Proceedings of the Federated Conference on
Computer Science and Information Systems pp. 641–647

ISBN 978-83-60810-51-4

Forecasting of threatening situations in Smart Space

Sania Kalitska, Przemysław Kukiełka, Maciej Jonczyk, Jarosław Legierski, Ewelina Szczekocka
Orange Labs Poland, Warsaw, Obrzeżna 7
Email:(Sania.Kalitska, Przemyslaw.Kukielka, Maciej.Jonczyk, Jaroslaw.Legierski, Ewelina.Szczekocka) @orange.com

***Abstract*—We propose conception of the identification and forecasting of threatening situations in a Smart Space. This applies to the problem of public safety hazards caused by natural disasters, human activity, equipments failures, and is the important element of a proper functioning of modern society. Protection against threats is becoming increasingly possible with the development of "Smart Connected World". Therefore, this article is an attempt to show a public safety vision in the future communication networks.**

I. Introduction

THREATS may arise as a result of natural disasters and human activity. In terms of responding to dangerous situations we should divide the threats into two groups: in open environments (natural or urban) and in closed one (inside the building), because the scale of these threats and responses to them are different.

The error price in the public safety task is very high. It is evaluated by the risk value, which is proportional to the threats probability and events result losses. Therefore services of threats early detection and prediction must be context-aware and use as much as possible information. Context-aware infrastructures of this services may be autonomous, e.g. for Crisis Management, or come in a set of services used for other purposes, e.g. for the Smart Home.

This article is composed as follows. In chapter 2 we defined the types of threats in smart spaces, divided conditionally on open and clouse. In Chapter 3 we present a strategy of actions, defined by Celtic-Plus in 2012 [1]. In chapters 4, 5, 6 we analysed the public safety impact on the context model, context-aware infrastructure and architecture choise. In Chapter 7, 8 we present our view on the privacy and security by automation and results of our analysis of problems in the public safety topic.

II. Threats In Open And Closed Spaces

We want to consider examples of threats in open and closed spaces.

A. Threats in open environment

Threats in open environment can be caused by different abnormal environmental parameters (temperature, wind, water level, etc.), acts of terrorism (explosions of gas / bombs / etc; attack on a shop / person), lack of electricity, traffic disruption, etc. In general, the threats in an open environment are massive, and may lead to a crisis situation or even to disasters. In every country there is a special multi-layer state Crisis Management (CM) system with Crisis Management Centers (CMC) in each county, province, city. CM analyses the monitored data, receives notification of threats from residents and different systems, operating during and after the crisis situation, modernizing themselves basing on an analysis of its weaknesses during crisis.

Unfortunately, the prediction of the crisis situation in the CM in widest scale does not exist. It is related to the problem difficulties and the extremely high costs. Now we can see only the beginnings of such approach, for instance, the information system of the national safety against exceptional risks ISOK (pol. Informatyczny System Osłony Kraju przed Nadzwyczajnymi Zagrożeniami) [2]) and GEM (Global Earthquake Model).[3] projects.

We give some examples for Poland.

- *Fire*. CM Center receives messages about the fire from residents or from the visual cameras. This information is long overdue, because in this moment the fire is already gathering their harvest.
- *Flood*. We had this summer in Poland huge unexpected flood, as a result of heavy rains. System ISOK was not helpful, despite of having full meteorological information, including weather forecasts. Prediction of water level in ISOK was calculated basing on different theories and water level monitoring. However, the practice showed that they were not interconnected large rainfall (context) with the water level (parameter) in mountain areas.
- *GEM and ISOK*. This two projects are independent and have no common relationships, e.g. information exchanging. However, the knowledge of the earthquakes forecasting in Europe is a context information for the flood forecasting in Poland

B. Threats in close environment

In a closed environment threats can be caused by attack, sudden events with the person (casualty, loss of consciousness, etc.), lack of regular electricity, gas or lighting, gas / bomb explosions, poisoning water, etc.

These threats are generally incremental, on a small number of people, especially when it comes to housing. Context–aware services with public safety functionalities

significantly increases the persons safety in this environment.

III. Strategy Research Areas

The main challenges in the telecommunication services are increasingly focusing on the user. The boundary between the physical and the digital worlds is gradually becoming more transparent, including the boundary between the network infrastructure and services. This fact has a huge impact on the research strategy today.

A. Research Areas definition

France Telecom (FT) strategy is compatible with European research initiative Celtic-Plus, described in [1]. It is proposed to divide all telecommunication problems in two parts: *get connected and while connected*, as shown on Figure 1 [1].

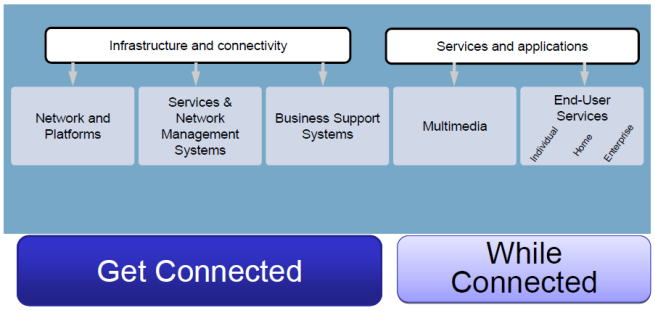

Fig. 1. Research areas in telecommunication [1]

Get Connected deals with the network components and infrastructure (wireless, optics, energy efficiency) as well as network architecture and connectivity (networking and autonomic network). By adding a new cheaper and more efficient infrastructure in this area, we make the system better adapted to new services,

While connected deals with the services and end-to-end applications, as well as security, public safety and identity, business aspects.

The area of services brings higher profits growth than infrastructure [1], but reaching of this profit is not possible without building a base, on which the services can be expanded.

B. Research in get connected area

Network infrastructure improving is mainly associated with bandwidth, mobility, responsibility, security / privacy / trust. In order to support new applications in real time and provide accurate information, we must solve many problems in which the main ones are:

- increasing of energy efficiency by creating an interdisciplinary and multidisciplinary integrated services;
- change the Internet architecture by adjusting the Internet protocol for mobile devices;
- arrangement for the mass market services and applications (such as video streaming or downloading huge files) requires capabilities that today's infrastructure can not offer;
- take into account scenarios of the performance degradation because of the lack Internet investment, sudden meltdown, increasing complexity, lack of innovation.

We want to pay special attention to the following two problems, what are important for us.

Wireless communication is a larger part of the smart space services. Without the use of mobile devices does not mention the creation of ubiquitous services. But they provide to their own problems, which also we need to solve. Accuracy of the mobile devices depends on the used spectrum (width and height) and environmental parameters. There is problem of a spectral efficiency, that is to say the limited available radio spectrum. Mobile devices have limited battery power too. A lot of problems bring wireless broadband, with such challenges as: architectural design, management of access network structure, high transmission errors probability and low accuracy.

Strong growth of Machine to Machine (M2M), Internet of Things (IoT), etc. services, built mainly in mobile technology, change the proportion of network traffic: a small number of 'large" session data of interchange (conversation, streaming video) migrates out to the huge amount of “small' session (meter reading, provide information about state changes) with a corresponding increase of signaling traffic. Architecture of future networks should be optimized for efficient network communication and to allow multiple sessions to respond back in real time. One major problem will be to prevent “signaling congestion”.

Service-based web 2.0 platforms. The acquisition of scattered information from various service execution environments, in a uniform manner through open interfaces allows us to create new services quickly and cheaply, using shared information technology, methodologies and best practices.

ISOK, GEM projects use this technology to allow local authorities and residents actively interact with them. That is they use the collective intelligence of users. Users can obtain information about a possible crisis situation in order to forecast it or add specifics to the analysis of the crisis that can arise. In this way, Web 2.0 let to increase safety in local area.

C. Systems for threat information, developed in Orange Labs Warsaw

Notification systems for emergency use the API exposed to the network operators on the Internet in a model Telco 2.0. [4]. In order to establish interaction with the person being in this situation, you can use one of the channels from the following table.

Table 1
Channels API for threats information

Interaction	Channel (API)
Notifies of users	SMS API (notification)
	USSD API (notification)

Locates users	Location API
	NMR API
Receives information from users	USSD API
	SMS API

Users notifying and *receiving information from them* about the threat can be carried out by the SMS channel and other media, for example, developed at Orange Labs applications Emergency Button [5] using the USSD channel. Warsaw Municipal Guard can also be informed on emergency situations via SMS [5].

Users Locating based on the location of their mobile terminals. However, due to the low accuracy of the method, more accurate algorithms must be used in the future, for example, reports based on NMR [6].

D. Research in while connected area

In "while connected" we take care of vertical services and applications end-to-end, such as digital citizens, digital homes, digital enterprise, digital city, digital school, digital transfers, e-health, and games and horizontal services such as security and identity, and business aspects, as the evolution of network value in business telecommunications field.

We will focus mainly on the context problems. Without of the context using is not possible to build a ubiquitous service, but on the other hand the context, itself creates substantial problems, that are waiting for a solution. Of particular interest in dealing with complex and open pervasive systems are:

(1) Context model representing context in a general way and consist from three hierarchy levels [7]: a) the basic raw data; b) meta-level concepts; c) the situation as a result of the contextual information analysis. Sometimes context model is defined as two-layer hierarchy [8], where layers b) and c) as above are consolidated in order to emphasize a different mode of operation in selected layers.

(2) Architectures that promote agility and autonomy of individual computing entities.

IV. Context Models And Public Safety

The inaccuracy and unreliability of sensors, that collect the basic raw data, may lead to mistakes in context reasoning.. To obtain more reliable information from the sensors we must have high redundancy, which in practice is carried out to measure the same parameter by different sensors or systems. It's very impotent the right choice of the context model

*A. **Context model approaches***

Currently there are three major trends in research on modeling context [10]: a) ontology and logic-based models; b) techniques for accumulation of sensor data and applications and c) Context Space.

We are interested in two approaches:

- Ontology and logic-based models allow the description of the universality of the context, the structure and semantics are often served in a context ontology. The reasoning is usually based on the claims of 'true or false'.
- Context Space model [7, 10] is a multidimensional space (Figure 2) consisting of domains of values for each relevant type of information, in which context can be detected.

If the first model is simple in realization at the expense of large database, then the second model needs to use high level mathematics, reducing the database volume by the same quality of processing (accuracy, speed of execution, etc.).

*B. **Ontology and logic-based models***

We think, simplicity and ability of high volume databases building causes that we have mass implementation of logic-based methods into the practice. There are almost ubiquitous in context-aware services and are integrated with others methods, e.g. semantics with multi-agent systems (MAS). In this case, semantics plays supportive role, enabling to exist more adequate and automatic agents communication, for instance in negotiation systems [11], trading agents environment [12] or access to biological resources [13].

The disadvantages of the logic-based models (the difficulty of obtaining an overall picture of the context model with a large number of systems context, the lack of context hierarchy depending on its importance and the inability to detect small changes in context during execution) [10] will interfere more and more in the future, particularly in issues related to public safety.

Orange Labs Warsaw activities in semantic

In Orange Labs Poland several activities are provided in the scope of semantic modeling for different purpose, such as: semantic search of the services according to user demands, modeling a high-level context of location (HLC) in order to present user meaningful information, composition in mashups.

*C. **Context Space model***

The *Context Space* model explicitly introduces the real conditions, formalizes them in formulas, charts, and in a severely logical, elegant way verified and solved problems, using powerful mathematical apparatus, among which as the principal is Context Spaces Algebra [10].

The model provides a unifying way to represent context and enables effective reasoning to be applied over the modeled information.

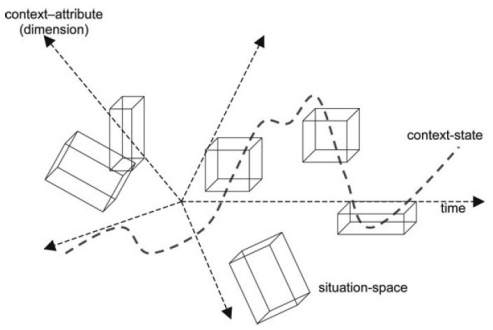

Fig. 2. Illustration of the model's fundamental elements [7, 10].

This model shows distinguishing between the context and situation definitions [14]. *Context Space* is the information used in the model for representing all possible parameters values in all possible situations. *Situation Space* is a meta-level over context, it is a parameters values set, suitable for real situation. *Context State* is a set of concrete parameters values, as the context data reasoning result.

Context state fluctuates in time within *Situation Space (if data are correct)*, reflecting sensor data changes. Different methods, particularly statistic methods in Context Space [15] will calculate the average value of sensor data errors, correct some of them, increasing their probability and accuracy, estimate the reliability of assessments, evaluate and forecast the situation, in our case, threats situation.

Approach Context Space allows to associate in the contexts analysis on the seemingly unlike components base in a joint action, expressing the result in terms of usability.

D. Propositions

We think also it is worth to face to the Context Space model. Elements of this model have a place not only in the works of one researchers group, but also in the works of other authors, independently entered this method, e.g. [16], that highlights its advantage in dynamic, incomplete and uncertain environment.

Using this approach we are able to define different metrics in this space. By the help this metrics we can separate the different situation spaces, automatically validate the resulting situation. Of particular importance, this approach has by the threats forecasting challenge.

In [9] was proposed to perform the verification and correction of the basic raw data at the context models top level, using an analysis of the whole set of the object parameters, collected for reasoning. That is, the vector analysis is performed in the multidimensional space of parameters.

We offer a slight transition to the Context Space model (as in [16]) and try to fit it to our systems, utilizing the ontology and logic-based models too. We believe, that combining of different approaches, can give very positive results, taking benefits from each of the methods. Such a combination of different techniques and methods takes place already in our company, as mentioned in this section a little higher.

V. Context-Aware Infrastructures And Public Safety

We have a choice from three types of *context-aware infrastructures*, known from the literature [10]:

- *based on the mobile autonomous agents* in the ubiquitous environment;
- *centralized* with autonomous agents, which do not cooperate among themselves in there activity [17, 18];
- *hybrid,* combines first two approaches [10].

The advantages of a centralized infrastructure are a common representation in the center (broker) and disambiguation of contextual information in the repositories, what allows to perform complex and highly accurate calculations. But the infrastructure is not flexible: failures or improper operation of a single point can lock system almost. Hybrid infrastructure add flexibility to centralized infrastructure by enabling agents to cooperate with each other personally in some specific tasks., [11], [12] [13].

*A. **Infrastructure for CM Center in no urban environment***

This approach presupposes the existence of following information, near to existing in Poland, (except for the first component):

- own sensor network for fire & smoke on the fixed points in the open environment (not in the forests areas where sensors data are very uncertain and unstable);
- actual information about humidity, measured in the fixed points in the forests of country and received from the departments of forestry, presented in Internet for every forest area of Poland with the decision about the situation (a fire hazard present or not in the forest);
- actual and forecast information about temperature, humidity, speed and direction of wind, water level, atmospheric pressure from ISOK system platform, presented in Internet for every area of Poland.

Note that the humidity is measured by the two different systems. Therefore, it is possible to compare this parameter and correct, reducing the wrong decision probability about the situation.

In our opinion, all existing platforms for the different risks (fire, flood, etc.) detection must cooperate. For this they need to commmunicate with each other (e.g. by the Internet) and transmit to each other information about the parameters values, monitored by each of them. Each of these platforms must be able to use information received from other platforms, as context

*B. **Infrastructure for CM Center in the Smart City.***

CM Center in the city responds on the massive or often repeated threats: fire, flood, huge congestion or accidents on the road, big disaster because of storm or heavy rain or riot, breakdown of municipal infrastructure (electricity, central heating, canalization, etc), contamination of water or/and air or/and food, explosions (gas, bombs), etc. This list can be continued long. We see, that there are a lot of very different threats in Smart City.

City with a lot of different devices on the streets, buildings, columns, transports, etc, is a very conducive for creation of ubiquitous computing environment. In this environment are extremely fit nomadic agents [1].

Today, every developed country already has some autonomous services, which belong to public safety. For example, Internet service informs about the traffic in any area on the country or about optimal path, where in defined period of time we want to drive. We receive also information, how far and how long he will drive, how much fuel will be used, etc. This service may give context information for different events, e.g. quickly locate the place, knowing about the traf-

fic jams, and the optimal route to the location by receiving information of a shooting in the city.

For *Smart City* fits hybrid infrastructure with a nomadic agents.

C. *Infrastructure for public safety in the building*

This example is presented in the dynamic form, to show of situation recognition as a automated reasoning process. Masked intruder enters the smart building. At the entrance the monitoring system shows his overall silhouette. No identification of individual causes the sending of information about the incident to the building platform (BP). Nomadic monitoring systems in the corridors, elevators and stairs try to identify the intruder and the situation, providing contextual information to BP about the direction of its movement and the eventual goal - apartment, to which it is going. BP must have a profile of entertainment (where live the elderly, lonely or sick persons and unaccompanied children; that apartments can be empty at this time, etc). If an intruder is identified, then it needs to classify the object as "known" or "unknown". If it will be in the category of "known" and fits the friend's profile of some occupant, to which tends, it is concluded that there is no threat and the case is closed. If a person is "unknown", must be considered whether it belongs to a group, that serves people or building. If an intruder does not belong to any of these groups or are not identified and will seek to enter the property, which is the context of "vulnerable", the police have to act.

Hybrid infrastructure with a nomadic agents can be implemented for this case.

D. *Infrastructure for public safety in the home (apartment)*

By addition of public safety functions to *Smart Home* we name it *Safe Smart Home.* We see two type of *Safe Smart Home*:

- *Safe Smart Home* 1 for old, ill, invalid persons, often alone and need help without risking of invasion to their privacy. It is not visible, how much threats they have in common house (e.g. collapsed and drowned in the bathtub by taking a bath). In these cases, we can not use visual monitoring, only the context to help threats situation reasoning. As the context may be used different parameters e.g., dimensional sizes of the body (horizontal, vertical, height over floor), lack of activity, constant on/off lights, no calls, long sleep, medicine data, behavior of pet animals (cats, dogs, birds, etc.).
  In threat situation we need to inform a close person (relative, friend, neighbor) and a medical institution, which takes care for this person. It performs remote surveys and reports to us the result. If an ambulance arrives, we must open the apartment door to enter medical teams and accompanying person. In this case it is necessary to browse this person profiles.
  For Safe Smart Home 1 fits hybrid infrastructure.
- Safe Smart Home 2 saving from fire, gas explosion, etc. for any family. This home type we can implement now by looking broadly at the problem in any home service. We think, that each such service must consider the problem of public safety just such as security. For example, in the system, being developed in the project UP-TO-US [19], which will be widely used, we have to add simply some sensors (fire, smoke, smell of gas, etc.) and create the appropriate device profiles in order to significantly enhance the safety.

Adding smart services in home environment does not change infrastructure type, typically it is a central infrastructure

VI. Context-Aware Architecture And Public Safety

We presented (see item 4) some examples of context – aware infrastructures for or with public safety functionality, that showed depending of results infrastructures on many factors.

In order to have context-aware Crisis Management system, we have to build a special platform. It will monitor some key parameters, and some correlated parameters will receive from other existing platforms, For example, for early detection or prediction of fire, platform monitors value of fire, smoke, whereas the values of temperature, humidity, wind speed, etc. receive from the platform ISOK by suspicion that it may be starts a fire.

Adding functionality public safety to the service in close spaces can change the architecture type from central to the hybrid without the addition of a specific platform.

Increase of services number, transparent to the client application enriches customers context awareness and correctness about situation reasoning.

B. *Context-aware services developed in Orange Labs Warsaw and Public Safety*

In Orange Labs Warsaw there are some interesting projects in the context-aware services topic.

Project [19] focuses on two direction: users in nomadic situations ("*My Personal Content Moves with Me*", allowing the user to access his personalized IPTV content in a hotel and be billed on his own bill), and users' mobility in his domestic sphere ("*My Content Follows Me in a Customized Manner*"- continuing accessing his IPTV service personalized according to his location and devices). To achieve this tasks, system must be capable to perform the follow function:

- monitoring and gathering of the user and his environment contexts and feed them in a dynamic manner to the IPTV system;
- constructing and dynamically updating of the users profiles according to the various contexts;
- managing of the different privacy levels for each user and the user personal information protecting.

In this case the service can be personalized with the content tailored to user preferences in different contexts and is able to conform to all requirements: quality, privacy, etc.

The project includes a lot of problems and solves them at a high level, but there is no mention about public safety.

Project [20] is the part of the ReactiveHome project, which is developing a functional prototype of the Home Area Network (HAN) technology. In turn, HAN subsystem is an integral component of the Smart Grid architecture whose main objective is the optimization of household energy consumption. In paper [19] we described scrupulously all home consumption aspects of measure, the acquired data characteristics, algorithms efficiency, and security problems. However [20] does not include public safety problems: how system will react, if energy in home system increases beyond the specified threshold? How much is this threshold?, etc.

In [21] we were developed device profiles related on the one hand, with the user and on the other hand with the situation, adjusted to a specific user or situation respectively. A main goal was the introduction of this profiles to tablets (multi-user and mobile devices), enabling to get localization information from a tablet about concrete owner on the basis of the tablet activity, supposing that tablet is close to this owner (father, mother, child, etc.). E.g., child's location is determined according the tablet activity in game. In normal situation this service operates without charge. But if this child during the game goes into the kitchen to eat the sandwich quickly, falls onto the floor and breaking his leg, he may be a long time without help.

In the project [22] we is designed to prepare a generic architecture (initially, on the Android basis) that will allow for advanced way to manage of his device resources, equipment detectable around and contextual data. The management of these aspects in an intelligent way will connect to the architecture some services and applications such as provide new elements of these resources.

We developed device profiles related to the user and the situation, in which the device works. It is usually a different location as the "work" or "house", but also the spaces within the home. Situation can be also a "Car", "Meeting", "Activity", which will also affect the settings, but their main criterion is not the location.

The user can be identified by his personal device localization, assuming, that it is always near. Situation of user can be resolved based on time of day, location, GPS, Wi-Fi, fingerprinting.

We also have implemented functionality to detect other devices in the environment and different protocols, among them UPnP, that hides from the user the communication between different protocols. Finally we plan to create nomadic services.

We have created software that in a Friendly User Tests will gather the data from the sensor device, the operations performed on the system in order to create a large context base of the user behavior. Among this base we will search of patterns that will be helpful in the future for situation reasoning and proposing new services according to user preferences.

We try to associate research and implementation, so as to be able to present concepts that are already at this point is possible to set up and user input.

Because this project will be continued and has a rich content, we are able to supply it with public safety services.

Orange Labs Warsaw has created a "Multimodal Interfaces" [23] program which may yield interesting results for public safety. They set out to create an ecosystem of multimodal devices and services that, from the user's point of view, would work as one, engulfing experience. The program proposes some very helpful services such as „Tap me!" or „Watch It!". In the „Tap me!" service, user taps phone and application detects this taps with built-in motion sensors. This service may be modified for Safe Smart Home 1 in such a way, that user would have a some critical points in the flat (bed, bath, kitchen, etc.) and phone will send alarm to a guardian. It will be very helpful for users in dangerous or uncertain situations, where phone can send SMS message like „SOS_my location" to police or user's friends.

VII. Privacy And Security By Automation

In everyday life everyone is no doubt, the more comfortable life he leads, the more happy. But there is a paradox, the higher level of comfort, the more there are conflicting threads, which earlier was not noticeable. For example, better is to ride than walk, but a result of car and bike comparison already is ambiguous. The car is a much more comfortable, but the bike helps to keep good health.

The introduction of automation in everyday life increases remarkably the quality of life, but adds some considerable negative aspects, namely:

- Threats increase with the civilization progress. The devices and systems are getting much more complex with higher intellect and adapting to the environment. Using this instrument, a man can perform works, which previously were impossible. But the reasoning and proceedings logic of machines and ordinary man are different. In addition, sometimes, even if a man understands the system, he can not physically change anything in its actions. For example, during the atomic power stations disaster in 2011 in Japan during tsunami the staff were not be able to stop reactors immediately.
- Changes of society are not avoidable, e.g. amount of citizens without activity necessity will increase.
- There is a growing concern about privacy through autonomous devices.

Invasion in the personal privacy is a big problem. However, in our opinion, there is still a large reserve of privacy safety. In order to increase privacy we can see now at least three approaches:

- receive private data from one database, for example, a variety of services in the home has to retrieve data only from the Smart Home base;
- use widely biological methods for private protection - fingerprints, hand, eye, ear, bottom, on the basis of which create a complete profile of the person;

- use Information Hiding (IH) methods, particular Digital Watermarking (WM) [24]. IH is a new enough information security topic, rapidly growing, especially within the last 10 years period. WM is very requested by private area, because it can be used in order to provide copyright and integrity of different products or documents. For example, Digital Rights Management (DRM) system is used for copyrights safe.

Turn to the example in Chapter 4, C about "intruder enters the building". This example shows how deep we enter the area of person's privacy, when we protect him or counteract him. In addition, next intruder can attack to break into the profile information when we process it.

In this example we touch simultaneously two problems:

- *Privacy*: we obtain information for business, not threatening to the person
- *Security*: the attacker is looking for "holes" in our searching procedure in order to threat to the person

The problem of security is almost always solved by personal private profiles building, good or bad – it is another matter. The problem of privacy is more complicated, since information about the person data allows us to perform services that are needed exactly for that person, in our case, for achieving the protection of his property and life.

Services designers try to hide context information, as they can now, for example: a) make context was passed only when recipient need to use it in computing and then it disappears from its area; b) the recipient does not know the other parameters of the object (e.g., get information about location, not knowing who is; etc.); c) using mobile personal devices (e.g. smart phone) enables to locate the private information in this device exclusively. These methods solve partly security problems too.

VIII. Conclusion

Philosophy of the services development is well represented today by the motto "Smart Connected World", forces already today to pay attention to public safety, starting with one person up to universe. The revolution in telecommunications greatly increases the quality of life and gives a chance to counter multiple threats. However, we should not forget that this revolution can bring additional threats, if not over-think and do not accept solutions, which can reset one. In [1] has been paid attention, if in hard competition some companies do not pay particular attention to the quality and reliability of services, what may sometimes lead to danger, and even to crisis. We can see such examples in the home, city, country and world. Therefore, we think, this direction can not be underestimated.

References

[1] Purple Book: Celtic_Plus *Programme of possible and recommended research items,* Version 2012

[2] http://www.wzp.pl/geodezja/projekt_isok.htm

[3] http://www.projectgemmn.org/

[4] P. Korbel, J. Legierski, *Telco 2.0 – examples of practical use of telecommunication service platforms' interfaces* KSTiT 2011 Conference materials, Telecommunications Review 8-9/2011

[5] S. Garbowski, J. Legierski, *Programming Interfaces In the Open Government Systems*. Submitted to IV conference PITWIN, Kielce, Poland 13.09.2012

[6] B. Zacharuk, A. Tylman, P. Pątek, S. Grabowski J. Legierski, *NMR API–nowy interfejs programistyczny w modelu Telco 2.0 i propozycje jego zastosowań,* KKRRiT 2012,

[7] Padovitz A., Zaslavsky A., Loke S. W., *A Unifying Model for Representing and Reasoning About Context under Uncertainty,* 11th International Conference on Information Processing and Management of Uncertainty in Knowledge-Based Systems (IPMU), July 2006, Paris, France

[8] Anders Kofod-Petersen,Marius Mikalsen *"Context: Representation and Reasoning Representing and Reasoning about Context in a Mobile Environment"*

[9] Amir Padovitz, Seng Wai Loke, Arkady Zaslavsky *On Uncertainty in Context-Aware Computing: Appealing to High-Level and Same-Level Context for Low-Level Context Verification1,* 2005, Australia

[10] Amir Padovitza,_, Seng W. Lokeb, Arkady Zaslavsky *"The ECORA framework: A hybrid architecture for context-oriented pervasive computing"* November 2007

[11] Koppensteiner G., Merdan M., Lepuschitz W., Moser T., Reinprecht C., *Multi Agent Systems combined with Semantic Technologies for Automated Negotiation in Virtual Enterprises,* http://cordis.europa.eu/fp7/ict/content-knowledge/fp7_en.html, 2011

[12] Y. Zou, T. Finin, L. Ding, H. Chen, R. Pan, *Using Semantic Web technology in Multi-Agent Systems: a case study in the TAGA trading agent environment,* 2003

[13] F. García-Sáncheza, J. T. Fernández-Breisa, R. Valencia-Garcíaa, J. M. Gómez, R. Martínez-Béjar, *Combining Semantic Web technologies with Multi-Agent Systems for integrated access to biological resources,* Journal of Biomedical Informatics, 2008

[14] Amir Padovitz, Seng W. Loke, Arkady Zaslavsky *Multiple Agent Perspectives* in Reasoning about Situations for Context-Aware Pervasive Computing Systems

[15] Andrey Boytsov *"Context Reasoning, Context Prediction and Proactive Adaptation in Pervasive Computing Systems",* Lilea University of Technology, 2012

[16] M. Kirsch-Pinheiro, Yves Vanrompay, Y. Berber, *Context-Aware Service Selection Using Graph Matching*

[17] Nigel Baker, Madiha Zafar, Boris Moltchanov, Michael Knappmeyer *Context-Aware Systems and Implications for Future Internet Towards the Future Internet* G. Tselentis et al. (Eds.), IOS Press, 2009

[18] Boris Moltchanov, Christian Mannweiler, and Jose Simoes *Context-Awareness Enabling New Business Models in Smart Spaces,* European ICT projects "C-CAST" and "G-Lab" funded by the German Ministry for Education and Research

[19] http://www.celtic-initiative.org/Projects/Celtic-projects/Call7/UP-TO-US/uptous-default.asp

[20] Gilles Privat, Przemysław Kukiełka, *Data fusion – artificial intelligence level techniques,* OLP, White Papier, France-Warsaw 2011

[21] Przemyslaw Pietrak, Maciej Jonczyk, Przemyslaw Kukielka, Tomasz Poczesny; Yves Feuillet, Ben Chen, Home Devices *Intelligent Profiling*: "Personal Devices", White Papier, Warsaw- France, 2011

[22] Jonczyk Maciej *Architecture for Context-Aware Pesonalization* [POL], Warsaw ,2012,

[23] Piotr Bączyk, Jan Dziekan, Kamil Madejek, Krzysztof Majewski, Jacek Milewski, Łukasz Szóstek, Maciej Uberna, Piotr Wiechno, Tomasz Wroniak *Multimodal Interfaces,* Research Program, OLP, Warsaw, 2012

[24] http://www.webopedia.com/TERM/D/digital_watermark.html