Tweeting 'When Online is Off'? Opportunistically Creating Mobile Ad-hoc Networks in Response to Disrupted Infrastructure

Amro Al-Akkad[1], Christian Raffelsberger[2], Alexander Boden[1], Leonardo Ramirez[3], Andreas Zimmermann[1]

[1]Fraunhofer Institute for Applied Information Technology (FIT)
Sankt Augustin, Germany
{firstname.lastname}@fit.fraunhofer.de

[2] Institute of Information Technology/Lakeside Labs,
Alpen-Adria-Universität Klagenfurt
Klagenfurt, Austria
christian.raffelsberger@aau.at

[3]Fraunhofer Headquarters
Berlin, Germany
leonardo.ramirez@zv.fraunhofer.de

ABSTRACT

In this paper, we present a system that enables people to post and receive tweets despite disruptions of existing network infrastructure. Our system opportunistically deploys mobile ad hoc networks (MANETs) based on Wi-Fi in which people can communicate with each other in a peer-to-peer fashion. A MANET per se constitutes an isolated island, but as people carry devices around that can join other MANETs, eventually people can transport previously collected data to the online world. Compared to other systems that aim to enable communication in crisis, our system differs in two ways: it does not rely on existing network infrastructure, and it exploits established protocols and standards allowing it to run on off-the-shelf, commercially available smartphones. We evaluated our prototype with a group of students and practitioners. Overall, we received positive feedback on the potential of our technology, but also were pointed to limitations requiring future work.

Keywords

Disruptions, Infrastructure, Smartphones, Opportunistic Communication

INTRODUCTION

In the last decade, broadband coverage via UMTS or LTE expanded enormously and also the availability of public Wi-Fi hotspots has grown significantly. At the same time, there has been a proliferation of increasingly powerful portable wireless devices such as smartphones or tablet computers. People are more and more relying on information and communication technology (ICT) in their daily routine, for example using texting and map-based services, as well as social networks and microblogging. Having access to such services can be crucial in crisis situations, when it is important to receive and send up-to date information on the current emergency.

An emerging set of studies (Farnham et al., 2006; Hughes et al., 2008; Perng et al., 2013) examined how people in distress use ICT services when the underlying network infrastructure is still working. However, the availability of ICT services can be severely disrupted in the aftermath of disasters, when people rely most on the ability to communicate emergency needs. Analyzing challenges people experienced in the aftermath of the 2011 Christchurch, NZ earthquake, Sutton (2012) framed this phenomenon as "online is off". She points out that while information is propagated on the World Wide Web, people without Internet access are left in an

"information vacuum" until network infrastructure can be restored. Furthermore, the study of Al-Akkad et al. (2013a) underlines that disturbances of ICT services caused by disruptions of the underlying technological landscape can have critical consequences during disasters. In the same vain, they account for the creative use of people using leftovers of technology to create new communication infrastructures.

Our work extends this stream of research by pursuing the design of a system, which accommodates opportunities in prevalent networking technology, i.e. we explore the potential of opportunistically creating ad-hoc peer-to-peer (P2P) networks to enable people to use ICT services despite disruptions of existing network infrastructure. Using a proof-of-concept system in the context of a study, we sketch how our system may fit into the work of practitioners whose work involves analyzing social media-generated data. Compared to other ad-hoc systems our approach requires little configuration by end users and runs on off-the-shelf mobile devices. This paper is organized as follows: In the first part of the paper, we classify network infrastructures into three possible forms that can emerge during emergency response operations. Afterwards, we provide a list of system requirements and discuss related approaches and how they conflict with our requirements. In the second part of the paper, we describe the design and evaluation of our prototype. First, we describe the design choices we made for the development of our system. Second, we present results from an evaluation in the scope of an experiment that we conducted at the premises of a university campus with a group of students and two emergency response practitioners. After a discussion of our findings, we close this paper with implications for the re-design of our system and in general for ad-hoc communication systems for crisis situations.

BACKGROUND: FORMS OF NETWORK INFRASTRUCTURE DURING EMERGENCY RESPONSE

During emergency response it is important to provide any means of communication despite disruptions of *existing* infrastructure. From a deployment perspective, we classify three forms of network infrastructures, which can emerge during an emergency response operation, namely: *(pre-) existing, deployable,* and *opportunistic*.

Existing infrastructure refers to network infrastructure already present on the incident site, which may survive the adverse effects of a large-scale disaster and is still operable to some extent. For example, cell towers providing GSM/UMTS or access points offering Wi-Fi networks in public or private spaces constitute a resource for communication that is available on site. Hotspots in public spaces could be re-configured to provide a means for communication during an emergency response, similar to hydrants being a central part for the work of fire fighters to extinguish a fire.

In addition, first responders can carry several tools for in-situ deployment of network infrastructure. These *deployable* elements are brought into and integrated with existing infrastructure. An example is the Landmarke platform (Ramirez et al., 2012), which enables to construct an ad-hoc deployable mesh of network nodes that can be placed by fire fighters as landmarks in order to support indoor navigation inside smoke-filled buildings. Even though this form of network infrastructure is at some points connected to larger, embedded infrastructures, these networks are mostly deployed as an ad-hoc element during the incident, similar to fire hoses that are deployed by fire fighters during an incident and attached to hydrants.

The third form of network infrastructure is *opportunistic*. It refers to the opportunistic use of resources integrated spontaneously to support the task at hand. This form of infrastructure can comprise cell phones, digital cameras or web-based services such as Google Maps already being used to support emergency response. People use these elements to create infrastructure that supports the emergency intervention in an improvised manner (Al-Akkad et al., 2013a). An example is the mobile S.O.S. system, described in (Al-Akkad et al., 2014), which facilitates short lived, serendipitous Wi-Fi connections between neighboring smartphones. Similarly, fire fighters in reconnaissance missions appropriate and combine any things at hand. For example Denef et al. (2009) describe how fire fighters carry seatbelts with them to tie things together.

From a construction perspective, deployed and opportunistic infrastructure can be grouped into the term ad-hoc constructed networks. As to some extent being isolated, the above-mentioned three forms of network infrastructure per se represent "islands" of connectivity (Al-Akkad et al., 2013a). "Islands" of connectivity can be concentrated on specific localities, extend to a large scale, or be geographically scattered along a territory with some places intermittently allowing temporal access. Several challenges arise from such "islands" of connectivity, such as temporary disconnections between network nodes. However, at the same time these challenged networks expose new opportunities to explore (Conti and Kumar, 2010). For example, the work of (Bruno et al., 2008) deploys special proxies that implement gateway capabilities in order to interconnect "islands" of connectivity.

In the following, we focus on the class of opportunistic infrastructures by presenting the design and evaluation

of a mobile system that enables people to post and consume Twitter messages, shortly tweets, in spite of disruptions of existing network infrastructure.

RELATED WORK AND DRAWBACKS IN THE SCOPE OF ELICITED REQUIREMENTS

Resulting from a literature research and our own fieldwork (Al-Akkad et al., 2013a) we have collected several high-level requirements that are relevant for facilitating opportunistic communications. Table 1 lists the set of requirements we considered for the design of our system. From these requirements and aligned to the approach of (Edwards et al., 2003), we started with the design of a lightweight prototype, described below, in order to explore the benefits and constraints of core ideas in an early stage of an ongoing design process.

ID	Summary (The system should…)
R1	Provide a mean for ad-hoc communication.
R2	Enable communication up to 30 meters.
R3	Construct or join networks requiring no cumbersome configuration efforts.
R4	Enable distribution of data across different networks.
R5	Use established and widespread technologies as far as possible.
R6	Be able to send multimedia data.
R7	Comprise a log of received and sent data.

Table 1 Set of System Requirements

There are a number of systems available that aim at supporting people during emergency response. For instance, the Federal Emergency Management Agency (FEMA) provides a mobile application[1] that enables people in distress to receive shelter information and also to submit images with a short description to the FEMA website, which will be placed on a map for public viewing. Before images become available online, the images need to go through a basic approval process in order to guarantee that they are relevant and do not disclose any personal information. SafeCity[2] allows the reception of live video streams from mobile devices reporting crimes or other distress situations. Professional responders use a dedicated app to stream video along with their GPS position to the command center or to other colleagues in the field. Users can install a free application called Bambuser[3], which enables them to view and stream live video. In order to report any video to authorities, users need to register for specific "shares", such as "Crime stoppers" or "Public Officials". All these existing emergency response systems represent promising tools for communication between the public and authorities or non-governmental organizations in crisis, when existing network infrastructure does still operate. However, their use for crisis situations is constrained as existing network infrastructure is subject to be disrupted in crisis situations, e.g. due to damage or overloading.

Furthermore, existing technologies can be utilized for building ad-hoc communication networks during large-scale disasters. For instance, OpenGarden[4] enables people being disrupted from the online world to consume online services. For this OpenGarden requires that at least one device is connected to the Internet to which other devices can tether by the use of low power Bluetooth radio. However, for our research we assumed that devices are completely disrupted from the Internet. More important, systems using Bluetooth are inadequate for serendipitous communications between devices, as Bluetooth's initial pairing mechanism for devices requires cumbersome manual configuration efforts, which fails to comply with R3. Wi-Fi Direct is an emerging communication standard that provides an interesting potential for creating ad-hoc networks. However, Wi-Fi Direct has several drawbacks. For Android OS basic operations such as pairing devices need user intervention which contradicts R3. For Apple iOS it is not available at all. Another constraint is that key mechanisms only work between Wi-Fi Direct certified devices but not with legacy Wi-Fi devices (Camps-Mur et al., 2013). Thus, Wi-Fi direct fails to comply with R5. In general terms, Wi-Fi Direct has been designed for quick, easy and secure peering of home devices, such as connecting a camera with a printer, while our system design originated

[1] http://1.usa.gov/P8V5sf.

[2] http://www.safecity.nl/english/

[3] http://bambuser.com/

[4] http://opengarden.com/

from the need to enable serendipitous communications between devices.

In the last five years, a lot of research has been conducted around the paradigm of opportunistic computing. Opportunistic computing aims to exploit the opportunity to enable communication between neighboring pairs of devices in order to share content as text or multimedia, resources, and services (Conti and Kumar, 2010). In everyday situations, the creation of opportunistic networks is a promising approach to fill the gap in terms of network coverage left by existing network infrastructures in the form of UMTS, LTE based cellular networks or Wi-Fi hotspots (Trifunovic et al., 2013). In crisis situations, ad-hoc constructed networks can complement one another to facilitate ad-hoc communication. The first comprehensive architecture that addressed the challenge to provide opportunistic communication in situations of disrupted network infrastructure was Haggle (Su et al., 2007). The Haggle platform enables mobile users in proximity to exchange content requiring no existing network infrastructure. Through a publish-subscribe system users can express interests via keywords and then receive content from other peers according to how well available content matches their interests. Haggle runs on Windows Mobile and Android. However, Haggle's Android distribution process requires special privileges not available to all users, so called root access, for both Bluetooth and Wi-Fi communication, and thus does not comply with R5. Similar to our system, Twimight (Hossmann et al., 2011) enables Twitter users in proximity to communicate with each other in spite of disrupted existing network infrastructure. Same as our system it runs on commercial Android devices. Twimight leverages Bluetooth to spread data in epidemic fashion from phone to phone. In contrast to our system, which leverages Wi-Fi, Twimight prefers the use of Bluetooth due to its lower energy consumption. Though, Bluetooth conflicts with two of our main requirements. First, compared to Wi-Fi which achieves ranges up to 100 meters, Bluetooth modules often only support ranges up to 10 meters (Ferro and Potorti, 2005), which conflicts with R2. Second, it requires cumbersome manual initial pairing of devices (Ferro and Potorti 2005) making it less suitable for serendipitous encounters of pairs of devices (R3). From a technical perspective Wifi-Opp (Trifunovic et al., 2011) comes the closest to our mobile S.O.S. system. Same as our system Wifi-Opp facilitates opportunistic networking requiring no root access on Android smartphones, and also utilizes Wi-Fi in Infrastructure mode by the use of the same Android API to create ad-hoc Wi-Fi networks. However, with regard to this mailing list[5] there exists no OpenSource distribution, which made it difficult for us to estimate the functioning of Wifi-Opp.

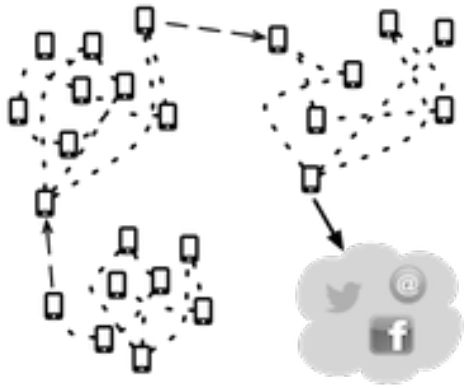

Figure 1 Leveraging MANETs to relay messages to the online world

DEVELOPMENT: THE LOCAL CLOUD SYSTEM

The Local Cloud concept envisions the idea of sharing information in a peer-to-peer (P2P) fashion by opportunistically creating mobile ad-hoc networks (MANETs) and interconnecting them by means of devices moving from one MANET to another until eventually data can be shared with the online world. This idea behind the Local Cloud concept is inspired by patterns observed in disasters with large geographic extension, such as the earthquake in Chile in 2010 (Al-Akkad et al., 2013a), which created "islands" of connectivity whose users stranded within the affected territory. As people travelled, they moved across these islands. This observation shows an interesting opportunity: people moving across separated "islands" of connectivity could propagate messages from one cloud to other clouds. Eventually, a device carried or deployed by a person may be able to gain Internet access and relay the collected data, acting as a mediator between isolated areas and the online world. This relaying mechanism can facilitate the construction of temporary bridges to move data across poorly connected areas, and support, among others, the distribution of important information for the population and the

[5] http://ml.ninux.org/pipermail/battlemesh/2011-October/000958.html

search for missing people. Figure 1 illustrates how messages could be shared inside a MANET (dotted lines) and transported from a MANET to another MANET (dashed lines) until it finally may flow into the online world.

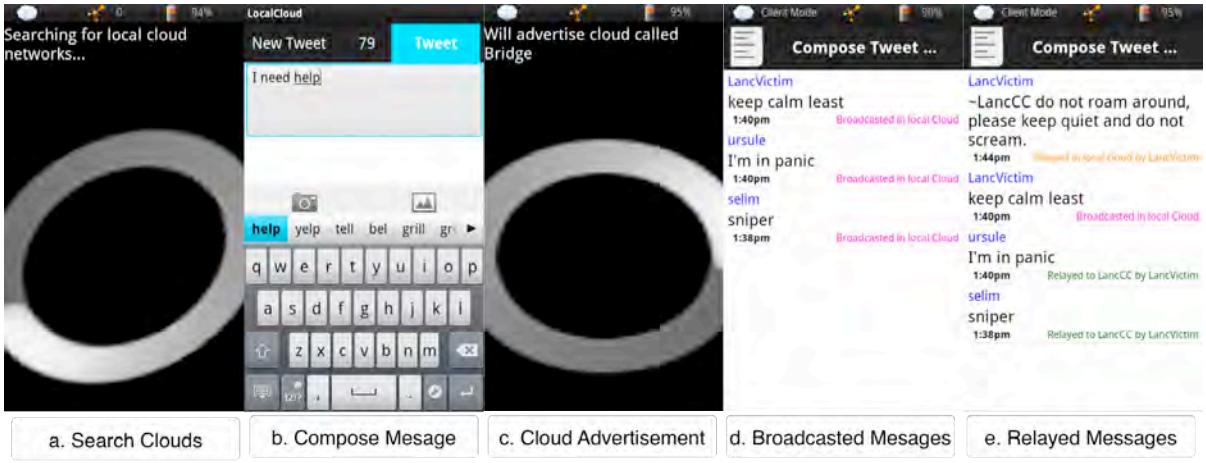

Figure 2 Screenshots of Local Cloud Prototype

The concept of our approach is similar to store-and-forward mechanisms. These mechanisms have been used successfully in other networks with restricted availability such as FidoNet[6], which in the mid 90's used residential phone calls to move millions of message posts and emails across bulletin board systems. Another interesting observation of using technology to relay data is the use of USB sticks in order to spread blog posts from restricted web sites in Cuba (Al-Akkad et al., 2013a).

Design and Implementation

The design of the Local Cloud system is based on the creation of a mesh of wireless devices, such as smartphones or tablet computers to establish clouds of connected devices. Once connected to a cloud, a device can be used to share text or images among the participants of the cloud. From a technical perspective, the cloud can be implemented leveraging the Wi-Fi capabilities in smartphones and other commonly available devices, namely Wi-Fi in Infrastructure Mode, which sets forth a topology consisting of a host and *n* clients. Our approach towards opportunistic communication initially comprises two or more devices with a Wi-Fi interface. At least one device needs to advertise the presence of a wireless network that represents a local cloud. This device, called the HUB, deploys a Wi-Fi network that advertises itself as a HUB by using a particular string of characters inside the wireless network name (i.e. the SSID). Further, the HUB runs a DHCP server for providing an IP address configuration for other client devices. Thus, the HUB provides the minimal basis for peer-to-peer messaging. If after a certain time interval no device has associated to the HUB device, it disables the advertised wireless network and switches into client mode to look for other potentially available HUBs. If a client joins a cloud, it can share data collected inside previously joined clouds. Finally, if one client device manages to connect to a network providing Internet access, it can relay all collected data to the online world.

In order to enable ad-hoc communication (R1) we utilize Wi-Fi instead of Bluetooth to be compliant with R2, although the latter has less impact on the battery life. Complying with R3, our goal was to hide from end-users the complexity of the following two tasks: 1) Configuring and creating a wireless network and deploying a P2P communication on top of it, and 2) Searching for a local cloud and joining its P2P communication. Though, the application notifies users of events related to the connectivity, e.g. that their device has joined or created a local cloud. This means, as soon as a user launches the Local Cloud application, the phone uses its Wi-Fi radio to search for available local clouds. To advertise the presence of a local cloud our prototype places a certain prefix in the SSID. If a local cloud is found, the device connects to its corresponding Wi-Fi network and joins the P2P communication overlay. In case no local cloud is available, the application triggers the deployment and advertisement of a new local cloud (see Figure 2a and 2c).

Our application runs on commercial, off-the-shelf Android devices (supported APIs range from 2.3.3 to 4.x). Android is the most widespread mobile OS and by supporting API versions ≥2.3.3, our system can be installed

[6] http://www.fidonet.org/

on over 97%[7] of all Android devices, which complies with R5. The methods to configure, enable or disable a wireless network are hidden in the Android API. Thus, we use the JAVA reflection API to invoke the relevant hidden methods. As a middleware for establishing P2P communication, we utilize Alljoyn[8], an open-source framework that supported the development of several commercial multiplayer games and multimedia chats.

Complying with R5, we decided to utilize Twitter as the basic everyday service to run over a 'recovered' infrastructure within our system. In recent years, microblogging services such as Twitter have played an increasingly important role in citizen involvement in crisis response (cf. (Perng et al., 2013; Starbird and Palen, 2012)). We posit that providing access to everyday services that are well known among the population, such as microblogging, has the potential to afford a more integrated response effort.

To compose and send a message, users can type in messages via a UI similar to Twitter clients (illustrated in Figure 2b). Users can opt for attaching images to their messages (R6). As soon as a message is broadcasted in a local cloud it appears on top of the list of messages (R7). As soon as a wireless device detects that a connection to a Twitter server is possible, for example via its cellular or Wi-Fi interface, locally collected data can be transported to the online world (R4). Tweets are posted to a dedicated Twitter account simulating a local command center. We leveraged the twitter4j[9] library to handle any Twitter related functionality, i.e. to post or query tweets.

Immediately after tweets have been posted successfully, the application queries latest tweets related to the Twitter username of the command center. In case, the local cloud to which the relaying device was previously connected is still in range, the user will be asked if s/he likes to reconnect to inform former peers. Having confirmed this, the device will synchronize the status of relayed tweets and tweets from the account of the command center. Further, it will send a request to former peers to send tweets that have been shared in the local cloud while the 'relaying' device was disconnected. This enables a two-way communication between peers in the local cloud and the command center.

As peers can join different MANETS and also connect to the online world, the mobile system distinguishes between five types of messages that have been: 1) Broadcasted inside a local cloud. 2) Relayed by a device into another local cloud. 3) Broadcasted inside a local cloud and sent to Twitter, i.e. messages that were composed by the author who carries the relaying device. 4) Relayed from a local cloud to Twitter, but the author of the message has not yet been informed. 5) Relayed from a local cloud to Twitter, and the author(s) of the message have been informed.

Due to the relay of data the fourth or fifth type of messages have implications on the originality of the content of tweets. Thus, to indicate that the content of a tweet has not been composed by the Twitter user who posted it, our systems uses the ~ sign before posting a tweet. Tweets are limited to 140 characters including whitespaces. For our purposes we constrained the length of a message to 90 characters, as we augmented a tweet to contain following constructs besides the actual message (see Figure 2d and 2e):

```
~<usernameOfOriginalAuthor>:_message_(<timestamp>_<day_and_month>)_<@usernameOfLocalPolice>
```

EVALUATION

This section describes the methodology and the results of our qualitative user evaluation.

Methodology and Setup

We evaluated our prototype in the frame of a simulated shooting at an English university. We took notes from interviews and informal conversations, and recorded semi-structured interviews with the students and practitioners, which were then transcribed. For analysis, we reviewed our notes and transcripts, and extracted near-term and long-term requirements. When analyzing our data, we took a stance being open to any unanticipated findings.

The goal of this evaluation was to explore to which extent our system can support the flow of tweets between students—being disrupted from existing infrastructure—and the local police. Four students (S1-S4) played casualties during the evaluation. The group of students comprised two females and two males ranging from 25

[7] http://developer.android.com/about/dashboards/index.html

[8] www.alljoyn.org/

[9] http://twitter4j.org

to 35 years (see two left-hand images in Figure 3). After giving a short introduction, we gave each student a smartphone on which our prototype was pre-installed. Two practitioners acted in the role as personnel at the local police (see two right-hand images in Figure 3): a police officer (PO) that in her unit is responsible for analyzing social media generated data and (MR) a leader of an organization that rescues people in remote environments like mountains.

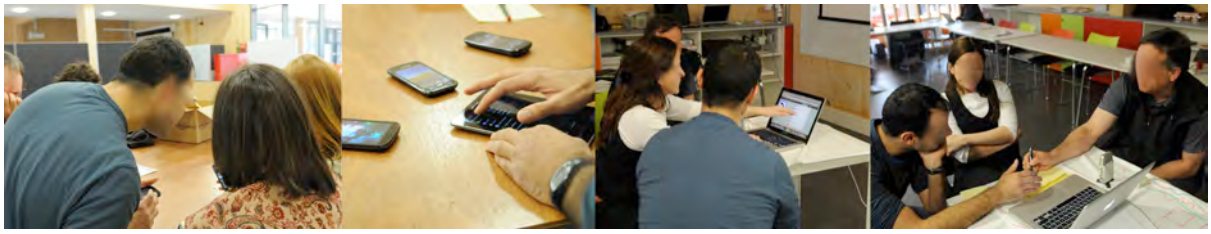

Figure 3. Evaluation with Students playing "Casualties" and Practitioners simulating Emergency Service

During our evaluation tweets that were relayed from the students to the local police were monitored and accordingly reacted to. For the test we agreed with the students to have one person (S3) who relays data, which has been previously shared in a local cloud, to the police as soon as s/he gains connectivity to Twitter. We created a fake Twitter account for the same person and another one for the police. In our evaluation we assumed, that the students know about the police's account, but not vice versa. Our prototype supported to broadcast messages inside a local cloud which then could be relayed to Twitter, but it did not yet support messages to hop from one cloud to another.

Tweets containing images have a high payload and require significantly more time to be sent than tweets that only contain text. Thus, we applied a simple heuristic to select the order to send tweets: first, 50% of the available text-only tweets are sent, followed by 50% of the image tweets. Other heuristics that better balance the bandwidth share of text-only and image tweets are a topic for future research.

Results

Generally, the students liked the concept, as it provides important uses for an emergency situation, building on their familiarity with Twitter. Users like the possibility to communicate despite a lack of mobile reception, even if it would not work perfectly, it would be *"better than nothing"* (S2). However, there were concerns about the degree of user interaction. During our evaluation, messages shared in a local cloud were relayed to Twitter via a wireless network corresponding to the university. In that regard, users suggested the application should switch to the right network automatically, because *"in an emergency my situation might deteriorate"* (S4). Further, some students found it difficult to distinguish right away the different types of messages *"[...] messages that have been tweeted by someone else's device or mine could be categorized into different groups. Listing the latest messages on top makes you neglect the state of previous messages"* (S1).

The practitioners, on the other hand, agreed on the need to consider that networks may break down as they had experienced. In that regard, users saw a potential in our prototype, because it could provide a way to get in touch when other systems would fail. Based on his experiences, one user elaborated on the benefit of using text-based technology instead of voice communication: *"If we are on a rescue and can't talk to people, we automatically send text messages with all our information to contact us when they get a signal. We actually ran a whole rescue on text [...]"* (MR).

However, both practitioners raised also concerns of deploying our system. The police officer was afraid of the awareness of the messages send on Twitter, which can be received by everyone: *"So in our case maybe the parents of the children would get a bit nervous, or it would attract bystanders, if they see our responses"* (PO). Further, the police officer pointed out ways to work around the limited size of tweets in order to communicate emergency needs, for example by using a website with information and point to the URL with our system.

Thereupon, we discussed the style of addressing police and people. In that regard, the police officer explained that it would be okay for him to receive direct messages from specific users over Twitter. He also explained that he would send direct messages to users himself in cases where he wanted to talk to people in an emergency situation directly, "*because then it is controlled what is for them and what is for general knowledge"*(PO).

However, the medical responder raised concerns of using our system in remote environments due to obstacles and long distances between people. Another aspect he stressed was the short battery lifetimes of mobile phones he continuously has to deal with. So one of the first questions he usually asks victims in an emergency situation

is *"how much battery you've got left?"* (MR). He would then regularly tell them to save their batteries, and not call anyone else until the situation has been resolved. "*We have to be forceful, because if you don't, often they waffle […]"* (MR).

Reflecting on the university campus the medical responder expressed the need of transporting data from one cloud to another before it enters the online world. In particular, he said it would not be sufficient to transmit information just in local *"pockets of people"*, but to span the whole area. *"You don't want to have a small cluster of information"* (MR).

The police officer and the medical responder also raised concerns regarding the trustworthiness of tweets in general. As the police officer explained, it would be important to know if a message is authentic, and not coming from a *"fake profile"*. The medical responder supported that view, and stressed the need to know if the situation or a person would be dangerous in order to ensure the safety of the personnel.

To scrutinize the potential of leveraging technology that supports the transport of data—despite disrupted infrastructure—to flow into social media streams, we also asked both practitioners how their organization uses social media in general. The police officer explained that the police see a certain need to use social media because they don't want to be *"left behind"*. So they would do as much as possible, and while there would be a set of policies regarding the use of social media, they don't restrict the use too much, "*because then that wouldn't be social media"* (PO). The medical responder further explained that they would use social media to inform people about what they are doing in order to get public support in terms of the necessary charity.

DISCUSSION

Our evaluation revealed interesting insights into the implications of our design for the practice of crisis response. The first insight is the advantage of our approach in exploiting Twitter as a ubiquitous stream of social media to push data into the online world. In this sense, the students addressed the Twitter account of the simulated local police, whose name was similar to the real local police. At some point the Twitter account of the actual local police was following our fake ones, as PO indicated. PO: *"We had a couple of followers, among them the local police. I blocked them [...] Then I protected the messages and wrote 'test' in the description of my profile"* MR: *"Which tells you the power of what you are doing. We're just having a test, and possibly creating panic throughout Cumbria and Lancaster."*

Both practitioners were able to see the benefit of our technology to enable communication between the public and authorities or non-governmental organizations. According to our evaluation, it is helpful to indicate the route which messages took before they were posted on Twitter, as the following quote from MR shows: "*Tracking of messages to see where they are going, I think this would calm people down."* In this context, the use of our micro-syntax proved to be promising as long as the application generates it automatically. PO: "*To put a ~ sign in the beginning of a message and the rest is clever […] I think as long as the system does this automatically it may help"*. In that regard, it is important to take into account the communication protocols of emergency responder organizations, which can be quite different even within the same countries (Denef et al., 2013). Also, our evaluation showed that the authenticity of information (e.g. fake profiles etc.) is an important issue for the practitioners, which needs to be addressed in future work. Further, an important, albeit Twitter-specific technical problem, is that a tweet is limited to 140 characters, and our approach brings that down to only 90 characters. Future work could investigate into micro-syntaxes that would allow for more space, but provide the same information. Of course, this would reduce the human readability of a tweet, but using tools that automatically extract the required information could resolve this issue. In this sense, our technology fits on the edge of discussions of micro-syntax systems to support the coordinated analyzes of social media generated data (Imran et al., 2013; Starbird and Stamberger, 2010).

On the other hand, our evaluation also pointed to a set of limitations: 1) The way of messages are interchanged between a local cloud and the online world also leaves room for improvement from a practical perspective. PO explained that sending direct messages would have the advantage to avoid peripheral worriedness of beloved ones or attracting bystanders. Our evaluation shows that the authenticity of information needs to be addressed in future work. Given the fact that our system currently communicates over open communication channels, the perpetrator might also get access to the exchanged information, which could even increase the threat. 2) Currently, our prototype supports only one hop communication between a local cloud and the online world. As pointed out by MR, we need to enhance our implementation to work over more than one hop. This implies a more complex synchronization between several MANETs. For future work, we will investigate into previous research of store-and-forward mechanisms (Delosieres and Nadjm-Tehrani, 2012; Raffelsberger and Hellwagner, 2013) in order to inform the design of our system for the use of a protocol to route and synchronize messages between clouds. 3) When a local cloud is instantiated and people join it, the topology of the

underlying MANET remains the same in the current prototype. Though, the host device of the local cloud (HUB) needs to consume significantly more battery than client devices, which can be problematic as our evaluation showed. To handle this complex issue, we investigated into the use of a protocol (Al-Akkad et al., 2013b) in order to switch roles between peers of a cloud on the basis of several parameters as the battery level, the number of clients connected to a local cloud, and more. 4) Currently, our implementation works only on Android devices. At the moment, there exists no API in iOS to create ad hoc networks, which makes it rather difficult to deploy our system for iOS. Though, it would be possible for users to setup hotspots manually. We will keep an eye on how APIs in this concern might evolve.

CONCLUSION

In this paper, we presented a system to facilitate the transport of tweets across areas of disrupted infrastructure. Our system constructs ad-hoc Wi-Fi networks whose SSIDs are prefixed with an emergency code. Other devices can scan for such nodes and associate to them in order to create "islands" of connectivity. While our approach is certainly not efficient in everyday situations, it does represent a promising approach for emergency or crisis situations. We have tested the system in an experimental setting at an English university with students and two practitioners for crisis response. The results of our evaluation showed that our system could foster communication between the public and emergency response services. Although similar systems have been described in the literature, our contribution lies in a design that is based on established standards and requires no complex changes in the underlying mobile OS. From a practical perspective, this has the advantage, that a broad range of devices supports our system in situations where existing infrastructure is disrupted.

We argue that our results on combining prevalent wireless network technology and everyday ICT services can generalize broadly across different cultures. Britain is a Western country in which since the latest 2011 England riots (Denef et al., 2013) it became noticeable that a lot of people use text-based services like BlackBerry Messenger and Twitter via their mobile phones. Further, since the riots, British authorities have started to consider social media generated data in their routine work practices (Denef et al., 2013). In other Western countries social media use by authorities is still evolving (Denef et al., 2011), while in Middle Eastern cultures like Egypt its use can be extensive as described in the work of Starbird and Palen (2012).

In future work, we plan to address some technical issues, described in the previous chapter. The results of this applied and ongoing research informs the development of an enhanced prototype, which we plan to test in a different exercise in order to gain further insights on how our system scales.

ACKNOWLEDGMENTS

The presented work is funded by the European Union as part of the BRIDGE project (FP7SEC-2010-1) under grant agreement n°261817. We thank the practitioners and students for providing insights, and Lisa Wood for organizing the 3rd BRIDGE user workshop in which we conducted our evaluation.

REFERENCES

1. Al-Akkad, A., Ramirez, L., Boden, A., Randall, Dave, and A. Zimmermann. (2014) Help Beacons: Design and Evaluation of an Ad-Hoc Lightweight S.O.S. System for Smartphones. *In Proceedings of the 32nd International Conference on Human Factors in Computing Systems* (*accepted for publication*).
2. Al-Akkad, A., Ramirez, L., Denef, S., Boden, A., Wood, L., Büscher, M., and A. Zimmermann (2013). "Reconstructing Normality": The Use of Infrastructure Leftovers in Crisis Situations As Inspiration for the Design of Resilient Technology. *In Proceedings of the 25th Australian Computer-Human Interaction Conference: Augmentation, Application, Innovation, Collaboration*, 457–466.
3. Al-Akkad, A., Ramirez, L., and A. Zimmermann (2013). Method for organizing a wireless network (*filed at European Patent Office*).
4. Bruno, R., Conti, M., and A. Passarella (2008). Opportunistic networking overlays for ICT services in crisis management. *In Proceedings of the 5th International Conference on Information Systems for Crisis Response and Management*.
5. Camps-Mur, D., Garcia-Saavedra, A., and P. Serrano (2013). Device-to-device communications with Wi-Fi Direct: overview and experimentation. *IEEE Wireless Communication*, 20, 96–104.
6. Conti, M., Kumar, M., 2010. Opportunities in Opportunistic Computing. *Computer*. 43, 42–50.

7. Delosieres, L., and S. Nadjm-Tehrani. (2012) BATMAN Store-and-Forward: the Best of the Two Worlds. *In Proceedings of the 10th International Conference on Pervasive Computing and Communications Workshops*, 727–733.
8. Denef, S., Bayerl, P.S., and N.A. Kaptein. (2013) Social Media and the Police: Tweeting Practices of British Police Forces During the August 2011 Riots. *In Proceedings of the 31st Conference on Human Factors in Computing Systems*, 3471–3480.
9. Denef, S., Kaptein, N.A., and P.S. Bayerl. (2011) ICT Trends in European Policing, *COMPOSITE Project*.
10. Denef, S., Ramirez, L., and T. Dyrks. (2009) Letting Tools Talk: Interactive Technology for Firefighting. In Proceedings of the Extended Abstracts of the 27th Conference on Human Factors in Computing Systems, 4447-4452.
11. Edwards, W.K., Bellotti, V., Dey, A.K., and M.W. Newman. (2003) The Challenges of User-centered Design and Evaluation for Infrastructure. *In Proceedings of the 21st Conference on Human Factors in Computing Systems*, 297–304.
12. Farnham, S., Kirkpatrick, R., and E. Pedersen. (2006) Observation of Katrina/Rita deployment: Addressing social and communication challenges of ephemeral groups. *In Proceedings of the 3rd International Conference on Information Systems for Crisis Response and Management*.
13. Ferro, E., and F. Potorti. (2005) Bluetooth and wi-fi wireless protocols: a survey and a comparison. *IEEE Wireless Communication*. 12, 12–26.
14. Hossmann, T., Legendre, F., Carta, P., Gunningberg, P., and C. Rohner. (2011) Twitter in disaster mode: Opportunistic Communication and Distribution of Sensor Data in Emergencies. *In Proceedings of the 3rd International Conference on Communication and Computing*, 1–6.
15. Hughes, A.L., Palen, L., Sutton, J., Liu, S.B., and S. Vieweg. (2008) "Site-Seeing" in Disaster: An Examination of On-Line Social Convergence. *In Proceedings of the 5th International Conference on Information Systems for Crisis Response and Management*.
16. Imran, M., Elbassuoni, S., Castillo, C., and P. Meier. (2013) Extracting Information Nuggets from Disaster-Related Messages in Social Media. *In Proceedings of the 10th International Conference on Information Systems for Crisis Response and Management*.
17. Perng, S.-Y., Buscher, M., Wood, L., Halvorsrud, R., Stiso, M., Ramirez, L., and A. Al-Akkad. (2013) Peripheral response: microblogging during the 22/7/2011 Norway attacks. *International Journal of Information Systems for Crisis Response Management*. 5, 41–57.
18. Raffelsberger, C., and H. Hellwagner (2013) A hybrid MANET-DTN routing scheme for emergency response scenarios. *In Proceedings of the 11th International Conference on Pervasive Computing and Communications Workshops*. 505–510.
19. Ramirez, L., Dyrks, T., Gerwinski, J., Betz, M., Scholz, M., and V. Wulf. (2012) Landmarke: an ad hoc deployable ubicomp infrastructure to support indoor navigation of firefighters. *Personal and Ubiquitous Computing*. 16, 1025–1038.
20. Starbird, K., and L. Palen. (2012) (How) Will the Revolution Be Retweeted?: Information Diffusion and the 2011 Egyptian Uprising. *In Proceedings of the 15th Conference on Computer Supported Cooperative Work*, 7–16.
21. Starbird, K., and J. Stamberger. (2010) Tweak the Tweet: Leveraging Microblogging Proliferation with a Prescriptive Syntax to Support Citizen Reporting. *In Proceedings of the 7th International Conference on Information Systems for Crisis Response and Management*.
22. Su, J., Scott, J., Hui, P., Crowcroft, J., De Lara, E., Diot, C., Goel, A., Lim, M.H., and E. Upton. (2007) Haggle: Seamless Networking for Mobile Applications. *In Proceedings of the 9th International Conference on Ubiquitous Computing*, 391–408.
23. Sutton, J. (2012) When Online is Off: Public Communications Following the February 2011 Christchurch, NZ Earthqauke. *In Proceedings of the 9th International Conference on Information Systems for Crisis Response and Management*.
24. Trifunovic, S., Distl, B., Schatzmann, D., and F. Legendre. (2011) WiFi-Opp: Ad-hoc-less Opportunistic Networking. *In Proceedings of the 6th MobiCom Workshop on Challenged Networks*, 37–42.
25. Trifunovic, S., Picu, A., Hossmann, T., and K.A. Hummel. (2013) Slicing the Battery Pie: Fair and Efficient Energy Usage in Device-to-device Communication via Role Switching. *In Proceedings of the 8th MobiCom Workshop on Challenged Networks*, 31–36.