XMPP to the Rescue: Enhancing Post Disaster Management and Joint Task Force Work

Ronny Klauck
Innovations for High Performance Microelectronics (IHP)
Leibniz-Institute for Innovative Microelectronics, Germany
eMail: klauck@ihp-microelectronics.com

Michael Kirsche
Computer Networks and Communication Systems Group
Brandenburg University of Technology Cottbus, Germany
eMail: michael.kirsche@tu-cottbus.de

***Abstract*—A flexible and easy-to-use disaster management system is essential for providing rescue teams with communication and accurate information. This work promotes a post disaster management system capable of providing communication in infrastructure as well as ad hoc scenarios, and of supporting on demand creation of joint task forces. The system is based on the Extensible Message and Presence Protocol (XMPP). Scenarios, problems, and adequate solution approaches are discussed to enhance post disaster management, specifically in the area of sensor grouping and joint task force cooperation.**

***Keywords*-XMPP; post disaster management; joint task force.**

I. Introduction

Crises like the Fukushima nuclear power plant incident or the recent earthquake catastrophe in Turkey have shown that an accurate and easily deployable Post Disaster Management System (PDMS) could enhance the work of rescue forces in various ways. One of the biggest problems of disaster management is the gathering and analysis of real-time data streams and the distribution of raw or analysed data to all participating rescue forces. A flexible and variable, yet easy-to-use system could help emergency forces in providing a solid and necessary data background to ease decision processes. Supporting adequate and accurate decisions is a characteristic PDMS capability. It should go hand in hand with the integration of various sensors, the capability of streaming sensed data in real-time, a support for flexible data analysis, and a seamless integration of all engaged partners (e.g. rescue teams, experts) from various locations.

The task of integrating all engaged stakeholders in the system and providing access to raw data and analysis outcomes is complex due to the scenario's distributed characteristic. Data has to be monitored in the field, while the analysis is often performed in a centralized fashion by experts and analysts. Communication between the engaged forces and teams is also required on demand on-site as well as through infrastructure network access to partners in remote locations. Matters get complicated because communication infrastructure or deployed sensor networks are often interrupted or destroyed by the disaster itself (cp. [1]). It is also clear that the batch of tasks that an ideal PDMS should handle cannot be provided through a single communication technology or plain sensor networks. A mobile and powerful hardware platform is needed with support for various communication technologies, yet minimal weight and battery powered operation, lasting at least a couple of days. We presented a first draft of such a system in [2], based on mobile terminals (smartphones) using XMPP [3] and interconnected collaborative cloud services for data processing and analysis.

While [2] provided an initial system outline, some aspects are still tentative and far from practical deployment. We discovered in interviews with several disaster management stakeholders that the area of creating and managing ad hoc joint task forces is often neglected despite its importance. Joint task forces enable an ad hoc cooperation of involved individuals or groups, depending on the situation and the circumstances. A disaster management system should support the creation of joint task forces through flexible communication and data sharing capabilities, alleviating decision processes. This support for joint task force management and the accompanied tasks and problems are the main subject of this paper. All introduced approaches aim at providing the participating stakeholders with a global view of the situation thus improving the decision making process.

The remainder of this work is structured as follows: Section II outlines the scenario of post disaster management, together with a distinction from other fields of research and an examination of related work. The design of our XMPP-powered system and the technical background is summarized in Section III. In Section IV we present our approaches for an automatic grouping of sensed data and a flexible creation of joint task forces. Section V provides the overall conclusions for this work.

II. Post Disaster Management - A Case Outline

Post disaster management is always situational. As every disaster is unique, flexibility is hence the major aspect in every part of the management of relief actions. Despite the uniqueness, certain basic presumptions can be made about natural or man-made disasters to categorize circumstances and steps necessary in the follow-up of any crisis. Subsection II-A introduces these presumptions and justifies the need for a flexible management of joint task forces.

A distinction from other fields of research is presented in Subsection II-B while work related to the key aspects of this paper is discussed in the final part of this section.

A. Scenario Considerations

Scenarios for post disaster management are manifold. Real life examples are the management of the Fukushima power plant site after the earthquake and tsunami catastrophe, the search for buried disaster victims in the aftermath of the earthquakes in Turkey and Japan, and the evacuation of people from ground zero on 9/11. All these cases showed that the hardest part in disaster management is the decision making process, since relevant data is neither always available nor well distributed to all engaged stakeholders. An example scenario is depicted in Figure 1 to highlight the typical problems. The following summary of assumptions, tasks, and problems is drawn from this example:

1) Various stakeholders need to interact and communicate with each other (e.g., central management team with different groups of individuals / joint task forces);
2) Centralized communication infrastructures are fault-prone and often destroyed during disasters (cp. [1]);
3) Knowledge about other actors is often not distributed on site to every participant;
4) Status data gathered from the disaster site is often not distributed between all participating stakeholders;
5) Real-time data access is crucial yet hard to achieve;
6) Grouping different actors into task forces could provide for better situation-dependant decisions / actions;
7) Communication between stakeholders is usually ad hoc but could also be provided on-demand by portable infrastructure (cp. [4]), leading to hybrid networking scenarios (ad hoc and infrastructure communication).

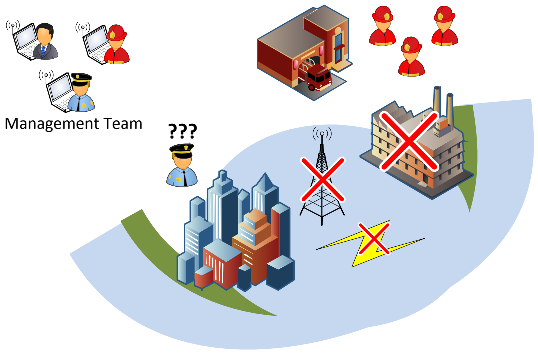

Figure 1. An example scenario for post disaster management

As the summary listing shows, on-site rescue forces and management teams need a global real-time view of gathered data. Only this enables precise and timely decisions, which are crucial for the safeguarding of disaster victims and rescue forces. It is important that analysed data is being distributed to every stakeholder while the data's representation must be clear and easy to understand. Cooperation support must include ad hoc as well as infrastructure-based communication, thus favouring our XMPP approach [2], which provides both (cp. Section III). It is also clear that complex gateway or bridging solutions should be avoided to reduce the overall complexity of the disaster management system.

B. Differentiation

Our work stands out in relation to comparable research because it takes the temporary character of post disaster management into account. Research in the area of structural health monitoring [5], [6], for example, is often realized with Wireless Sensor Networks (WSNs), which provide a lifetime up to years compared to our approach. WSNs might be designed for a longer lifetime, but they lack the processing power to stream and process high resolution data streams, in contrast to our concept of using powerful hand-held devices. WSNs also use hop-by-hop transmissions to forward data to a centralized sink [7], causing delays in real-time streams [8]. Another drawback that we want to avoid is the limited packet size of WSN standards (e.g., 127 Bytes max. packet size for IEEE 802.15.4). Data resolution can be limited by such small Maximum Transmission Units (MTUs), when compared with WWAN or WLAN standards (1280 Bytes min. for IPv6 packets).

We prefer smartphones as mobile terminals because they come equipped with a variety of built-in sensors, e.g.: camera, light sensor, gyroscope, accelerometer, proximity/IR sensor, digital compass, and microphone. Smartphones are therefore well suited as both communication and mobile sensing platforms [9]. Additional sensors can be plugged in if needed [10], thus enabling the smartphone to provide a rich set of environmental data, in contrast to the often limited number of sensors attached to wireless sensor nodes. Section III gives more information on our system design.

C. Related Work

An overview of existing work related to our XMPP-based system design is presented in [2]. A discussion of related work in terms of combining sensor and cloud technology is not included, refer to [2] for information on cloud technology aspects. [11] provides a generic reflection on decision support systems and their role in disaster management.

A multi-agent system for task allocation in disaster scenarios is introduced in [12]. The system, called Overseer, extends the idea of using mobile devices in disaster scenarios with continuous monitoring of users and tasks, while dynamically evaluating the mobile contexts. Through continuous evaluations, a dynamic reassignment of tasks to members of the emergency force team is enabled. An important difference in relation to our work is the basic assumption that the communication infrastructure is intact, although the authors discuss a peer-to-peer (P2P) communication approach in case of defective infrastructure. Another difference is that

Overseer is based on a so-called *disaster response engine*, a complex centralized entity, which we avoid by using incorporated and already available cloud-based services and ad hoc (P2P) communication support through the XMPP extension (XEP) *XEP-0174 Serverless Messaging* [13].

[14] presents a novel mechanism for the information exchange between various stakeholders, by using a role-based access control scheme. One distinctive assumption of this work is the need for a *liaison officer*, which establishes connections between the stakeholders. The paper focuses on the collaboration and the ensuing security aspects, leaving networking and technical aspects unconsidered.

Partial aspects of (post) disaster management are considered, analysed, and evaluated in [7] and [15]; both papers skip the management of joint task forces. While [7] evaluates the reconfiguration of IEEE 802.15.4 topologies and the efficient selection of central coordinator devices, [15] presents an application-layer multicast solution to deliver emergency messages over best-effort networks.

III. System Concept and Technical Overview

Today, smartphones are available for moderate prices in a wide variety as commodity hardware. While carried by users, smartphones offer the chance to monitor the environment and to deliver real-time data streams with a high resolution directly to any sink in the Internet. They can provide complex data types, such as radiated noise or images and videos, in contrast to sensor networks, which usually collect primitive data types (e.g. temperature, humidity). Results for measured and analysed data can be displayed directly on the screen of the mobile device to provide the user with a direct feedback. Users are generally familiar with handling smartphones, which makes access to functionalities and accumulated data easier for them. In comparison, dedicated sensor nodes mostly omit showing results directly in favour of energy saving. More important then providing a long life time for pervasive post emergency scenarios is to provide an uncomplicated system with an easy setup and comprehensible data access through standardized communication technologies like WWAN or WLAN instead of proprietary solutions. Hand-held terminals for our approach run up to a couple of days and support access to various networks via GPRS, UMTS, and WLAN [16].

A. Used System Design

To fulfil the need for a flexible, user-friendly, and cooperative solution, we use a monitoring system of XMPP-driven entities with data gathering and analysis support through collaborative cloud services, as described in [2]. Basically, the whole design is kept simple so that every device capable of running an XMPP client can be connected and everyone who has such a device can use the system. This also includes untrained volunteers who need an easy-to-use and easy-to-learn software to participate. Our proposal for a system design consists of sensor-equipped hand-held devices (not to mix with typical sensor nodes) and the cloud services. Figure 2 shows an example configuration, where sensor-equipped devices run XMPP software clients through which users can publish measured raw data. The depicted cloud service manages the sensor data storage that acts as a normal XMPP client inside the network. XMPP domains are additionally provided by cloud service instances, allowing for interconnection and data exchange between different stakeholders (refer to [2, Section IV-D.4]).

The system is designed to support a grouping of sensor devices, a simple creation of joint task forces, and a remote task monitoring by the management team. Pervasive monitoring and collaboration is thus provided for all involved parties. Section IV describes these specifics. The system supports a wide range of network access technologies, although a direct Internet access is preferred. If necessary, Internet access will be shared, in case only few devices can connect directly to the Internet. For this case, routing over WLAN or Bluetooth via *XEP-0174 Serverless Messaging* is used throughout the XMPP network. Mobile entities in the system detect their neighbours automatically inside their ad hoc networks. This also allows for a direct access for rescue workers in the outer quarter of the operational area. In case of a breakdown of the centralized infrastructure or for areas where radio transfer is short-staffed, a dedicated Internet connection can be provided by a wireless radio mast [4]. This situation is exemplified in Figure 2 by the truck.

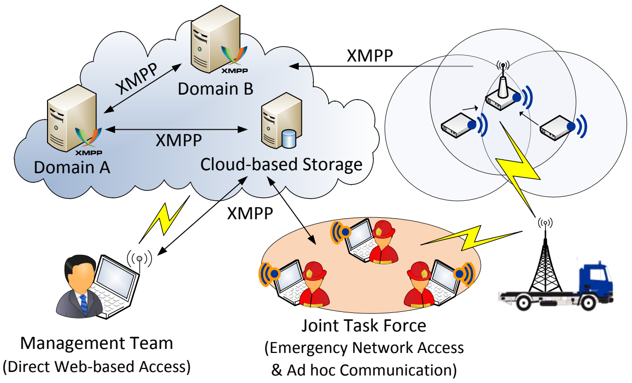

Figure 2. System design

B. Technical Background

XMPP [3] is an established standard for collaborative communication to realize instant messaging, user collaboration, and Voice-over-IP (VoIP). Moreover, XMPP implements the publish-subscribe paradigm, providing an effective way of distributing relevant events [2, Sec. IV-B]. An important aspect of XMPP is the support for hybrid networks: it can interact with a server infrastructure as well as ad hoc communication by using *Serverless Messaging* [13].

A detailed introduction and the usage of XMPP in hybrid networks can be found in [2, Sec. III & Sec. IV-C].

IV. Enhancing Support for Joint Task Forces

During an emergency situation it could happen that several organizations from different kinds or countries have to work hand in hand. Sometimes they all need access to the same collected data to get an overview of the current situation. A flexible data sharing is essential, because this can ease the decision-making process by identifying dangerous spots and prioritising next tasks for all involved parties. Another important aspect is to bundle resources by grouping rescue workers into a *joint task force*. This can be a serious enhancing factor, because it supports the collaboration between all involved parties while exchanging sensor specific data and enforcing cooperative solution generation for specific tasks in smart teams of experts. This way the crisis management can monitor each task as well as each detailed step of a task. With this information they can remotely control the complete emergency task and react in real-time to upcoming bottlenecks like the deficit of resources for example. Moreover, the crisis management team can include the actual feedback of the joint task forces and can find appropriate decisions for all involved parties.

A. Grouping of Sensor Devices

Sensor devices may be composed of several detectors (e.g., compression, humidity, acceleration, etc.). The publish-subscribe paradigm, as a system core functionality, is used to propagate new sensor data to the Internet. A threshold can be adjusted on every sensor device separately, depending on its integrated detectors. As soon as the threshold value is exceeded, sensed data is propagated to the Internet. Grouping detectors will help handling a large quantity of devices and provide a better overview in an XMPP client software by using the XMPP roster management or chat rooms. This way various entities become eventually well-arranged and can be easily managed in a single sensor group.

1) XMPP Chat Rooms: During the boot-up phase devices start connecting to the Internet and register themselves in an XMPP domain. Afterwards, sensor devices automatically join the virtual sensor groups, depending on their GPS position and attached detectors. The virtual groups will be created through XMPP chat rooms by the crisis management or autonomously by a sensor device, if a detector-specific group does not exist. With the protocol extension *XEP-0045 Multi-User Chat* new chat rooms can be created or searched and existing chat rooms can be monitored or joined. Several rooms are conceivable for emergency scenarios:

- *GPS group:* used to map GPS coordinates to the corresponding device. Only one group from this type is used. All sensor devices will publish their current GPS coordinates, thus enabling a position monitoring.
- *Detector specific groups:* used to map the detector to the corresponding sensor device. Several groups of this type can be created depending on the variety of used detectors. A sensor device participates in every group corresponding to its integrated detectors. As devices only will send data when their threshold value is exceeded, a clear overview of a corresponding sensor device to its streamed data is provided.

This implies that for every kind of integrated detector, an appropriate XMPP chat windows needs to be opened. A proper chat windows arrangement enables a slim yet effectual overview of all detectors. The chat window itself is a helpful instrument to locate and symbolize the status of a sensor and its monitored environment. An XMPP chat window normally consists of the list of joined sensor devices with their presence status (via an icon) and the chat history. Depending on the threshold value for the measured data of a sensor device, its presence status can be signalised through the chat icon and be depicted like traffic lights:

- *Green:* the sensor data is below the threshold value, no change of data is reported to the chat room.
- *Yellow:* the sensor data exceeds the threshold value, every data change is reported to the chat room.
- *Red:* the sensor data overloads the threshold value, all measured data are reported to the chat room.
- *Grey:* no sensor data is reported to the chat room. Sensor device is either not available or destroyed.

The chat history holds the measured sensor data in chronological order and enables a posterior analysis to identify the cause. Changes of values can be recognized by following the chat conversation and can be reported or delegated to the corresponding rescue forces. In total, no special training, software, nor hardware is needed to monitor the measured sensor data. Commodity hardware like smartphones and laptops can be used instead of expensive dedicated hardware. Freely available XMPP software [17] will also reduce software development and licence costs.

With the help of the virtual groups the crisis management and rescue workers will identify changes in the monitored environment in real-time and recognize dangerous spots in an emergency scenario. The marked spots can be identified simply by searching the GPS position of the corresponding devices in the GPS group. This approach is compatible to all existing XMPP chat applications and will have a wide acceptance rate due to its already available implementation in several XMPP libraries, servers, and clients.

2) XMPP Roster: An alternative approach to group sensor devices is the direct use of the XMPP roster management. The roster is a simple contact list that holds registered Jabber IDs (JIDs) from all sensor devices as roster items of locally and remotely accessible XMPP domains. The XMPP chat application will depict each roster item with the name (JID) and the presence status as an icon of the sensor device.

Detailed information (e.g., GPS position, available detectors, data values) of the sensor device state will be shown when highlighting its corresponding roster item, which will extend the graphical view. Selected roster items can be consolidated under a specified group name to ease the view on the elements in the contact list and to group the sensor devices according to their used detectors. The roster enables a global and sorted view on all measured sensor data for any observer. An icon of each roster item signalizes critical changes in the monitored environment. Dangerous spots can be identified through the GPS position of the corresponding sensor device in the roster (refer to Section IV-A).

Unfortunately, the grouping in the roster has to be done manually for each sensor device. This is both bothersome and time consuming for an observer who manages a variety of sensor devices in emergencies. Therefore we have implemented an automatic grouping method based on *XEP-0163 Personal Eventing Protocol* (PEP) to solve this issue. PEP provides an easy way to broadcast notifications as events to contacts in the user’s roster. It defines a simplified subset of *XEP-0060 Publish-Subscribe* that can be followed by XMPP client and server developers to distribute personal events across the XMPP network. The definition of event is quite broad, for example the current location of the user (*XEP-0080 User Geolocation*). On every change of a sensor value the corresponding sensor device should generate events of their properties, which include their available detector types and the current values to each detector. Elements of actually defined properties are shown in Table I. The properties can simply be extended with new elements. We call this extension *User Property*.

Table I
ELEMENT LIST OF USER PROPERTY

Element	**Description**	**Example**	**Datatype**
protype	Defines the sensor type	Accelerometer	xs:string
value	Sensor type value	1.354	xs:double
unit	Unit of sensed vlaue	G	xs:string

Each sensor device will publish the *User Property* event to the XMPP server. The following listing depicts an example of a User Property XML messages:

```
<iq from="x@amp.le/" type="set" id="pub1">
   <pubsub
      xmlns="http://jabber.org/protocol/pubsub">
      <publish
         node="http://jabber.org/protocol/prop">
         <item>
            <property>
               <protype>accelerometer</protype>
               <value>1.354</value>
               <unit>G</unit>
            </property>
         </item>
      </publish>
   </pubsub>
</iq>
```

When the *User Property* event arrives at the subscriber’s XMPP client, an automatic grouping of sensor devices and its measured data can be realized in the user’s roster by following these steps:

I: The XMPP library extracts the properties from the received User Property event;
II: The XMPP chat client automatically searches for existing group entries according to the extracted properties;
II.1: If a matching group entry is found, follow step V;
II.2: If no matching group entry is found, follow step III;
III: The XMPP chat client creates a new group entry in the roster according to the extracted properties and informs the roster management about a pending roster update;
IV: The roster management sends group updates for the user’s roster to the XMPP server, the XMPP chat client displays the sensor device in its new group in the roster;
V: The XMPP chat client shows extracted values for each property of a sensor device as extended presence status.

On the one hand, this approach is more user-friendly than the XMPP group chat, because the observer does not need to open a new chat window for every supported detector of the sensor devices. On the other hand, this approach is not yet backward-compatible to existing XMPP clients and libraries. Clients need to adopt the proposed extension so that users benefit from the automatic sensor grouping function. Overall this extension will ease the use of data gathering and analysis through XMPP coupled with sensor devices.

B. *Creating Joint Task Forces*

Creating a joint task force can be provided by granting access to the XMPP network. This enables a direct exchange and further analysis of collected data between crisis management and rescue forces. During collaboration, new tasks for each rescue team can be adjusted ad hoc and managed from the crisis management as a joint task. Separately collected data can be shared directly and analysed between all involved stakeholders. Communication groups created via *Multi-User Chat* offer the possibility to coordinate joint forces easily, classified, and task specific.

XMPP chat rooms can be created either by the central crisis management or autonomously by rescue forces. The crisis management will use a chat room primarily to create joint forces. The involved rescue workers normally belong to different departments (e.g., police, fire, or medical service) and a stakeholder could require specific devices, resources, or skills and expertise. XMPP chat rooms enable an immediate interconnection and collaboration in an easy way by using commodity hardware like smartphones. Furthermore, the rescue workers of the new joint task force can exchange instructions and data while the crisis management can monitor each step and the progression of the ongoing rescue tasks. Each step can also be tagged with a rescue worker’s GPS coordinates to display his whereabouts on a map.

Creating exclusive groups of rescue workers can be used for undisturbed internal group interactions in critical situations while global coordination information could be announced via a public chat room to all rescue forces. In some situations it is helpful to ask other rescue worker for support or resources. Idle rescue workers can then publish their availability in a predefined chat room and inform others seeking for assistance. In the end, only a simple XMPP client and no dedicated hardware is needed to enable a range of collaboration options, again reducing software and hardware costs. Involving and controlling volunteer citizens in emergency situations can now be simplified, because they can be provided with the same XMPP software. The volunteers just need a commodity smartphone or laptop with an XMPP client to support the rescue forces or to receive tasks from the crisis management.

V. Conclusions

This paper promoted an XMPP-driven pervasive monitoring system for post disaster management, which enables the support for an adequate and accurate decision making process. We showed that smartphones can be used for environmental monitoring with a clear and easy to understand representation of gathered data as well as for the connection of rescue workers and the crisis management in a collaborative manor powered by using only a standardized communication protocol (XMPP) and no proprietary software. We introduced the collaboration characteristics of our system, which can be used to support crisis management as well as rescue workers in the handling of emergency situations by exchanging tasks, distributing sensed data to all engaged stakeholders, and by forming joint task forces coupled with flexibility and user friendliness.

Through the implementation and evaluation of a protocol extension named *User Property*, we gathered new insights on the applicability of XMPP for the exchange of measured sensor data through smartphones as terminals instead of using only sensor nodes from WSNs. As a result of the implementation process, we showed that XMPP can be used for management teams that need a global real-time view on gathered data and that XMPP can also be extended for the needs of the crisis management to handle emergency situations with joint task force support.

References

[1] A. M. Townsend and M. L. Moss, “Telecommunications Infrastructure in Disasters: Preparing Cities for Crisis Communications,” Center for Catastrophe Preparedness and Response, New York University, Tech. Rep., April 2005.

[2] R. Klauck, M. Kirsche, J. Gaebler, and S. Schoepke, “Mobile XMPP and Cloud Service Collaboration: An Alliance for Flexible Disaster Management,” in *Proc. of the 7. Int. Conference on Collaborative Computing: Networking, Applications & Worksharing (CollaborateCom 2011)*. IEEE, Nov. 2011.

[3] P. Saint-Andre, “Extensible Messaging and Presence Protocol (XMPP): Core,” IETF, Request for Comment 6120, Mar. 2011. [Online]. Available: http://www.ietf.org/rfc/rfc6120.txt

[4] T. PLC, “Case Study: IPSTAR Helps Restore Cellular Networks in Tsunami Hit Japan,” http://www.ipstar.com/pdf/case_study/CS_IP_restorejp.pdf, 2011.

[5] S. Kim, S. Pakzad, D. E. Culler, J. Demmel, G. Fenves, S. Glaser, and M. Turon, “Health Monitoring of Civil Infrastructures Using Wireless Sensor Networks,” EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2006-121, Oct 2006.

[6] N. Xu, S. Rangwala, and et al, “A Wireless Sensor Network For Structural Monitoring,” in *Proceedings of the ACM Conference on Embedded Networked Sensor Systems*. ACM Press, Nov. 2004, pp. 13–24.

[7] E. Cipollone, F. Cuomo, and A. Abbagnale, “Topology Reconfiguration in IEEE 802.15.4 WPANs for Emergency Management,” in *Proceedings of PerCom Workshops 2010*. IEEE, 2010.

[8] J. Heidemann, F. Silva, C. Intanagonwiwat, R. Govindan, D. Estrin, and D. Ganesan, “Building Efficient Wireless Sensor Networks with Low-Level Naming,” *Proceedings of the 18th ACM Symposium on Operating Systems Principles (SOSP ’01)*, Oct. 2001.

[9] D. Christin and M. Hollick, “We Must Move We Will Move: On Mobile Phones as Sensing Platforms,” *Proceedings of the 10. GI/ITG KuVS Fachgespraech Sensornetze*, 2011.

[10] Y.-S. Kuo, “Project HiJack,” 2011. [Online]. Available: http://www.eecs.umich.edu/~prabal/projects/hijack/

[11] W. A. Wallace and F. DeBalogh, “Decision Support Systems for Disaster Management,” *Public Administration Review*, vol. 45, pp. 134–146, 1985.

[12] F. Luqman and M. Griss, “Overseer: A Mobile Context-Aware Collaboration and Task Management System for Disaster Response,” in *Proceedings of the 2010 Eighth International Conference on Creating, Connecting and Collaborating through Computing*. IEEE Computer Society, 2010, pp. 76–82.

[13] P. Saint-Andre, “XEP-0174: Serverless Messaging,” XMPP Standards Foundation, http://xmpp.org/extensions/xep-0174.html, Standards Track, Nov. 2008.

[14] A. D. Brucker and D. Hutter, “Information Flow in Disaster Management Systems,” in *Proceedings of the International Conference on Availability, Reliability and Security (ARES 2010)*. IEEE Computer Society, 2010, pp. 157–164.

[15] R. Lent, O. H. Abdelrahman, G. Goebil, and E. Gelenbe, “Fast Message Dissemination for Emergency Communications,” in *Proceedings of PerCom Workshops 2010*. IEEE, 2010, pp. 370–375.

[16] HTC America Inc., “HTC HD2 Specifications,” http://www.htc.com/us/products/t-mobile-hd2#tech-specs, 2011.

[17] “XMPP Software,” http://xmpp.org/xmpp-software/, 2011.