Crowdsourcing-based architecture for post-disaster geolocation: A comparative performance evaluation

Florent Coriat, Anne Fladenmuller, Luciana Arantes, Olivier Marin

Crowdsourcing-based architecture for post-disaster Geolocation: a comparative performance evaluation

Florent Coriat*†, Anne Fladenmuller*†, Luciana Arantes*†,‡ and Olivier Marin§
* Sorbonne Universités, UPMC Univ Paris 06, UMR 7606, LIP6, F-75005, Paris, France
E-mail: [florent.coriat, anne.fladenmuller, luciana.arantes]@lip6.fr, ogm2@nyu.edu
† CNRS, UMR 7606, LIP6, F-75005, Paris, France
‡ Inria, REGAL project-team, Paris-Rocquencourt, France
§ New York University Shanghai (NYU Shanghai), Shanghai, China

***Abstract*—In the aftermath of a natural or industrial disaster, locating individuals is crucial. However, disasters can cause extensive damage to the network infrastructures and a generalized loss of communication among survivors. In this article, we present a network support solution that provides a post-disaster geolocation-collecting service that relies on inter mobile device connections. On top of this dynamically built network, survivors' mobile devices exchange information about geolocation of others they have encountered. Such information is routed towards predefined data collection centers using either the DTN Epidemic or Spray and Wait DTN protocol. Experiments were conducted on the ONE simulator and performance evaluation results confirm the effectiveness of our proposal.**

***Index Terms*—geolocation, DTN, early post-disaster management, mobile devices**

I. Introduction

After a natural or human-made disaster, regular communication infrastructure is often damaged and/or overloaded by witnesses, survivors, or their relatives who keep repeatedly trying to get information about the current situation, in order to help or simply to reassure themselves. Yet global information assessment is a crucial issue for rescuers. Thus, establishing, as soon as possible, a dedicated communication network, until the regular network works normally, remains a top priority and a great challenge [1]. Ideally, such a communication network should also provide support for real-time mapping of the disaster area, danger zones and resources, as well as geolocation information of victims and survivors. In other words, the support must help to assess and deal with the emergency situation, mapping accident areas, locating users, warning users about the accidents, and maintaining contact between survivors, rescue teams, and emergency operation centers.

Many existing solutions deploy emergency network infrastructures (e.g. mobile cell sites, balloons, etc.). However, these solutions are often expensive, can take several hours after the disaster to be operational, depend on dedicated equipments, or are frequently restricted to rescue teams.

Hence, considering the above constraints, a feasible, relatively cheap, and easily available solution would be to build an ad-hoc network composed of people's (victims and survivors) mobile devices, i.e., to exploit existing mobile devices without counting on additional dedicated network infrastructure. Since users' mobile devices usually have wireless interfaces (Wi-Fi and/or BlueTooth), it would be possible to establish, maybe intermittently, ad-hoc communication links between mobile nodes, similarly to MANET (mobile ad-hoc network) or DTN (disrupted-tolerant network).

In this paper, we present a post-disaster network support solution that exploits such an ad-hoc dynamically built communication approach, requiring a minimum of fixed support. We consider that dedicated software for disaster situations runs on peoples' mobile devices as well as the existence of well-known places, denoted convergence points *CPs* (e.g., hospitals, railway stations, schools, etc.). Some of these CPs are also collecting data centers, denoted *hotspots*. The latter are endowed with processing and storage resources. Seeking to be in safe area when a disaster takes place, people move towards one of the *CPs*, establishing the ad-hoc communication links between his/her mobile device and those of the persons he/she crosses along the path to the *CP*. Furthermore, whenever a communication link exists between two persons' devices, they can exchange information about geolocation of other persons they have met. Therefore, users mobility contributes to both build an ad-hoc network and propagate information about users location. Through such a network, users can also be informed about accidents which might help them to find a better path to the most convenient *CP*.

Since a network composed of persons' mobile devices is intermittently connected, i.e. connections between them and the hotspots are built over time, similarly to DTNs, we applied (and adapted) two well-known DTN routing protocols, *Epidemic* [2] and *Spray and Wait* [3], for routing geolocation data towards the hotspots. Based on such disaster context, we also propose a mobility model, denoted *Danger Movement*. Extensive experiments were conducted with both protocols on *Danger Movement*, varying different parameters, on top of the ONE[1] simulator [4]. Performance evaluation results confirm the effectiveness and feasibility of our approach.

The paper is organized as follows: Section II gives a brief background about DTNs and the protocols *Epidemic* and *Spray and Wait*. In Section III, we summarizes some existing related

[1]The Opportunistic Networking Environment

work. Our solution is described in Section IV which also includes the description of the *Danger Movement*. Section V presents and discuss some evaluation performance results with both protocols. Finally, Section VI concludes the paper and gives some directions for future work.

II. Disruption-tolerant Networking

Base radio stations are statically placed aiming at offering network coverage to users. However, if they have been damaged by a disaster or the latter caused a power failure, their re-establishment or the deployment of mobile cell sites to complete or replace the failing infrastructure can take from hours to several days, wasting valuable time for victims and rescuers. Thus, autonomous and fast operational solutions to offer some communication support in the first moments of a disaster are crucial in such a context. To this end, disruption-tolerant networking (DTN) technology has been largely considered for post-disaster communications.

A disruption-tolerant network (DTN) is an opportunistic network where each node acts as a router for the network packets. Nodes can be pedestrians' mobile devices, on-board vehicle specialized devices, fixed relays, etc. In [5], the authors present a classification of these types of nodes, their mobility patterns, and communication abilities (terminals, stationary relays, dedicated fixed or mobile routing facilities, etc.) from the perspective of post-disaster communication and coverage.

Devices like mobile cell stations, satellite relays, etc. can be components of a DTN. However, the main purpose of DTNs is to exploit non specialized, not expensive devices, usually with limited resources, but which are fast deployed and, thus, very suitable for disaster context.

DTN routing: Many protocols have been developed for DTNs and evaluated on different network architectures. "Simple" protocols like First Contact, Epidemic, or Spray and Wait do not rely on any assumption or network structure measures for their routing rules. They are often used as references in comparative studies, regardless of the study context.

Epidemic [2] is one of the most simple DTN routing protocols: whenever two nodes meet, they compare their respective sent and received message histories and exchange their "new" messages. The advantage of the *Epidemic* protocol is its high delivery probability. On the other hand, it consumes a lot of storage, power, and bandwidth resources. To circumvent such a problem, a FIFO policy is usually used to discard messages when the node's storage buffer is full. Hence, dissemination is limited by both bandwidth and storage and, in the long term, by available remaining energy.

Spray and Wait (SnW) [3] is a simple trade-off between replication-based routing protocols, like *Epidemic*, and forward-based routing ones. The source of a message replicates it in L copies. The latter are firstly disseminated to $L-1$ other nodes. This *spray phase* accepts some variants. For instance, in *Binary SnW*, any node that has $n > 1$ message copies (source or relay), and encounters a second node (with no copies), gives to it $\lfloor \frac{n}{2} \rfloor$ and keeps $\lceil \frac{n}{2} \rceil$ for itself. *Binary SnW* has a lower delivery delay than the original *Spray and Wait*. Whenever a node has only one copy left, it switches to *wait phase*: it stores the message until it crosses the destination node to directly transmit the message. In other words, the *Spray and Wait* protocol manages the number of copies messages in the spray phase and uses Direct Delivery in the wait phase. As a result, the protocol presents fewer message transmissions than the *Epidemic* protocol.

Other protocols more "complex" than the previous ones, such as Spray and Focus [6], PRoPHET [7], MaxProp [8], rely on history of nodes' crossing or specific characteristics of a mobility model (Time To Return) which predicts future nodes meeting probabilities. These protocols assume a somewhat redundant contact approach. In particular, a node S can efficiently route a message to a node D if and only if S *knows* D, i.e., if a packet (whichever it is a data or protocol packet) already followed a path from D to S, provided that this path still exists or at least part of it. However, these protocols perform at best as efficiently as the "simple" ones when this condition is not met. As we shall see later, geolocation messages of our protocols mainly follow such unknown paths.

We should also point out that DTN protocols are usually evaluated and compared under various scenarios and/or large randomly-generated data transfers. On the contrary, our scenarios rely on small geolocation messages, whose generation depends on each specific scenario.

III. Related Work

In the context of disasters, we summarize in this section some existing solutions that provide support for diffusion of information and/or communication coverage as well as some mobility models proposed in some works.

A. Existing Solution for Support

Rescue workers typically use a dedicated trunked network infrastructure, based on a specific protocol like P25 or TETRA [9]. These protocols provide support for encrypted voice and data transmission throughout a fixed mesh infrastructure, or using direct (point-to-point) communications. However, these networks are restricted to licensed professionals, and their design would not scale to a large use. Furthermore, P25 and TETRA do not provide multi-hop routing when using point-to-point communications, thus preventing their use for data collection without a resilient infrastructure.

Some hardware solutions have also been proposed with the goal of temporarily replacing or restoring part of the damaged infrastructure, In this case, mobile cell sites (e.g.,"Cell On Wheels", "Cell On Truck", etc.), can be deployed to address emergencies and usually connected through wired connections, parabolic antennas, a satellite network, or a network of helium-inflated balloons, as proposed by the Loon project [10] for restoring access to the internet. Nevertheless, these solutions remain expensive — tens of thousands of dollars per cell — and their post-disaster deployment requires time.

In recent years, different disasters led to the emergence of many projects whose goal is to inform people about

the disaster and to include them in the situation assessment process. For instance, after the earthquake in Japan in 2011, more than 150 applications were developed [11] to face the disaster consequences. Most of these applications rely on crowdsourcing, offering information about the current situation, risks, needs, resources, people locations, etc. to victims, rescuers, and/or authorities. Ushahidi [12], Sahana Eden [13], Google Crisis Response [14], UbAlert Disaster Alert Network [15] or People Locator [16] are examples of projects that make available collaborative maps on top of which the above information can be added. These applications consist of web sites or mobile applications. Even if some of them exploit alternative communications channels, like Ushahidi, which is able to collect information by SMS/MMS, they all rely on regular infrastructures as communication support.

Aiming at tolerating network failures and disruption, some other projects provide solutions that decentralize communication. Twimight [17] ("Twitter in disaster mode"), is a Twitter client that can work without internet connection, exchanging tweets in an opportunistic way between terminals. Firechat [18] is a messaging application that can communicate with or without internet connection: Wi-Fi and BlueTooth interfaces are responsible for building a mesh network where each message can be stored, carried and forwarded on any available link. The Serval project [19] developed a yet experimental messaging application that can transmit all sorts of data (messages, maps, voice, pictures, etc.) over an ad-hoc mesh network. These projects are not specially tailored to tackle with disaster situations but they are general solutions for regions or situations where network coverage is not working properly.

B. Mobility Models

The use of MANET or DTN to deal with a crisis situation has already been proposed [20], [21]. Several studies have compared known protocols in a crisis scenario [5], [22]–[26], or the in everyday life [7], [27], [28]), and have shown the impact of mobility on system performance.

Despite its lack of realism [29], RWP is often used for simple [26] or non-crisis-specific [30] evaluations or even as a reference or a sub-model of a more specific model. In [5], the authors compare a set of DTN routing protocols in the scenario of Uttarakhand floods (India, 2013, 4 days of intense rainfall, 4200 affected villages, 5700 deaths). The impact of RWP, Map Based [4], Cluster Movement and Post Disaster Mobility (PDM) [31] mobility models is evaluated on top of the ONE simulator. Among those, the last two ones also use RWP and Map Based as sub-models. For instance, PDM assigns different roles to nodes, with different mobility patterns: patrol, exploration, round-trip. Some of these patterns are based on RWP. PDM is also used in the experiment scenario in [32], which addresses mobility prediction in a crisis situation.

The Disaster Area (DA) model is used in [25] and [33] to evaluate DTN routing or broadcast protocols. The DA model introduces the concept of zones which are deployed by rescuers. Pedestrians follow a zone-restrained RWP mobility model with obstacles, whereas vehicles go back and forth between two zones.

There exist several other models in the literature which were conceived for disaster situations such as CORPS [34], Dispatched Ambulance [35], Reference Point Group Mobility (RPGM) [36], Human Behaviour for Disaster Areas (HBDA) [37], etc. However, all these models focus on rescue teams mobility, neglecting the movement of other people present in the disaster scenario [38]. In other words, victims and survivors are poorly represented, if not simply ignored, or follow a simplistic generic model (e.g., RWP or similar).

IV. Our Proposed Post-disaster System

In this section, we present our post-disaster system that aims at gathering geolocation and mapping information in collecting centers (*hotspots*) as well as informing users about accident locations. Moving to convergence points *CPs*, which can also be a hotspot, persons' mobile devices that get into contact with others, exchange information about geolocation of other persons they have met. Users mobility contributes then to both build a connected network and propagate information.

Our solution is deployed as a specific application, installed on people's mobile devices beforehand. We denote *holder* a person that holds a mobile device running this application and is within the disaster area. Note that a *holder* can be also a motionless victim, such as injured or dead victims as well as active dropped mobile devices.

Our goal is to provide a post-disaster geolocation system with the following features:

- *Public availability:* the network built by holders' devices must be available and usable by everyone that has a mobile device (smartphones, tablets, etc.).
- *Fast operational capacity / ad hoc routing:* exploiting the holders' mobile devices, the network must be fully operational without considering, except hotspots, any additional fixed support. In other words, no specific devices and support should be used for routing messages, which would, then, require the assumption that holders' devices handle them.
- *Collection of data:* data should be routed to central points (hotspots).
- *Freshness of information:* collected data mainly consist of geolocation of persons' mobile devices in the area. However, only recent information about their respective location should be considered, which means that those messages with old information must be discarded.
- *Informing users about accident locations*: holders should, as much as possible, be informed about where there are accidents in order to allow them to change their path and circumvent risking zones.

In the following, we firstly describe the environment and assumptions that we consider for our system. Then, since the majority of existing mobility models of the literature concern rescue teams (see Section III), we propose a new mobility model, denoted *Danger Movement*, that takes into account the considered environment and the movement of persons towards

CPs. Finally, in this context, we propose to use (and adapt) both *Epidemic* and *Binary Spray and Wait* DTN protocols in order to route persons information to hotspots and disseminate accidents geolocation information.

A. Environment and Assumptions

We consider that there exist fixed places, denoted convergence points *CPs*, like hospitals, railway stations, schools, etc., which are known by all people and towards which they move when a disaster takes place. By default, every user chooses the closest *CP* in relation to his/her position when aware of the disaster. Nonetheless, a person can choose (with a certain probability) to reach another one, randomly chosen. Such an option improves the realism of the model, enriching it with "human" behaviors as, for example, parents fetching their children from school (a *CP*) instead of directly reaching the nearest rescue center.

Holders trying to reach a *CP* can be blocked by accidents. An *accident* is an event that permanently blocks an intersection of roads. Accidents are triggered on randomly chosen intersections following an exponential law with a chosen mean time between two accidents (MTBA).

Some *CPs* are endowed with storage, processing, and energy resources which render them collecting centers, denoted *hotspots*. The latter are interconnected by long-range resilient wireless links (laser, parabolic antenna, satellite, etc.). Periodically, hotspots synchronize themselves, exchanging collected data. Notice that this resilient communication infrastructure is not contradictory with our aim of providing a post-disaster solution which does not rely on a dedicated infrastructure. In our case, the latter is only used for synchronization between hotspots and not for connecting people or routing geolocation information to hotspots. If such a hotspot synchronization does not take place, the system still works with each hotspot having a partial view of people geolocations.

We also assume that both holder's devices and hotspots have Wi-Fi and/or Bluetooth wireless interfaces, which are widely available among the devices of holders nowadays. While, Wi-Fi benefits from better signal ranges than BlueTooth, BlueTooth consumes significantly less energy than Wi-Fi. Each of these interfaces runs a DTN router. We consider that a unique constant identifier (e.g., phone number) is assigned to each holder's device which is also equipped with a global positioning system (GPS).

B. Mobility Model: Danger Movement

Danger Movement is a map-based mobility model which takes into account the context described in the previous section. Basically, it characterizes the movements of survivors who move towards *CPs*, exchanging information about people and accident locations, which are routed to hotspots. A preliminary version of the model was presented in [39].

In accordance with our assumptions, hotspots are placed on the map as static nodes. Initially, *Danger Movement* randomly places holders over the map. The latter can then walk over the map at fixed or random (bounded) speeds.

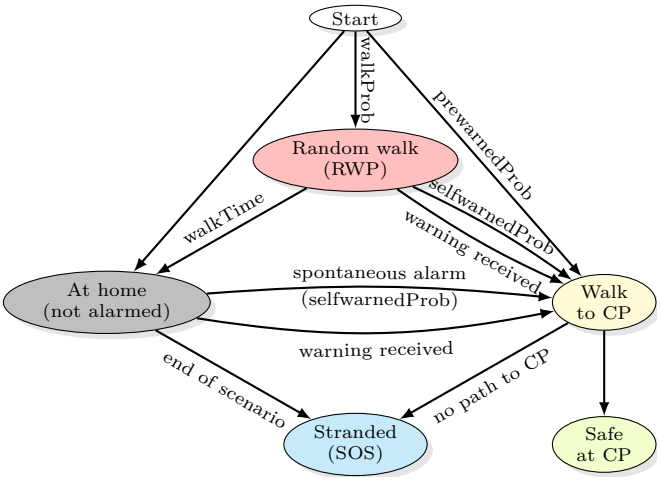

Fig. 1. Danger Movement : state (sub-models) diagram of a holder

Holders running *Danger Movement* may be aware or not of the crisis situation. We denote *alarmed* a holder aware of the situation. Four cases are possible for a holder in *Danger Movement*: (1) he/she is *alarmed* from the beginning; (2) he/she spontaneously realizes the situation during simulation; (3) the holder is warned by another *alarmed* holder; (4) the holder is never *alarmed*.

The map is known by all holders. Therefore, they are always able to find the shortest *off-disaster* path to any *CP*. However, holders have only knowledge of an accident provided they have seen it or another holder informed them of it. Upon having knowledge of a new accident, a holder may recompute his/her current path. Note that an alarmed holder may become *stranded* if there are no more accessible paths left towards his/her target *CP*.

Once arrived to the target *CP*, holders stop moving and, after transmitting all their data to the hotspot (if the *CP* is a hotspot), they disable their interfaces.

Figure 1 describes the different states of a holder, depending on its awareness and whether he/she is at home, walking outside or "stranded" by accidents. Notice that, in order to ensure that simulations based on *Danger Movement* finish, it is not required that all holders reach the safe state. Once a given defined percentage of holders are safe, all remaining holders become stranded ones.

The probabilities $prewarnedProb$ and $walkProb$ respectively concern the probability that a holder is *alarmed* from the beginning of the simulation (case 1) and that he/she starts walking without being *alarmed* (case 3). The $selfwarnedProb$ is the probability, every $1/10\,\mathrm{s}$, for a non-alarmed holder to become spontaneously *alarmed* (case 2).

C. Protocols and Messages

As explained, every holder's interface runs a DTN router. However, since all geolocation data should be directed to hotspots, applying "complex" DTN protocols would be unfeasible in such a disaster context. Furthermore, the size of the messages is very small and those with old information should

be dropped. Therefore, we have chosen to apply and adapt the simple and well-known DTN protocols *Epidemic* and *Spray and Wait* (see Section II).

Three message types are used by the protocols:

- *geolocation*: contains the GPS coordinates of a holder;
- *accident*: the GPS coordinates of an accident;
- *warning*: a special message which renders *alarmed* those holders who received the message.

Since every holder has a GPS receiver, it is able to build a *geolocation message* at any time.

Warning messages are automatically created by already *alarmed* holders while *accident* messages are generated by holders when getting knowledge about an accident. When they cross each other, holders may exchange *geolocation* information about the holders and accidents of which they are aware. Each of this information consists of a single message whose size does not exceed $20\,\mathrm{B}$. However, MANET/DTN routing protocols are usually evaluated with larger messages: from $64\,\mathrm{B}$ for MANETs to $100\,\mathrm{KiB}$ for DTNs. Thus, aiming at preventing holders from sending numerous small messages, which would induce high network overhead, messages are grouped into frames of a predefined maximum transmission unit (MTU) size before being transmitted.

In order to satisfy the *freshness of information* requirement, messages about persons' geolocation must be versioned, i.e., timestamped. In this way, only the most recent ones (last version) are collected and kept by holders and hotspots. A status can also be added to each *geolocation* message, giving more information about the holder (not injured, injured, motionless victim, etc.). Our solution should, thus, ensure a anycast routing service for versioned messages, dropping those with old version.

As argued, we have chosen to implement both the Epidemic and Spray and Wait DTN protocols (see Section V), adapting them to the described disaster environment. In the case of Spray and Wait, we adapted the Binary SnW, where every node (holder), keeping more than one copy of a message, transmits half of them on the next node (holder) contact.

The two protocols have been modified to deal with messages versions: a message is automatically dropped as soon as a more recent version is received. In the case of Spray and Wait protocol, this message dropping may concern several copies of the same message, independently of the number of copies received for the new version of the message. Lastly, a transmission delay is applied to more recent versions of an already sent message, preventing continuous update flow transmissions.

It is worth noting that *warning* and *accident* messages have to be disseminated among all holders, i.e., in an epidemic way, so that only geolocation data are affected by the protocol choice.

Collected data are forwarded to hotspots, which periodically synchronize themselve, keeping only last versioned data.

TABLE I
SIMULATION PARAMETERS – REFERENCE SCENARIO

Map	Santiago Center, $29\,\mathrm{km}^2$
Simulated time	10000s
Walk speed	constant : $1.3\,\mathrm{m\,s^{-1}}$ ($\sim 4.7\,\mathrm{km\,h^{-1}}$)
Accidents	10, MTBA : $500\,\mathrm{s}$
Number of CPs	3 | 5 | 20
of which hotspots	3
Survivors / victims	$1800/200$
walkProb	.14
preWarnedProb	.8
selfWarnedProb	10^{-6} at each $1/10\,\mathrm{s}$-step
CP choice	the nearest one
Interface (range)	Wi-Fi ($100\,\mathrm{m}$) | BlueTooth ($10\,\mathrm{m}$)
Bitrate	$250\,\mathrm{ko\,s^{-1}}$
MTU	$1500\,\mathrm{bytes}$
Retransmission delay	$300\,\mathrm{s}$
Protocol	Epidemic | Spray and Wait
Param. Spray and Wait	binary, 8 copies

V. PERFORMANCE EVALUATION

Experiments were conducted on the ONE simulator [4] using a map of the center of Santiago ($29km^2$). CPs are placed on real amenities, with hotspots chosen among hospitals. Both protocols, Epidemic and Spray and Wait (Binary SnW) have been evaluated. Firstly, we explain and define the metrics used to evaluate these protocols. Then we describe the parameters of the simulation testbed. Finally, some results are presented and discussed.

A. Metrics

In order to estimate the ability/efficiency of routing protocols to deliver messages, performance metrics such as packet delivery fraction (PDF), throughput or end-to-end delay [22] are commonly used, while protocol overhead is evaluated through metrics of normalized routing load (NRL) [25] or energy cost per message.

However, in a disaster scenario, it is important to deliver only up-to-date information, discarding obsolete messages before they can reach their final destination (a hotspot). Hence, usual performance metrics (e.g., throughput, PDF, NRL) become irrelevant or very difficult to evaluate. In our context, we aim at gathering as much geolocation information as possible while keeping low energy consumption. Consequently, to compare the efficiency of different routing protocols, we propose a new metric that better reflects the quantity of the accurate geolocation information gathered on hotspots. This efficiency metric is denote *fraction of discovered holders*, known by at least one hotspot. The overhead entails by the protocols is estimated by measuring the *average number of frames sent* by a holder over the time. Note that this second metric gives an overview of the global energy consumption of our protocol.

B. Simulation Testbed

For each parameters set, 10 simulation runs were executed. The curves of the figures show the average values for these runs.

Table I summarizes the parameters for our reference scenario. Note that the number of convergence points can vary

between scenarios (3, 5, or 20), but the number of hotspots is always fixed to 3.

C. Evaluation Results

We have conducted our simulations on different scenarios. The first one is used as a reference to evaluate the impact of the type of interfaces, routing protocols, and number of *CP*s on the efficiency and energy consumption metrics.

Reference scenario: Figure 2 and the first columns of Table II show results of the simulations, considering the parameter set of Table I.

Firstly, we observe that all simulations stabilize within 90 minutes or less and none of them ends with a complete knowledge of the position of all individuals: the best simulation results yield a knowledge of $\sim 99.5\,\%$ of the holders' positions, leaving only a dozen of holders unreachable.

Efficiency performance: Since only 3 CPs are hotspots which collect geolocation information, in scenarios with more CPs, device holders are statistically less likely to reach a hotspot. Consequently, performance in terms of number of discovered holders clearly drops as the number of CPs increases.

As expected, Wi-Fi interfaces produce better results than BlueTooth ones. The BlueTooth's best performance (BlueTooth / Epidemic) results stand out $\sim 5\,\%$ below Wi-Fi worst case (Wi-Fi / SnW). Since Wi-Fi propagation range is broader, Wi-Fi devices have a higher chance to forward their positions to a holder moving towards a hotspot. Hence, for similar scenarios (same number of CPs), Wi-Fi outperforms Bluetooth, with the difference on the number of detected holders growing with the number of CPs. The gap is of 5% when considering 3 CPs and up to 15% with 20 CPs.

Epidemic and SnW perform similarly on BlueTooth, but Epidemic gives slightly better results on Wi-Fi. The reason is that Epidemic seems to be more resilient to the dispersion of holders when the number of CPs increases: whereas both of them acquire $\sim 99.5\,\%$ knowledge about holder positions with 3 CPs, SnW misses $\sim 5\,\%$ more holders position information than Epidemic with 5 CPs, and $\sim 10\,\%$ with 20 CPs. Such degradation is easily explained by the bound in the number of copies of SnW: some relevant holder relays are *missed* by the protocol since there is no more copy left upon the encounter moment.

We also observe that Epidemic discovery convergence time takes place $10 \sim 15\,\mathrm{min}$ earlier than SnW one, regardless of the number of CPs, probably because SnW messages are stuck in the *wait* phase of the protocol until their respective holders reach a hotspot.

Energy consumption: Table II shows that BlueTooth clearly stands out with less than 30 frames sent per holder on average, regardless of the protocol: forwarding is limited by interfaces propagation range more than by the choice of the protocol.

However, with Wi-Fi broader propagation range, energy consumption becomes more significant: around 20 times more frames than BlueTooth (note the difference in scales between the 2 figures). It also impacts the choice of the protocol since SnW outperforms Epidemic by a factor of about three to five. Thus, SnW significantly reduces energy consumption when deploying Wi-Fi interfaces while keeping relatively acceptable decrease in performance (especially with few non-hotspots *CPs*). We could, therefore, consider SnW as a the best option when deploying with Wi-Fi interfaces.

Given the low consumption of Epidemic, choosing SnW seems rather useless With BlueTooth: both protocols can be used interchangeably, with slightly better results for Epidemic.

From the above discussions of the results, we can say that Wi-Fi / SnW and BlueTooth / Epidemic are interesting tradeoffs, which will, therefore, be taken as reference in the rest of this performance evaluation study.

Intermittent interfaces: In a crisis context, where energy networks may be inoperative, holders who cooperate to define a cartography of the crisis zone must take care about the consumption of their battery-powered devices. In this context, energy aware transmissions which rely on disabling the radio interface for a certain duration of time, seems quite suitable. Hence, it is important to study the impact of intermittent radio interfaces on the propagation of our geolocation information. To this end, we have defined an environment with *intermittent interfaces*: each interface is powered up and shut down periodically. On the other hand, as hotspots are not concerned by energy issues, they always keep their radio interface active.

Since synchronization to get all wireless interfaces active simultaneously is not realistic, we consider that holder devices operate independently from one another. Thus, for the current simulations, we have chosen an intermittency functioning which is based on one of the discovery protocols of Wi-Fi Direct[2].

To circumvent the risk of having devices which are never active at the same time, the intermittency has been implemented as a *pseudo-periodic* process: interfaces are up for $active = 30\,\mathrm{s}$, then down for a random amount of time between $minInactive = 30\,\mathrm{s}$ and $maxInactive = 90\,\mathrm{s}$, and so on. In this way, two holder's devices whose active time are originally mutually exclusive will eventually be able to communicate with each other.

Figure 3 and the second section of Table II present the intermittency results. With a Wi-Fi interface running SnW, intermittency has nearly no impact on the performance (number of discovered devices), whereas the average number of messages is reduced by $\sim 25\,\%$. Conversely, Bluetooth performance degrades due to these interruptions. The number of messages is virtually unchanged but performance efficiency drops. For example, with 3 hotspots, the number of missed holders doubles from $5\,\%$ to $10\,\%$.

Overall, we can conclude from the results that performance of both protocols are similar, though slightly reduced, and that intermittency might be useful with Wi-Fi.

[2]a Wi-Fi standard enabling devices to connect with each other without requiring an infrastructure.

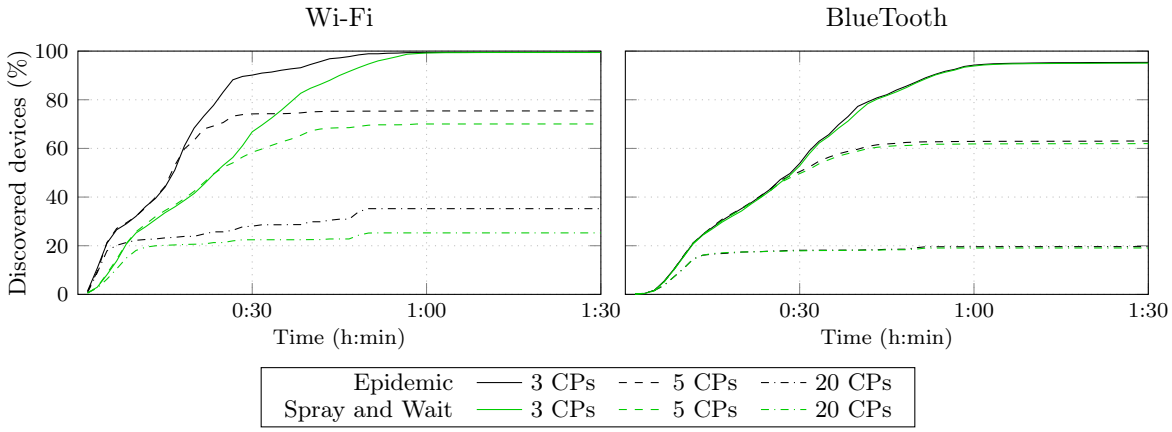

Fig. 2. Reference scenario: Epidemic vs. Spray and Wait – proportion of discovered devices

TABLE II
AVERAGE NUMBER OF SENT MESSAGES PER HOLDER

	Reference				Intermittent		V. Speed		Random CP	
	Wi-Fi (WF)		BlueTooth (BT)		WF	BT	WF	BT	WF	BT
# of CPs	Epi	SnW	Epi	SnW	SnW	Epi	SnW	Epi	SnW	Epi
3	684.4	126.0	26.0	15.8	90.7	13.6	139.3	86.1	120.9	59.7
5	150.6	93.7	13.4	12.1	67.8	8.2	102.4	43.1	96.9	71.3
20	123.3	46.2	6.3	5.9	29.1	3.6	47.9	11.9	58.3	48.2

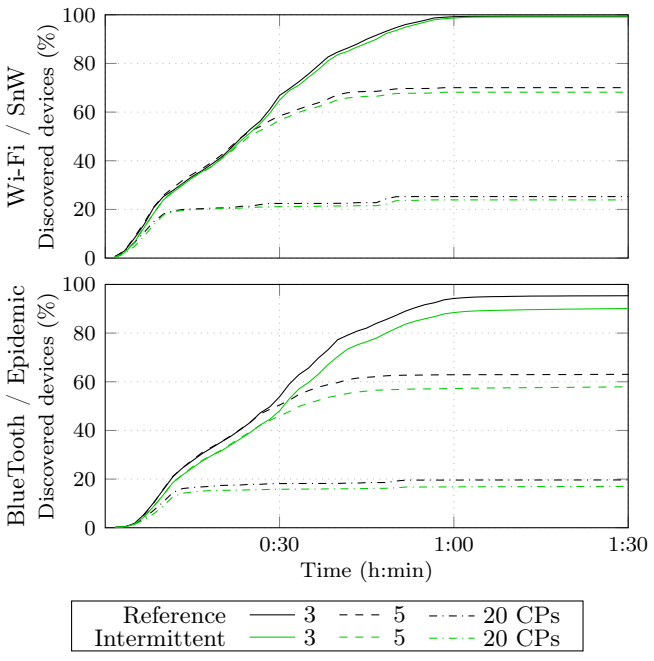

Fig. 3. Intermittent interfaces

Mobility - variable speeds, CP selection: Based on the reference scenario, we change, for the current simulation, the value of some parameters in order to evaluate their influence on the overall system performances. The first experiments concern the walking speed of holders. In our reference scenario, all mobile holders walk with a constant speed of $1.3\,\mathrm{m\,s^{-1}}$. Only victims or individuals unaware of the crisis remain static. On the other hand, speed variations may have an influence on contact occurrences and durations.

Thus, for the simulations, we considered the parameter values of Table I except for the walk speed, that randomly varies from $0.7\,\mathrm{m\,s^{-1}}$ to $2.0\,\mathrm{m\,s^{-1}}$. Figure 4 shows the results. Except for a hardly significant improvement of convergence time with BlueTooth / Epidemic, performances remain comparable: the average speed being still the same, the sets of encountered contacts remain very similar.

However, speed variations have an impact on contact patterns since irregularity in the mobility speed of holders increases both disconnections and new contacts leading to more data exchanges. Such an impact is reflected by the increase in the number of exchanged frames, observed in the third section of Table II.

Finally, simulations are run considering a constant speed but mobility is modified by allowing holders to head towards a random CP, which may not be the closest one in relation to their current positions.

Results are presented in Figure 4 and the last section of Table II. Performance efficiency remains quite similar with 3 CPs. However, with more CPs added, this mobility variation yields to spectacular improvements (more than 60% better with 20 CPs and Wi-Fi / SnW). The reason for such great performance improvement is that divergent holders disseminate information among holders with different target CPs, and, thus, mitigate holders' dispersion.

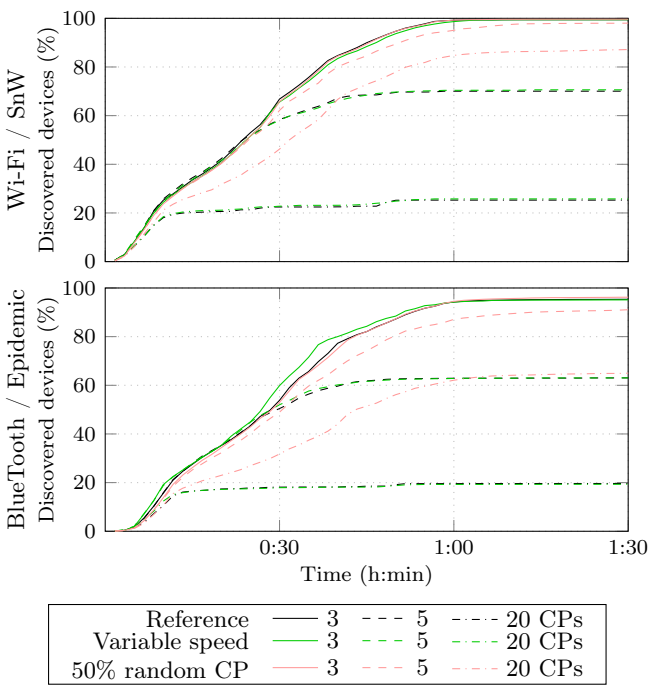

Fig. 4. Mobility variations – walk speed & CP choice

VI. Conclusion

In this paper, we have proposed a new post-disaster ad hoc communication architecture for collecting geolocation information about victims and survivors. Our study focused on efficiency and speed of information gathering as well as energy cost in terms of number of exchanged messages. By defining a reference scenario, we conducted several experiments on top of the ONE simulator to assess the effect of different parameters on the overall performance. Mobility patterns and interface choices were revealed to have a significant impact on both efficiency and energy consumption, whereas protocol choices and interface intermittence have a limited (and interface-range specific) one. Furthermore, walk speed has shown to have little interest in the considered scenario.

Aiming at optimizing protocols routing choices, future directions involve the study of the characteristics of dynamic graphs built over time induced by holders encounters. In a close future, we intend to enrich our disaster scenario considering, for instance, larger disaster areas or adding other participants such as vehicles, rescue teams with specific mobility patterns, etc.

References

[1] C. Reuter, T. Ludwig, and V. Pipek, "Ad hoc participation in situation assessment: supporting mobile collaboration in emergencies," *ACM Trans. Comput.-Hum. Interact.*, vol. 21, no. 5, 26:1–26:26, 2014.

[2] A. Vahdat and D. Becker, "Epidemic routing for partially-connected ad hoc networks," 2000.

[3] T. Spyropoulos, K. Psounis, and C. 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, pp. 252–259.

[4] A. Keränen, J. Ott, and T. Kärkkäinen, "The ONE simulator for DTN protocol evaluation," in *Proceedings of the 2nd International Conference on Simulation Tools and Techniques*, 2009.

[5] S. Bhattacharjee, S. Roy, and S. Bandyopadhyay, "Exploring an energy-efficient DTN framework supporting disaster management services in post disaster relief operation," vol. 21, no. 3, pp. 1033–1046, 2014.

[6] T. Spyropoulos, K. Psounis, and C. 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, pp. 79–85.

[7] A. Lindgren, A. Doria, and O. Schelen, "Probabilistic routing in intermittently connected networks," in *SIGMOBILE Mobile Computing and Communication Review*, 2004, p. 2003.

[8] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "MaxProp: routing for vehicle-based disruption-tolerant networks," in *Proc. of IEEE INFOCOM*, 2006.

[9] P. Stavroulakis, *Terrestrial Trunked Radio - TETRA*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, ISBN: 978-3-540-71190-2. [Online]. Available: http://link.springer.com/10.1007/3-540-71192-9 (visited on 07/19/2016).

[10] Project loon, [Online]. Available: https://www.google.com/loon/ (visited on 03/08/2016).

[11] A. Utani, T. Mizumoto, and T. 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.

[12] Ushahidi, [Online]. Available: http://www.ushahidi.com (visited on 03/08/2016).

[13] SahanaEden, [Online]. Available: http://eden.sahanafoundation.org/ (visited on 10/28/2014).

[14] Google crisis response, [Online]. Available: https://www.google.org/crisisresponse/about/ (visited on 03/08/2016).

[15] Disaster alert network - ubAlert, [Online]. Available: https://www.ubalert.com/ (visited on 06/20/2014).

[16] G. Pearson, M. Gill, S. Antani, L. Neve, G. Miernicki, K. Phichaphop, A. Kanduru, S. Jaeger, and G. Thoma, "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, pp. 11–18.

[17] T. Hossmann, F. Legendre, P. Carta, P. Gunningberg, and C. Rohner, "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.

[18] FireChat, [Online]. Available: http://opengarden.com/ (visited on 03/22/2016).

[19] The serval project, [Online]. Available: http://www.servalproject.org/ (visited on 03/08/2016).

[20] A. Meissner, T. Luckenbach, T. Risse, T. Kirste, and H. Kirchner, "Design challenges for an integrated disaster management communication and information system," in *Prociding os The First IEEE Workshop on Disaster Recovery Networks*, vol. 24, 2002.

[21] K. Fall, "A delay-tolerant network architecture for challenged internets," in *The 2003 ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, 2003, pp. 27–34.

[22] D. Reina, S. Toral, F. Barrero, N. Bessis, and E Asimakopoulou, "Evaluation of ad hoc networks in disaster scenarios.," in *the Third International Conference on Intelligent Networking and Collaborative Systems*, 2011, pp. 759–764.

[23] S. Saha, Sushovan, A. Sheldekar, R. J. C, A. Mukherjee, and S. Nandi, "Post disaster management using delay tolerant network," in *Proceedings of Recent Trends in Wireless and Mobile Networks*, 162, 2011, pp. 170–184.

[24] C. Raffelsberger and H. Hellwagner, "A hybrid MANET-DTN routing scheme for emergency response scenarios," in *The IEEE International Conference on Pervasive Computing and Communications Workshops*, 2013, pp. 505–510.

[25] A. Martín-Campillo, J. Crowcroft, E. Yoneki, and R. Martí, "Evaluating opportunistic networks in disaster scenarios," vol. 36, no. 2, pp. 870–880, 2013.

[26] L. E. Quispe and L. M. Galan, "Behavior of ad hoc routing protocols, analyzed for emergency and rescue scenarios, on a real urban area," in *Expert Systems with Applications*, 5, vol. 41, 2014, pp. 2565–2573.

[27] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek, and M. Degermark, "Scenario-based performance analysis of routing protocols for mobile ad-hoc networks," in *The 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, 1999, pp. 195–206.

[28] M. Boc, A. Fladenmuller, M. D. de Amorim, L. Galluccio, and S. Palazzo, "Price: hybrid geographic and co-based forwarding in delay-tolerant networks," in *Computer Networks*, 9, vol. 55, 2011, pp. 2352–2360.

[29] J. Yoon, M. Liu, and B. Noble, "Random waypoint considered harmful," in *INFOCOM 2003*, vol. 2, 2003, pp. 1312–1321.

[30] B. Karp and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in *The 6th Annual International Conference on Mobile Computing and Networking*, 2000, pp. 243–254.

[31] M. Uddin, D. Nicol, T. Abdelzaher, and R. Kravets, "A post-disaster mobility model for delay tolerant networking," in *Simulation Conference (WSC), Proceedings of the 2009 Winter*, 2009, pp. 2785–2796.

[32] S. Ganguly, S. Basu, S. Roy, and S. Mitra, "A location based mobility prediction scheme for post disaster communication network using DTN," in *Applications and Innovations in Mobile Computing), 2015*, 2015, pp. 25–28.

[33] D. G. Reina, J. M. León-Coca, S. L. Toral, E. Asimakopoulou, F. Barrero, P. Norrington, and N. Bessis, "Multi-objective performance optimization of a probabilistic similarity/dissimilarity-based broadcasting scheme for mobile ad hoc networks in disaster response scenarios," in *Soft. Computing*, 9, vol. 18, 2013, pp. 1745–1756.

[34] Y. Huang, W. He, K. Nahrstedt, and W. Lee, "CORPS: event-driven mobility model for first responders in incident scene," in *IEEE Military Communications Conference, 2008. MILCOM 2008*, pp. 1–7.

[35] N. Aschenbruck, E. Gerhards-padilla, M. Gerharz, M. Frank, and P. Martini, "Modelling mobility in disaster area scenarios," in *The 10th ACM 10th ACM Symposium on Modeling, Analysis, and Simulation of Wireless and Mobile Systems*, 2007.

[36] X. Hong, M. Gerla, G. Pei, and C.-C. Chiang, "A group mobility model for ad hoc wireless networks," in *The 2nd ACM international workshop on Modeling, analysis and simulation of wireless and mobile systems*, 1999, pp. 53–60.

[37] L. Conceição and M. Curado, "Modelling mobility based on human behaviour in disaster areas," in *Wired/Wireless Internet Communication*, 7889, Springer Berlin Heidelberg, 2013, pp. 56–69.

[38] D. G. Reina, M. Askalani, S. L. Toral, F. Barrero, E. Asimakopoulou, and N. Bessis, "A survey on multihop ad hoc networks for disaster response scenarios," in *International Journal of Distributed Sensor Networks, International Journal of Distributed Sensor Networks*, vol. 2015, 2015, p. 647 037.

[39] F. Coriat, L. Arantes, O. Marin, A. Fladenmuller, N. Hidalgo, and E. Rosas, "Towards distributed geolocation for large scale disaster management," in *WSDP - Chilean Workshop on Distributed and Parallel Systems*, 2014.