The original appeared at:
2014 IEEE Annual Conference on Pervasive Computing and Communications Workshops (PerCom)
http://dx.doi.org/10.1109/PerComW.2014.6815175

Enabling Reliable and Secure IoT-based Smart City Applications

Elias Z. Tragos*, Vangelis Angelakis†, Alexandros Fragkiadakis*, David Gundlegard†, Cosmin-Septimiu Nechifor‡, George Oikonomou§, Henrich C. Pöhls¶, and Anastasius Gavras‖

*FORTH-ICS, Greece, †ITN, Linköping University, Sweden, ‡Siemens SRL, Romania
§Faculty of Engineering, University of Bristol, UK, ¶University of Passau, Germany, ‖Eurescom, Germany

Contact author: Elias Z. Tragos {etragos“at"ics.forth.gr}

***Abstract*—Smart Cities are considered recently as a promising solution for providing efficient services to citizens with the use of Information and Communication Technologies. With the latest advances on the Internet of Things, a new era has emerged in the Smart City domain, opening new opportunities for the development of efficient and low-cost applications that aim to improve the Quality of Life in cities. Although there is much research in this area, which has resulted in the development of many commercial products, significant parameters like reliability, security and privacy have not been considered as very important up until now. The newly launched FP7-SmartCities-2013 project RERUM aims to build upon the advances in the area of Internet of Things in Smart Cities and develop a framework to enhance reliability and security of smart city applications, with the citizen at the center of attention. This work presents four applications that will be developed within RERUM, gives a general description of the open reliability and security issues that have to be taken into account and gives an overall view of the solutions that RERUM will develop to address these issues.**

I. Introduction

Urban population is expected to grow by an estimated 2.3 billion in the next 40 years, having almost 70% of the world population living in cities by 2050[1]. This rapid growth of cities aggravates many challenges associated with living in urban environments and are directly related to public safety, transportation management, waste disposal, noise, air and water pollution. Meanwhile, the current Eurozone crisis has decreased dramatically the state funding to cities, hampering their vision to provide better quality of life to their citizens.

The concept of “Smart Cities" (SCs) has emerged recently as a very promising solution for providing advanced services to the citizens enabled by Information and Communication Technologies (ICT). Smart Cities drive competitiveness, sustainability and improve Quality of Life (QoL). SCs can be used as a driving force for economic growth and are also connected with energy efficiency [1], [2]. To this goal, current cities have to deploy new ICT infrastructures as environments for innovation and growth with the heavy participation of citizens and businesses. The successful deployment of SCs calls for a unified ICT infrastructure to support the diverse set of applications for urban development and “Future Internet" is one solution towards this direction. The Internet of Things (IoT) presents itself as a basic collection of enablers to interconnect heterogeneous “things" (where physical and virtual objects) in a global network infrastructure supported by several communication protocols [3].

IoT has enabled the deployment of many SC applications and there are both research projects and many commercial products dedicated to such applications. The literature reveals a variety of efforts to employ “Smart Objects" (SOs) for traffic and environment monitoring. The OpenSense project is conducting research into adopting pervasive technologies and community-based sensing with “Wireless Sensor Networks" (WSNs) in the context of air pollution monitoring [4]. The MOBESENS FP7 project uses a low power WSN solution for water quality monitoring (e.g. in lake Geneva) [5]. In the literature several attempts regarding the design of WSN systems for environmental monitoring have been made [6], [7], [8], [9]. Road traffic monitoring is another active area of research, with a very comprehensive review of related issues and techniques presented in [10]. One of the projects that stands out is the CVIS Integrated Project [11]. Embedded SOs have also been used to control lighting in an operational road tunnel [12]. Commercial products for SC applications have been developed by Zolertia[2], Libelium[3], TST[4]. A common characteristic of existing approaches is that they focus on providing fast and easily deployed solutions, but most are missing strong elements of security, privacy and reliability.

A key challenge for IoT towards SC applications is ensuring their reliability, incorporating the issues of security, privacy, availability, robustness and flexibility to changing environmental conditions. As the SOs become more intelligent, autonomous, active and seamlessly integrated in the everyday life of SCs, new problems and new security issues arise. Without guarantees that the SOs are: (i) sensing correctly the environment, (ii) exchanging the information securely, (ii) safeguarding private information, users are reluctant to adopt this new technology that will be a part of their everyday lives, which decreases the market value of SC applications for the service providers. Therefore if these concerns are not addressed proactively at the early stages of IoT deployment for SCs they may act as a barrier to the adoption of this technology by

[1] http://www.alcatel-lucent.com/eco/low-carbon/travel_less.html

[2] http://zolertia.com/products

[3] http://www.libelium.com/products

[4] http://www.tst-sistemas.es/en/solutions/monitoring-control/

978-1-4799-2736-4/14/$31.00 ©2014 IEEE

users and businesses. In this respect, the FP7 project RERUM aims to improve the IoT technology making it more reliable, trustworthy and secure for enabling both users and service providers to adopt it and enjoy its benefits. In Section 2 the basic description of project objectives towards the smart city domain is given. Section 3 presents the general description of the four SC applications that will be developed and deployed within RERUM. Section 4 presents an initial analysis of the open reliability and security issues of the existing deployments of SC applications. Section 5 presents the RERUM approach towards enhancing the reliability of SC applications, while Section 6 presents the conclusions of this work.

II. SMART CITIES AND RERUM

Smart cities are striving to deploy and interconnect ICT infrastructures and services to guarantee that authorities and citizens enjoy a reliable access to applications. The ultimate goal of RERUM is to allow IoT to become the fundamental enabler towards a *truly* Smart City. Having the citizen at the centre of attention, RERUM designs and develops an IoT-based framework for infrastructures and services to improve the QoL in future cities. RERUM addresses the interconnection of large numbers of heterogeneous SOs (devices, software, and services) enabling the provision of innovative applications in Smart Cities. The IoT is heterogeneous by nature comprising a large number of hardware and software smart objects such as interconnected sensors with different communication technologies (RFID, Zigbee, 802.11ah) carrying different tasks (cameras, microphones) over different carrier networks, as well as other ultra-low power autonomic devices and systems. Mobile phones are also smart objects, with a variety of hardware and smart software objects.

In SCs, objects are penetrating peopleŠs lives, forming dynamic networks, gaining cognition and intelligence, and communicating with each other. Thus, new threats arise in this new symbiotic ecosystem of objects and citizens. A very holistic view of the IoT framework is required to address the new threats and this can be achieved with the applications' requirements as the driving elements. Thus, one of the key objectives of RERUM is to develop a holistic framework that incorporates security, privacy and reliability in its core elements, following the "reliability, security and privacy by design" concept. The framework will include cross-layer proactive and reactive security and privacy-enhancing mechanisms to ensure the secure establishment of networks of SOs, as well as their secure communication on top of several underlying technologies. This calls for the autonomous design of a large heterogeneous network, where objects, users and services will interact with each other in a seamless, secure and reliable way.

The ultimate goal is to enhance the reliability of the IoT paradigm in two directions: (i) **telecom operators and service providers:** proven system efficiency, robustness, and security will enable operators and service providers to support and invest on IoT infrastructures and applications, and (ii) **users:** trustworthiness-, security-, and privacy-by-design will allow users to embrace this new technology and demand applications enabled by the IoT. Still, as with the current Internet, users must trust the medium up to a certain level that will not expose them to risks. In the SC ecosystem, this balance has to be achieved step by step, and the first step is to increase as much as possible the credibility and reliability of the IoT itself.

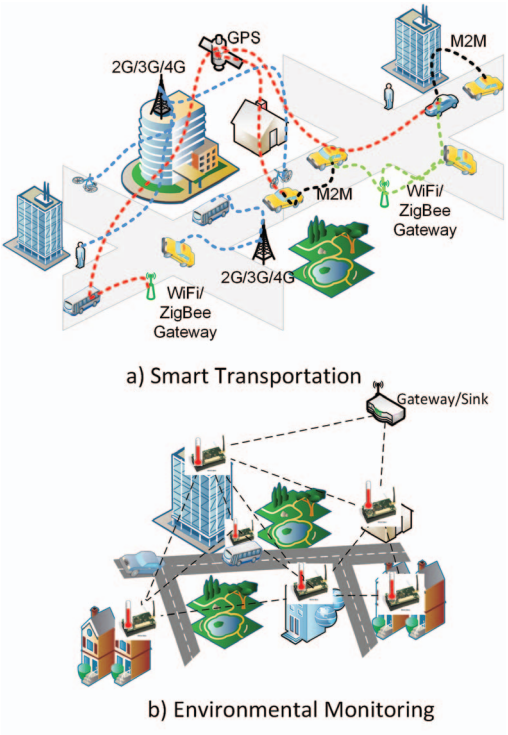

Fig. 1. RERUM's outdoor use cases

III. THE RERUM FRAMEWORK USE CASES

Within RERUM, the SC applications play a major role in both system design and evaluation. With two cities (Tarragona, Spain, and Heraklion, Greece) participating in the project, it is ensured that applicationsŠ requirements become the core of the system design. The cities have identified four applications of major interest for their citizen and these have constituted the RERUM Use-Cases (UCs) presented below that will be deployed and evaluated in both cities to assess the portability of the framework. Figure 1 depicts the outdoor use cases.

A. Use Case #1 (Outdoor): SMART TRANSPORTATION

The transportation system in large cities has a huge impact on daily life of the citizens. Due to economical and physical constraints, in many cases it is no longer possible to improve transportation by improving the infrastructure. Instead we need to make the transportation network more efficient using advanced planning and control tools with the integration of smart sensing and communication infrastructure.

The first step towards making a transportation system more efficient, environmentally friendly, comfortable, and safe is to estimate its state at any given moment and predict its trends and future behavior. Accurate estimation and prediction from a large number of sensors enables proactive traffic management, which has the potential to increase efficiency and reduce congestion substantially [13]. The sensor data play a crucial role in managing the transport system, thus a sensing infrastructure that enables robust, timely and secure communication and

processing of this data while maintaining privacy of users in the system is of major importance.

For state estimation and prediction of the transport network, sensors are deployed and typically combined with models that can predict the traffic evolution in space and time. Sensors can be fixed or placed on vehicles traversing the city. Fixed sensors, such as radars, bluetooth detectors and license plate cameras can be used to measure speed, flow and travel times. To extend the state estimation coverage beyond main freeways and arteries, an increasing part of these sensors are located in vehicles. The focus of RERUM is to leverage the participatory involvement of citizens and authorities for measuring the trust end-users have in the system. Of specific interest are smartphones, which are equipped with a multitude of sensors for point measurements (GPS, accelerometers, etc) but their id's can also be utilized to measure travel times that can capture how speed evolves in space [14].

Overall the goal of this UC is to use a heterogeneous network of SOs using different communication technologies (as shown in Figure 1a) in order to perform real time traffic estimation in the cities. To do so, both vehicle mounted SOs in professional fleets as well as SOs carried by citizens will be deployed. The first will be placed in city vehicles (i.e. buses), while the latter include the users' mobile phones. Citizens will be able to use their mobile phones (with the RERUM mobile application installed) for contributing to the participatory sensing framework. The type of vehicle that the SO is placed on can fundamentally determine the characteristics of how the measurements will be used to infer knowledge about the state of the transportation network. Different types of vehicles and fleets also poses substantially different type of vulnerabilities in terms of robustness, security and privacy:
a) **City Busses:** The key characteristic is that they run on main streets and, when no dedicated bus lanes exist, they can: (i) directly provide trip durations for segments of their route, (ii) indicate increased demand (by extended delays on the bus stops), and (ii) identify themselves as cause of congestion.
b) **Taxis:** Taxis constitute a constantly running fleet in more diverse routes than those of busses, following dense patterns around points of interest like airports/ports, tourist sites, and can provide input in traffic load and trends. [15]
c) **Citizens:** Citizens volunteering to provide mobility data can be instrumental in providing baselines for travel time estimation, which in turn could be fed back to users to provide incentives to measure and share traffic data. Participatory sensing measurements are also important to reduce bias introduced by measurements from professional fleets, such as effects of using dedicated bus and taxi lanes.

B. Use Case #2 (Outdoor): Environmental Monitoring

There is a plethora of studies and reports regarding the negative health effects of living in urban environments due to pollution. One report[5] shows that more than 90% of people living in cities breathe dangerous air. A study from MIT [16] shows a very disturbing result that the air pollution could be blamed for more than 200.000 early deaths each year in the US, while another report[6] shows that more than 1 billion people are exposed to outdoor air pollution annually. The devastating effects of environmental pollution in cities have forced the development of applications and infrastructures for monitoring the environmental pollution and the air quality. Such infrastructures have been realised with the deployment of WSNs, with sensor devices been installed in key locations, i.e. city squares.

Within RERUM, the goal of the UC for Environmental Monitoring is to perform reliable measurements for pollution in city environments. Specifically, the measurements that will be gathered can be split in four major categories:
a) **Weather:** for getting real-time or average data for the weather conditions in the city areas the following measurements will be gathered: (i) temperature, (ii) humidity, (iii) barometric pressure, (iv) rain levels, (v) wind speed, and (vi) wind direction.
b) **Air pollution:** for getting average values (over a time period) for parameters that indicate pollution of the air quality within cities. These parameters are: (i)**Carbon dioxide (**CO_2**)**, which is emitted by vehicles, factories and electricity generation. High concentrations of CO_2 in the atmosphere can cause headaches, dizziness, confusion and loss of consciousness and should be monitored especially for warning the elderly and the vulnerable groups of people. (ii)**Carbon monoxide (CO)**, which is a gas emitted by vehicle exhaustions and is formed when carbon fuels are not burned completely. CO can be toxic in high concentrations. (iii)**Nitrogen dioxide (**NO_2**)**, which is emitted from motor vehicle exhaustions, can irritate lungs and have devastating effects of respiratory illnesses to children when they are exposed to high concentrations of NO_2 [17].
c) **Noise measurements:** for getting average values of sound levels in streets to ensure that no excessive noise that could damage the citizens' health is encountered. When noise levels exceed health thresholds an alarm will be raised and forwarded to the relative authorities to act for resolving the issue.
d) **Radio pollution:** for monitoring the levels of the Electro-Magnetic Field (EMF) radiation that is caused by the various types of antennas (mobile, wireless, TV/radio, etc.) within either the city area in general or in specific areas near hospitals, schools and other places that are of high civic interest.

For the implementation of this UC, two types of sensors are considered as depicted in Figure 1b: (i) fixed sensors will be placed in key locations identified by the city authorities (i.e. parks, squares, congested areas, etc.), and (ii) mobile sensors will be placed on top of vehicles (i.e. buses) that will help gather measurements in many areas in the cities. The fixed sensors will be connected either with standard WiFi, ZigBee wireless technologies or with ethernet, while the mobile sensors will be naturally wireless (using WiFi and Delay Tolerant Networking [18], so that the measurements will be stored and transmitted only when there is internet connectivity) or mobile (using GPRS or 3G technology when available). All the above parameters do not need to be measured at real-time, so only the average values within a specific time period will be gathered and sent to the application server.

C. Use Case #3 (Indoor): Home Energy Management

Residential and commercial buildings consume large amounts of electricity, (in the United States alone they constitute 73% of the total electricity produced [19]). Although there

[5]http://www.theguardian.com/environment/2013/oct/15/european-cities-dangerous-air-pollution

[6]http://www.unep.org/urban_environment/issues/urban_air.asp

have been attempts to control the building energy consumption with the development of low-power appliances and efficient heat pump systems, the results are not as expected. In the current context of the fight against climate change, in June 2011 the European Commission published a proposal for a directive[7] setting the objective of reducing the energy consumption by 20% as one of the five targets of the Europe 2020 strategy for smart, sustainable and inclusive growth.

Aiming to monitor closely the energy consumption in households, RERUM will install SOs in high-consuming devices such as washing machines, fridges, heating devices and lights. Since the number of such devices in a household is limited, the deployment will be very small. The SOs will transmit their data wirelessly (to avoid cabling the whole household) to a gateway, which, in turn, will forward the data to the application server that will visualize the energy consumption of the devices. Due to the short range of the application scenario the SOs will be able to transmit their data directly to the gateway, without the need of forming a multi-hop network. While each installation on its own will be considerably small this setup is envisioned to be rolled out in each apartment of an apartment block and likewise in neighbouring apartment blocks, calling again for scalability and reliability issues of the used SOs.

The parameters that will be monitored are: (i) total and (ii) average energy consumption within a specific period (i.e. a day, or when they are turned on), and (iii) percentage or duration the device is functioning within a period of a day. When this energy monitoring network is combined with an automation system that has efficient algorithms and maybe access to additional information or sensor readings, the energy consumption of the monitored devices may be reduced significantly. For example, lights or the TV/PC screen can be automatically switched off when there is none in the room, the fridge may function in low/medium power when it is empty/half full and the heating system could function less if the windows are closed. However, both the monitoring and automation systems should be combined in a secure and reliable way.

For the case of a closed system that is described above there is no need for disclosing fine-grained consumption data to utility providers or the city. Keeping these data within the closed system raises less privacy concerns. However, when considering a *truly* Smart City, consumption data should be utilized by the electricity company or the public administrations in order to monitor the total energy consumption in the city. Utility providers will use these data for forecasting and control over the energy consuming devices and this is one of the many features discussed in the so-called Smart Grid [20]. Public administrations can utilize the energy consumption data to identify/monitor the results of any incentive programs e.g. checking if the subsidising the instalment of low-consumption heat pump systems has actually reduced the consumption of this household or not. The privacy and security concerns that are brought forward with the sharing of such data [20] have spawned research for solutions, e.g. [21], [22]. These and other works are revisited when dissecting this use case in RERUM.

[7]http://ec.europa.eu/energy/efficiency/eed/doc/2011_directive/com_2011_0370_en.pdf

D. Use Case #4 (Indoor): Comfort Quality Monitoring

Comfort Quality Monitoring (CQM) is an indoor UC for monitoring of the air quality and the overall indoor environment. RERUM differentiates between monitoring buildings, offices and houses comparing to museums and art galleries. The first case considers the human's health, so the SOs will monitor primarily the factors that can harm peoples. According to studies indoor air quality has a major impact on the people's wellbeing and comfort since, except health issues, it can also lead to reduced productivity and impaired learning in schools [23]. In the second case, the artifacts are under consideration due to their sensitivity in terms of environmental conditions (temperature, humidity, extreme light etc.).

In general, this UC could be seen as a variant of the outdoor "Environmental Monitoring" use case, but this is just a superficial reading. The CQM system will include only fixed sensors that could be placed in any area within a building/museum/gallery. Due to the limited range of the indoor areas and the need to minimize cabling, the SOs will be connected wirelessly forming a multi-hop mesh network with only one gateway, so opportunistic routing mechanisms like in [24] will be needed. Furthermore, the SOs may be moved from time to time according to some requirements, i.e. new paintings in other locations, moved artifacts, changes in the furniture, etc., so they will be equipped with batteries and their configuration has to be dynamic.

The parameters that will be measured for the CQM UC are: (i) temperature, (ii) humidity. (iii) light, (iv) smoke, and (v) CO_2. Humidity and temperature are important factors that can identify on the one hand when the indoor climate is optimal for humans and will not lead to mold or fungus and on the other hand if the indoor climate is appropriate for the artifacts. Smoke measurements can be used to detect and prevent fires. Finally, the monitoring system can be very easily combined with a building management/automation system for acting in order to keep the values of the measured parameters under predefined security/health thresholds. In this respect, SOs will include actuators that will control the lights, the air conditioning and the doors in order to maintain the indoor environment in normal conditions.

IV. Reliability and Security Issues

From the discussion on RERUM's four use cases, an immediate observation is that all of them are facing a common set of security threats, many of which stem from the heavy use of wireless and mobile networking. A non-comprehensive list of threats includes: (i) measurement reliability loss (due to e.g. node failure); (ii) connectivity loss due to wireless interference or denial of service attacks; (iii) eavesdropping; (iv) data falsification. Especially since most SOs are going to be wireless, the SC applications are susceptible to all wireless attacks, i.e. jamming and interference, which can decrease significantly the system performance as proved in [25] and result in connectivity loss. Additionally, the adoption of battery-powered smart objects and wireless sensor networking techniques raises the requirement to investigate and address battery depletion, since this has an impact on network reliability and deployment lifetime. Lastly, in the special case where SOs are used as actuators, special attention must be

paid to the trustworthiness of control messages sent to them, which requires authentication, authorisation and access control mechanisms. The two outdoor scenarios are additionally susceptible to threats related to network reliability loss due to physical phenomena, such as wind, humidity or rain and to threats related to physical destruction of hardware due to accidental or intentional damage.

Confidentiality, authenticity and integrity of data gathered within the IoT are key issues for the SC applications. The more autonomous and "smart" these objects become, the more threats arise when they interact with people. Reliable and resilient SC applications require network infrastructures to interconnect the large number of SOs in a secure way, guaranteeing the availability of resources in an efficient and effective manner and ensuring the autonomous and responsible handling of resources. Revamping existing security-by-design or resilience-by-design methodologies for heterogeneous access networks into the IoT is inappropriate.

A. Trust

All UCs either act directly upon the sensed data or assume that a different application will use them to provide input to informed decisions. Especially in the SC domain this will allow the stakeholders to make more informed and timely decisions. This means that the notion of trust gains a major relevance and must play a key role in the IoT deployment. Trust is seen as a quantifiable expectation that a SO will act as originally planned, or within a set of protocol parameters. Trust has to be bi-directional: the SOs have to trust each other and the application server with which they interact and the server has to trust the information it gets from the SOs. The reliability of the data that are exchanged between the SOs plays a significant role on determining the trustworthiness of the system. Especially when actuators are involved, the data/commands they receive have to come from trusted origins, because their actions can have direct impact on citizens. Without proper mechanisms, malicious or misbehaving SOs sending false data/commands can have severe effects on the system performance, which decrease the credibility of the SC applications and the trust that the citizens have on them.

B. Privacy

For all UCs the preservation of citizen and user privacy is important. In the Smart Transportation UC citizens will provide location and mobility data, which constitute personally identifiable information and must be protected by i.e. anonymisation or pseudonymisation. In the Home Energy Management UC, data regarding extensive periods of unused home appliances and patterns in usage and consumption could indicate that the property is vacant at specific periods and indirectly provide indications as to the whereabouts of its inhabitants. For the other two UCs the requirement for data privacy is not obvious at first sight. However, information regarding pollution could affect nearby businesses (i.e. if a square is polluted, nearby cafes and restaurants will not be attractive for citizens) so if required they could also be protected.

C. Vulnerability Assessment

In order to identify and address vulnerabilities in a satisfactory fashion, it is essential to determine the type, relative severity and extent of each threat. To do so, RERUM will conduct vulnerability assessment based on an established methodology [26], in accordance with the principles of methodical security testing: *reliable, repeatable, reportable* [27]. The assessment methodology to be followed includes the 5 modules presented in [26].

Technology \ Use-Case	UC #1	UC #2	UC #3	UC #4
Cognitive Radio SOs	~	*	*	*
Operating System Security Enhancements for the SOs	-	*	*	*
Malleable Signatures (MSS)	*	~	*	~
Compressed Sensing (CS)	*	*	*	*
Secure self configuration and bootstrapping	-	*	*	*
Reputation management framework	*	*	-	*
Cryptographic integrity and authenticity	*	*	*	*
Secure Object-to-Object configuration	-	*	*	*

TABLE I. RERUM'S TECHNOLOGIES FOR EACH UC

V. RERUM INTENDED SOLUTIONS

For enhancing the reliability of the SC applications, RERUM aims to develop a holistic security framework based on the concept of "Reliability, Security and Privacy by design" as described in [28]. The technologies that will be implemented for each UC are shown in Table I, where "~" means that the technology can be used only if needed in the specific use case. RERUM will support the always connected nature of both the mobile and the fixed SOs, by avoiding wireless interference using Cognitive Radio technology as described in [29]. That way, the SOs will only operate on unutilized frequencies employing intelligent spectrum sensing and assignment techniques (as described in [30]), with the basic constraint to minimize the energy consumption To ensure the reliable operation of the system and avoid network failures, mechanisms for self-monitoring statistics like energy, status (on or off), link status, and lost packets will be implemented. RERUM will also focus on the secure auto-configuration and bootstrapping of the SOs to avoid intrusion of unauthorized or malicious users/nodes. Secure auto-configuration will also enable the "plug-and-play" of the SOs with minimum human intervention, but with enhanced security so that no outsider will be able to change the SO settings.

To address the notion of Trust, RERUM will introduce the concept of trust in the core of the system and facilitate this through all its layers developing a cross-layer reputation management framework. The key concept is that using advanced fusion techniques only trusted SOs will be allowed to exchange data and malicious or misbehaving nodes sending false data will be excluded from the network. Thus, the reliability of the gathered data will be ensured. To measure the trustworthiness of SOs, a weight model capturing the data context will be used. Weight will not only determined by the input provided by users, but also by the time it was last updated and by the effect that the context really has in the related service. Additionally, the reputation management framework will use advanced fusion techniques for the data gathered by all SOs for evaluating the results to identify malicious or misbehaving objects. Finally, the cryptographic mechanisms that RERUM will employ are also able to identify the source, integrity and accuracy of the information exchanged by the SOs.

To keep the data from prying eyes, RERUM will deploy cryptographic mechanisms to ensure sufficient confidentiality on the communication channel. Driven by its privacy-by-design approach, RERUM ensures the privacy of data that is given to third parties by deploying adopted Privacy Enhancing Techniques (PETs) [31]. The main obstacle here is that to enable security and judge trustworthiness sensed data must be protected starting already from the originating sensor. Thus, sensors will need to sign the measurements to enable the sensed data to detect any subsequent modification. In such situations executing a PET will probably change the datum, e.g. reduce its accuracy by adding noise or lowering the resolution of the fine-grained power consumption, which will be in violation of the protection applied by the sensor. The resulting broken seal will however indicate that such data are no longer trustworthy, greatly diminishing the reliability of the sensed data for decision-makers. RERUM will encounter this by adapting cryptographic technologies allowing specified PET gateways to modify data in pre-defined ways to enable the exchange of privacy-preserving and reliable data. This would allow RERUM to tell a smart meter, trusted by the utility company, that a specific privacy gateway acting on behalf of the citizen will be allowed to add a certain amount of noise, thereby decreasing the accuracy, to protect the citizen's privacy. Finally, to combine privacy preservation and energy efficiency, Compressive Sensing techniques will be employed for optimizing data sampling and transmission.

VI. Conclusion

This work discusses the visions of the newly launched FP7 project RERUM towards enhancing the reliability and the security of SC applications. Although recent advances in IoT have opened up new business opportunities in the area of SC applications, both citizens are reluctant to adopt this new technology especially due to the inherent fear of publishing private data. This in return makes service providers also reluctant to investing in SC applications. RERUM has the citizen at the center of attention and by including city administrations in all phases of the project, it ensures that the citizens requirements will drive the system design. Additionally, RERUM adopts the concept of "reliability, security and privacy by design" and employs a number of security, privacy and trust mechanisms, most of which will be embedded on the SOs to provide inherent security and reliability to the SC applications.

Acknowledgment

The research leading to these results has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement n^o 609094.

References

[1] L. M. Correia and K. Wünstel, "Smart cities applications and requirements," *Net!Works European Technology Platform White Paper*, 2011.

[2] H. Schaffers, N. Komninos, and M. Pallot, "White paper smart cities as innovation ecosystems," *Fireball FP7 project White Paper*, 2012.

[3] G. Santucci, "From internet of data to internet of things," *International Conference on Future Trends of the Internet*, 2009.

[4] R. HÃd'nninen and J. Blom, "Every breath you take: Use of sensitizing methods in the design of air quality services," *12th biennial Participatory Design Conference (PDC)*, 2012.

[5] P. Dallemagne, D. Piguet, A. Restrepo, and M. SÃl'nÃl'clauze, "Wsn mobility support for long term water monitoring," *European Conference on Wireless Sensor Networks*, 2010.

[6] M. Lazarescu, "Design of a wsn platform for long-term environmental monitoring for iot applications," *Emerging and Selected Topics in Circuits and Systems, IEEE Journal on*, vol. 3, no. 1, pp. 45–54, 2013.

[7] L. Zhang, "An iot system for environmental monitoring and protecting with heterogeneous communication networks," in *CHINACOM*, 2011.

[8] E. Tang, F. Chen, and Q. Zhu, "Environment monitoring system based on internet of things," in *Emerging Technologies for Information Systems, Computing, and Management*, 2013, vol. 236, pp. 125–132.

[9] L. Oliveira and J. Rodrigues, "Wireless sensor networks: a survey on environmental monitoring," *Journal of Communications*, vol. 6, 2011.

[10] A. Pascale, M. Nicoli, F. Deflorio, B. Dalla Chiara, and U. SpagnoL.i, "Wireless sensor networks for traffic management and road safety," *Intelligent Transport Systems, IET*, vol. 6, no. 1, pp. 67–77, 2012.

[11] G. P. Grau *et al.*, "Vehicle-2-vehicle communication channel evaluation using the cvis platform," *IEEE, IET International Symposium on Communication Systems, Networks And Digital Signal Processing*, 2010.

[12] U. Raza *et al.*, "What does model-driven data acquisition really achieve in wireless sensor networks?" *IEEE PerCom*, 2012.

[13] Cambridge Systematics Inc., "Effective practices for congestion management: Final report," *U.S. Department of Transportation*, 2010.

[14] A. Bayen *et al.*, "Mobile century: Using gps mobile phones as traffic sensors: A field experiment," *UC Berkeley, Institute of Transportation Studies (ITS)*, 2010.

[15] T. Hunter *et al.*, "Large-scale estimation in cyberphysical systems using streaming data: A case study with arterial traffic estimation," *IEEE Transactions on Automation Science and Engineering*, vol. 10, 2013.

[16] F. Caiazzo *et al.*, "Air pollution and early deaths in the united states. part i: Quantifying the impact of major sectors in 2005," *Atmospheric Environment*, vol. 79, no. 0, pp. 198 – 208, 2013.

[17] Y. S. H. Najjar, "Gaseous pollutants formation and their harmful effects on health and environment," *Innovative Energy Policies*, 2011.

[18] V. Angelakis *et al.*, "Probabilistic routing schemes for ad-hoc opportunistic networks," *In I. Woungand et al. (eds.) Routing in Opportunistic Network*, 2013.

[19] Department of Energy, "Buildings share of electricity consumption/sales," *Buildings Energy Data Book.*, 2011.

[20] A. Cavoukian, J. Polonetsky, and C. Wolf, "Smartprivacy for the smart grid: embedding privacy into the design of electricity conservation," *Identity in the Information Society*, vol. 3, no. 2, pp. 275–294, 2010.

[21] A. Rial and G. Danezis, "Privacy-preserving smart metering," in *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society*. ACM, 2011, pp. 49–60.

[22] M. Jawurek, M. Johns, and F. Kerschbaum, "Plug-in privacy for smart metering billing," in *Privacy Enhancing Technologies*. Springer, 2011.

[23] R. A. Hobday, "Indoor environmental quality in refurbishment," *Historic Scotland Research Report 12*, 2011.

[24] N. Gazoni *et al.*, "A framework for opportunistic routing in multi-hop wireless networks," in *Proc. of the 7th ACM PE-WASUN 2010*.

[25] E. Tragos *et al.*, "The impact of interference on the performance of a multi-path metropolitan wireless mesh network," in *ISCC*, 2011.

[26] T. Tryfonas, I. Sutherland, and I. Pompogiatzis, "Employing penetration testing as an audit methodology for the security review of voip: Tests and examples," *Internet Research*, vol. 17, no. 1, pp. 61–87, 2007.

[27] N. Barrett, "Penetration testing and social engineering: Hacking the weakest link." *Inf. Sec. Techn. Report*, vol. 8, no. 4, pp. 56–64, 2003.

[28] H. C. Pöhls *et al.*, "Rerum: Building a reliable iot upon privacy- and security- enabled smart objects," in *Proc. of the IEEE WCNC 2014*.

[29] E. Tragos and V. Angelakis, "Cognitive Radio Inspired M2M Communications (Invited Paper)," in *IEEE Global Wireless Summit 2013*.

[30] E. Tragos, S. Zeadally, A. Fragkiadakis, and V. Siris, "Spectrum assignment in cognitive radio networks: A comprehensive survey," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 3, 2013.

[31] G. Van Blarkom, J. Borking, and J. Olk, "Handbook of privacy and privacy-enhancing technologies," *Privacy Incorporated Software Agent (PISA) Consortium, The Hague*, 2003.