PISTES EXPLORÉES POUR DÉVELOPPER UNE SOLUTION « PAIR-À-PAIR » PASSANT PAR BLUETOOTH SUR IPHONE

Rapport scientifique - Livrable 1.5.a

Partenaires du projet

Avec le soutien financier de

Rédacteurs :
Gilles MARTIN (ATRISC), Johnny DOUVINET (UMR ESPACE 7300 CNRS), Alexandre JEAN-JEAN (SIMPLON)

Participants :
Amine EL GHAYATE, Pauline MARCATO & Alban JUBERT (SIMPLON)

Décembre 2021

Sommaire

Synthèse des résultats obtenus et recommandations

Cette étude a permis de mettre en avant plusieurs constats et de formuler plusieurs recommandations, qu'il faut considérer à l'horizon des JOP 2024, pour améliorer la diffusion de l'alerte à la population en France. Aucune hiérarchie n'est retenue dans les propositions ci-dessous.

CONSTATS	RECOMMANDATIONS
Il est possible d'intégrer une solution « pair-à-pair » dans la future application des JOP 2024, fonctionnant par Bluetooth (ici sous iPhone), ce qui permettrait de garantir l'acheminement de l'alerte en contexte dégradé, à condition d'associer Apple dans la conception	**Il faut travailler avec Apple, Android et l'ensemble des fournisseurs d'OS (*Operating Systems*, ou systèmes d'exploitation) pour intégrer cette fonctionnalité dans les OS de façon native et améliorer leur utilisation.**
La solution déployée peut servir lors de grands événements, notamment en extérieur ou dans une enceinte ouverte, nécessitant une proximité élevée entre les personnes présentes (communication possible jusqu'à 30m)	**Il faut développer une fonctionnalité de communication pair à pair dans les applications de gestion des grands évènements**
Ce dispositif vient compléter de manière évidente l'ensemble des autres canaux d'alerte, qu'il convient d'interfacer au protocole CAP.	**Il faut intégrer ce dispositif dans les futures plateformes d'alerte, en complément de canaux existants**

1. Apports et objectifs des solutions « P2P »

Le pair-à-pair (*peer-to-peer*, ou P2P), définit un **modèle de réseau informatique** d'égal à égal entre ordinateurs, ou entre téléphones, qui distribuent et reçoivent des données ou des fichiers. Dans ce type de réseau, comparable au réseau client-serveur, chaque client devient lui-même un serveur. Le P2P facilite et accélère les échanges entre plusieurs ordinateurs au sein d'un réseau.

1.1. Des solutions multiples et diversifiées

Différents scénarios ont été explorés pour tester la résistance, voire la robustesse, de l'architecture du réseau cellulaire, notamment en cas de crise. On peut ici citer quelques exemples, sans prétendre à un bilan exhaustif, loin de là. *ProximAid* (*Proximal adhoc networking to Aid emergency response*) est une application développée par des chercheurs de l'université de Chypre (Koumidis et al. 2015) dans le cadre du projet COncORDE. Elle se base sur un mécanisme de balises wifi, pour une solution de réseaux ad hoc complètement distribuée et localisée pour l'aide aux d'interventions d'urgence. En plus de permettre la découverte de périphérique, les balises émettent deux métriques liées au réseau, l'une pour connecter les appareils (Local Connectivity), et une autre pour les connecter via un pont réseau (Browl Connectivity), qui sont utilisés par l'ADS (Alert Dissemination Strategy). Il s'agit en fait d'une stratégie intelligente de diffusion des alertes, basée sur l'expédition des messages vers les parties du réseau contenant le plus d'appareils localisés en vue de réduire la consommation d'énergie des batteries.

En situation post-catastrophe, il est aussi vital de restaurer les communications le plus vite possible. Actuellement, les systèmes sans fils mobiles sont utilisés comme solutions de secours. Mais ces systèmes demandent du temps de configuration, ont une couverture spatiale limitée et font appel à des accès satellites très onéreux. Les solutions alternatives s'appuient, de leur côté, sur les potentiels d'auto-configuration des périphériques, à travers la création de réseaux *mesh*. Les travaux de Ghafoor et al. (2015) portent sur la réalisation d'un système radio en vue d'évaluer le potentiel de ces nouveaux dispositifs. Basé sur l'exploitation des ondes wifi IEEE 802.11s pour le contact avec le périphérique, et sur le réseau GSM pour des accès extérieurs, le prototype de ce système intègre la gestion des appels ainsi que la transmission des données. Les premiers retours d'expérience relèvent que dans des conditions idéales, le système supporte un très grand nombre de connexions et d'appels simultanés mais qu'au-delà, la qualité des communications s'amenuise (**Figure 1**).

D'autres scénarios sont également imaginés lorsque l'infrastructure supportant le réseau cellulaire est encore fonctionnel. Les appareils mobiles pourraient servir de distribution des opérations de sauvetage et de secours dans les zones sinistrées, mais on doit s'attendre, dans ce cas-là, à une saturation du réseau, donc à une réduction de la qualité des communications. En effet, en pareille situation, la connectivité totale ne peut pas être garantie en continu, notamment entre la source et la destination d'un point à l'autre du réseau. Dans le cadre d'un tel scénario, Do-Duy et Vázquez-Castro (2015) ont proposé une architecture réseau pour pallier les difficultés que peuvent engendrer une telle situation, en se fondant sur les appareils mobiles existant, où la livraison de contenu à partir du centre de commandement de la gestion des catastrophes est garantie à tous les utilisateurs via une connectivité intermittente (**Figure 2**). Par ailleurs, l'ensemble des ressources du réseau cellulaire peut être répertorié en utilisant des techniques de coopération entre les liens wifi et le réseau cellulaire.

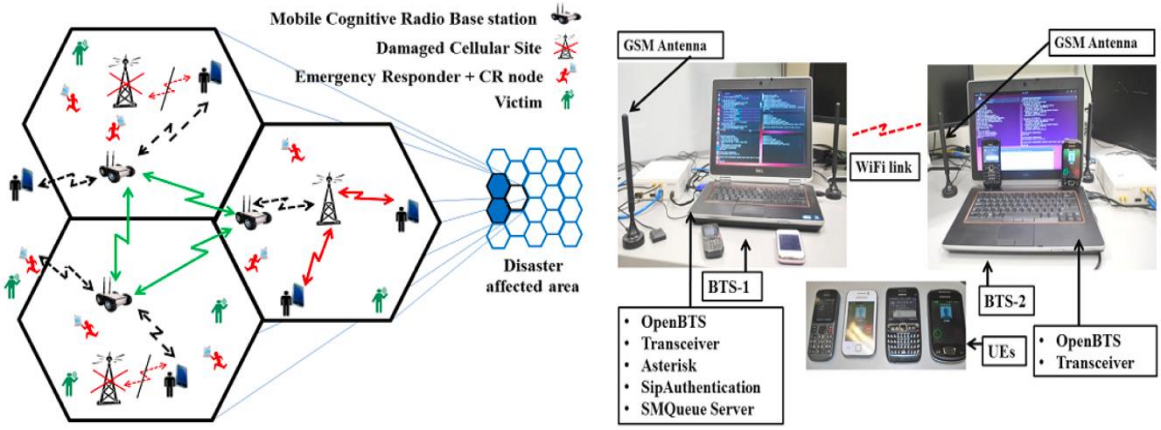

Figure 1. Solutions alternatives classiques et prototype de réseau *mesh* (Ghafoor et al. 2015).

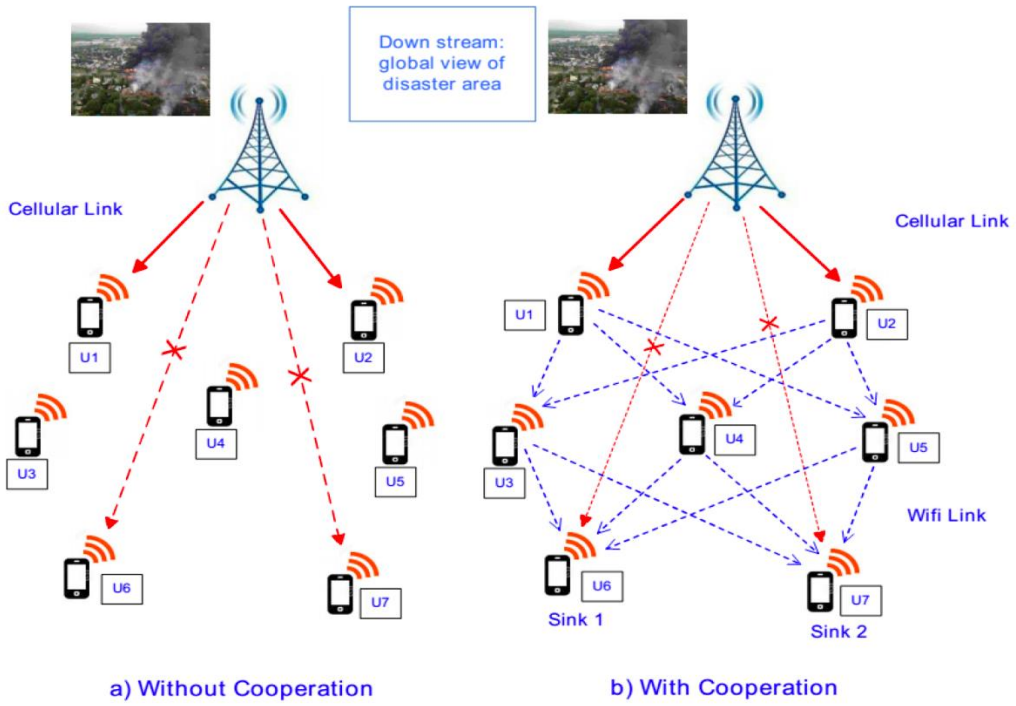

Figure 2. Topologie du réseau proposée par Do-Duy et Vázquez-Castro (2015)

On peut aussi imaginer que les opérationnels et les services de secours soient sur le terrain, dotés de smartphones et qu'ils aient besoin d'informations en provenance du centre de commandement pour être plus efficaces. L'architecture proposée permet alors de convertir les terminaux en appareil de multidiffusion interconnecté, pouvant directement communiquer entre eux. Le modèle de réseau se compose alors de deux groupes. Le premier est composé des utilisateurs directement connectés à la station de base avec des antennes relais. Toutefois, en raison des effets de l'environnement sur la qualité du signal et des obstacles présents, certaines interruptions peuvent survenir et donner lieu à une connectivité saccadée et plus ou moins intermittente. Pour pallier ce problème, le second groupe d'utilisateurs est utilisé comme source indirecte pour relayer le contenu multimédia demandé, sur la

base de liens wifi, créant ainsi un réseau ad-hoc. Le réseau proposé peut alors être adapté par le remplacement de la station de base avec une station sans fil portable, qui est équipée d'une liaison satellite et radio (de courte portée).

1.2. Un objectif prioritaire : pallier toute panne généralisée

En contexte dégradé, les P2P viennent pallier une panne généralisée, des réseaux électriques et/ou de télécommunication. Ils peuvent aussi être utiles si la violence de l'orage perturbe les liaisons et les relais (Serre et al., 2012), ou si la mise en relation des victimes avec les secours est interrompue (Boyd et Ellison, 2007 ; Corvey et al., 2012). C'est pour cette raison que les acteurs du monde humanitaire se sont très vite saisis de cette question, en développant plusieurs applications (Ushaidhi, 18, HumanLife, Red Cross) pour permettre à leurs agents de faire des états des lieux, des points de situation ou des évaluations sur l'étendue des dégâts après les catastrophes.

C'est le début du Mobile Data Collection Systems (MDCS) : sans avoir besoin d'un téléphone mobile, on peut renseigner des informations à partir d'un formulaire et les transmettre à un centre de décision (Laurila et al., 2013 ; Chen et Chan, 2010). En parallèle, c'est le début de la communication à double sens, qui se fait au départ à travers une implication assistée et contrôlée des citoyens dans la collecte. Cette demande se traduit désormais par le développement d'applications spécialisées, qui sont souvent multirisques. Si les premières applications dédiées à l'alerte inondation sont apparues dès 2009 à l'échelle mondiale (*FloodAlert* puis *Flash Flood Guidance* aux Etats-Unis), il faut plutôt attendre 2013 en France pour voir, sur le marché, des solutions logicielles et matérielles sur cette thématique. Des structures publiques ou privées (communes, bureaux d'étude, services de l'Etat) se sont lancées dans cette direction et les exemples se multiplient. La « guerre » ou la « jungle » des applis est désormais lancée, tellement les solutions foisonnent (Kouadio et Douvinet, 2016).

Cependant, dans certains cas, les communications classiques comme Internet ou les téléphones (fixes ou mobiles) peuvent être hors service (pendant, voire après une catastrophe), à cause d'une panne électrique ou de la violence de l'orage qui gêne ou interrompt les liaisons et les relais (Serre et al., 2012). Lors des inondations du 15 juin 2010 dans le Var (France), par exemple, les pompiers ont du intervenir (2 357 hélitreuillages entre 16h38 et 23h15) sur de nombreux secteurs (sur 35km), alors que les transmissions étaient inexistantes (plus de téléphone filaire, plus de GSM, plus de radio analogique, et seuls quelques SMS passaient de temps de temps, d'après le COL E. Grohin, SDIS06, communication orale ; Douvinet *et al.,* 2017). Plus de 200 000 personnes n'avaient plus d'électricité.

Autre exemple : le 3 octobre 2015, de nombreux habitants sont restés injoignables pendant plus de 2 heures (de 20h30 à 22h30), notamment dans un quartier à Biot (le Hameau du Carimaï) où les habitants ont eu jusqu'à plus de 2m d'eau dans leur maison (Saint-Martin, 2014).

Ces problèmes perturbent la réactivité des acteurs opérationnels, et notamment la mise en relation des victimes avec les secours (Boyd et Ellison, 2007 ; Corvey et al., 2012). Aussi, il faut trouver des solutions plus souples et non dépendantes de ces réseaux. A ce titre, les réseaux opportunistes paraissent intéressants à explorer. Dans ce cas, on parle de MANET (Mobile Ad-Hoc Networks) (Brownlee et Liang, 2011) ou de réseau *mesh* (Takahashi et al., 2008). Ces solutions permettent de s'affranchir des réseaux de télécommunication officiels et le smartphone devient un relais pour établir un réseau « pair-à-pair » entre plusieurs smartphones (Sicard et al., 2010 ; Zhuang ; 2013), autrement dit sans avoir un nœud central, pour aboutir à un réseau de plus en plus « résilient ». Des systèmes de routage, appelé BATMAN (*Better Approach To Mobile Ad-hoc Networking*), ou AODV (*Ad hoc On-demand Distance Vector*), ont aussi été créés pour être opérationnels lorsque les réseaux sont hors service (Wirtz et al., 2011).

1.3. Un objectif complémentaire : garantir une connectivité permanente

Les solutions P2P peuvent aider les citoyens en cas d'alerte. Se préparer à une crue consistait, il y a dix ans, à avoir un kit d'urgence, un Plan Familial de Mise en Sureté (PFMS) et ne conserver que l'essentiel. Les solutions P2P ont en revanche créé de **nouvelles pratiques**. En situation d'urgence, un citoyen qui a un téléphone peut avoir accès à des numéros de secours intégrés (police locale, pompiers), créer un groupe de contact à l'aide d'une application de messagerie instantanée, se connecter sur un RSN ou utiliser une application informant de manière automatique les proches ou les familles de la situation.

Quelle que soit la nature de la crise (naturelle, technologique ou géopolitique), on remarque que le flux informationnel est désormais très différent. Chaque citoyen est en capacité d'agir à travers le web social constitué des interrelations entre individus connectés (Millerand et al., 2010) et ce ne sont plus seulement l'État et les autorités qui sont détenteurs de l'information et qui en déterminent le contenu et la temporalité de la diffusion. Ces multiples interactions permettent, voire favorisent, une forme de dé-hiérarchisation de l'information. Cette dernière, jusque-là cantonnée à un flux « topdown » des autorités vers la population, voit désormais apparaître des flux d'information ascendants et horizontaux, autrement dit du citoyen vers les autorités et entre les citoyens eux-mêmes (Coyle et Meier, 2009). Ceux qui sont très proches de l'épicentre du phénomène utilisent les technologies embarquées dans leurs outils (smartphones et autres objets communicants) pour envoyer des messages, poster des photos, des vidéos... (Vieweg et al., 2010), avant même que les autorités ne s'en saisissent puisque les protocoles de régulation institutionnelle de l'information ne sont pas dimensionnés pour gérer des temporalités aussi courtes et rapides. L'impératif d'authenticité et de garantie des communications officielles ne cadre pas non plus avec ces modes de diffusion.

Dès 2011, aux États-Unis, Chris Fugate, le responsable de la *Federal Emergency Management Agency* (FEMA), suggère d'arrêter d'utiliser les réseaux sociaux comme des mégaphones et d'engager plutôt des dialogues avec le public (*we need to stop just using social media as a megaphone to broadcast information and instead use it to have a two-way conversation with the public* cité par Holdeman, 2013), dans une optique de communication interactive et non directive. Déjà en 2011, il proposait au *Department of Homeland Security* de considérer le public comme une ressource et non un handicap durant les crises (Fugate, 2011).

Plusieurs outils permettent également aux citoyens de contribuer à la cartographie de crise (crisis mapping), en ayant recours à des plateformes participatives basées sur les solutions libres comme OpenStreetMap et Google Map. Goodchild (2007) appelle la contribution venant des citoyens « l'Information Géographique Volontaire » (Volunteered Geographical Information) et dès 2007, il insistait sur le rôle que doivent jouer ces citoyens-capteurs. Les catastrophes survenues depuis lui donnent raison. Le logiciel Opensource Ushahidi, développé au départ dans un contexte de crise géopolitique au Kenya pour avoir des informations géolocalisées, a été utilisé lors du séisme en Haïti par le bureau de coordination de l'aide humanitaire de l'ONU (*United Nations Office for the Coordination of Humanitarian Affairs, UNOCHA*). Ces approches de type « crowdsourcing », se fondent une fois de plus sur du volontariat. Parmi les contributeurs, il existe deux catégories qui ne se situent pas dans les mêmes temporalités d'action ni dans les mêmes lieux : les « veilleurs » se situent en amont de l'événement et vont alerter les « suiveurs » qui seront directement impactés par la crise. En schématisant, la première catégorie recouvre une temporalité qui va de la prévention à l'alerte, tandis que la seconde émerge durant l'alerte et se positionne dans la crise.

2. Limites et craintes face aux solutions « P2P »

2.1. Des limites propres aux smartphones

Le développement de solutions P2P basées sur la géolocalisation (via le système GPS) est tout d'abord limité en France à cause de contraintes réglementaires et/ou juridiques. Sur ce point, le smartphone cristallise aujourd'hui la même crainte que celle d'il y a quelques années avec la sécurité pour les PC : sommes-nous vraiment les seuls à accéder à nos données ?

La réponse est vite négative (en tout cas pas pour tous les smartphones). Avec d'un côté, la variété de plates-formes disponibles aujourd'hui, et de l'autre l'augmentation de la présence digitale des administrations tant publiques que privées, les utilisateurs sont en interaction constante avec leurs réseaux sociaux, chacune de ces interactions se traduisant par un nouveau point-source de données mesurables. Une enquête CNIL (2014) (Commission Nationale de l'Informatique et des Libertés) a démontré que la majorité des applications accèdent en permanence ou dès qu'elles en ont l'occasion, à la mémoire interne ou à la liste des contacts ; elles lisent et modifient des données ; elles accèdent au GPS et transmettent tout cela via internet et cela sans consentement des usagers.

Plusieurs études révèlent aussi l'impossible anonymisation véritable des données collectées sous leur forme actuelle. La collecte massive de données sur l'individu constitue une véritable source de profilage psychologique et comportemental (WEF, 2011). Si au niveau des empreintes digitales, il faut 12 points pour identifier sans équivoque une personne, Montjoye et al. (2013) nous apprennent que seulement 4 données spatiotemporelles suffisent aujourd'hui pour nous distinguer dans une foule.

Des données sont donc collectées en temps continu, surtout à partir des terminaux fonctionnants sous Androïd. Non seulement à cause des mises à jour régulières de ce système, de son ouverture à des améliorations tierces (téléchargées avec de moins en moins de contrôle) que Xing et al. (2014) qualifient de phénomène de « fragmentation Androïd », mais aussi et surtout parce qu'en tant que leader actuel du marché des systèmes d'exploitation (selon IDC, 2013). D'après Kaspersky Lab et INTERPOL (2014), Android était d'ailleurs la cible privilégiée des attaques malveillantes collectant de façon frauduleuse des données privées. Où vont exactement ces données et dans quelle mesure ?

Face à l'ampleur de ce constat, il est délicat, sans mesures préalables, d'inviter les citoyens à contribuer de façon volontaire au sens de Goodchild (2007), Mericskay et Roche (2011) à la remontée ou à la diffusion d'une alerte même en cas de panne généralisée. Ainsi, quelles données peuvent être partagées en toute sécurité ? Sous quelle forme et avec qui ? Dans quelle mesure pouvons-nous développer un cadre approprié pour protéger la vie privée ? Comment empêcher l'utilisation abusive de ces données ?

La protection des personnes physiques à l'égard de l'utilisation et des traitements des données de géolocalisation demeure régie en France par les lois 2004-669 du 9 juillet 2004 et 2004-801/182 du 6 août 2004 (portant sur les protections individuelles au sens large). Afin d'éviter que des personnes non autorisées n'accèdent aux données, il est obligatoire de prendre des mesures de sécurité (accès à un site avec un identifiant et un mot de passe), selon la norme 51 de la CNIL. Cet usage est aussi protégé par un ensemble de lois associées au droit pénal (article 226-1 et suivants sur la protection de la vie privée ; article 226-16 relatif aux droits des personnes résultant de traitements informatiques ; loi du 6 janvier 1978). Ces contraintes semblent être un frein important, alors même que le développement d'applications récentes prouve le contraire (Kouadio, 2016).

2.2. Des solutions qui doivent s'adapter aux futurs utilisateurs

Les solutions mises en œuvre dans une logique « top-down » (descendante) ont montré leur inefficacité à plusieurs reprises. Dès lors, il faut éviter de rester dans les mêmes schémas : pour accroître l'usage des applications, il faut qu'il existe une sorte de « terreau social propice à se saisir de ces outils pour la fertiliser » (Villard, 2015 ; Douvinet et al., 2017). Les pratiques doivent ainsi préexister en amont d'une crise (ce qui passe par des mises en situation ou des exercices d'entraînement) et les institutions doivent faire la promotion (on peut craindre que l'abandon de SAIP® aura des conséquences négatives pour l'ensemble des autres applications et auprès de la population française).

Les niveaux de langage ne sont pas identiques selon (voire entre) les acteurs (individus et/ou autorités). Certaines applications ont alors essayé de mieux s'adapter aux utilisateurs en intégrant une sémantique plus appropriée et des termes plus simplifiés par rapport au contexte de crise, en réduisant le nombre de menus, ou en allégeant la description d'un phénomène (Vialert®, Notico®, Signalert® par exemple). Des langages spécifiques ont même été développés, comme le Humanitarian eXchange Language Situation and Response Standard (HXL40) (Kebler et Hendrix, 2015) ou le Management Of A Crisis Vocabulary (MOAC). Ces initiatives sont toutefois globalement occultées dans les applications en France (car les niveaux de langage apparaissent pour les décisionnaires trop simplistes), alors que plusieurs applications déployées à l'échelle mondiale, comme Donate-N-Request® et WeReport® (Li et al., 2015), ont démontré que les usages pouvaient être démultipliées quand l'ergonomie, le design ou les contenants étaient conçus avec les futurs utilisateurs (soit dès la phase de conception).

On doit donc mieux comprendre les **conséquences des messages reçus par les utilisateurs** pour savoir si les solutions P2P répondent à l'ensemble des besoins. En France, les applications restent un outil supplémentaire sans réelle appropriation, avec des usages se situant « à la marge » ou qui suscitent de la défiance. Envoyer une alerte via la géolocalisation est une source d'inquiétude avérée (Aloudat et al., 2014), et qui a des impacts négatifs car les individus ont besoin de le savoir avant, afin de ne pas ressentir une « perte de contrôle ».

Les applications analysées au début du projet (de février à juin 2020) illustrent la théorie de la réactance (Brehm et Brehm, 1981), connue en psychologie ou en marketing, et qui repose sur l'idée qu'une trop forte contrainte sur un individu (que l'on souhaite impliquer) le pousse à se comporter à l'opposé même de cette contrainte (par effet de rejet). Les applications smartphones pourraient alors disparaître à court terme si les concepteurs ne s'adaptent pas (à l'image du premier smartphone Simon, créé en 1992, qui a été un échec commercial à cause d'une difficile prise en main par les futurs utilisateurs) et les applications apparaissent ainsi fragiles à long terme.

Une solution serait par ailleurs de détourner la technique au service des individus (Gisclard, 2017) et les formes de réappropriation peuvent prendre différentes formes. Le darknet est par exemple un réseau internet parallèle au web classique, qui permet l'anonymisation des données et autorise à s'affranchir des tutelles « GAFA » (Google, Amazon, Facebook, Apple), ou de la surveillance d'états « autoritaires ». Il regroupe à la fois le pire de la cybercriminalité et des réseaux d'activistes oeuvrant pour l'open source et la protection des libertés individuelles (Guitton, 2013). Cette volonté de lutter contre les mésusages du numérique a vu, depuis le début des années 2000, surgir la génération de nouveaux hackers, qui détournent, créent et améliorent des programmes en marge des prestataires, notamment en cas de catastrophes naturelles (à l'image de l'association HAND).

Cette « culture du détournement » est aujourd'hui ancrée dans la société civile, dépassant les réseaux d'initiés et se prolongeant dans des espaces collaboratifs de partage tels que sont les hackerspaces, hackatons, civictech ou makerspaces (Gershenfeld, 2007 ; Huguet, 2017). Ces ateliers partagés se développent à travers le monde depuis 2011, et ouvrent la voie à de nouveaux champs d'exploration dans des domaines très variés (Bosqué, 2015). Sans en faire la promotion, ces expérimentations incitent à la réappropriation par les individus de leurs capacités d'action sur les objets et systèmes issus du numérique pour répondre à une question centrale : « dans quel monde voulons-nous être connectés ? » (Allard, 2015).

Commentaires de l'équipe projet : Une notification « push » envoyée en mode « pair à pair » reste une solution crainte mais intéressant à explorer : **le message est reçu par l'utilisateur, même si l'application est en veille** (Charland et Leroux, 2011), et son utilisation ne dépend pas, au préalable, de la collecte des numéros de téléphone. Les individus n'ont ainsi pas besoin de télécharger une application spécifique ou dédiée à la thématique du risque, dont ils ne verraient l'intérêt qu'en cas de crise ou de risque avéré. A condition toutefois que les utilisateurs autorisent l'accès aux données de géolocalisation, et les nouvelles contraintes imposées par le Règlement Général sur la Protection des Données depuis le 26 mars 2018 en France, ajoutent un niveau de complexité supplémentaire.

3. Notre démarche

Suite à cet état des lieux, et suite au retrait de QWANT du projet (acté en mai 2020), nous avons choisi de nous orienter vers SIMPLON PROD (une agence solidair de création d'applications mobiles), pour définir ensemble une technologie qui permettrait de créer un réseau *mesh* en cas d'urgence, dans un contexte de communication dégradée. Notre choix s'est porté sur le *Bluetooth Low Energy*, technologie qui est apparue avec le déploiement du Bluetooth 4.0 en 2010. Solution **économe** en énergie, **gratuite**, **présente** sur la majorité des smartphones et des systèmes d'exploitations existants sur le marché.

3.1. Hypothèses et pistes suivies

Après étude du fonctionnement du *Bluetooth Low Energy*, nous avons cherché les solutions existantes développées en **réact-native** afin d'accélérer la mise en place d'une preuve de concept. Une application offrant la possibilité de détecter un signal précis a été imaginé, dans le but d'établir une connexion entre deux téléphones mobiles. Une fois la connexion établie, l'appareil récepteur (central ou client), était en mesure de réceptionner l'information émise par notre appareil émetteur (peripheral ou serveur), et à son tour de basculer en mode serveur. **Les premiers tests ont démontré que nous pouvions transmettre un message texte d'une longueur de 400 caractères.**

Dans un second temps, nous avons testé un certain nombre d'hypothèses en vue de maintenir l'émission et la réception d'un message texte au travers du *Bluetooth Low Energy,* alors que les applications étaient mises en arrière-plan (mode background).

Parmi ces hypothèses figuraient :

- La mise en place d'une liste de tâches à effectuer en arrière-plan dès le passage en mode background ;
- Exploiter la géolocalisation en mode background pour réaliser nos scans réseaux
- Utiliser la technologie iBeacon
- Utiliser la technologie Proximity Contact Tracing (comme *TousAntiCovid*)
- Hacker l'overflow area, zone de transmission des trames Bluetooth entre smartphones Apple en mode background

Grâce à ces multiples pistes, nous avons pu délimiter le cadre dans lequel nous pouvons exploiter les fonctionnalités mises à disposition par Apple. Nous savons aujourd'hui, qu'il est possible de déclencher une tâche lorsque l'application se trouve en mode background à une fréquence d'au minimum 15 minutes. Cette fréquence reste indicative, puisque le système se réserve le droit d'élargir, et/ou de planifier ces tâches en fonction de la fréquence d'utilisation de l'application. D'autres critères d'usage entrent en jeu comme le niveau de batterie, la priorité d'un processus sur l'autre etc.

Toutefois, il était impossible d'établir une connexion entre deux smartphones, si les deux applications étaient fermées. Lorsque le serveur ou le client sont ouverts, si le scan réseau a été fait en mode background au bout de 15 minutes, nous pouvons établir un échange de données. De plus, Apple nous a confirmé qu'il nous serait très difficile de réaliser une communication en mode background par le biais du Bluetooth Low Energy, étant donné le nombre de facteurs limitants qui sont à prendre en compte dès le moment où l'application est mise en sommeil.

Suite à cela, nous nous sommes occupés d'amener notre prototype plus loin, pour réaliser des tests au plus proche de la réalité (tests planifiés pour le séminare Envirorisk 2021 à Aix en septembre 2021). Pour cela, nous avons mis en place un système d'envoi de notifications push via Google Cloud Messaging, ainsi que la réception de ces dernières dans l'application. Notre prototype, dès réception d'une nouvelle notification, analyse la notification, l'affiche dans l'application et bascule en serveur pour transmettre à son tour son contenu. Enfin, nous avons étudié la possibilité de géolocaliser les notifications diffusées en cas d'urgence. Pour répondre à cette demande, les notifications silencieuses semblent être un moyen parfait pour déclencher une application fermée ou en sommeil **(Figure 3)**.

Grâce à cela, en envoyant une push notification contenant les coordonnées gps de la zone concernées par l'urgence, nous pouvons décider d'afficher ou non la notification (**Figure 4)**. En ce qui concerne la prise en charge du Cell Broadcast (CB), nous n'avons pas été en mesure de trouver une solution offrant les moyens de lire ce type de notifications sur iOS (le système d'exploitation Apple). Par défaut, nous avons testé (et avec succès) l'envoi d'un message CB, en prenant l'exemple du vrai message d'alerte diffusé par CB au Royaume-Uni, pour annoncer l'arrivée imminente d'inondations (**Figure 5).**

Nous pouvons conclure, en disant que les limites imposées par le fabricant Apple sont jusqu'à un certain point, incontournables. Cependant, nous pouvons affirmer qu'il est possible de créer un réseau *mesh* au travers de la technologie *Bluetooth Low Energy*. En considérant de nouveaux cas d'usages, il est tout à fait possible de dire que ce type de dispositif développé en langage natif et intégré au sein d'une application, serait une solution de secours intéressante.

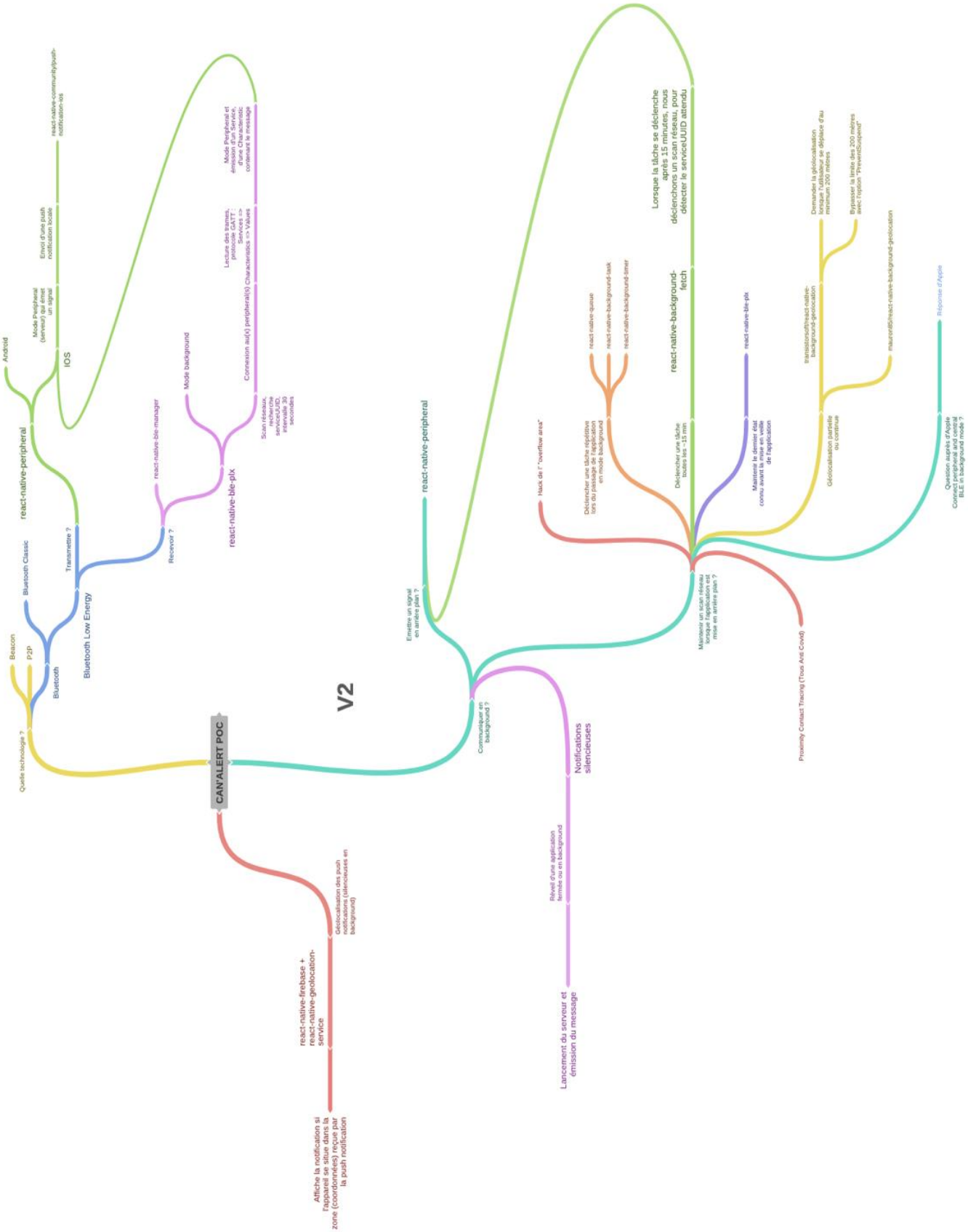

Figure 3. *Minp map* résumant les pistes suivies et les résultats (ou les freins) découverts

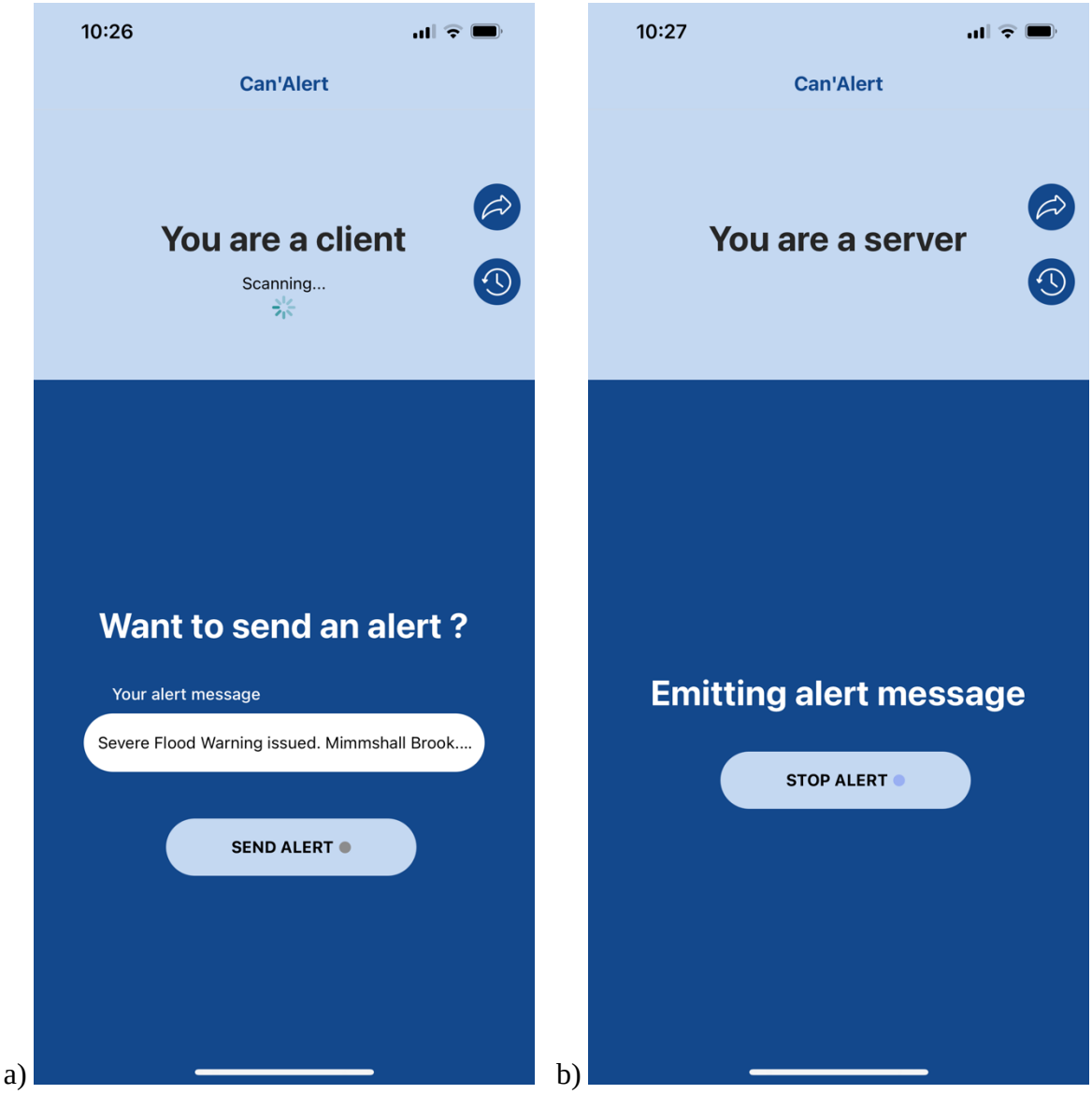

Figure 4. *a) Affichage de l'application lors du scanning dans un environnement proche ; b) envoi du message (il faut attendre au maximum 20 secondes avec la réception par un autre téléphone)*

Figure 5. *Texte pris pour exemple (notification CB au Royaume-Uni)*

3.2. Tests et expérimentations

Plusieurs séries de tests ont pu avoir lieu :

- Du 23 au 24 septembre 2021 (Envirorisk) > besoin d'avoir un accusé de la notification
- Du 12 au 13 octobre 2021 (Havre) > pas de contact en cas de déplacement en voiture
- Du 18 au 19 octobre 2021 (Avignon) > effets de distance et blocage des murs
- Le 9 décembre 2021 (lors du séminaire de restitution à Paris).

Il en ressort que l'on peut transmettre des messages entre 2 smartphones hors réseau via l'application jusqu'à une cinquantaine de mètres. Les messages ne passent pas entre 2 véhicules à proximité. Le reste des limites et contraintes est dû au système d'exploitation (OS, pour *Operating System*) qui n'autorise que peu de fonctionnalités.

D'autres tests ont aussi été imaginés avec SIMPLON, pour détecter tout problème technique.

1\ Test dans une salle de dimension restreinte

Objectifs : Ce test serait intéressant pour mesurer le taux de réussite, avec un groupe de personnes plus large que ceux des tests précédents. Dans une petite salle, avec un nombre d'une dizaine de personnes, déclencher l'envoi d'une notification push sur le téléphone cible. Ce téléphone devrait automatiquement, ouvrir l'application en background, et déclencher le serveur.
Conditions : Il sera nécessaire d'avoir les applications "clients" ouvertes.
Indicateurs : Permet de mesurer la rapidité de réception, le taux de réception, le taux d'échec, etc.

2\ Test en répartissant les appareils dans plusieurs salles à différentes distances

Objectifs : Un test avec plusieurs appareils séparés par différents murs serait intéressant, pour évaluer la portabilité du Bluetooth low energy. Peut-être serait-il intéressant d'essayer dans un bâtiment avec des mûrs constitués de différents matériaux (béton, placo...), différentes épaisseurs.
Conditions : Même procédure à appliquer que pour le test 1.
Indicateurs : Permet de mesurer la rapidité de réception, le taux de réception, le taux d'échec, etc.

3\ Test dans un centre commercial

Objectifs : Un test au sein d'une grande surface où se croisent beaucoup de monde, pourrait être intéressant. Il permettrait là aussi de mesurer la portabilité et la fiabilité de l'information échangée.
Conditions : Même procédure à appliquer que pour le test 1.
Questions : La distance de 30 mètres est-elle atteinte ? La connexion est-elle aussi rapide ?

Pour plus de détails, voir le livrable 1.5.c du projet Cap-4-MultiCan-Alert, produit par SIMPLON PROD.

4. Conclusions et perspectives

Suite à cette recherche, et face aux limites identifiées, nous préconisons les points suivants :

- Développer une **fonctionnalité de communication pair à pair dans les applications de gestion des grands évènements** (JOP 2024),
- Travailler avec les fournisseurs d'OS (Apple et Android) pour intégrer cette fonctionnalité dans les OS de façon native et améliorer leur utilisation,
- Intégrer ce dispositif dans les futures plateformes d'alerte en complément des canaux existant.

Ce constat fait directement écho à des recherches déjà publiées par Laflaquière (2005) :
À travers les attaques subies par les technologies P2P, c'est non seulement toute une technologie que l'on cherche à museler, mais ce sont aussi des dizaines de solutions innovantes offertes par le P2P que l'on menace, alors que ces dernières pourraient bien constituer une des plus grandes mutations à venir de l'Internet et de son usage.
Il existe (…) une multitude d'applications au P2P, qui restent dans l'ombre. Au-delà de leur diversité, il faut souligner que certaines applications sont le fruit d'un travail approfondi pour répondre à des besoins engendrés par de nouvelles problématiques. Leur succès ne doit rien au hasard, ni à la mauvaise image dont bénéficie le P2P en général. La technologie P2P est tout simplement apte à accompagner l'évolution des pratiques qui convergent vers une « intelligence collective », quelle que soit sa forme ou son domaine d'application.

Liste des figures et des tableaux

Liste des références bibliographiques

Allard, L. (2015). L'engagement du chercheur à l'heure de la fabrication numérique personnelle. *La Revue*, Hermès, 73, 159-167.

Aloudat A., Michael K., Al-Debei M. (2014). Social acceptance of location-based mobile government services for emergency management. *Telematics and informatics*, 31, 153-171.

Bosqué, C. (2015). Des Fabs-Labs dans les marges : détournements et appropriation. *Journal des Anthropologues*, 142-143, 49-76.

Boyd D., Ellison N. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13,1.

Brehm, J. W. (1966). A theory of psychological reactance. New-York, USA : Academic Press, 243 p.

Chen B., Chan M. (2010). Mobicent: a credit-based incentive system for disruption tolerant network, Proceedings of IEEE INFOCOM, 2010, 1–9.

CNIL (2014). Mobilitics, saison 2 : Les smartphones et leurs apps sous le microscope de la CNIL et d'Inria. *La lettre innovation et prospective de la CNIL N°08* | novembre 2014.

Corvey, J.W., Verma, S. Vieweg, S. Palmer, M. & Martin, J.H. (2012). Foundations of a multilayer annotation framework for Twitter communications during crisis events. *LREC 2012, 8 International Conference on Language Resources and Evaluation*, Istanbul, Turquie.

Coyle D. et Meier P. (2009). *New Technologies in Emergencies and Conflicts: The Role of Information and Social Networks.* Washington D.C. and London, UK, UN Foundation-Vodafone Foundation.

Do-Duy T. et Vázquez-Castro M. A. (2015). Efficient communication over cellular networks with network coding in emergency scenarios," 2015 *2nd International Conference on Information and Communication Technologies for Disaster Management* (ICT-DM), Rennes, 2015, 71-78.

Douvinet J., Kouadio J., Grasland C. (2017). Développer une application smartphone pour face aux inondations rapides : le jeu en vaut-il vraiment la chandelle ?"*Actes du colloque Géorisques, Publications de l'Université Paul-Valéry*, Montpellier III.

Fugate C. (2011). *Improving the nation's response to catastrophic disasters: how to minimize costs and streamline our emergency management programs*.
http://www.dhs.gov/news/2011/03/30/administrator-craig-fugate-federal-emergency-management-agency-transportation-and

Gershenfeld, N. (2007). *Fab: the coming revolution on your desktop. From personal computer to personal fabrication.* New-York, USA : Basic Books.

Ghafoor S., Brown K. N. et Sreenan C. J. (2015). Experimental evaluation of a software defined radio-based prototype for a disaster response cellular network. 2015 2nd *International Conference on Information and Communication Technologies for Disaster Management* (ICT-DM), Rennes, 2015, pp. 57-63. doi: 10.1109/ICT-DM.2015.7402034.

Gisclard B. (2017). *L'innovation sociale territorialisée : un levier de réappropriation du risque inondation par les habitants. L'exemple des crues rapides dans les territoires ruraux du Gard et du Vaucluse (France).* Université d'Avignon et des Pays du Vaucluse, 324 p.

Goodchild M.F. (2007) - Citizens as sensors: the world of volunteered geography. GeoJournal n° 69(4), pp. 211-221. Reprinted in M. Dodge, R. Kitchin, and C. Perkins, editors, *The Map Reader: Theories of Mapping Practice and Cartographic Representation*, 370-378. Hoboken, NJ: Wiley.
Huguet, F. (2017). Le déploiement des réseaux communautaires sans fil (MESH), *Netcom*, 31 (1/2), 33-52.
International Data Corporation (IDC) (2013). Chiffres clés : les OS pour smartphones.
Kaspersky Lab et INTERPOL (2014). Mobile cyber-threats: a joint study by Kaspersky Lab and INTERPOL, 38p. http://media.kaspersky.com/pdf/Kaspersky-Lab-KSN-Report-mobile-cyberthreats-web.pdf
Keßler C. et Hendrix C. (2015). The humanitarian exchange language: coordinating disaster response with semantic web technologies. *Semantic Web*, 6(1), 5-21.
Kouadio J.K. (2016). *Les technologies smartphones comme outils d'aide à l'alerte aux crues rapides en France – Expérimentations dans le Var et le Vaucluse*. Thèse de Géographie, Université d'Avignon et des Pays de Vaucluse, 220 p.
Kouadio J.S. et Douvinet J. (2016) - Diffuser une alerte aux crues rapides via une application Smartphone en France : de la théorie à la mise en pratique. *Ingénierie des Systèmes d'Information, Revue des sciences et technologies de l'information* (http://isi.revuesonline.com/accueil.jsp).
Koumidis K., Kolios P., Panayiotou C., Ellinad G. (2015). ProximAid: Proximal adhoc networking to aid emergency response, Proceeding of 2nd *International Conference on Information and Communication Technologies for Disaster Management (ICT-DM),* Rennes, 2015, 65-72-63.
Laflaquière J. (2005). Les « autres » applications des technologies Peer-to-Peer, *Multitudes*, 2005/2 (21), p. 59-68. URL : https://www.cairn.info/revue-multitudes-2005-2-page-59.html
Laurila, J. K., Gatica-Perez, D., Aad, I., Blom, J., Bornet, O., Minh Tri Do, M., Dousse,O., Eberle, J. & Miettinen, M. (2013). From big smartphone data to worldwide research: the mobile data challenge. *Journal Persuasive and Mobile Computing*, 9(6),752-771.
Mericskay B. et Roche S. (2011) - Cartographie 2.0: le grand public, producteur de contenus et de savoirs géographiques avec le web 2.0., *Cybergeo: European Journal of Geography*.
Millerand F., Proulx S. et Rueff J. (dir.) (2010) - *Web social. Mutation de la communication.* Québec, Canada : Presses de l'Université du Québec, Coll. « Communication »
Montjoye Y.-A., Hidalgo C.A., Verleysen M. et Blondel V.D. (2013) - Unique in the Crowd: The privacy bounds of human mobility. *Sci. Rep. 3*, 1376 ; DOI:10.1038/srep01376
Saint-Martin C. (2014) - *Intégration, au système d'avertissement de la méthode AIGA, du facteur d'exposition des territoires au risque inondation.* Rapport de stage effectué au sein de IRSTEA en vue de l'obtention du grade de Master Gestion des Catastrophes et des Risques Naturels (G.C.R.N.) 87p.
Serre D., Barroca B., Laganier R. (2012). *Resilience and Urban Risk Management*, CRC Press Balkema, Taylor & Francis Group, ISBN 978-0-415-62147-2.
Takahashi D., Hong X. et Xiao Y. (2008) - On-demand anonymous routing with distance vector protecting traffic privacy in wireless multi-hop networks. *Proc. of 4th International Conference on Mobile Ad-hoc and Sensor Networks,* 145-151.
Vieweg S., Hughes A. L., Starbird K. et Palen L. (2010) - Microblogging During Two Natural Hazard Events: What Twitter May Contribute to Situational Awareness. In *Proceedings of the International Conference on Human Factors in Computing Systems* (CHI '10), ACM Press, 1079-1088
Villar C. (2015). "Quels apports des réseaux sociaux à la résilience d'un territoire ?", Récupéré le 17 mai 2015 du site du Centre d'Étude et d'expertise sur les risques, l'environnement la mobilité et l'aménagement (CEREMA)
Wirtz H. Heer T., Backhaus R., et Wehrle K. (2011). Establishing mobile ad-hoc networks in 802.11 infrastructure mode. In *Proceedings of the 6th ACM workshop on Challenged networks* (49-52). ACM