0223-6*
5. ***El gran libro de Android****, Jesús Tomás Gironés, 3a edición, any 2013, ISBN: 978-84-267-1976-8*
6. ***http://en.wikipedia.org/wiki/MD5***
7. ***Simple and Complex Activity Recognition through Smart Phones****, Stefan Dernbach, Department of Computer Science Whitworth University Spokane, USA and Barnan Das, Narayanan C. Krishnan & Brian L. Thomas, Diane J. Cook, School of EECS Washington State University Pullman, USA.*
Ponència en la conferència "Intelligent Environments (IE), 2012 8th International Conference (Guanajuato, Mèxic)", juny del 2012.