Architecture de collecte pour la géolocalisation en situation de crise : évaluation comparative

Florent Coriat, Anne Fladenmuller, Luciana Arantes

Compas'2018 : Parallélisme/ Architecture / Système
ENSEEIHT - Toulouse, France, du 03 au 06 juillet 2018

Architecture de collecte pour la géolocalisation en situation de crise : évaluation comparative

Florent Coriat, Anne Fladenmuller, Luciana Arantes

Sorbonne Université, CNRS
Laboratoire d'Informatique de Paris 6 (LIP6)
F-75005 Paris, France
<prenom.nom>@lip6.fr

Résumé
Dès qu'une catastrophe naturelle ou humaine se produit, cartographier et localiser les personnes est un enjeu crucial et complexe à mettre en œuvre, les infrastructures de communication « classiques » se trouvant alors endommagées ou inopérantes. Nous présentons ici une architecture de collecte de données de localisation après-crise, qui repose sur des échanges pair-à-pair pour acheminer les données vers les centres de secours, ainsi que son évaluation sur simulateur.

Mots-clés : géolocalisation, pair-à-pair, gestion de crise, terminaux mobiles

---

1. Introduction

Après une catastrophe naturelle ou humaine, les infrastructures de communication « classiques » sont le plus souvent endommagées et/ou surchargées par les tentatives répétées des équipes de secours, mais surtout des victimes et de leurs proches d'obtenir des informations sur la situation, pour pouvoir aider ou simplement se rassurer. Or l'évaluation de la situation dans sa globalité est un enjeu crucial dès les premiers instants pour les secours : l'établissement de communications *de crise*, dédiées, est une priorité en attendant que le fonctionnement normal du réseau puisse être rétabli. Une architecture de communications de crise aiderait idéalement à évaluer et gérer la situation, en cartographiant la zone en temps réel (localisation des zones à risques, ressources, etc.), en localisant les victimes et rescapés, et en maintenant un contact entre rescapés, secouristes et centres de contrôle des opérations.
Suite à différentes catastrophes ces dernières années, de nombreux projets ont ainsi émergé en proposant de diffuser des informations aux victimes, aux secouristes et/ou aux autorités et de les inclure dans l'évaluation de la situation. Après le séisme de 2011 au Japon par exemple, plus de 150 applications ont été développées [18] pour faire face aux conséquences de la catastrophe. La plupart de ces applications reposent sur le crowdsourcing [17, 13, 5, 3, 10] pour fournir des informations sur la situation, les risques, les besoins, la localisation des ressources et des personnes, etc. Cependant, toutes reposent sur les infrastructures classiques pour leurs communications.
Or, quand la catastrophe détruit les stations de bases du réseau de téléphonie mobile ou provoque un défaut d'alimentation électrique, leur rétablissement ou le déploiement d'infrastructures réseau de secours (stations radio mobiles, ballons [11]...), est coûteux et peut prendre de quelques heures à plusieurs jours. Leur utilisation est, de plus, souvent restreinte aux secouristes.
Dans ces conditions, la seule solution viable, exploitable dès les premiers instants et intéropérable, consiste à construire un réseau *ad hoc*, ne reposant sur aucune infrastructure dédiée, à

partir du matériel existant, mobile : les terminaux des personnes présentes sur la zone sinistrée, équipés d'interfaces sans-fil (Wi-Fi et/ou Bluetooth), et communiquant en pair-à-pair.
Afin de résister aux défaillances et coupures du réseau, d'autres projets proposent donc de décentraliser les communications, comme Twimight [6], (« Twitter in disaster mode ») FireChat[4] ou le projet Serval [16] qui reposent sur le pair-à-pair pour fournir des communications pour les situations de crise, mais aussi plus généralement pour les régions ou situations où la couverture réseau est insuffisante ou défaillante.
Nous présentons ici une architecture de collecte de données en situation de crise, qui exploite des communications *ad hoc* dynamiques pour s'affranchir des infrastructures fixes.
Nous avons implémenté notre solution sur le simulateur ONE, avec notre modèle de mobilité *Danger Movement* [2] et en adaptant deux protocoles de routage DTN bien connus pour acheminer les informations : Epidemic et Spray and Wait. Nous avons ensuité testé le système avec les deux protocoles et en variant différents paramètres. L'évaluation des performances en simulation confirme l'efficacité et la faisabilité de notre approche.

2. Disruption-Tolerant Networking

Les DTN sont des réseaux opportunistes dans lesquels chaque nœud est un routeur pour les paquets du réseau. Les nœuds considérés peuvent être des terminaux mobiles de piétons, des équipements spécialisés embarqués dans des véhicules, des relais fixes, etc.
De nombreux protocoles ont été développés pour les DTN, et évalués sur différentes architectures. Des protocoles simples comme First Contact, Epidemic ou Spray and Wait, ne s'appuient sur aucune hypothèse ni aucune mesure de la structure du réseau. Ils sont souvent utilisés comme référence dans les études comparatives, quel que soit le contexte.
Epidemic [19] est l'un des protocoles de routage sur DTN les plus simples : chaque fois que deux nœuds se rencontrent, ils comparent leurs historiques respectifs de messages émis et reçus et échangent leurs « nouveaux » messages. Une politique FIFO est utilisée pour supprimer des messages lorsque le buffer est plein.
Spray and Wait [15] (SnW) limite la réplication. L'expéditeur d'un message le réplique en L copies, d'abord diffusées à $L-1$ autres nœuds (spray), puis chaque copie reste en attente (wait) que son hôte rencontre son destinataire. Plusieurs variantes de la phase *spray* sont possibles ; nous avons choisi d'utiliser Binary Spray and Wait, qui présente de meilleurs délais de délivrance que la version originale : tout nœud disposant de $n > 1$ copies, lorsqu'il rencontre un autre nœud qui n'en a pas, en transmet $\lfloor \frac{n}{2} \rfloor$ et en garde $\lceil \frac{n}{2} \rceil$. Spray and Wait présente ainsi un nombre de transmissions bien inférieur à Epidemic.
D'autres protocoles plus complexes, comme Spray and Focus [14], PRoPHET [8], ou MaxProp [1], s'appuient sur l'historique des rencontres ou sur des caractéristiques de la mobilité pour estimer les probabilités de rencontre futures des nœuds.
Ces protocoles supposent une certaine redondance des contacts, irréaliste dans notre scénario, et sont souvent évalués et comparés sur des échanges de données volumineuses, contrairement à notre scénario qui suppose la transmission de petits messages de géolocalisation.

3. Architecture après-crise

Notre architecture vise à collecter dans des centres de collecte des informations de localisation, ainsi qu'à informer les personnes présentes de l'emplacement des zones atteintes. En se déplaçant vers les points de convergence, les personnes, porteuses de terminaux mobiles qui s'échangent mutuellement des données à chaque contact, contribuent à la construction du réseau et à la

propagation de l'information. Notre solution est déployée sous forme d'une application spécifique préalablement installée sur les terminaux mobiles des personnes sur la zone. On appellera « porteur » une personne présente sur la zone touchée qui porte un terminal mobile exécutant l'application. Un porteur peut être une personne immobile, comme une victime blessée ou décédée, voire par extension un terminal actif abandonné.
L'objectif est de construire un système de géolocalisation qui soit **accessible** et **utilisable** par n'importe quelle personne disposant d'un terminal. De plus, le système doit offrir un **routage *ad hoc***, reposant sur les terminaux des porteurs, pour être **opérationnel** dés les premiers instants sans dépendre d'équipements additionnels autres que les centres de collecte.
Les données collectées sont centralisées vers des centres de collectes (hotspots) et comprennent principalement les coordonnées des terminaux (donc de leurs porteurs) sur la zone. Les données sont versionnées afin de ne prendre en compte que la localisation connue la plus récente.

Environnement et hypothèses : Nous supposons l'existence de lieux fixes, connus de tous et vers lesquels se déplacent les populations, nommés *points de convergence* (PC). Normalement, chaque porteur choisit, dès lors qu'il est conscient de la situation, le PC le plus proche de sa position courante. Un porteur peut cependant choisir (avec une certaine probabilité) d'en choisir un autre, tiré aléatoirement. Ceci permet de modéliser des comportements plus « humains », comme le réflexe des parents de récupérer leurs enfants à l'école au lieu de se rendre à une gare ou au centre de secours.
Les porteurs peuvent être bloqués en chemin par des *accidents*.
Certains des points de convergence sont aussi des *centres de collecte* ou « hotspots », dottés de capacités de stockage, de traitement et d'énergie suffisantes. Les hotspots sont supposés interconnectés par des liaisons sans fil résilientes à longue portée (laser, parabole, satellite. . .). Ils peuvent ainsi régulièrement s'échanger les données collectées. On notera que cette hypothèse n'entre pas en contradiction avec notre objectif de fournir une solution de crise ne reposant sur aucune infrastructure : ces communications spécifiques ne sont utilisées que pour synchroniser les hotspots, non pour connecter les terminaux ou acheminer les données vers les hotspots. Dans le cas où cette synchronisation serait défaillante ou inexistante, le système fonctionnerait tout de même, avec une information partielle sur chaque hotspot.
Terminaux et hotspots sont supposés disposer d'interfaces Wi-Fi et/ou Bluetooth, largement répandues. Une interface Wi-Fi bénéficie d'une portée de signal plus élevée, mais Bluetooth présente une consommation énergétique bien plus faible. Chacune de ces interfaces est gérée par un routeur DTN. Un identifiant unique (numéro de téléphone p.ex.) est assigné à chaque terminal, supposé équipé aussi d'un récepteur GPS.

Protocoles et messages : Trois types de messages – d'au plus 20 octets chacun – sont utilisés par notre système. Les messages de *géolocalisation*, générés par chaque porteur, contiennent ses coordonnées, et éventuellement un indicateur d'état (OK, blessé, etc.), destinés aux hotspots. Les *coordonnées d'accident*, sont émises par le porteur qui l'a découvert. Les *alertes*, enfin, rendent tout récepteur *alerté*.
Afin de ne conserver que les informations les plus récentes, les messages sont estampillés à la création. Pour éviter la surcharge inutile qu'induirait l'envoi de nombreux petits messages, ceux-ci sont agrégés en trames d'une taille maximale fixée (MTU). Enfin, un délai de retransmission de 300 s est appliqué aux versions plus récentes d'un message déjà envoyé, afin d'éviter l'envoi de mises-à-jour en flot continu.
Nous avons adapté les protocoles Epidemic et Binary Spray and Wait à ces contraintes spéci-

Tableau 1 – Paramètres de simulation – scenario de référence

Carte	Santiago Center, 29 km^2	Nœuds/victimes	1800/200
Temps simulé	10000s	PC	3 | 5 | 20
Accidents	10, MTBA : 500 s	dont hotspots	3
Pwalk	.14	Vitesse	constante : 1,3 $m\,s^{-1}$ (~4,7 $km\,h^{-1}$)
PpreWarned	.8		
PselfWarn	10^{-6}	Choix PC	plus proche
Interface (portée)	Wi-Fi (100 m)	Débit	250 koctets s^{-1}
	BlueTooth (10 m)	MTU	1500 octets
Protocole	Epidemic | Spray and Wait	Param. SnW	binaire, 8 copies

fiques : un message – et toutes ses copies dans le cas de Spray and Wait – est automatiquement supprimé dès réception d'une version plus récente. On notera que les messages d'alerte et d'accidents doivent être diffusés à tous les porteurs, de manière épidémique, et ne sont donc pas concernés par le choix de protocole.

Les données collectées sont ainsi acheminées vers les hotspots, qui se synchronisent à leur tour, ne gardant que les informations les plus récentes.

4. Évaluation des performances

Des tests ont été réalisés sur le simulateur ONE [7], sur une carte du centre de Santiago ($29km^2$). Les PC sont placés dans des bâtiments publics, et les hotspots choisis parmi les hôpitaux. Nous décrivons d'abord les métriques utilisées pour évaluer notre architecture, puis les paramètres de notre scénario de test, avant de présenter et discuter les résultats obtenus.

Métriques d'évaluation : Les métriques couramment employées pour l'évaluation de protocoles de routage mesurent principalement leur capacité à délivrer les messages – *Packet Delivery Fraction* (PDF), *throughput* ou *end-to-end delay* [12] – et la consommation énergétique induite – *normalized routing load* (NRL) [9] ou *energy cost per message*.

Dans notre scénario, une grande partie des messages est rendue obsolète et supprimée automatiquement. Ceci rend la mesure d'un taux de délivrance peu pertinente et la surcharge difficile à mesurer. Les propriétés du système qui nous intéressent sont sa capacité à recueillir la géolocalisation du plus grand nombre de personnes, avec la plus faible consommation possible. Nous avons donc défini des métriques spécifiques. D'abord les fractions de nœuds – rescapés mobiles et victimes immobiles – connus (%) par au moins un hotspots, mesurées séparemment pour évaluer en particulier les performances de collecte sur les nœuds immobilisés, cibles prioritaires de la localisation après-crise. La mesure du nombre moyen de trames envoyées par un nœud, à chaque instant, donne ensuite une première évaluation de la consommation énergétique globale du système.

Banc de test : Pour chaque ensemble de paramètres, 10 simulations ont été effectuées. Les courbes présentées représentent les valeurs moyennes.

Le tableau 1 résume les paramètres de notre scénario de référence. Notez que le nombre de PC peut varier entre les scénarios (3, 5 ou 20) mais le nombre de hotspots est toujours fixé à 3.

Résultats d'évaluation : Ce scénario de référence est décliné en plusieurs jeux de paramètres, afin d'évaluer dans un premier temps l'impact du type d'interface, du protocole de routage et du nombre de PC.

Performances de collecte : On peut tout d'abord observer que tous les scénarios se stabilisent avant $1h30$, et qu'on atteint dans le meilleur cas presque ~100 % de nœuds mobiles et ~96 % immobiles connus, soit seulement une douzaine de porteurs non localisés.

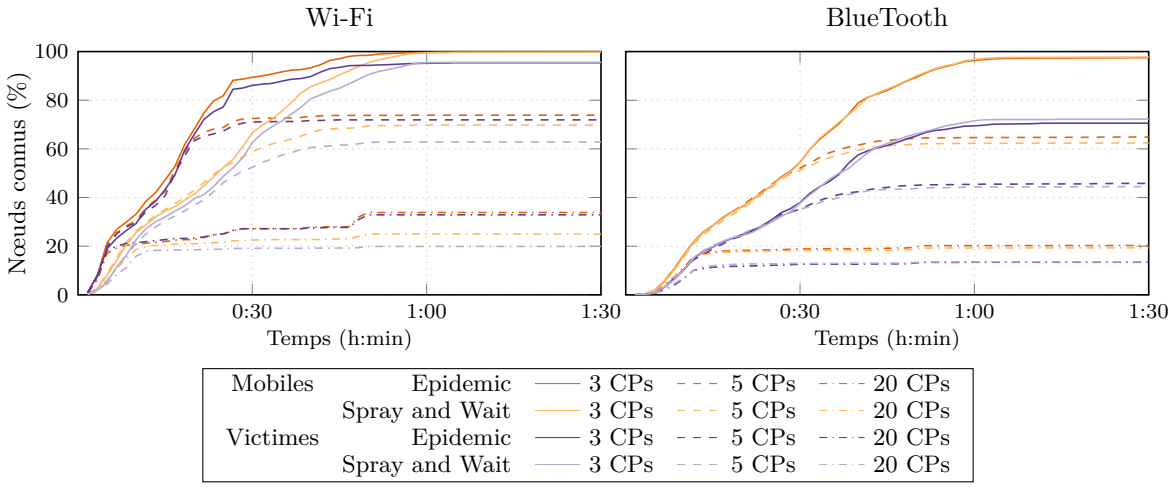

FIGURE 1 – Scénario de référence : Epidemic vs. Spray and Wait – fraction de nœuds connus

TABLEAU 2 – Nombre moyen de messages envoyés par porteur

	Référence				V. Speed		Random CP	
	Wi-Fi (WF)		BlueTooth (BT)		WF	BT	WF	BT
# of CPs	Epi	SnW	Epi	SnW	SnW	Epi	SnW	Epi
3	684.4	126.0	26.0	15.8	139.3	86.1	120.9	59.7
5	150.6	93.7	13.4	12.1	102.4	43.1	96.9	71.3
20	123.3	46.2	6.3	5.9	47.9	11.9	58.3	48.2

Seuls 3 points de convergence (PC) étant des hotspots, l'ajout de PC supplémentaires provoque une dispersion des porteurs parmi les PC, réduisant leurs chances de les atteindre les hotspots ou de leur transmettre leur position. En conséquence, les performances en terme de nœuds connus baissent de manière significative avec le nombre de points de convergence.

Comme on pouvait s'y attendre, les interfaces Wi-Fi donnent de meilleurs résultats que Bluetooth, et les nœuds statiques sont de loin les plus touchés par cette perte de performance. La portée du Wi-Fi étant plus grande, les terminaux ont de plus grandes chances de transmettre leur position, en particulier à un nœud en déplacement vers un hotspot. Les interfaces Wi-Fi donnent ainsi de meilleurs résultats en terme de nombre de nœuds connus, et l'écart se creuse avec le nombre de points de convergence. La faible portée du Bluetooth limite fortement la détection des victimes isolées, éloignées des grands axes de déplacement.

Les deux protocoles Epidemic et Spray and Wait (SnW) donnent des résultats similaires sur Bluetooth, mais Epidemic se montre légèrement meilleur que SnW sur Wi-Fi. Epidemic semble aussi plus résistant à la dispersion des porteurs due aux points de convergence suplémentaires. Cette dégradation des performances en Spray and Wait s'explique facilement par les contraintes de Spray and Wait : des « bons relais » peuvent être manqués par manque de copies, et sa phase *Wait* limite la transmission, ralentissant la convergence.

Consommation énergétique : D'après le tableau 2, Bluetooth est clairement meilleur sur ce point, avec moins de 30 trames par porteur dans tous les cas : la transmission est limitée par la portée plus que par le protocole. Wi-Fi présente une consommation 20 fois plus importante, en particulier avec Epidemic.

SnW peut donc réduire significativement la consommation sur une interface Wi-Fi, avec une perte de performances relativement acceptable. Sur Bluetooth par contre, si tant est que son usage puisse être considéré malgré ses faibles performances sur les nœuds immobiles, l'utilisation

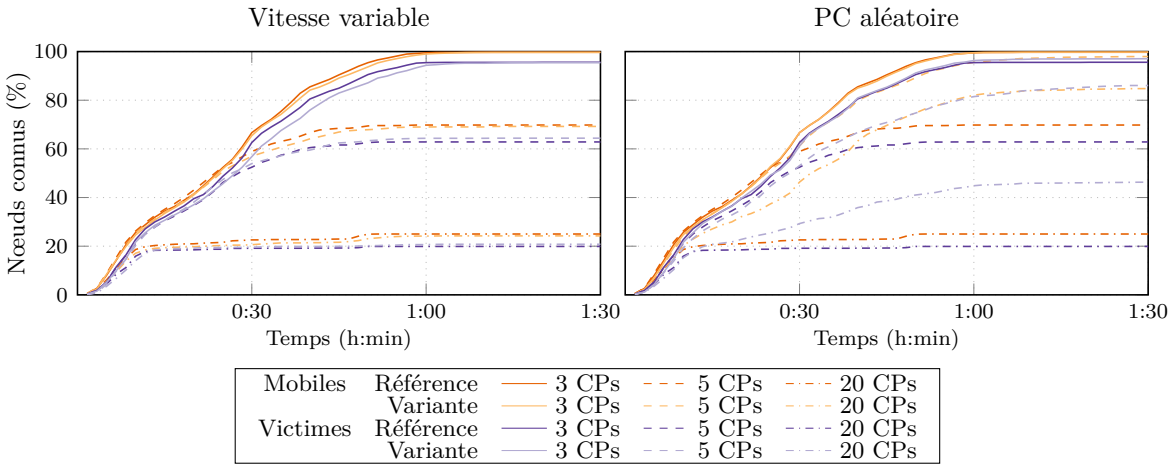

FIGURE 2 – Vitesse variable et choix de PC aléatoire (Wi-Fi/SnW) – fraction de nœuds connus

de SnW présente peu d'intérêt. Nous nous concentrons donc sur la combinaison Wi-Fi / SnW.

Mobilité – vitesse variable et choix du PC : À partir du scénario de référence, nous avons modifié, pour les simulations suivantes, les valeurs de différents paramètres de mobilité, pour évaluer leur impact sur le système. Les premières expériences concernent la vitesse de déplacement des porteurs, constante à $1{,}3\,\mathrm{m\,s^{-1}}$ dans le scénario de référence, que nous tirons ici aléatoirement entre $0{,}7\,\mathrm{m\,s^{-1}}$ et $2{,}0\,\mathrm{m\,s^{-1}}$. Nous avons ensuite effectué des simulations avec une vitesse constante, mais en permettant aux porteurs, avec une probabilité de 50%, de choisir leur destination aléatoirement parmi les PC, au lieu de choisir systématiquement le plus proche.

Les résultats sont présentés en figure 2 et dans les dernières sections du tableau 2. À l'exception de quelques variations non significatives, la variabilité de la vitesse n'a aucune influence sur les performances de collecte. En revanche, les variations de vitesse ont un impact sur les contacts entre porteurs, provoquant des connexions et déconnexions plus fréquentes, ce qui augmente le nombre de trames transmises.

Au contraire, permettre à une partie des porteurs de choisir son PC améliore considérablement les performances dès qu'il existe des PC non-communiquants (5 et 20 PC). On obtient ainsi jusqu'à 60% de nœuds mobiles ou 25% de nœuds immobiles connus supplémentaires. Cette amélioration est due aux porteurs « divergents » qui, en se déplaçant à travers la carte, diffusent l'information parmi des porteurs se dirigeant vers des PC différents – et en particulier à des hotspots – au lieu de rester cantonnés à la zone de son PC par défaut. Cette diffusion contribue largement à compenser la dispersion des porteurs vers les PC non-communiquants.

5. Conclusion

Nous avons présenté dans cet article notre système *ad hoc* de géolocalisation après-crise. Notre étude s'est concentrée sur les performances de collecte des données sur les personnes mobiles et en particulier immobiles, ainsi que sur la consommation énergétique. À partir d'un scénario de référence, implémenté sur le simulateur ONE, puis décliné en plusieurs variantes, nous avons évalué l'effet de différents paramètres sur l'efficacité du système.

Afin d'optimiser les décisions de transmission, l'étude des caractéristiques du graphe dynamique induit par les contacts semble être une bonne piste. Le scénario pourrait ainsi être enrichi avec des porteurs présentant des mobilités différentes, comme des véhicules, plus rapides, ou des secouristes avec des comportement spécifiques, etc.

Références

[1] John Burgess et al. « MaxProp : Routing for Vehicle-Based Disruption-Tolerant Networks ». In : *Proc. of IEEE INFOCOM*. 2006.

[2] Florent Coriat et al. « Crowdsourcing-based architecture for post-disaster geolocation : A comparative performance evaluation ». In : *2016 IEEE 15th International Symposium on Network Computing and Applications (NCA)*. The 15th IEEE International Symposium on Network Computing and Applications (NCA 2016). Cambridge, Boston, MA, USA, 31 oct. 2016, p. 1–9. doi : 10.1109/NCA.2016.7778583. url : http://hal.upmc.fr/hal-01416297/document (visité le 28/03/2017).

[3] *Disaster Alert Network - ubAlert*. url : https://www.ubalert.com/ (visité le 20/06/2014).

[4] *FireChat*. url : http://opengarden.com/ (visité le 22/03/2016).

[5] *Google Crisis Response*. url : https://www.google.org/crisisresponse/about/ (visité le 08/03/2016).

[6] Theus Hossmann et al. « Twitter in disaster mode : Opportunistic communication and distribution of sensor data in emergencies ». In : *Proceedings of the 3rd ACM Extreme Conference on Communication : The Amazon Expedition*. 2011, p. 1.

[7] Ari Keränen, Jörg Ott et Teemu Kärkkäinen. « The ONE Simulator for DTN Protocol Evaluation ». In : *Proceedings of the 2nd International Conference on Simulation Tools and Techniques*. 2009.

[8] Anders Lindgren, Avri Doria et Olov Schelen. « Probabilistic Routing in Intermittently Connected Networks ». In : *SIGMOBILE Mobile Computing and Communication Review*. 2004, p. 2003.

[9] Abraham Martín-Campillo et al. « Evaluating opportunistic networks in disaster scenarios ». In : 36.2 (2013), p. 870–880.

[10] Glenn Pearson et al. « The Role of Location for Family Reunification During Disasters ». In : *Proceedings of the First ACM SIGSPATIAL International Workshop on Use of GIS in Public Health*. New York, NY, USA, 2012, p. 11–18.

[11] *Project Loon*. url : https://www.google.com/loon/ (visité le 08/03/2016).

[12] D.G. Reina et al. « Evaluation of Ad Hoc Networks in Disaster Scenarios. » In : *the Third International Conference on Intelligent Networking and Collaborative Systems*. 2011, p. 759–764.

[13] *SahanaEden*. 2004. url : http://eden.sahanafoundation.org/ (visité le 28/10/2014).

[14] Thrasyvoulos Spyropoulos, K. Psounis et C.S. Raghavendra. « Spray and Focus : Efficient Mobility-Assisted Routing for Heterogeneous and Correlated Mobility ». In : *Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops*. 2007, p. 79–85.

[15] Thrasyvoulos Spyropoulos, Konstantinos Psounis et Cauligi S. Raghavendra. « Spray and Wait : An Efficient Routing Scheme for Intermittently Connected Mobile Networks ». In : *Proceedings of the ACM SIGCOMM Workshop on Delay-tolerant Networking*. 2005, p. 252–259.

[16] *The Serval Project*. url : http://www.servalproject.org/ (visité le 08/03/2016).

[17] *Ushahidi*. url : http://www.ushahidi.com (visité le 08/03/2016).

[18] Arifumi Utani, Teruhiro Mizumoto et Takashi Okumura. « How Geeks Responded to a Catastrophic Disaster of a High-tech Country : Rapid Development of Counter-disaster Systems for the Great East Japan Earthquake of March 2011 ». In : *Proceedings of the ACM Special Workshop on Internet and Disasters*. 2011, 9 :1–9 :8.

[19] Amin Vahdat et David Becker. *Epidemic Routing for Partially-Connected Ad Hoc Networks*. 2000.