SIREN – A Network Infrastructure for Emergencies

by Ioannis Askoxylakis, Paschalis Papagrigoriou, Diomedes Kastanis, Panos Karampelas, and George Spanoudakis

The SIREN project (Secure, Interoperable, UAV-assisted, Rapid Emergency Deployment Communication and sensing Infrastructure) implements a secure, distributed, open, self-configured and emergency-aware network and service platform for automated, secure and dependable support of multiple mission critical applications in highly demanding and dynamic emergency environments.

In emergencies or disasters a key support factor for situation awareness, decision making and response is to provide a secure and dependable network infrastructure that aggregates connectivity over all available heterogeneous wireless broadband access technologies, including those employed for commercial network access. The infrastructure must be able to adapt to mission critical application requirements and to enable immediate and robust communications among command centres, rescue workers and the affected population.

Existing civil protection and emergency response systems do not take advantage of commercial network infrastructures, since they are not typically designed to be relied upon in the event of major extrinsic failures and are thus deemed potentially unfit to sustain the requirement of massive mission critical operations [1].

SIREN federates two existing platforms, REDComm and SecoCard, and develops a secure and dependable overlay network and service infrastructure that hides the heterogeneity of the underlying networks and supports the multiplicity of communication needs across different types of users and user groups in emergencies.

REDComm, which stands for Rapid Emergency Deployment Communication, is a trailer based communication node that utilizes several communication technologies in order to provide multiple communication services in emergency and crisis situations [2]. Such services include not only traditional communications of emergency response authorities, but also modern services to these authorities such as live video streaming and multimedia content sharing as well as public addressing and victim communication. A REDComm node includes a hybrid power source based on both renewable and non-renewable energy generators and batteries to provide electric autonomy. A pneumatic telescopic mast is installed to support communication antennas providing mobility and increased coverage range.

One or more REDComm nodes can be easily and quickly deployed anywhere to provide communication services. The usage of mesh networking forms a redundant, seamless, self-healing, backbone network that is able to route communication traffic dynamically over the most appropriate path and technology. Eight REDComm nodes have been designed and implemented by FORTH-ICS and will be evaluated in drills and real-life situations with the Hellenic emergency response authorities such as police, fire department, the national emergency aid center and the Region of Crete that participate in the REDComm project [1].

SecoCard is an intelligent - and at the same time highly secure - external token with its own screen and capacitive touch keypad, which communicates with a non-modified smartphone or tablet over Bluetooth or WiFi and runs all the security applications, while the smartphone or the tablet, respectively, just provides connectivity and their normal unshielded applications [3]. The dedicated hardware is not much larger than a few credit or key cards stacked on one another, and can operate with practically every new smartphone and tablet model being sold today or unveiled in the future by the mobile industry.

With the federation of REDComm and SecoCard, SIREN implements an integrated comprehensive security architecture based on dedicated security mechanisms, taking into

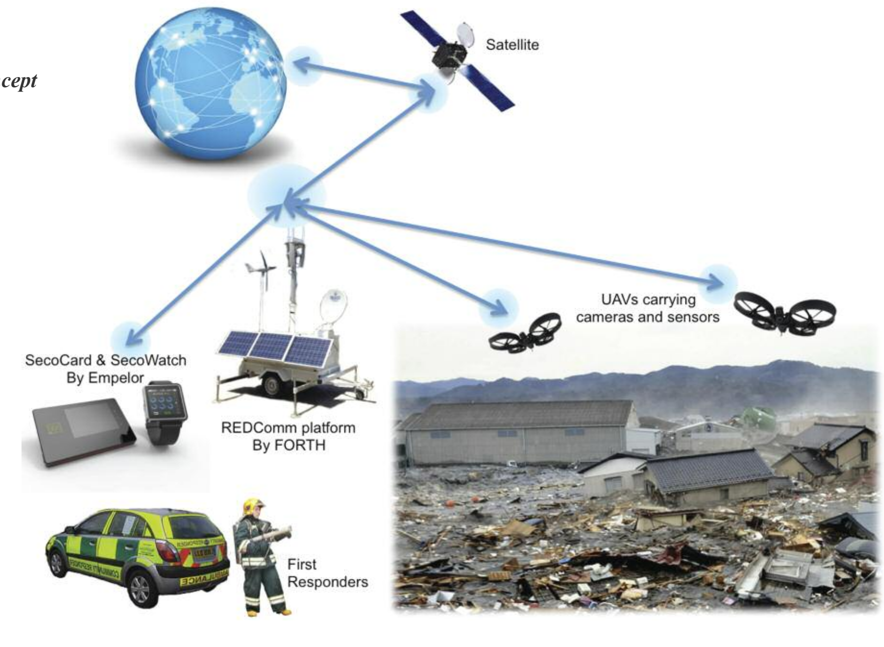
Satellite
UAVs carrying cameras and sensors
SecoCard & SecoWatch By Empelor
REDComm platform By FORTH
First Responders

Figure 1: The SIREN concept

account cross-layer considerations and multi-operator emergency environments. In terms of cryptographic functions, SIREN implements a family of key agreement methods with particular focus on password-based, weak to strong authentication associated with several multiparty contributory key agreement schemes.

SIREN is also inspired by the opportunities and threats to the security of individuals owing to the convergence of the cyber and physical world, especially in urban environments. Increasingly within such environments, the everyday life of people takes place around cyber-physical objects that are becoming smarter and more inter-connected. This creates the possibility of continual acquisition, correlation and analysis of information that can improve citizen security and safety. It is, for example, possible to combine surveillance camera information with human physiological data and incident alerts created by mobile phone users in order to establish the occurrence of incidents and reacting to them on the spot and in a personalized manner. At the same time, the closer coupling of the physical world with cyber systems creates new threats and risks for people. Access to the location of individual (or groups of) people may, for instance, trigger targeted actions against them, and mass surveillance can compromise the privacy of individuals. Risks and threats may also increase significantly if functions, critical for the security and safety of citizens, depend on a cyber-physical infrastructure and Smart City applications that are not well protected against attacks (e.g., jamming communications between emergency responders).

Enhancing these opportunities and managing the associated risks can be based on SIREN, which in the future will enable the development and runtime operation and management of different Cyber-Physical and participatory sensing applications, including aerial unmanned vehicles (drones), supporting the acquisition and sharing of security related information through the use of SIREN infrastructure. The SIREN platform will enable the development and runtime operation and management of such applications by offering an open and extensible set of integrated basic capabilities, with particular focus on emergency response and crisis management.

Links:
http://www.redcomm-project.eu
http://redcomm-project.eu/
http://www.secocard.ch/

References:

[1] A. Miaoudakis et al.: "Communications in Emergency and Crisis Situations", Distributed, Ambient, and Pervasive Interactions, Springer International Publishing, 555-565, 2014.
[2] I. Askoxylakis et al.: "A Rapid Emergency Deployment Mobile Communication Node", IEEE Computer-Aided Modeling Analysis and Design of Communication Links and Networks (CAMAD), 2014
[3] P. Papagrigoriou, et al.: "Discrete Hardware Apparatus and Method for Mobile Application and Communication Security", Human Aspects of Information Security, Privacy, and Trust. Springer International Publishing, 102-112, 2014.

Please contact:

Ioannis Askoxylakis, FORTH-ICS, Greece
E-mail: asko@ics.forth.gr

MYVISITPLANNER: Cloud-based Recommender for Personalized Tourism

by Ioannis Refanidis and Christos Emmanouilidis

Following the masses is one way of being a tourist. But the modern creative tourist is eager to forge a personal trail. Tailoring an itinerary to individual desires has always been the realm of highly specialized tour operators. Context-aware computing and recommender systems make it possible to offer personalized services in tourism. MYVISITPLANNER is a cloud-based service employing a recommender engine to offer personalized suggestions for tour activities and a planning tool to create appropriate tour itineraries. Recommendations are offered on the basis of a hybrid approach that takes into account both a taxonomy of possible activities, as well as user preferences and past recommendations, thus offering recommendations tailored to the visit profile [1].

A creative tourist is a traveller who is not simply satisfied with visiting TOP10 attractions but seeks to enjoy a personal experience when visiting a place. Whether the visit involves outdoors activities off the beaten track or certain cultural preferences, an individual traveller is often a more demanding tourist but also one that intends to better blend with local culture and people when travelling. The personalization of the tourist product can now be achieved by advanced computer-assisted tourism services.

Visitors may obtain: (i) activity recommendations contextualized by the time, duration and area of a visit, as well as by personal preferences and visit profiling; and (ii) tour itineraries created by a world-class scheduler, on the basis of the offered recommendations, while taking into account individual visitor calendar constraints and scheduling preferences, as well as available time for the visit. Activity providers can benefit from having their services enlisted and included in the itineraries recommendations (Figure 1).
While many recommender systems base their recommendations on either distance - based retrieval principles or collaborative filtering performed over past evaluations, the MYVISITPLANNER cloud-service employs a hybrid recommender engine the fuses both approaches and is thus able to offer relevant recommendations even in the absence of historical data and past user evaluations feedback (Figure 2).

In the absence of past visit data, recommendations are based on a dedicated activities ontology. Specifically, a new visit profile is mapped on the activities ontology and based on a dedicated distance function, relevant recommendations are retrieved. Past user evaluations are handled by hybrid clustering performed over the cloud employing the Mahout cloud-oriented machine learning library. Specific care is taken so that privacy-preserving data management is involved: visit profiling is preferred instead of user profiling, avoiding handling sensitive private data. The user has the option of editing the recommendations by removing activi-