SafeTrekker: towards privacy-aware ubiquitous safety assistants for mountain excursions

Claudio Bettini and
Sergio Mascetti
EveryWare Lab
University of Milan, Italy
{claudio.bettini,sergio.mascetti}@unimi.it

Abstract

We present preliminary work on the design of a ubiquitous service that could support the participants of outdoor excursions, like trekkers, climbers or ski-mountaineers in identifying potentially dangerous situations as well as to alert with useful information the rescue teams in case of critical conditions. The system is based on a form of privacy preserving crowdsourcing: precise location and sensor-based information is acquired real-time by a trusted system component and can be used in case of emergency, while an anonymized dataset of each excursion is processed by a central component to create a model of "normal" situations. Together with a model of "potentially dangerous" situations created with specific domain knowledge, the system offers a decision support service that can also operate offline on the mobile device of the users.

Author Keywords

context awareness, data privacy, rescue system, anomaly detection, activity monitoring

ACM Classification Keywords

J.3 [Computer Applications]: Life and medical Sciences

Introduction

On April 20 2016, a 27 years old expert ski-mountaineer left his house in a Italian village in the central Alps for a solo daily excursion on a mountain in his valley. He did not return home. Rescue teams as well as many volunteers looked for him for five days. Helicopters could not fly for bad weather conditions. He was never found.

Mountain activities are potentially dangerous for sudden changes of weather conditions, orienteering problems, minor or major accidents that may happen even to the more experienced. In this contribution we present the design of the SafeTrekker system that is aimed at promptly warning rescue teams and provide them crucial information.

The overall idea of the SafeTrekker system is the following: a smartphone application collects contextual information acquired from the on-board sensors including GPS and inertial sensors as well as from external ones, like wristbands, chest straps, and sensors embedded in technical garments and footware that can measure acceleration, pressure, and temperature. User trajectory, vital parameters and in general all sensor data are stored and processed on the smartphone in order to detect anomalies and raise warnings. Consider the following example: during the excursion a fall is detected from inertial sensors and a pattern in heart rate frequency is also observed. After that, no significant user movement is detected for 30 seconds. In order to avoid false alarms, before sending an alert signal, the application starts beeping; if the excursionist does not intervene, after one minute a warning message is sent to a server, together with current location, fall data and vital parameter. The server can then forward the warning to a rescue team.

Unfortunately, as discussed in the following, it can be the case that the smartphone cannot contact the server due to lack of connection. For this reason a critical situations should also be detected on the server, even in absence of communication from the client. Consider the following example: the night before the hike, the excursionist plans the excursion and inserts its data, including starting point, destination and path. While walking, every 20 minutes the application sends to the server the excursionist's position. After walking for two hours, the excursionist reaches an area where no connection is available, and hence no update can be sent to the server. The server knows that, after approximately one hour of walk, the excursionist should reach a region where connection is available again. However, after three hours no message is received. Then, also considering that severe weather conditions are reported in the area, the server raises a warning to a designated person (or rescue team), which includes all available data, in particular the last known position, vital parameters and the expected trajectory and destination.

The development of the SafeTrekker system poses a number of challenges. First, in order to detect a critical situation it is necessary to have a model of "normal" and "potentially dangerous" situations. False positives must be carefully limited. At communication level, the challenge is to provide a reliable service despite network connection is not always available. Last, but not least, there are privacy risks involved with sending health (and location) information to a potentially untrusted server. In this contribution we briefly describe how we intend to tackle these challenges.

Related Work

There are several dedicated devices, smartphone apps and related services that exploit GPS receivers to store position and trajectories. Most of them store the trajectories locally for later upload to a server and possible sharing with other users (See, for example, http://www.shareyouradventure.com/). Shared trajectories are often used as a reference during an excursion, as well as while planning the excursion. Existing software solutions support this feature, as well as reporting live location (see e.g., http://www.viewranger.com/). Smartphones, smartwatches as well as a number of body-worn devices offer monitoring of well-being and health related parameters that hikers, and more generally sport fans, use mostly for personal training monitoring.

When excursions take place in the snow additional devices are involved: avalanche beacons tightened to the chest as well as passive trasponders (RECCO) sewn into the clothing. However, their purpose is only to guide rescuers that are in close proximity (some beacons also report vital signs). None of them has the goal or the ability for remote communication.

The research literature on this subject is limited. A system for location aware rescue coordination in mountain territory has been proposed in [3] reporting also experimental results performed in a mountain area in the northwest of the UK with the collaboration of a mountain rescue team. The focus of that work was on networking aspects related to quickly alerting and coordinating rescue team members.

In our work we would like to complement the utility of location information for the rescue operations with an intelligent analysis of data that may lead to more informed decisions and avoid some of the accidents.

Finally, uploading location information as well as health related information to untrusted servers may expose subjects to privacy risks. Despite location related to mountain excursions is usually not sensitive, health related data may be, and a privacy preserving solution is desirable. A survey of privacy risks in pervasive computing and possible mitigating solutions is presented in [1].

Modeling normal and abnormal situations

We model a potentially dangerous situation as a particular combination of observed events and conditions. Hence, a basic component is the ability to recognize relevant events. While some of them may be straightforwardly obtained, like weather conditions or actual and expected position, events like a fall or physical stress have to be detected by low level analysis of sensor data. In the first case accelerometers and pressure sensors are critical, while heart rate, heart rate variability, peripheral skin temperature, and Galvanic skin response may be used for the second. State of the art techniques are mostly based on data-driven approaches [2], usually involving the collection of a sufficiently large labeled dataset, and the training of a machine learning algorithm on that dataset in order to recognise new events. Despite specific systems already exist (e.g., Philips lifeline products to detect elderly falls), our algorithms need to address multiple and diverse events and need specific tuning for the mountain environment. In order for this approach to be successful *a crowdsourcing* method of data collection is needed to acquire a sufficiently large dataset for the statistical models to be robust and hence the recognition of events to be reliable.

A second challenging task is for the system to decide if the recognition of a certain combination of events and conditions is indeed "potentially dangerous". This task is related to the problem known in the literature as *anomaly detection* [5] or *abnormal activity recognition* [2], in the security and e-health domains, respectively. Considering the complexity of this task we plan to initially take a knowledge-based approach in which the combination patterns are built from experts knowledge, taking also into account user profiles since, for example, age and level of training may be very relevant. However, when the globally collected data grows to a statistically significant size we plan to experiment also

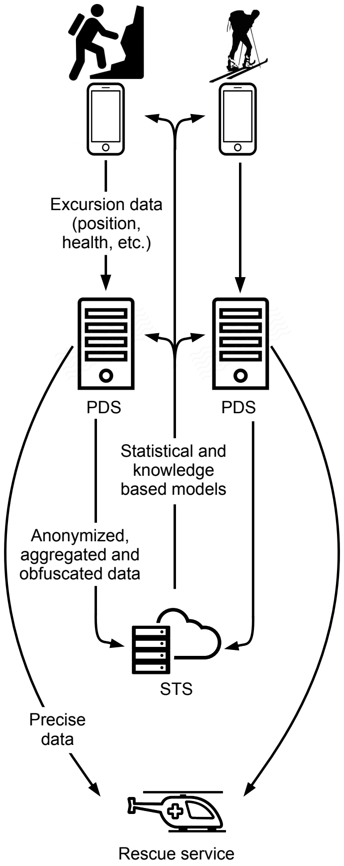

Figure 1: System Architecture

the dual approach, using machine learning to model *normal* situations, and generate warnings when significant deviations are observed. Note that the two approaches are not alternative but complementary.

In order to mitigate the problem of false warnings (very relevant for the second approach), we plan to follow the idea of filtering illustrated in [4]. A set of semantic rules defines explainable scenarios, i.e., scenarios in which detected anomalies are actually normal and should not generate warnings (e.g., physical stress during a competition, no communication due to previously observed low level of batteries).

Privacy-Preserving System Architecture

A common problem in the deploy of privacy-aware services is to find a trade-off between data utility and privacy preservation. In the SafeTrekker system we need to distinguish two different roles of data: in case of a possible dangerous situation, data utility is predominant and all relevant information should be sent to rescue team including excursionist identity, trajectory, health status, etc.

In all other situations (e.g., to monitor the user during a trek or to crowdsource the statistical model) privacy should be protected. We intend to adopt a solution based on a privacy-preserving architecture (see Figure 1): the client communicates with a Personal Data Service (PDS), that collects and processes data from a single user. One of the main functions of the PDS is to monitor user updates and raise warnings. To achieve this the PDS uses information crowdsourced from other users by the SafeTrekker Server (STS), which is shared by all users. Each user contributes to the crowdsourcing through the PDS that transmits to STS anonymized, aggregated and obfuscated information.

Communication

The detailed design of the system network communication is beyond the scope of this paper. However, some ideas can be sketched. Despite many mountain areas (e.g., in the Alps) are covered by GSM signal and coverage is being extended, there are certainly many areas that are not. The most frequent situation in the Alps is to find mixed conditions, i.e., along the same route there are covered as well as uncovered areas. This call for a system that buffers data on the client that are then uploaded at the first connectivity opportunity.

Regarding the location/context updates by the client, we envision a best effort system that, similarly to what proposed in [3], identifies the best available channel (3G over GSM, SMS, or WiFi). WiFi will be probably limited to the case of dedicated hotspots (possibly connected by satellite communication) installed in mountain refuges or in strategic locations for safety reasons. Since in some cases the use of SMS can be charged, it should be tuned according to user's preferences, possibly using SMS only when no other connection is available and for the most important messages only (e.g., a warning).

Conclusions

Most outdoor mountain activities involve an intrinsic risk for the excursionist. We believe that the use of sensing technology coupled with statistical analysis based on crowdsourced data may enable innovative services for the early identification of risky situations and for providing crucial information to the rescue team. The envisioned *SafeTrekker* system is designed to address three main challenges that we identified: detection of abnormal situations, communication through unreliable connections, and user's privacy preservation.

REFERENCES

1. Claudio Bettini and Daniele Riboni. 2015. Privacy protection in pervasive systems: State of the art and technical challenges. *Pervasive and Mobile Computing* 17, PB (2015), 159–174. DOI: http://dx.doi.org/10.1016/j.pmcj.2014.09.010

2. Liming Chen, Jesse Hoey, Chris D. Nugent, Diane J. Cook, and Zhiwen Yu. 2012. Sensor-based activity recognition. *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews* 42, 6 (2012), 790–808. DOI: http://dx.doi.org/10.1109/TSMCC.2012.2198883

3. Panagiotis Georgopoulos, Ben McCarthy, and Christopher Edwards. 2010. Location Awareness Rescue System: Support for Mountain Rescue Teams. In *2010 Ninth IEEE International Symposium on Network Computing and Applications*. IEEE, 243–246. DOI:http://dx.doi.org/10.1109/NCA.2010.44

4. Enamul Hoque, Robert F. Dickerson, Sarah M. Preum, Mark Hanson, Adam Barth, and John A. Stankovic. 2015. Holmes: A Comprehensive Anomaly Detection System for Daily In-home Activities. In *2015 International Conference on Distributed Computing in Sensor Systems*. IEEE, 40–51. DOI: http://dx.doi.org/10.1109/DCOSS.2015.20

5. Rupali Kandhari, Varun Chandola, Arindam Banerjee, Vipin Kumar, and Rupali Kandhari. 2009. Anomaly detection. *Comput. Surveys* 41, 3 (2009), 1–6. DOI: http://dx.doi.org/10.1145/1541880.1541882