SHORT TERM SCIENTIFIC MISSION (STSM)
SCIENTIFIC REPORT

This report is submitted for approval by the STSM applicant to the STSM coordinator

Action number: CA15127 - 37637
STSM title: Secured P2P adhoc wireless network for resilience infrastructureless communication
STSM start and end date: 02/07/2017 to 08/07/2017
Grantee name: Dr. Panayiotis Kolios

PURPOSE OF THE STSM:

The aim of this STSM is to investigate how to improve resiliences, when the communication infrastructure fails, using adhoc wireless networks formed by personal mobile devices found in proximity of each other. A prototype of this technology has been developed at the KIOS Research Center of the University of Cyprus and the proposed STSM aims to further advance this prototype by investigating P2P technology that could improve the resilience of information sent through the proximal adhoc network. The Network Architectures and Services, of the Department of Informatics, Technical University of Munich has ample expertise in this area and the collaboration will greatly benefit both parties since there are complementary skills from both parties.

DESCRIPTION OF WORK CARRIED OUT DURING THE STSMS

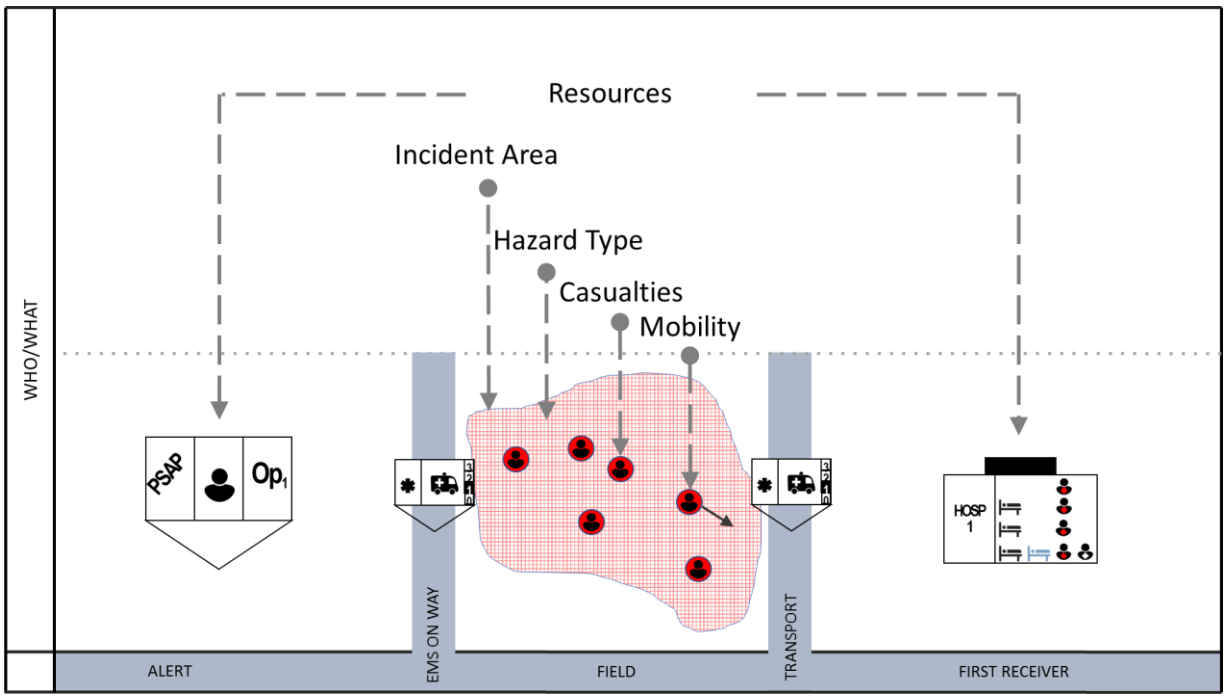
On the 3rd of July, a presentation was given by Panayiotis Kolios on the work conducted by the home institution (KIOS CoE, University of Cyprus) on Critical Infrastructure Systems. In its first part, the talk covered general research topics that are under investigation by the Center while in the second part the specific challenges of secured adhoc communication for emergency management were reviewed. From this initial interaction with the group of the host institution (Network Architectures and Services at the Department of Informatics at TUM), a first key challenge has emerged, namely the development of benchmark disaster/emergency scenarios which can be used to evaluate existing and future proposed solutions. We identified as a good source of information for these challenge, the first-responder end-users that are currently in collaboration with the KIOS CoE that are actively participating in large exercises and from which scenarios and scripts can be used to developed the benchmarks. Moreover, literature review has been done through the duration of the visit and a very relevant book, namely “The structure and dynamics of Cities: Urban Data Analysis and Theoretical Modeling” by Marc Barthelemy has been identified as a good starting point for modeling the suggested benchmarks after the scenarios are set. Panayiotis Kolios will lead future work on this challenge that includes the following benchmarking scenarios and characteristics.

Benchmarking scenarios and characteristics:
Emergency management is split into a sequence of phases (including detection, decision, alarm and response/evacuation, recovery) in which specific operations take place. The better these phases are handled (increasingly through innovative Information and Communication Technologies - ICT) the better they can be planned and interlinked, which eventually leads to better response efficiency and significantly reduced evacuation times. ICT tools enable mutual visibility, timely information exchange, early situational awareness, and intelligent decision support).

However, to date, there is no standardized way of creating emergency scenarios to test against for the plethora of existing/envisioned ICT tools. This is attributed primarily to the fact that data on the structure and dynamics of both urban and rural areas has been absent to date. The increasing availability of data including infrastructure networks, spatial and social organization, as well as individual mobility patterns, has helped create quantitative descriptions of these areas and build models that can be used for scenario generation. With this models at hand, correct estimates can be made on information related to, for example:

1. Incident Area: Field location (Urban/Rural, Residential/Industrial), Size
2. Hazard Type: Natural (Flood/Fire/Earthquake), Technological (Oil/chemical leak), Man-made (CBRN)
3. Causualties: Location, name, gender, age, injury, mechanism of injury, priority as set by PSAP
4. Victim/Bystander Mobility: Stranded, Limited, Frantic
5. Resources: Hospital Info (Specialists, bed availability), EMS Availability (Numbers, capacity, status)

The figure below shows how such data, that can be extracted from representative models for the case of benchamarking, falls in place for the different phases of emergency management.



With these benchmarking scenarios in place, ProximAid (other complementary solutions) will be better evaluated under varying characteristics of device availability, mobility, usage behavior, contextual information and a variety of other settings. The analysis of these results will better demonstrate the impact of each of the proposed solutions.

Throughout the days that followed, daily discussions were made on the security aspects of the developed mobile adhoc emergency response network and use-case scenarios were drafted on the security aspects, including integrity and confidentiality, of alert messages send between stranded survivors and first responders. The discussions on this topic, which was the main goal of the STSM, resulted to valuable insights on how to best design a secured P2P wireless adhoc network based on the ProximAid technology. Indicatively, a number of parameters need to be considered when introducting security mechanisms in services running on top of resource-constrainted computing devices. Firstly, the additional processing overhead for operations like verification and encryption consume more resources. Moreover, there is additional network overhead associated with the exchange of information for establishing secured communication, including public keys and dedicated sessions, that increases communication delay and energy consumption. Clearly, these factors affect performance and user experience. Since mobile devices

have limited battery capacity, resource-demanding protocols will result in limited useability and decreasing network longevity. Hence, we have identified proper mechanisms for achieving the necessary security measures when data is to send from victims to first responders and the other way around as well. Specifically, for data sent from victims to first responders, both confidentiality and integrity is needed in order to avoid, among other things, selfish behavior and man-in-the-middle attacks, respectively. For communication from first responders to victims, consisting mainly of broadcasted information of general interest, the integrity of the data needs to be ensured while confidentiality is less important.

Hence, a single encryption key can be distributed when downloading the ProximAid app to be used for commicating data from victims to first responders while simpler hash values can be used to ensure just the integrity of the data communicated from first responders to the victims. The technical aspects and the implementation of the proposed solution is part of the ongoing collaboration.

Both these activities contribute to the activities of WG3 (WG Leader: Carmen Mas Machuca (Technical University of Munich, DE) and fully meet the goals of the STSM.

DESCRIPTION OF THE MAIN RESULTS OBTAINED

Identified benchmarking scenarios as one of the key challenges in evaluating the various different resilience solutions proposed. Already I have been in contact with both the Cyprus Civil Defence and the Cyprus Fire Service which both confirmed that there is no standardize way of building scenarios for benchmarking performance. Hence there is potentially great value in finding ways of standarding the testing scenarios.

At the same time, the security mechanisms to ensure confidentiality and integrity of the data exchanged between survivors, and between survivors and first responders were established.These mechanism will then be formally defined and stadied in terms of performance, overhead and security level.

FUTURE COLLABORATIONS (if applicable)

Both parties expressed interest for another short term visit to further enhance the collaboration while ongoing work on the subject matter is expected to deliver at least two initial research publications.

FORESEEN PUBLICATIONS/ARTICLES RESULTING FROM THE STSM (if applicable)

Both parties expressed interest for another short term visit to further enhance the collaboration while ongoing work on the subject matter is expected to deliver at least two research publications.