IEEE WCNC 2014 - Workshop on IoT Communications and Technologies
Original at: http://dx.doi.org/10.1109/WCNCW.2014.6934872

RERUM: Building a Reliable IoT upon Privacy- and Security- enabled Smart Objects

Henrich C. Pöhls*, Vangelis Angelakis†, Santiago Suppan‡, Kai Fischer‡,
George Oikonomou§, Elias Z. Tragos¶, Rodrigo Diaz Rodriguez‖ and Theodoros Mouroutis**

*University of Passau, Germany, †ITN, Linköping University, Sweden, ‡Siemens AG, CT RTC ITS, Germany,
§Faculty of Engineering, University of Bristol, UK, ¶FORTH-ICS, Greece, ‖Atos, Spain, **Cyta Hellas, Greece.

Contact author: Henrich C. Pöhls {hp@sec.uni-passau.de}

***Abstract*—The Internet of Things (IoT) provides a platform for the interconnection of a plethora of smart objects. It has been widely accepted for providing Information and Communication Technologies (ICT) applications in many "smart" environments, such as cities, buildings, metering, and even agriculture. For several reasons though such applications have yet to achieve wide adoption; a major hurdle is the lack of user trust in the IoT and its role in everyday activities. RERUM, a recently started FP7 European Union project. aims to develop a framework which will allow IoT applications to consider security and privacy mechanisms early in their design phase, ensuring a configurable balance between reliability (requiring secure, trustworthy and precise data) and privacy (requiring data minimization for private information, like location). The RERUM framework will comprise an architecture, built upon novel network protocols and interfaces as well as the design of smart objects hardware. To highlight the challenges and evaluate the framework, RERUM will employ several Smart City application scenarios, which will be deployed and evaluated in real-world testbeds in two Smart Cities participating in the project. Here we detail the key technologies RERUM will investigate over the coming three years to reach its vision for IoT security, privacy and trust.**

***Keywords*—IoT, Smart City, Security, Privacy, Trust**

I. Introduction

The Internet of Things (IoT) is considered to be an important factor of economic growth. This massive network of heterogeneous devices (or interchangeably: machines, or things, or objects) is becoming part of peoples' everyday lives and will continue penetrating our day-to-day activities, as smart devices become ubiquitous. The IoT has gained much research attention the last few years due to the plethora of applications it supports for improving and simplifying peoples' lives. Everyday objects are being interconnected, communicate with each other and exchange the information they sense, and thus become "smart". However, users and service providers are reluctant to exploit this IoT potential without assurance for the safety of private information. With Smart Objects new security and privacy issues arise, regarding i.e. confidentiality, data integrity, information privacy, and safety. The IoT has the potential to create a new "cyber-physical" world, in which "things" can directly operate, act and influence the physical world, e.g. by closing doors, controlling heating, switching on the toaster, at least indirectly. In the Smart Cities context, information extracted from the environment can influence decisions taken by city administrations. For instance, in public transport routes or schedule changes. Furthermore, the IoT raises the issue of "life-logging", with the constant monitoring of our actions and data [1], [2]. Therefore the preservation of people's privacy and the assurance of no disclosure of information to any third parties become major challenges that the IoT systems must overcome.

A. RERUM's vision

This work presents the objectives and intended contribution of the newly launched EU-FP7 project RERUM, with an application on the Smart City domain. RERUM, standing for "REliable, Resilient and secUre IoT for sMart city applications", targets at increasing the reliability of IoT technologies while preserving the privacy of citizens and end-users. Doing so requires to define and attain a stable balance between :

- sensing the environment effectively, efficiently, timely, and trustworthily, and
- exchanging data securely i.e. safeguarding the privacy of human input and object sensed information.

Aiming to do so, RERUM will develop a framework and accompanying smart object (SO) hardware prototypes. These will allow adjustable levels of privacy and security at the earliest possible stage, focusing on embedded security, privacy and trust. Fig. 1 shows RERUM's technologies and illustrates the project's understanding of the privacy- and security-by-design paradigm.

RERUM's architecture will be configurable to suit a wide range of applications, not limited to the Smart City domain.

B. RERUM's key technologies to address the challenges

RERUM's primary goal is to enhance the reliability of the IoT while providing privacy protection mechanisms for Smart City applications. The main efforts are in three distinct but still intertwined areas: (i) Security, (ii) Privacy, and (iii) Trust. Table I presents technologies of key interest.

C. Outline

In Section II we briefly position RERUM's work plan with respect to existing work. We describe the envisioned contributions of the key technologies in each of the areas, i.e., Security (Sect. III), Privacy (Sect. IV), and Trust (Sect. V). Before we conclude, we describe our prototype hardware platform in Sect. VI.

978-1-4799-3086-9/14/$31.00 ©2014 IEEE

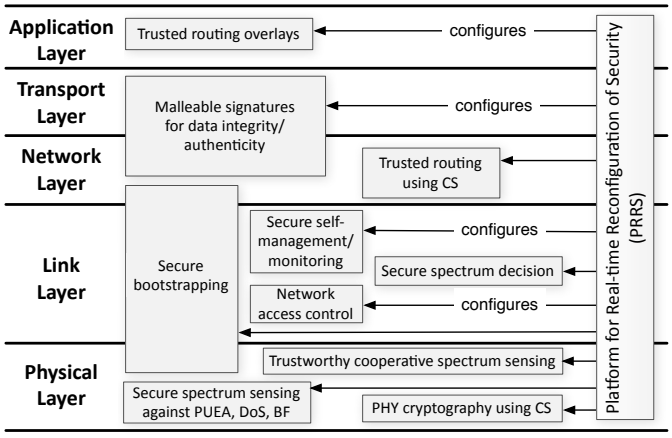

Fig. 1. RERUM holistically covers all layers of the ISO/OSI network stack, but concentrates on lower ones

II. Related Work

The growing number of wirelessly interconnected smart objects impacts the availability of spectrum resources, causing increased radio interference and network congestion. To tackle interference issues, RERUM utilises the advantages of Cognitive Radio (CR) technology, using dynamic spectrum access (DSA) in cooperation with spectrum sensing and spectrum assignment mechanisms [3]. These techniques are by now well-investigated for fixed and mobile devices, but not for objects within the IoT paradigm. Regarding security, the CR technology itself can be a technique to mitigate attacks like jamming in wireless environments, however it also raises new threats, especially in devices with very limited resources. The main open security and trust issues of CR-based devices and sensors are related to: (i) the integrity of the data exchanged during collaborative spectrum sensing, (ii) primary user emulation attacks, (iii) power consumption attacks, and (iv) unauthorised access to spectrum [4], [5]. However, up until now the research interest on CR-based smart objects or sensors has been limited, because of the inherent difficulty of their implementation due to their limited technical capabilities.

For the establishment of shared secrets at the Medium Access Control (MAC) layer, in recent research, cryptographic keys are pre-distributed among sensor nodes (see for example [6] and the references therein). Other approaches rely on dynamic key management and exchange [7], [8]. Meanwhile, the IEEE 802.15.4 standard specifies a framework for the encrypted exchange of layer-2 frames [9], without specifying key exchange methods. In addition to encryption at the MAC layer, methods have been proposed for the secure packet exchange at the network and transport layers. For example, there have been attempts to implement IPv6 IPSec for embedded devices [10], to establish public key based cryptosystems [11] and to implement Transport Layer Security (TLS) for wireless sensor nodes [12]. For constrained devices, Elliptic Curves can provide energy-efficient key exchange, such as the embedded implementation of Elliptic Curve Diffie-Hellman in [8].

Regarding the evaluation of reputation and trust, existing research proposes methods and algorithms based on user ratings (e.g. see [13] and the references therein). Consequently, they are not valid when addressing trust in IoT networks. In this respect, Gligor and Wing [14] present a theory of trust in networks of humans and computers that consists of elements of computational trust and behavioural trust. They present a simple communication model of entities (humans, hosts and applications) and channels. Within this model, a behavioural trust following a game-theoretical approach is used for human users. For computational trust, the existence of a secure communication channel is assumed, and the receiver will trust the received information when the value of the information is higher than the costs of trusting. This model has several limitations, such as the assumption of the existence of a secure channel. This can be considered true in the Internet domain, but it is not always true in IoT networks where devices are usually subject to resource restrictions (memory, power consumption, processing power, etc.).

TABLE I. RERUM's technologies to tackle IoT challenges

Technology \ Challenge	Security	Privacy	Trust
Communication & networking over Cognitive Radio (CR)-inspired M2M objects	*	*	*
Security Enhancements for the Contiki OS and compatible hardware	*	*	*
Malleable Signatures (MSS)		*	*
Compressed Sensing (CS)	*	*	
Secure self configuration	*		*
Reputation management framework			*
Cryptographic integrity and authenticity	*		
Secure Object-to-Object configuration	*		
PRRS	*		

The ability to identify the origin and verify the integrity of information can be used as one input to evaluate the trustworthiness of information. Mechanisms like Message Authentication Codes or Digital Signatures for origin authentication and integrity protection have been proposed for WSNs [15] or data stored in distributed systems [16]. However, classic integrity protection mechanisms do not cater for privacy enhancing techniques (PETs) that manipulate or remove integrity protected values in order to achieve privacy. For example, a classical digital signature over location information generated by a trusted sensor gets invalidated as soon as a PET applies obfuscation techniques to achieve location privacy [17]. However, RERUM foresees that applications can tolerate privacy enhancing modifications, if they can be identified as legitimate. RERUM will apply and extend a cryptographic technique called malleable signatures. This will enable the IoT to sanitize [18] or redact [19] privacy violating data if needed, while keeping a lowered, but still defined, level of integrity and origin on originally signed values.

III. Security

To thoroughly analyse the security of any ICT system, a concrete application scenario and attacker model is needed to define the protection goals. For RERUM the application domain is the IoT enabled Smart City. Smart City environments have very stringent security requirements, because they are used by a large number of users any security breach can harm citizens and infrastructures. This environment can be attacked in several ways: for example pushing erroneous data into the network and thus affecting accuracy and availability, accessing personal or otherwise sensitive information, compromising the systems' confidentiality and breaching the citizen's privacy, or manipulating smart objects in a large scale, tampering with the

system's integrity, or even disabling network parts. RERUM's research focus will create a new security tool-set for the IoT, considering and accompanying its realisation and deployment in Smart City environments. This will enable the interaction between security, privacy and trust and will be embedded in the architectural design.

A. Integrity

RERUM sees data integrity, broadly as a verifiable "property that data has not been altered or destroyed in an unauthorised manner" [20]. Under this ISO definition, RERUM envisages integrity paired with other relevant properties [21], such as (i) external consistency, (ii) availability and (iii) origin authentication.

The possibility that smart object readings carry a verifiable integrity and authenticated origin allows the Smart City applications to determine the amount of trust they can put onto these data. To achieve this, RERUM plans to employ and appropriately adapt existing cryptographic integrity and authenticity preserving mechanisms to detect integrity breaches on information exchanged.

B. Confidentiality

Confidentiality is a significant factor for Smart City applications since they inherently deal with private data. Citizen privacy and possibly well-being are endangered if personally identifiable information (see [22]) is disclosed. This becomes critical, in case an attacker obtains such information, but also in case of an unauthorised access by a smart object, which is considered an actor in the Smart City context as well. In accordance with common approaches in the literature, RERUM aims to address two major challenges for reaching confidentiality: First, RERUM will work on the definition of an access control mechanism, that is able to overpeer the vast amount of dynamic actors, switching in and out of the system. Secondly, RERUM will work on the definition of an authentication process for heterogeneous objects with different computational and connection capabilities [23]. Related efforts on access control for smart objects, that is, for data streams generated by the objects rather than data hosted in statistical databases, can be found in [24] and the references therein.

RERUM will give fresh impetus to a common understanding for access control approaches in the IoT, i.e. to expressive RBAC and query rewriting mechanisms that could help to protect data streams. Identity management will be handling the identity of smart objects, natural persons and their authorisation. This will imply an authorisation process, that will be handled inside a smart object federation.

RERUM will also design and implement mechanisms for secure object-to-object and object-to-internet communication, to ensure that no intruders or unauthorised users/objects gain access to the system. RERUM will research hop-by-hop, end-to-end and PKI-based authentication considering the limited resources of smart objects. The project will use related work as a reference point, as found in [25] for intermediate hop-to-hop authentication, [26], [27] for end-to-end authentication and [28] for an adoption of the public-key cryptography based schemes for data concealment in wireless sensor networks.

C. Availability

The importance of availability in the Smart City environment is evident due to the criticality of the smart objects for certain public services. Distributed denial of service (DDoS) attacks on battery-limited smart objects pose a major challenge to be addressed. RERUM will extend research on availability aiming to circumvent attacks on the Smart City infrastructure and factor in existing investigations such as [29] for the development of preventive countermeasures.

Another common DoS attack is the result of jamming at the ISM 2.4GHz (IEEE 802.15.4, 802.11) frequencies. Since these devices are normally exchanging small packets with low bitrate, even "legitimate" nearby 802.11 transmissions can have a dramatic effect on network performance (see e.g. [30]). To mitigate this issue, RERUM will enhance the sensor devices and the hardware smart objects with cognitive radio capabilities. However, since most sensors and smart objects are battery-limited, the focus will be on the optimization of the spectrum sensing and assignment techniques primarily considering their energy efficient. These techniques, consuming a minimum amount of energy, aim at avoiding jamming or congestion attacks by finding the most appropriate band for transmission. To achieve this, as discussed in [31] the CR-based smart objects (CR-SOs) will have to include new energy-based modules in the cognitive cycle. Using spectrum occupancy history, statistical analysis of the spectrum usage and variable sensing periods the CR-SOs will be able to identify the candidate available frequencies that they could use and that would need a minimum transmission energy when activated. This way, the CR-SOs will be capable of simultaneously mitigating both jamming and power consumption attacks. Furthermore, in a centralized network infrastructure, the combination of intelligent spectrum allocation with new light-weight authentication mechanisms, at a fusion center, will mitigate unauthorized access of spectrum by malicious or misbehaving nodes.

D. Secure Setup and Configuration

Self-X IoT properties present a potential attack surface to the Smart Objects and the applications depending on them. Therefore securing the RERUM framework for Smart City IoT requires a security architecture with the appropriate mechanisms. These typically require cryptographic credentials that can be symmetric and/or asymmetric, depending on the scenario and the requirements. The bootstrapping process to install them efficiently presents a significant challenge, especially for the large number of devices in an IoT deployment.

Typically, operational credential bootstrapping and key management protocols require the existence of some initial credentials as a starting point. Also key pre-distribution protocols, e.g. applied in wireless sensor networks, assume the configuration of some initial credential information before operation. RERUM will take approaches to initially bootstrap credentials on smart objects, and how to use them to update operational keys, and analyze their applicability on the desired Smart City applications. To avoid any incidents during network bootstrapping, RERUM will take into account existing bootstrapping protocols (such as EAP, PANA, 802.1x, CoAP, and 6LoWPAN) and will define mechanisms to optimise the process, enhance the security to minimise attacks for the desired Smart City applications.

Autonomous management of configuration should handle not only the initial setup but also the adaptation to any changes occurring during operation. Therefore, a continuous

monitoring of nodes is required to provide stability, security and QoS. The IoT supporting network should be able to self-heal and react promptly to any security attacks, glitches and degradation, originating either from internal causes (i.e. object failures) or external ones (i.e. jamming).

In this respect, RERUM will re-design basic self-X properties of smart objects to embed security and privacy mechanisms. Auto-configuration mechanisms will also be developed with built-in security and context-awareness, enabling the secure exchange of security settings through the network. RERUM will also develop distributed self-management and self-monitoring mechanisms for detecting faults in the network and monitoring smart object status. Key statistics to be monitored are energy, status (on or off), link state, lost packet count etc. That way, any object or link failures will be automatically detected and efficient self-healing algorithms will be applied to resolve these issues.

For monitoring and management of the security events the Platform for Run-time Reconfigurability of Security (PRRS), a component in the Future Internet core architecture [32], will be adapted to the IoT domain. This allows an end-user application to request its particular security requirements. In response, the PRRS framework looks for the most appropriate solution, deploys the selected security solution into the end-user environment, and installs a runtime monitor, which is responsible for detecting anomalous behaviour or non-conformance. If the latter occurs, the framework takes compensation actions. Moreover, an automated adaptation of the deployed security mechanisms allows smart object self-configuration according to changing context conditions.

IV. Privacy

Smart City applications require a large amount of sensed data with a high level of accuracy. These gathered data can generate privacy concerns in probably any IoT deployment. RERUM follows the "privacy-by-design" approach and will re-think current technology-focussed design decisions in the light of privacy when adapting the technology for the use in RERUM's architecture. Naturally, when smart objects are interconnected using other protocols, like GSM's cellular networks or the Internet, the application of privacy enhancing technologies is no longer solely within the hands of RERUM's smart object. To optimize privacy in these cases, RERUM aims at deploying Privacy Enhancing Techniques (PET) at the earliest point, i.e., on the sensed data already in the smart object, being able to ensure an adequate level of privacy on the level of the sensed data before it is sent into the network.

Citizen location is among the most common personal data collected for many IoT applications. Within RERUM, the location information gathered by the system will be protected via user-controlled privacy rules. The end-user will be able to consent the collection and use of his location information for clearly identified purposes, and he can select among the receivers of the location information and the granularity of the information, [33]. Within this context RERUM will also utilize further privacy-enhancing technologies (like mix-zones, etc.)..

With respect to the adoption of PETs, consider the following example of applying PET onto the unique hardware identifier of the network hardware with Contiki-based embedded smart objects. Here, PETs may have adverse effects on the network stack as core networking functions, such as Neighbour Discovery (ND), assume not only unique but also persistent hardware identifiers. PETs may therefore break such core functions, causing a chain reaction, potentially leading to objects being unable to communicate even with each other. RERUM targets to address this, investigating also other protocols (e.g. unicast and multicast routing, service discovery, header compression adaptations). The performance impact from adding privacy while still preserving a reliable mode of operation will be evaluated and tuned in RERUM.

A. Privacy Preserving Changes without breaking Integrity

Malleable Signature Schemes (MSS), like the classical digital signatures, aim to protect data from malicious modifications. The concept of malleable signatures allows a designated party, called the *sanitizer*, to be authorized by the signer to modify a previously signed message in an approved way. For actions not authorized and for parties who are not sanitizers, any modification results in a signature verification failure.

RERUM will work with a strong cryptographic privacy for MSS as the one in [34]. This will, inhibit an adversary from reverting the modification of a signed value by a PET mechanism with the help of the additional information contained in the still valid signature. Additionally, RERUM will analyze whether the so called unlinkability [35], can also be used for the IoT, introducing stronger notions of Privacy. By not allowing an adversary to learn the original information after it has been modified, MSS become a valuable tool allowing the anonymization of personally identifying data to conform with user requirements as well as with data protection rules.

With the control processes inherent in MSS's cryptographic mechanisms one controls which party is authorized to perform changes, as well as the scope of those changes. RERUM aims to refine the granularity and flexibility of MSS, thereby advancing current state of the art. RERUM will further try to offer implementations efficient enough for the IoT, following up on the latest runtime improvements [35], e.g. by building on elliptic curve cryptography.

B. Privacy by CS-based encryption

Compressive Sensing (CS) will be of major importance within RERUM since it achieves a high level of encryption combined with energy efficiency, two basic requirements of IoT applications. To achieve this within RERUM, typical signals of representative smart objects/sensors have to be analysed for their sparseness and if/how CS can be applied on them. Then, each smart object can simultaneously compress and encrypt its data using CS and forward it to the next hop. In this respect, existing routing protocols that use standard metrics, such as the ETX, with no focus on data encryption can be extended with CS-based metrics. These metrics will be used in the routing protocols used within RERUM for calculating dynamically the route of the packet, and when it should be transmitted depending on the compression/encryption gain at each node. Moreover, data from multiple smart objects will be combined, compressed and encrypted at intermediate nodes with larger battery capacity, thus increasing both the privacy of the data and the compression gain. The compression gain on

a node can be calculated as the number of own compressed packet bits transmitted over the total number of own packet bits plus packet bits from others. This ratio can be used as a metric to identify the next hop so that the total number of packets/bits sent through the network is minimised, thus saving energy. At the same time, by exploiting channel asymmetry, CS ensures that (i) packets encoded at the transmitter can be almost perfectly reconstructed at the legitimate receiver when the signal-to-noise-ratio (SNR) is greater than a given threshold, and (ii) that they cannot be decrypted with high probability by an eavesdropper, when the size of the encryption/compression matrix is accurately selected. RERUM will analyse the parameters of specific smart object signals in order to get both these benefits of CS.

V. Trust

In the context of smart object machine-to-machine networking within the IoT domain, the notion of trust gains a major relevance and can play a key role in IoT acceptance. Trust can in this setting be quantified as the expectation that an object will act as originally planned, or within a set of protocol parameters. To address the notion of Trust RERUM will introduce the concept in the core of the system through all its layers, with a specific focus on smart objects. The key concept is that only trusted smart objects will be allowed to exchange data. In order to measure smart object trustworthiness, 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, a reputation management mechanism will be developed, fusing the data gathered by all smart objects and evaluating the results to identify malicious or misbehaving objects.

RERUM will extend the state of the art for the earlier-mentioned MSS and enable to allow detecting potentially reduced integrity, which is suitable for the applications in the Smart City context. In other words, it becomes possible for RERUM's framework, through the use of MSS, to define who is allowed to breach integrity up to a defined level. An authorized modified value is less trustworthy than an unmodified value. However, MSS control the level of integrity and authenticity protection and thus can guarantee a certain level of protection, even if PETs have made modifications. RERUM's trust model will then be able to use this data governance information provided by such an enhanced MSS with the capability to signal occurred authorized changes as input for their trust decision. One of the most common attacks described in the literature for Cognitive Radio (CR) is the Spectrum Sensing Data Falsification (SSDF) attack. SSDF can be anticipated in a system with cooperative spectrum sensing, in which multiple CR-SOs exchange sensing local reports for available spectrum bands. In such a system, false reports may come either intentionally (from malicious nodes) or unintentionally (from misbehaving or faulty nodes). That way, smart objects may end up not using bands that are actually available. To avoid this, there is a need for developing a reputation management framework in the IoT domain, as the one presented in [36]. This will ensure that malicious/misbehaving objects will not be able to strongly impact system decisions. Existing approaches to mitigate SSDF are centralised and use one node (Fusion Center - FC) for gathering the reports, fusing them and taking the decisions. However, this raises the issue of a central point of failure that can cause system instability or unresponsiveness, e.g. when under a DoS attack. To avoid this, RERUM aims to develop a distributed reputation management system and sophisticated cooperative sensing algorithms with multiple distributed nodes playing the role of mini-FCs, analysing the reports of the CR-SOs and extracting their reputations according to fusion rules. The distributed FCs will exchange results periodically to fine tune the reputations of the CR-SOs.

VI. RERUM Prototyping and Technologies

For networks of battery-powered smart objects, deployment lifetime is an key concern. As discussed, RERUM will deploy new protocols and algorithms to enhance security, privacy and trust. These new mechanisms increase processing and signaling overhead, thus consuming more energy. RERUM will conduct simulations and proof of concept test-bed experiments, to quantitatively assess the trade-off between security, network performance, scalability and energy consumption.

RERUM's embedded components will be implemented for the Contiki OS, which runs on a wide range of IEEE802.15.4-capable devices. For the simulated evaluation, RERUM will use Cooja, a simulator for networks of smart embedded objects [37]. Energy consumption will be based on Contiki's "ENERGEST" module and the accompanying Powertrace tool. Contiki supports TCP/IP and many key low-power wireless standards, such as 6LoWPAN, the Routing Protocol for Low-Power and Lossy Networks (RPL) [38] and the Constrained Application Protocol (CoAP) [39]. The combination of those tools makes it possible to simulate a network of nodes running the same firmware as the one which will be subsequently used on the test-bed experiments.

RERUM will finally conduct tests on real hardware in laboratory test-beds, enabled primarily by the cutting-edge Zolertia Z1 platform[1], which is fully supported by Contiki. Prototype end-user Android applications will be developed and their energy consumption will be evaluated using PowerTutor.

VII. Conclusion

Although a significant amount of research has been recently performed in the area of the IoT, the fields of security and privacy in Smart City applications are comparably untouched. With Smart Cities currently gaining attention, service providers and public administrations are looking to exploit its benefits to provide services to the citizens. To do so, they need assurances that IoT-based applications will be reliable and will not affect citizen well-being due to malfunctions, misconfigurations, or security vulnerabilities. RERUM aims at enhancing the current IoT frameworks with built-in reliability, security and privacy, increasing the trustworthiness of the IoT. As a result, RERUM will have significant impact not only on the technological level, but also on business, the economy and the society. The "privacy-by-design" concept will ensure that user data will not be disclosed to any third parties and that private lives will remain private. Thus, a great barrier for the wider use of IoT applications from the citizens can be overcome.

[1] http://www.zolertia.com/products/Z1_Starter_Platform

RERUM enables the direct involvement of a good sample of both IoT and security stakeholders in defining, planning and evaluating the proposed architecture and framework. Thus it reinforces a virtuous circle since positive results will encourage even more citizen participation in the Smart City applications. In addition to that, RERUM's framework can open up opportunities for new businesses in the area of smart city applications for: (i) hardware manufacturers that will build sensors, actuators and smart objects with embedded security, privacy and reliability, (ii) telecom operators that will upgrade their infrastructure for handling the large volumes of IoT data and will become key players in the new market for providing the backbone connectivity for the smart objects, and (iii) the service providers that are the key IoT players and will benefit significantly by the technological advances of RERUM.

The proposed technological novelties and applications will be deployed and evaluated in real-world trials [40] in the cities of Heraklion (Greece) and Tarragona (Spain) to assess the performance of the framework in their actual environments with actual users, enabling a hands-on experience on the advantages of IoT in the Smart City domain.

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° 609094.

REFERENCES

[1] N. Petroulakis, et al., "A lightweight framework for secure life-logging in smart environments," *Information Security Technical Report*, 2012.

[2] A. Fragkiadakis, et al., "Secure and energy-efficient life-logging in wireless pervasive environments," in *Human Aspects of Information Security, Privacy, and Trust*. Springer, 2013, pp. 306–315.

[3] E. Tragos, et al., "Spectrum assignment in cognitive radio networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1108–1135, 2013.

[4] A. Araujo et al., "Security in cognitive wireless sensor networks. challenges and open problems," *Journal on Wireless Communications and Networking*, vol. 48, 2012.

[5] A. Fragkiadakis, E. Tragos, and I. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 428–445, 2013.

[6] W. Bechkit, et al, "A highly scalable key pre-distribution scheme for wireless sensor networks," *Wireless Communications, IEEE Transactions on*, vol. 12, no. 2, pp. 948–959, 2013.

[7] R. Roman, et al., "Key management systems for sensor networks in the context of the Internet of Things," *Computers & Electrical Engineering*, vol. 37, no. 2, pp. 147—159, Mar. 2011.

[8] P. Ilia, G. Oikonomou, and T. Tryfonas, "Cryptographic key exchange in ipv6-based low power, lossy networks," in *Proc. of WISTP '13)*, ser. Lecture Notes in Computer Science. Springer, May 2013, pp. 34–49.

[9] "802.15.4-2006: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Low Rate Wireless Personal Area Networks (LR-WPANs)," IEEE Standard, 2011.

[10] S. Raza, et al., "Securing Communication in 6LoWPAN with Compressed IPsec," in *Proc. 7th IEEE DCOSS '11)*, Jun. 2011.

[11] H. Wang, et al., "Public-key based access control in sensornet," *Wireless Networks*, vol. 17, no. 5, pp. 1217–1234, 2011.

[12] R. Mzid, et al, "Adapting TLS handshake protocol for heterogenous IP-based WSN using identity based cryptography," in *Int. Conf. on ICWUS '10)*, 2010, pp. 1–8.

[13] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decis. Support Syst.*, vol. 43, no. 2, pp. 618–644, 2007.

[14] V. Gligor and J. M. Wing, "Towards a theory of trust in networks of humans and computers," in *19th Int. Workshop on Security Protocols, ser. LNCS. Springer Verlag*, 2011.

[15] A. Perrig, et al., "SPINS: Security protocols for sensor networks," *Wireless networks*, vol. 8, no. 5, pp. 521–534, 2002.

[16] B. Carminati, E. Ferrari, and E. Bertino, "Securing XML data in third-party distribution systems," in *ACM CIKM*, 2005, pp. 99–106.

[17] B. Gedik and L. Liu, "Location privacy in mobile systems: A personalized anonymization model," in *Proc. of 25th IEEE ICDCS '05*. IEEE, 2005, pp. 620–629.

[18] G. Ateniese et al., "Sanitizable signatures," in *Proc. of 10th ESORICS '05*. Springer, 2005, pp. 159–177.

[19] R. Steinfeld, L. Bull, and Y. Zheng, "Content extraction signatures," in *Proc. of 4th ICISC '01*, vol. 2288. Springer, 2002, pp. 163–205.

[20] "7498-2: Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture," ISO/IEC Standard, 1989.

[21] D. Gollmann, "Veracity, plausibility, and reputation," in *Proc. of WISTP'12*. Berlin, Heidelberg: Springer-Verlag, 2012, pp. 20–28.

[22] "29100: Information technology – Security techniques – Privacy framework," ISO/IEC Standard, 2011.

[23] D. Miorandi, et al., "Survey paper internet of things: Vision, applications and research challenges," in *Ad Hoc Networks*, vol. 10. Elsevier, 2012.

[24] B. Carminati, et al., "A framework to enforce access control over data streams," *ACM Transactions on Information and System Security (TISSEC)*, vol. 13, no. 3, p. 28, 2010.

[25] M. Bagaa et al., "SEDAN: secure and efficient protocol for data aggregation in wireless sensor networks," in *Proc. of IEEE LCN*. IEEE, 2007, pp. 1053–1060.

[26] R. Riggio and S. Sicari, "Secure aggregation in hybrid mesh/sensor networks," in *Ultra Modern Telecommunications & Workshops*. IEEE, October 2009, pp. 1–6.

[27] A. Coen-Porisini and S. Sicari, "SeDAP: Secure data aggregation protocol in privacy aware wireless sensor networks," in *Proc. of the 2nd Int. Conf. on Sensor Systems and Software*. Springer Verlag, 2010.

[28] E. Mykletun, J. Girao, and D. Westhoff, "Public key based cryptoschemes for data concealment in wireless sensor networks," in *Proc. of IEEE ICC'06*. IEEE, September 2006, pp. 2288–2295.

[29] J. Gubbi, et al., "Internet of Things (IoT): A vision, architectural elements, and future directions," in *Future Generation Computer Systems*, vol. 29. Elsevier, September 2013, pp. 1645–1660.

[30] V. Angelakis et al., "Adjacent channel interference in 802.11a is harmful: Testbed validation of a simple quantification model," *IEEE Commun. Mag.*, vol. 49, no. 3, pp. 160–166, 2011.

[31] E. Tragos and V. Angelakis, "Cognitive Radio Inspired M2M Communications (Invited Paper)," in *Proc. IEEE GWS 2013*, Jun. 2013.

[32] A. Garcia, et al., "FI-WARE Security: Future Internet Security Core," in *Towards a Service-Based Internet*, ser. Lecture Notes in Computer Science, vol. 6994. Springer Berlin Heidelberg, 2011, pp. 144–152.

[33] J. Cuellar et al. (2007, February) RFC 3693: Geopriv Requirements. IETF. [Online]. Available: http://tools.ietf.org/rfc/index

[34] C. Brzuska, et al., "Security of sanitizable signatures revisited," in *Proc. PKC 2009*. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 317–336.

[35] C. Brzuska, H. C. Pöhls, and K. Samelin, "Efficient and perfectly unlinkable sanitizable signatures without group signatures," in *Proc. of EuroPKI 2013*, ser. LNCS. Springer, 2013.

[36] A. Mihovska et al., "Design considerations for a cognitive radio trust and security framework," in *IEEE CAMAD 2012*, 2012.

[37] F. Österlind, "A Sensor Network Simulator for the Contiki OS," Swedish Institute of Computer Science technical report, 2006.

[38] T. Winter, et al., "RPL: IPv6 Routing Protocol for Low power and Lossy Networks," RFC 6550, Mar. 2012.

[39] Z. Shelby, K. Hartke, and C. Bormann, "Constrained application protocol (CoAP)," Internet Draft, Jun. 2013, (draft-ietf-core-coap-18).

[40] E. Tragos, et al., "Enabling Reliable and Secure IoT-based Smart City Applications," in *IEEE PerCity' 14*, 2014, to be published.