# GPS-based solution for tracking and protecting humanitarians in conflict zones

**V. Lanfranchi**
Department of Computer Science, University of Sheffield
v.lanfranchi@sheffield.ac.uk

**N.Noori**
Centre for Integrated Emergency Management (CIEM), University of Agder
saadnouri@gmail.com

**T. Sirbu**
K-Now ltd.
tudor@k-now.co.uk

**ABSTRACT**

The operational environment in which humanitarians operate is unstable and high-risk; when operating in such environments, time becomes a critical factor. Thus, real-time location systems (RTLS) are often deployed in the operational environment to provide awareness of the location of personnel and assets in real-time that would support an informed decision making in the event of responding to emergency. Whilst standard RTLS are very precise, they are not suitable to outdoor spaces; GPS position technology can be used to identify the location of objects and people and to track them. In this paper, first, we present a description of threat scenarios identified based on information from existing security incidents datasets and from interviews with aid workers and security professionals operating in high-risk regions. Second, we describe the implementation of a GPS-based real-time location tracking and alert system for humanitarians operating in conflict zones that supports the identified scenarios.

**Keywords**

Humanitarian aid work, Real-time location systems, security threats, threat detections, situational awareness.

## INTRODUCTION

The operational environment in which humanitarians operate to deliver aid can be described as unstable and high-risk (Duffield, 2012). Daily missions are carried out in highly dynamic and volatile environments. There is a rapid change in the needs and ability to access to various locations, routes and beneficiary groups. Different humanitarian organizations also access various locations and may use different types of cooperation partners and implementing partners for last mile distribution, making the processes difficult to track. In addition, the deep impact of security risks takes its toll on the daily lives of humanitarians (Schreter & Harmer, 2007).

Managing risks and threats in a timely manner is of fundamental importance (Davis, 2017); thus, there is a growing need of integrated tracking systems for situation awareness (Endlsey, 2004) that can enable better informed decisions related to mission planning, risk assessment and response to emergency situations.

Real-Time Location Systems (RTLS) have been often considered in the past as ideal solutions for the identification and tracking of movements of objects and/or people as they happen. They normally consist of fixed location sensors that receive or read a signal from moving sensors attached to people and/or objects and many techniques and systems are available (Liu et al, 2007). This technology has had applications in many fields, such as healthcare, but they do not support tracking in outdoor spaces (Kamel Boulos & Berry, 2012; Notobartolo et al, 2011; Fisher and Monahan, 2012). When needing to geolocate objects and/or individuals in outdoor spaces, GPS-based solutions tend to be adopted. GPS-based solutions have become increasingly popular in the last few years, with the advent of smartphones and smart devices that integrates motion and location sensors, and they are often integrated in Command and Control systems (C2) to support communication and collaboration between operators in an emergency.

Bakopoulos et al. (2011) have suggested a system based on smartphones and GPS to enhance real-time communication between first responders and control rooms. Wahde et al. (2016) developed a smartphone-based solution to improve ambulance dispatch time using GPS data: users can request ambulances using a mobile app; the nearest ambulance is then dispatched based on the user's current location. A similar solution was proposed by Vasic et al. (2014), focused on dynamic relocation of emergency ambulances and by Balamurugan et al (2015) for automatic routing of ambulances using IoT and GPS-enabled smartphones. Smartphone-based tracking solutions are also utilized for increasing safety: for example Moorty and Joseph (2015) developed a solution to improve women's' safety, based on a mobile app that allows its users to see other users and Police authorities in their nearby vicinity in order to alert them in the eventuality that they are in danger. Police forces and first responders often use GPS-based systems to track their vehicles and resources, integrated in commercial GIS systems[1].

In the humanitarian field, recent work has been done to assess the suitability of smartphone technologies to support humanitarian operations, concluding they can be helpful to support efficiency and effectiveness of missions but intensive evaluation is needed to ensure they support the logistics of humanitarian support (Abushaikha & Schumann-Bölsche, 2016). Sandvik et al (2014) have conducted a critical review of the application of new technologies to humanitarian missions, highlighting how sometimes using new digital technologies could change the process that is used and increase the time required to perform a task, therefore impairing the effectiveness of the mission.

The context in which we have been carrying out this study is a European Project iTrack that aims to deliver an intelligent, integrated tracking and threat identification system for humanitarian missions in conflict zones, mainly in the Middle East. The purpose of the iTrack real-time location system is to provide real-time localization capabilities of staff who are on a mission, to allow a control centre to monitor their location and maintain situation awareness. In order to achieve this, staff will have on them smartphones equipped with a Global Positioning System (GPS) that will allow to track their location. Along with the GPS component the app will monitor the staff movements and allow for real-time communication about threats, by enabling reports submissions, including text, images and videos.

[1] https://esri.ca/sites/default/files/resources/cr/EC2_0039_1201_7B_Public_Safety_1.pdf https://www.indracompany.com/sites/default/files/emergency_management_1.pdf

As part of the project we have conducted user studies to understand which are the main possible scenarios and use cases and we have derived requirements to guide the design and development of the solution, using a hybrid design approach, presented in the next section.

## A HYBRID DESIGN APPROACH

A hybrid design approach was chosen to maximise the novel technology advancement with the requirements emerging form desk studies, user interviews and simulation exercises and the requirements and constraints emerging from the ethics and privacy analysis.
A humanitarian mission simulation exercise was run at the beginning of the project iTrack, to derive feedback and requirements. These requirements were crossed with desk research and user interviews to identify a set of highly probable threat scenarios and develop a set of use cases and system users based on the threat scenarios, that were then verified with the original users. In parallel, the technical work packages have been providing details of how the state of the art in tracking and threat identification could be advanced by technical innovation and the Ethics and Privacy work package has been analysing what would be the ethical implications of the innovations. All these contributions were analysed and cross-referenced to ensure the technical innovation would be matching the user requirements and would not be violating any privacy or ethics principles. The outcome of the analysis was a set of uses cases and associated requirements. In the next section we will present the threat scenarios, use cases and requirements.

### Threat scenarios and system use cases for humanitarian aid missions in conflict zone

The scenarios and user requirements were based on data was collected from set of interviews with security experts and aid workers from International NGOs operating in the Middle East Region. In addition, we extracted information about security incidents and attacks carried against humanitarian mission from publically available security incidents repositories: 1) Aid Worker Security Database[2], 2) Aid in Danger project[3] , 3) Security in Numbers Database (SiND)[4], and 4) Uppsala Conflict Data Program[5].
The threat scenarios, identified from the information gathered from the field and historic data, are the following:

#### *Scenario 1: Attack on an aid convoy or warehouse*

Attacks on humanitarian aid convoys are the most frequent type of incidents. The convoys are either attacked whilst travelling (in transit) or whilst docking and unloading at the warehouse. There are different tactics used by terrorist groups or militias or other groups to carry out those attacks, such as aerial bombardments, or an ambush, or shooting. In Figure 1, we show the event chain of an attack targeting an aid convoy with three possible tactics (i.e. aerial bombardment, militants attack-shooting, and sniper shooting). The convoy scenario can show some of the aspect where technology can support the safety of the convoy: tracking technologies can be employed to maintain awareness of the convoys and individuals; alerts and warning mechanisms should be created to support quick reactions; real-time reporting can be useful to gain situational awareness to help rescue and secure the survivors.

[2] https://aidworkersecurity.org
[3] http://www.insecurityinsight.org/aidindanger/
[4] www.insecurityinsight.org/projectshumanitarian.html
[5] http://www.ucdp.uu.se/#/exploratory

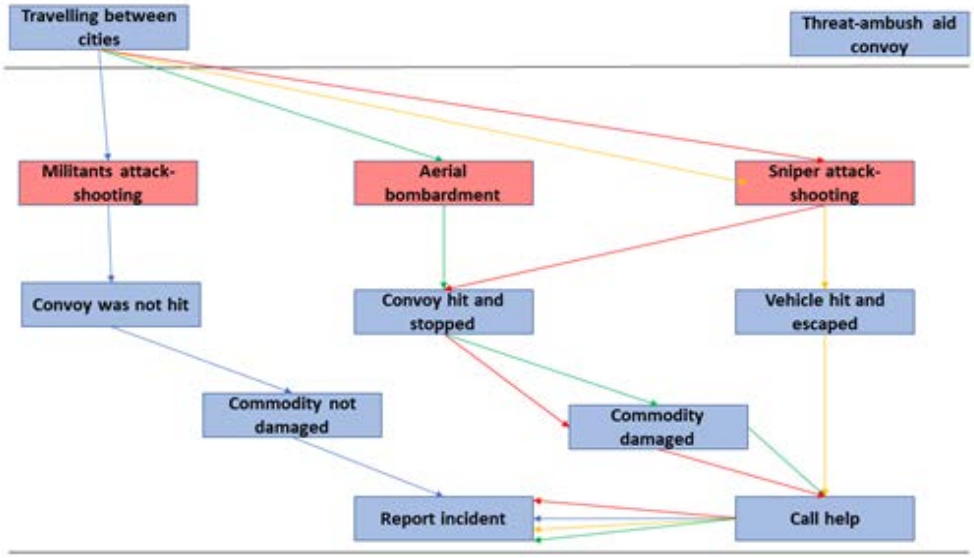


**Figure 1 – Three different types of convoy attack: militants attack, aerial bombardment and sniper attack.**

*Scenario 2: Ambush and kidnapping of aid workers*

Kidnapping is the second most prevalent security threat in security incidents targeting humanitarian aid workers. There are different motivations behind kidnapping aid workers, such as political or financial reasons or just being at the wrong place at the wrong time. In Figure 2, we show the events chain of a kidnapping incident and related actions and outcomes. There have been some kidnapping cases where victims lost their lives (Fisk, 2008) and some they were released after some time or after negotiations (Macharia, 2012). Similar to the previous scenario, technology could support such situations by providing a GPS trace of the victim position and also by providing victims the possibly to alert colleagues in real-time of the danger.

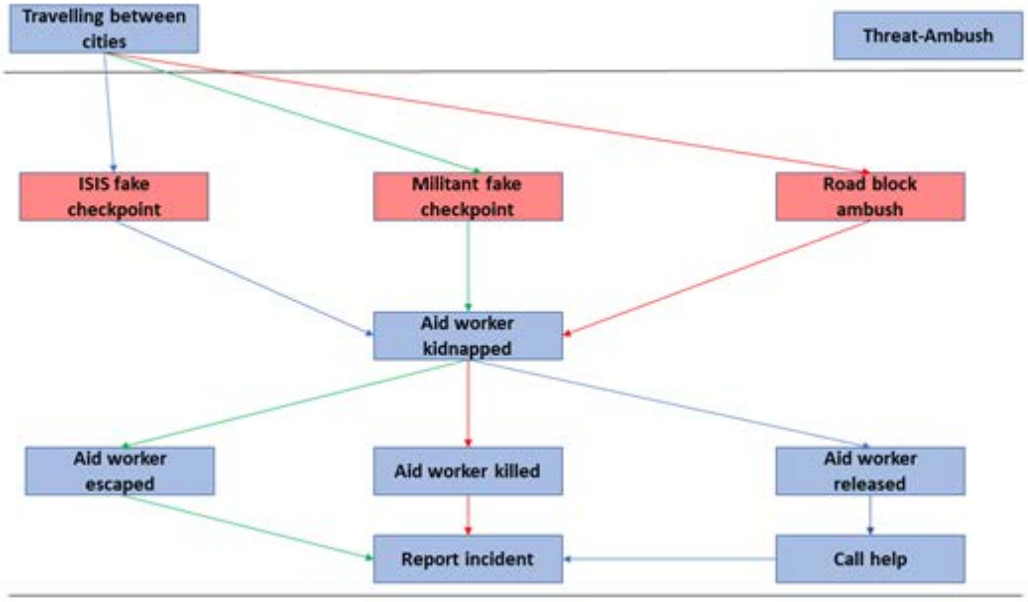


**Figure 2 - Ambush and kidnapping of aid workers – events chain**

*Scenario 3: Shooting aid workers (Individual attacks)*

Aid workers coming under crossfire is another type of prevalent incident (see Figure 3). Often assailants are after money or other valuables or after the cargo of the convoy. Similar to the convoy scenario, a tracking mechanism for both the personnel and the assets can help providing information on the location of the event. The ability to send distress signals to security personnel in real-time combined with information about the location, threat and if possible, images can be very valuable for responding rapidly and achieving the best possible outcomes for involved parties.

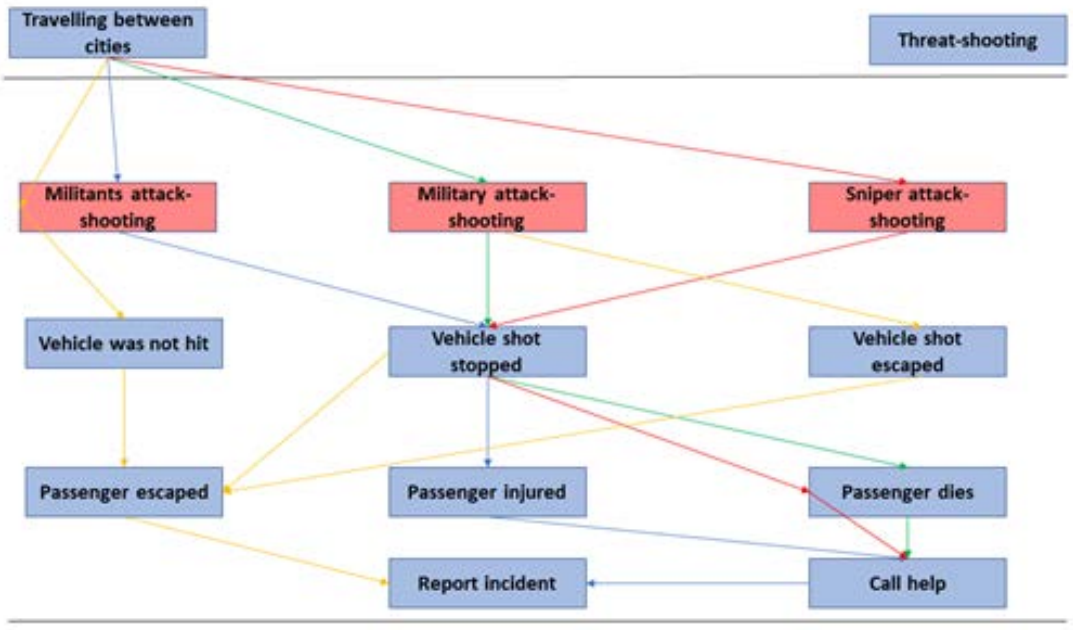


**Figure 3 - Individual attacks - events chain**

After analyzing the data and the scenarios, we have defined a set of actors involved in the aid delivery process: aid workers, missions' leaders, translators, drivers, and mission coordinators (or officers), warehouse managers, distribution managers. In addition, a person that would be manning a command post (or a control room) to perform information collection, analysis and risk assessments and handle the incident response. Usually those tasks are performed by a security officer or sometimes, an information manager or a control room officer.

From the different threat scenarios, we were able to identify the following use cases:

1. *Use case 1*: Users accompanying the convoy should regularly report their location to the command post or control room. The user *(mission leader, aid worker, driver, translator, security officer*) reports his/her position to the main RTLS-server application via a mobile application by selecting the position on a digital map. The operation can be done manually or set to automatic.
2. *Use case 2*: Mission leader and drivers can send information on status and location of the convoy to the command post or control room, where a security officer or information manager collects and analyze the information and continuously assess the risk situation. The information is sent via a mobile application and can contain geographical coordinates and /or images of the surrounding environment.
3. *Use case 3*: Security officer or information manager in the command post or control room are able to track and locate both the personnel and assets in the convoy in real-time. From information provided in *Use case 1*, the RTLS-server application displays the tracked objects (personnel or assets) as pins on a digital map. Security officer or mission controllers can obtain information of tracked objects by selecting the pins.
4. *Use case 4*: Users accompanying the convoy should be able to report the current status of their safety and/or security incidents in their surrounding to the command port or control room. The user can report his/her status via a status or incident report screen in the mobile application to the RTLS-server application. The status report includes information about the threat type (if any) and location of the incident (either current location or a nearby location selected on a digital map).
5. *Use case 5*: In the case of the attack, users accompanying the convoy (e.g. mission leaders or aid workers) should be able to send an immediate alert to the control room or command post. The command room personnel would issue an alert and forward to all persons operating in the area of the threat. The field workers would activate an *emergency/panic button* either by voice command or by shaking the mobile device. Immediately an alert/notification will be forwarded (including information about the tracked object location) to the RTLS-server application system. Then, the command post operators will receive an alert through the RTLS-dashboard application.
6. *Use case 6*: The command post personnel (security officer, information officer, project officer) should be able to receive and view safety and/or incident reports from the convoy in real-time. The users in the convoy send status report via the mobile application to the RTSL-server application. The command post or control room personnel then will receive a notification of the status update from the field and can retrieve the report and view the information (location, threat status, and /or image) via the RTLS-dashboard application. Incidents will be marked read or unread accordingly.
7. *Use case 7*: Users in the convoy will be able to receive security status updates and threat alerts form the command post. The information will be presented to the convoy personnel via two channels, a mobile application and an onboard-dashboard application. A notification window at the applications will be showing the type of threat, location, a timestamp and it may also come attached with information about its

severity. The threats are also presented according to the prioritization that is predefined and also their effective and expiration time. Additionally, all threats are represented in a different way depending on whether they have been validated or not.

8. *Use case 8*: Convoy users should be able to communicate or message their peers (either in the same convoy or other convoy or back at the office or at the command post or at the warehouse). Similarly, users at the NGO office and command post should be able to communicate or message back the personnel on the convoy(s) or project sites (e.g. warehouse or hospital). The message exchanges will be done via a dedicated messaging screen on the mobile application or the system dashboard.

#### REQUIREMENTS

In the following section we will highlight the requirements for the location tracking application for humanitarian mission members. Please note not all requirements are reported here, only those that relates to the scenarios above (i.e. more "common" requirements such as the need for user login are not reported here).

##### Functional Requirements

After analyzing the data and the scenarios, we have defined a set of actors involved in the aid delivery process: aid workers, missions' leaders, translators, drivers, and mission coordinators (or officers), warehouse managers, distribution managers. In addition, a person that would be manning a command post (or a control room) to perform information collection, analyzing and risk assessments and handle the incident response. Usually those tasks are performed by a security officer or sometimes, an information manager or a control room officer.

| **User login/registration** | **Actor** | **Scenario** |
|---|---|---|
| To guarantee security, the mobile application shall store a token received by the iTrack platform during the initial login process. All communication between the mobile application and the iTrack platform besides these initial step should include this token and not other information that if intercepted should reveal the identity of the user (first name, last name, email, username, etc.) | Aid worker, mission leader, driver, mission coordinator, translator | All |
| **Personnel tracking** | | |
| Automatic and manual tracking must be available | Aid worker, mission leader, driver, mission coordinator, translator | All |
| The mobile application must acquire the device's current location data through the embedded GPS and sends the user's location to the iTrack platform. The process is executed | Aid worker, mission leader, driver, | All |

| | | |
|---|---|---|
| automatically without need for user interaction | mission coordinator, translator | |
| The user shall be able to report her/his current location by triggering the location functionality | Aid worker, mission leader, driver, mission coordinator, translator | All |
| The user shall be able to report her/his current location by selecting her/his position on a map displayed by the application. | Aid worker, mission leader, driver, mission coordinator, translator | All |
| The control room can request the user to report her/his current location through an app notification. | Security officer, information manager, a control room officer | All |
| **Personnel alerts** | | |
| The mobile application displays notifications/alerts received by the iTrack platform. Each notification should be marked according to its severity. | Aid worker, mission leader, driver, mission coordinator, translator | All |
| The user shall be able to review the notifications/alerts history list. Each notification should be marked also for its current validity (still valid or expired) | Aid worker, mission leader, driver, mission coordinator, translator | All |
| **Messaging** | | |
| The control room shall be able to send messages to users on the ground, set up groups of users and choose groups to message. | Security officer, information manager, a control room officer | All |

| | | |
|---|---|---|
| Users shall be able to communicate directly with one another or within groups using the app | Aid worker, mission leader, driver, mission coordinator, translator | All |
| **Threats reporting** | | |
| The user must be able to activate a panic button by voice command, automatically reporting geolocation. | Aid worker, mission leader, driver, mission coordinator, translator | All |
| The user shall be able to report a current or forthcoming threat at her/his current location or at a location selected on a map presented by the application. The threat could affect the current user or others. | Aid worker, mission leader, driver, mission coordinator, translator | All |

**Table 1 - Functional requirements for real-time location tracking system for humanitarians**

**Non-Functional Requirements**

| Category | Consolidated Description |
|---|---|
| Usability | Users should be encouraged to use the proposed solution. Therefore, the design and development must be responsive to adapt to the user's screen size and orientation.<br><br>The iTrack solution should be easy to learn, with a small learning curve.<br><br>The iTrack registration and the login process should be easy, requiring that kind of data from the users that will not discourage them from using the proposed solution.<br><br>The iTrack solution should be flexible to adapt to different contexts, increasing the social awareness, so that users deployed in different areas where different frameworks should be respected can use it (a context can be a country for example).<br><br>The iTrack solution should be easily and fast deployable to encourage users to use it. Users tend to prefer a solution that covers their needs and that is easy and quick to deploy. |
| Security | The solution should support communication between the parts of the system and the users that respects all legal constrains per context. All confidentiality information flow should also be protected. |

| | |
|---|---|
| | Encryption should be used (whenever possible) for transmitting information.<br><br>The solution should support a role-based authentication and authorization mechanism. Each user will be assigned a role and will be given unique credentials. Only authorized users will be able to use the solution so as to ensure transparency and security.<br><br>The solution should support data deletion mechanisms to ensure that the data that is no longer required or must be deleted due to restrictions is appropriately destroyed. All ethical and privacy constrains and terms, as well as all individual rights and liberties must be respected by the proposed solution.<br><br>The solution must have mechanisms to store information securely. |
| Confidentiality | The solution must protect any information, especially if personal data is included, from loss, misuse and unauthorized access to the data. |
| Availability/ Accessibility | The solution must be available 24/7. If it is not possible, an offline mode should be considered. |
| Performance | The solution must optimize performance for what regards battery usage and data transmission. |

**Table 2 – Non - Functional requirements for real-time location tracking system for humanitarians**

#### DESIGN AND IMPLEMENTATION

The purpose of the iTrack real-time location system is to maintain situation awareness between personnel on a mission and a control center. The system takes the form of a smartphone app (available for Android and iOS) that starts monitoring the user's location once it detects that the subject has started moving.
The main app functionalities are:

- Tracking: automatic or manual location reporting
- Reporting: threat reporting
- Alarm: panic button
- Communication (internal chat)
- Security

Due to the difficult characteristics of the operational environment, the app is designed and implemented to be used in humanitarian missions, attention has been paid to ensure minimal battery consumption and data traffic and ability to cope with network loss. In the following sections we will present the main app functionalities.

##### Tracking

The app supports automatic and manual location tracking of an individual. When auto-tracking is enabled (enabled by default) the location position is identified through the GPS sensors and other sensors present on the device, is recorded, stored in a secure manner in device's internal memory and sent to the backend immediately, if a network connection is

available, or as soon as a network connection becomes available. To improve battery consumption the location is only monitored when movement is identified – i.e. if the user has been in the same place for the past few hours the location will not change. This reduces drastically the amount of time when the GPS and other sensors are on, reducing the battery impact. As a side effect this also reduces the amount of network data sent as only actual changes in locations are sent to the iTrack platform.
As per the use cases described above, there may be the need for the control room to request the user's position. In this case a pop-up notification is sent through the app asking the user to report their current location by selecting their position on a map (see Figure 4).

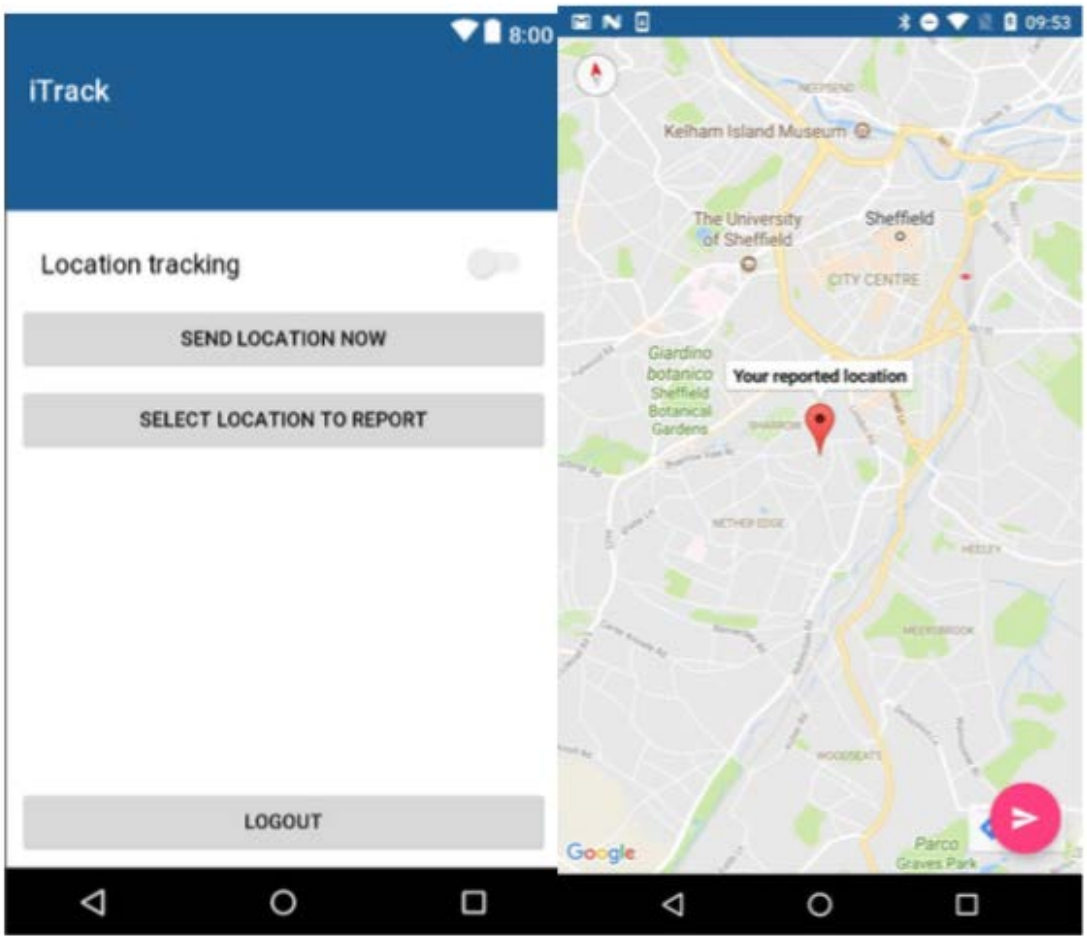


**Figure 4 - Location Reporting**

#### Threat reporting

Given the dangerous nature of the operational setting, it is important for the user to be able to report a current or forthcoming threat (either at their location or at in a different one). To make the interaction easier (given the potential risks) and more efficient users just need to select the threat between a pre-existing list (derived from the user studies performed) and either use the location automatically detected or move the pin to a desired location on the provided map (see Figure 5). The interaction can take place through a single interface, again to maximise efficiency and ease of use. Once submitted this report goes automatically and in real-time to the iTrack platform and will be visible to other users.

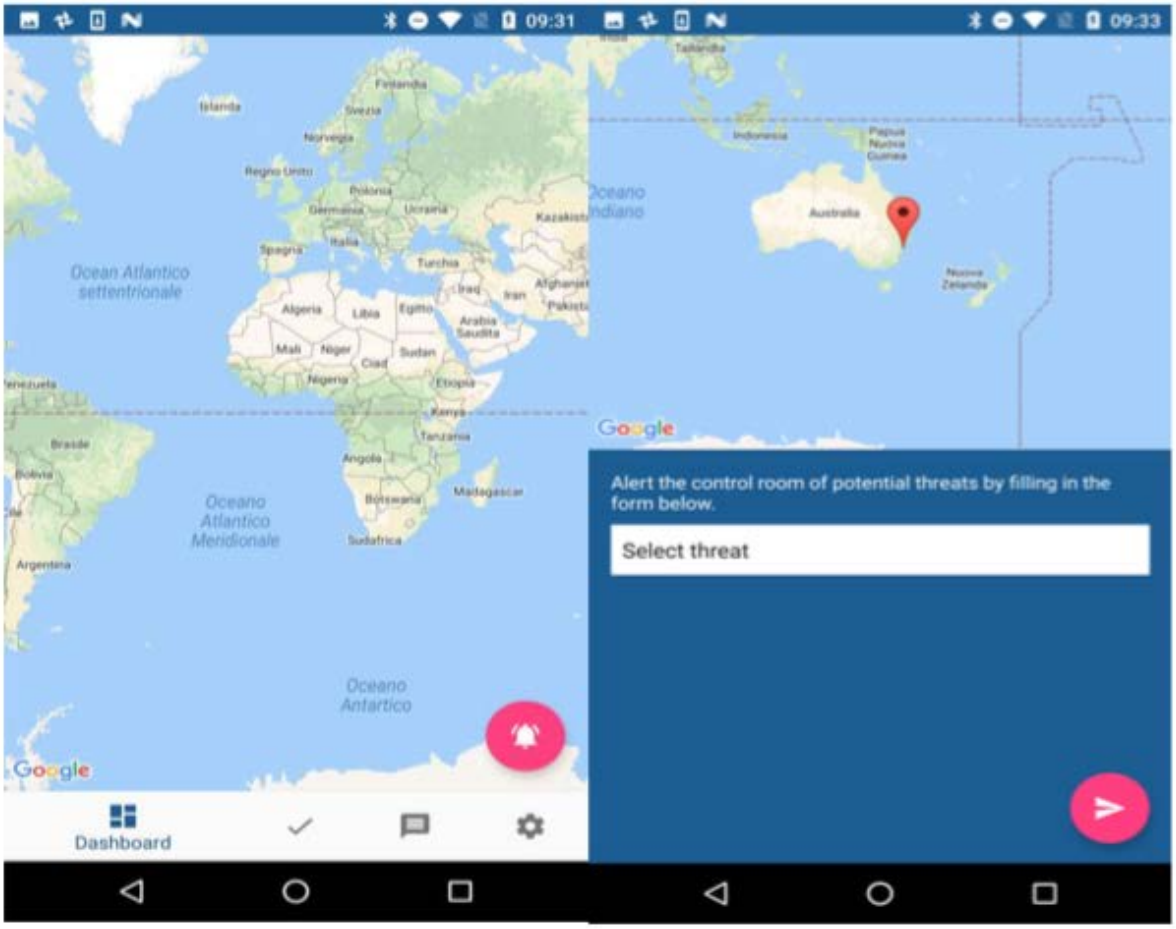


**Figure 5 - Threats reporting**

**Panic button**

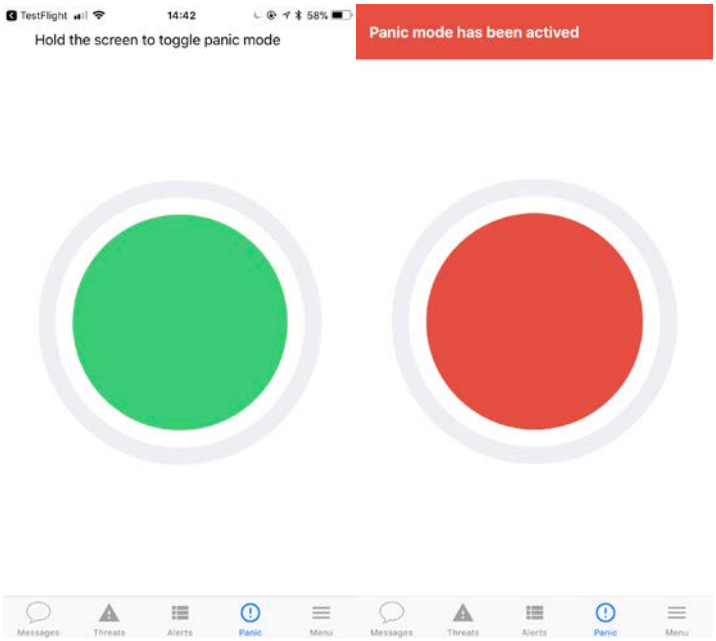


**Figure 6 - Panic button alert**

A panic button (see Figure 6) has been implemented for situations where the safety of on-field workers is at danger. In order to decrease the number of false alarms the user need to

press and hold the panic button for three seconds and only after that the application goes into panic mode. Once panic mode has been activated, the application alerts the control room and automatically switches on the location tracking in real-time if the user did not have it enabled already. For security reasons, the panic mode cannot be disabled until the user has confirmed with the control room that they are safe.

#### Communication

The app contains a messaging feature, enabling control room users to message users on the ground, to set up user groups and choose groups to message. The users on the ground are able to communicate directly with one another and with other groups. Using this feature users are able to Send, View and reply to messages and to store messages as evidence. As part of the messaging feature, notifications can be sent to users (see Figure 7).


**Figure 7 - Notification feed**

#### Security

In order to protect data and individuals' security (i.e. to avoid that a user's location could be intercepted and used for nefarious actions) the system has been built with the highest security standards. The login process is handled using iTrack Keycloak OAuth API. Upon successful authentication, none of the entered credentials are stored and only the returned authentication tokens are stored for further use in communications with iTrack. All communication between the mobile application and the iTrack platform besides these initial step includes this token and no other information that if intercepted should reveal the identity of the user (first name, last name, email, username, etc.). Each token received has an expiration date. When using the application, the token is refreshed so re-authentication is not required.
The application also supports an extra layer of security through encrypted communication. The control room have the ability to ask all devices to use encrypted communication by

enabling this feature from the iTrack's dashboard. Once enabled all payloads are encrypted on the mobile application's side and decrypted once received by the backend server. Encryption is, however, optional and it is decided on a use case basis due to legal reasons (e.g. in case of usage in countries where encryption techniques are illegal).

#### Architecture

The application is based on three major sub-systems; server application, client application (on mobile phones) and databases.
The Android application has been developed natively, using JAVA and XML with based on an MVP architecture. This facilitated a better separation of concerns within the application and it also increased the readability of the project should future work be required. Libraries such as Room, for data persistence, and Retrofit for networking have been used. These are used frequently in the industry and are well tested and documented. Similarly, the iOS application has been built using Swift and the MVVM design pattern for separation of concerns, Realm has been used for data storage and Alamofire for networking.
Both applications rely on a Unix server-side backend which facilitates communication between users, which has been built using Ruby on Rails in an MVC pattern. The communication between the client and server is performed using JSON, however, the transport of data is complex, with backend servers sitting in a DMZ. The following diagram (Figure 8) shows a simplified version of the client-server communications layer:

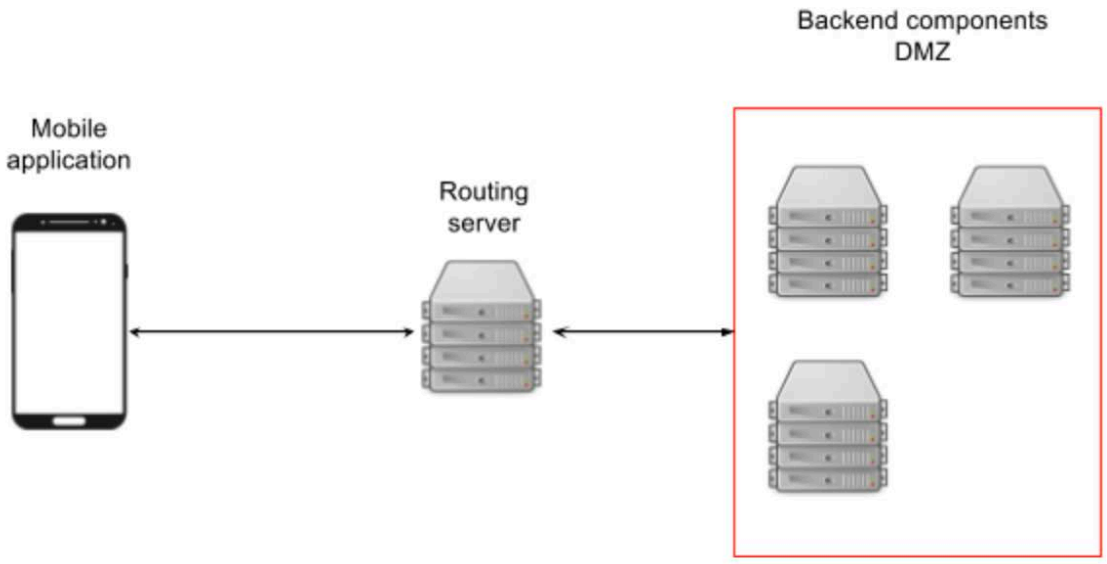


**Figure 8 - Architecture diagram**

The routing server is responsible for verifying requests and redirecting payloads to the correct component which needs to respond to the client. Responses to the mobile application are provided in an asynchronous manner through push notifications.

## CONCLUSIONS AND FUTURE WORK

In this paper we have presented the initial work for designing and implementing a GPS-based system for tracking and protecting humanitarians operating in conflict zones such as the Middle east, Afghanistan, and Africa. The operating settings of such humanitarian missions are high-risk and there is therefore the need to develop new solutions that can support real-time situation awareness both for the humanitarians on the field and for control rooms, in order to: a) protect the humanitarians; b) enable control rooms to use situational awareness to

inform decision-making. Given the complicated settings, the project has carried out an extensive phase of hybrid design, where requirements, threat scenarios and use cases derived from simulations, user interviews and desk research were crossed with technical innovations suggested by the technical partners and with ethics and privacy considerations. A first version of the application has now been implemented and it's in the process of integrating with other components to provide a global situation awareness platform.

In order to test the app in action, the project is running an evaluation of the integrated platform with Ngo users. The evaluation will take place in Delft and will last for one week, during which the different scenarios will be simulated and feedback collected from observers and participants on the suitability of the app to the specific scenarios. Moreover during the week usability tests will be run, to assess interface and features and provide feedback for the next phase.
Future work will concern the implementation of the evaluation feedback plus enhancements to the app usability and functionalities. One example is the current implementation of the panic button: ideally a user should be able to trigger the panic button by voice command. Unfortunately, this functionality is not available in Android therefore its implementation has been postponed for the moment. After the evaluation we will revisit the requirement and, if considered fundamental, it will be implemented for iOS platform. Another future development could be linked to health sensors: at the beginning of the project we investigated the possibility of a mobile application for wearable devices that could detect dangerous situation by looking at users' vital signs during a mission. When discussed with real users, this has raised serious privacy concerns, which rendered the feature impractical and further research and development has not been carried out but future work could consider this.

## ACKNOWLEDGMENTS

This work has been carried out as part of the iTrack project. The iTrack project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700510.

## REFERENCES

Abushaikha, I., Schumann-Bölsche, D. (2016). Mobile Phones: Established Technologies for Innovative Humanitarian Logistics Concepts, Procedia Engineering, Volume 159.

Pages 191-198, Bakopoulos, M., Tsekeridou, S., Giannaka, E., Tan, Z.-H., & Prasad, R. (2011). Command & Control: Information Merging, Selective Visualization and Decision Support for Emergency Handling. *Proceedings of ISCRAM 2011*, Lisbon, Portugal

Balamurugan, A., Navin Siva Kuma, G., Raj Thilak, S., Selvakumar, P. (2015) Automated Emergency System in Ambulance to Control Traffic Signals using IoT. International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 4 Issue 4..

Davis, J. et al. (2017). Security to go: a security risk management toolkit for humanitarian aid agencies. *EISF Publication*. https://www.eisf.eu/library/security-to-go-a-risk-management-toolkit-for-humanitarian-aid-agencies/

Duffield, M. (2012). Challenging environments: Danger, resilience and the aid industry. *Security Dialogue*, 43(5), 475-492.

Endsley, M.R. (2004). Situation awareness: Progress and directions. *In S. Banbury & S. Tremblay (Eds.), A cognitive approach to situation awareness: Theory and application (pp. 317–341)*. Aldershot, UK: Ashgate Publishing.

Fisher, J.A., Monahan, T. (2012). Evaluation of real-time location systems in their hospital contexts. International Journal of Medical Informatics,Volume 81, Issue 10, Pages 705-712, ISSN 1386-5056, https://doi.org/10.1016/j.ijmedinf.2012.07.001.

Fisk, R. (2008). The tragic last moments of Margaret Hassan. *The Independent*. http://www.independent.co.uk/voices/commentators/fisk/the-tragic-last-moments-of-margaret-hassan-887135.html. Accessed on 19/01/2018/

Kamel Boulos, M. N., & Berry, G. (2012). Real-time locating systems (RTLS) in healthcare: a condensed primer. *International Journal of Health Geographics*, 11, 25. http://doi.org/10.1186/1476-072X-11-25

Liu, H., Darabi, H., Banerjee, P. and Liu, J. (2007). Survey of Wireless Indoor Positioning Techniques and Systems. *Trans. Sys. Man Cyber Part C 37, 6* (November 2007), 1067-1080. DOI=http://dx.doi.org/10.1109/TSMCC.2007.905750

Macharia, J. (2012). Gunmen kidnap aid workers from Kenya camp, driver killed. *Reuters*. https://www.reuters.com/article/us-kenya-kidnap/gunmen-kidnap-aid-workers-from-kenya-camp-driver-killed-idUSBRE85S0KN20120629

Moorthy, A, Joseph M. (2015). Emergency App Using Real Time GPS Tracking. Online: *International Journal of Innovative Research in Computer and Communication Engineering.*

Notobartolo, C., Ma, W. and D'Souza, I. (2011). Real-Time Location Systems for Hospital Emergency Response. *IT Professional*, vol. 13, no. , pp. 37-43. doi:10.1109/MITP.2011.31

Sandvik, K., Gabrielsen Jumbert, M., Karlsrud, J., & Kaufmann, M. (2014). Humanitarian technology: A critical research agenda. *International Review of the Red Cross, 96*(893), 219-242. doi:10.1017/S1816383114000344

Schreter, L.; Harmer, A. (2013) Delivering aid in highly insecure environments. A critical review of the literature, 2007-2012. *Humanitarian Outcomes Ltd.*, London, UK 70 pp.

Vasic, C., Predic, B., Rancic, D., Spalevic, P., Avdić, D. (2014). Dynamic Relocation of Emergency Ambulance Vehicles Using the AVL Component of the GPS/GPRS Tracking System. *Acta Polytechnica Hungarica*. 11. 39-59.

Wadhe P., Pandharkar R., Raut R., Modi D. (2016). Emergency Service using GPS Tracking. Online. *International Journal of Advanced Research in Computer and Communication Engineering*