Security and Privacy in your Smart City

A. Bartoli*, J. Hernández-Serrano†, M. Soriano*†, M. Dohler*, A. Kountouris‡ and D. Barthel‡
*Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Spain
†Universitat Politècnica de Catalunya (UPC), Spain
‡Orange, France Telecom, France

Abstract—**With the majority of the population living in urban environments today, the concept of Smart Cities has become an urgent necessity. It refers to an urban transformation which, using latest ICT technologies, makes cities more efficient. Composed of a growing Internet of networks, such as the one connecting humans via cellular systems, computers via broadband connections, or objects and sensors via low-cost data links, the greatest challenge today is to meaningfully manage such systems. Given that these systems will greatly impact human lives, issues related to privacy and security have come into limelight. With a surge in security breaches, not only in the Internet but also with mobile phones and now sensing infrastructures, engineers are very conscious to include privacy and security requirements into architectural designs from the very beginning. This paper summarizes the key challenges, emerging technology standards, and issues to be watched out for in the context of privacy and security in smart cities. A key observations is that privacy can be achieved i) by imposing high security requirements onto the used technology to avoid third party abuses; and ii) by decoupling technical smart city data streams from the personal one to avoid abuse of data by insiders.**

I. Introduction

The vision of "Smart Cities" is the urban center of the future, made safe, secure, environmentally, green, and efficient because all structures, whether for power, water, transportation, etc. are designed, constructed, and maintained making use of advanced, integrated materials, sensors, electronics, and networks which are interfaced with computerized systems comprised of databases, tracking, and decision-making algorithms. The concept of Smart City is a natural evolution because current global trends in energy supply and consumption are patently unsustainable; environmentally, economically, and socially. The scientific community believes that the future of human prosperity depends on how successfully we (people) tackle the two central energy challenges facing us today: securing the supply of reliable and affordable energy; and effecting a rapid transformation to a low-carbon, efficient and environmentally benign system of energy supply. In a few words: an energy revolution.

The research and engineering challenges along the way to this vision encompass many technical fields including physics, chemistry, biology, mathematics, computing science, systems, mechanical, electronics and civil engineering. At the simplest level is the basic component and its associated "“feedback” or self-monitoring mechanism(s). Each must be identified or, if already existing, tailored for the appropriate application. At the next level is the design of the system making use of these components. Associated with this would be the interface to the computerized "monitoring" capability for each given function. Next, is the full structure or service supplied (databases), and lastly, the integration (specific protocols) of information across all related and seemingly unrelated aspects of an urban centers essential infrastructure. These topics will be populated in more details in Sections II and III,"Smart City elements" and "Smart City architecture".

So-called Smart City will take advantage of communication and sensor capabilities sewn into the cities' infrastructures to optimize electrical, transport, and other logistical operations supporting daily life, thereby improving the quality of life for everyone. It would be overly simplistic, and probably a big mistake, to believe that traditional networking technologies can simply be added into a city's critical infrastructure to make it "smarter". New solutions are absolutely necessary not only to improve the quality of daily-life with innovative efficient protocols but also in terms of security/reliability. Security/reliability because the networks will be exposed to a broad range of attacks, internal and external parties are not trusted and privacy will be a vital prerequisite to consumer acceptance. In addition, since the assumptions and requirements for smart critical infrastructures are very different, implying that networks for smart cities should be engineered quite differently, this also raises an integration problem.

This paper discusses the importance of security in this scenario of Smart Cities, where different kinds of communications will be implemented together with new secure and efficient solutions/protocols to realize all the several opportunities that Smart City can offer. The paper is structured as following: Section II, deals with the principle elements fundamental to provide "smartness" to "old" infrastructures. Section III, presents the architecture for future Smart City focuses on its components and the communications technologies implemented there. Section IV, is the core of this paper and deals with the security in Smart City highlighting sensitive problems identified in this context. Section **??** and Section **??** respectively focus on the Capillary Smart City M2M Standards solution of the present and the Cellular Smart City M2M Standard solution that are studied for the future implementation of the Internet of Thing concept in Smart City and for various future cellular applications. The proposal paper is concluded with Section VII.

II. Smart City Elements

The Smart City principle development elements are forming the overall smart city framework. They need to be debated starting from the infrastructure preparation stage. Old structure of the utilities has to be re-studied and in this context three elements have to be taking into account to provide “smartness”:

- **Hardware/Software elements:** The smart concept is represented in transmitting and receiving the data using communication protocols from and to the network element (asset). The asset’s data sending and receiving is the base of monitoring and controlling the functional operational framework needed for smartly network assets managing. The most practical way is to embed the required hardware (operational sensors) and software during the design phase.
- **Databases elements:** The second element for creating Smart City is to build up the proper database that would reflect the existing/proposed infrastructure networks. The database has to reflect the completeness of the network assets as well as the consistency and data integrity. The assets positional accuracy is extremely important aspect that has to be taken care for all of network assets which will reflect the physical reality of the system that would be the base for all network spatial analysis actions. On the other hand the database has to manage the data communication protocols between the assets programmable logic controllers and the data servers.
- **Management System elements:** After preparing the database that reflects the physical reality of the assets/network components. The third element is to build up the most practical and efficient Management System (MS). The MS has to have an automation work frame that has to be smartly operated in order to save energy and accordingly reduce the running cost. The magnitude of energy saving produced due to the economical automation and comfortable/easiness operation reflects the level of the smartness that the building has.

III. Smart City Architecture

The main goal of the Smart City architecture is to provide a structure for the implementation of information services for monitoring critical infrastructures and organize the Smart City data-bases. The Smart City architecture, which is majority applied in five cities in the world (Malta, Dubai Internet City, Dubai Media City, Dubai Festival City and Kochi), has four principle unites that cover almost all the networks, processes, applications and several associated activities in different trends. These four unites are:

- **Application unit:** Applications are related to physical assets monitoring using surveying technologies such as satellite imagery; WS, M2M and embedded networks; aerial mapping; GPS/GNSS reference station and laser/LIDAR technologies. These technologies permits to operate the following applications: city security processes, industrial monitoring, building management system for building’s automation, Closed Circuit Television (CCTV) for several types of monitoring and controlling, Community Access Television (CATV), Geographic Information System (GIS) for overall visualization, analysis and data banking.
- **Information unit:** The city information unit is very essential in order to realize the function of using the mentioned applications. The majority of the information units that used to communicate the city applications are as follow: user information for monitoring the public behavior; document information for better statistical and feasibility studies; industry information for monitoring the market demand, inflation and others; business information for more commerce and financial analysis; revenue information for better understanding of the market cash flow and daily business activities; circulation information for treating the new emerged business cases.
- **Management unit:** The third principle component is process management. It is really important because it defines the relationship, rules, strategies and policies between the city applications and related information unites. The management has to participate in the following parties which will substantiate the overall city components.
- **Integration communication protocol unit:** The closer of this activity city cycle is the connection between these three principle components. The connectors (integration communication protocols) might be utilizing the conventional wiring network or using fiber optic cables for the systems that depending on the physical network connectivity concept. Wireless, Bluetooth, Wi-Fi and different GSM technologies are going to be mature in the near future, which make them more practical and feasible solutions for data sharing and information exchange processes. In addition of them, also M2M and embedded network will be implemented for low-power networks; they will be key actors for real-time monitoring and networking communication in critical parts of Smart City (e.g.: Smart Grid).

More in details, smart nodes are responsible to produce and/or to consume (query/subscribe) notifications of events (application unit). Notifications describe the events as observed locally by smart nodes and the decision to publish a notification is a core part of the publisher smart nodes internal logic. If is needed, notifications are simply stored in data-bases (information unit), otherwise, for example, if they are high priority notifications, they are sent to the decision-maker unit (management unit). The management unit will elaborate them and the output result can be a notification directed to the information unit or a query directed to both information and application units. The cooperation between nodes, data-base, and decision-makers is possible thanks the integration communication protocols unit. A set of suitable security policies allows the system to restrict the notifications only to the smart nodes that have subscribed with appropriate credentials and protect the sensible information with advanced security techniques. Security will be treated more in details in Section number IV.

In conclusion, with this architecture, Smart Cities permit to respond to the needs for a system that serving the decision-makers for following up the daily activities with a proper design that will definitely reduce the operational consumption for the long term, saving energy and reducing costs with efficient and secure real-time monitoring protocols.

IV. Security in Smart Grid

As part of the development of Smart City, control systems have to become more sophisticated, allowing better control and higher reliability. Smart City will require higher degrees of network connectivity to support new sophisticated features. This higher degree of connectivity also has the potential to open up new vulnerabilities. For this reason, one of the biggest challenges facing Smart City development is related to Cyber Security of Systems [1]. Cyber security is a critical issue due to the increasing potential of cyber attacks and incidents against critical sectors in Smart City. Cyber security must address not only deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists, but inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the system in unpredictable ways. To protect Smart City in a proper way, a number of security problems have to be faced according to a specific design/plan; here, some of the issues that have to be taking into account in the design phase are described:

- **Privacy:** If users deem a system as insecure for his/her sensitive information (privacy), it will not be able to establish itself successfully in the market. Important social challenges stem from the necessity to adapt Smart City services to the specific characteristics of every user. A service has many configurations options, depending on user expectations and preferences; the knowledge of these preferences usually means the success or failure of a service. In order to adapt a service to the specific user's preferences, it is necessary to know them, and this is basically done based on a characterization of that specific user. Nevertheless, a complete characterization of user preferences and behavior can be considered as a personal threat, so the great societal challenge for this, and for any service requiring user characterization, is to assure user's privacy and security. Thus, in order to achieve user consent, trust in, and acceptance of Smart Cities, integration of security and privacy preserving mechanisms must be a key concern of future research. The overall priority must be to establish user confidence in the upcoming technologies, as otherwise users will hesitate to accept the services provided by Smart Cities.
- **Networking connectivity:** Keeping the network private, i.e. where all transport facilities are wholly owned by the utility, would greatly minimize the threats from intruders, as there would be no potential for access from intruders over the Internet. But having a completely separate network is not feasible in today's highly connected world; it makes good business sense to reuse communications facilities, such as the Internet. A minimally secured Internet-connected Smart City approach, as commonly found with commercial networks, opens the door to threats from multiple types of attacks. These include cyber attacks from hostile groups looking to cause an interruption of the services. Another type of attack is worm infestations which have proven to negatively impact critical network infrastructures. Such threats have largely been the result of leaving a network vulnerable to threats from the Internet. For example, there have been denial of service ("DoS") attacks on a single network that disrupted all directory name servers, thus prohibiting users from connecting to any of the resources. This demonstrates the fragility of an Internet-connected network.
- **Complexity:** By interconnecting systems that serve totally different purposes (e.g., traffic control and energy management), and thereby creating a "system of systems", the complexity of such collaborating systems increases exponentially. As a result, the number of vulnerabilities in a Smart City system will be significantly higher than that of each of its sub-systems. Furthermore, the pure interconnection of two systems might open the door to new attacks that have not been considered before, when securing either of the individual systems. Therefore, research into ways of handling the increasing complexity of distributed systems from the security perspective is required, which includes: cost-effective and tamper resistant smart systems or device architectures (crypto and key management for platforms with limited memory and computation); evolutionary trust models (i.e., trust is not static but dynamic, and associated values can change a long time) for scalable and secure inter-system interaction; abstract and comprehensive security policy languages; self-monitoring and self-protecting systems, as well as development of (formal) methods for designing security and privacy into complex and interdependent systems; overall thread models that allow to take multiple sub-systems into account.
- **Security services:** The Smart City industry requires access to cost-effective, high-performance security services, including expertise in mobility, security, and systems integration. These security services can be tailored per utility to best fit their needs and help them achieve their organizational objectives. An experienced security services organization would need to provide the following capabilities: Proven expertise in information security, for organizations such as governments, large enterprisers and service providers; holistic security framework that operationalizes security across the people, process, policy and technology foundations of each organization; experience in Security and Compliance Pre-Audit Assessments; threat Management expertise - Design, Managed Service, and Integration; policy Design and Related Services - Incident Response Planning, Risk Management, Compliance.
- **Sensitive data organization:** The number of users, and the volume and quality of collected data, will also increase with the development of Smart Cities. When personal data is collected by smart meters, smart phones, connected plug-in hybrid electric vehicles, and other types of ubiquitous sensors, privacy becomes all the more important. The challenge is, on the one hand, in the area of identity and privacy management, where, for instance, pseudo-nomination must be applied throughout

the whole system, in order to separate the data collected about a user (which is required in order to provide high-quality personalized services) from the user's real identity (which is required for purposes such as accounting); this includes that the usage of addressing identifiers, such as IP or MAC addresses, for the purpose of identification must be avoided in future systems. On the other hand, security technologies, such as advanced encryption and access control, and intelligent data aggregation techniques (interesting secure data aggregation scheme for low-power networks [2])must be integrated into all systems, in order to reduce the amount of personal data as far as possible, without limiting the quality of service.

- **Availability:** The availability of the services depends on the proper operations of many components and the proper connectivity between these components. To disrupt a service, an attacker might attempt to gain electronic access to a component and misconfigure it or to impersonate another component and report a false condition or alarm, but one of the simplest types of attacks that an adversary might attempt is the denial of service attack, where the adversary prevents authorized devices from communicating by consuming excessive resources on one device. For example, it is a well-known issue that if a node, such as a server or an access control device uses an authentication protocol which is stateful prior to authentication and authorization, then the node may be subject to denial of service attacks. Smart City protocol designers must ensure that proper care and attention is given to this threat during protocol development. Interesting solution to provide availability against DoS attacks is presented in [3].
- **Emergency plan:** The components, systems, networks, and architecture are all important to the security design and reliability of the Smart City communications solution. But it's inevitable that an incident will occur at some point and one must be prepared with the proper Incident Response plan. This can vary between commercial providers and private utility networks. A private utility network is likely to provide better consistency of the incident response plan in the event of a security incident, assuming the private network is build upon a standardized framework of hardware and software. The speed of the response decreases exponentially as the number of parties involved increases. Conversely, a private network would ideally depend on fewer parties, therefore a more efficient incident response process would provide for more rapid response and resolution. The rapidity of the response is critical during emergency situations.
- **Key management:** Some sort of key management is necessary to provide a reliable crypto security. Considering that the Smart City will contain millions of devices, spread across hundreds of organizations, the key management systems used must be scalable to extraordinary levels. Further, key management must offer strong security (authentication and authorization), inter-organization interoperability, and the highest possible levels of efficiency to ensure that unnecessary cost due to overhead, provisioning, and maintenance are minimized. It is likely that new key management systems (specialized to meet the requirements of Smart City) will be needed. State of Art is poor in this specific field.

V. Capillary Smart City M2M Solutions – IoT of the Present

In this Section we present the short range capillary Smart City M2M solutions, that are being standardized by various SDOs (notably the IEEE, IETF and interest groups relying thereupon) and that represent the IoT of the present. These solutions are the basis on which to build the Smart City of the future.

A. IEEE Standards Solutions

The IEEE is standardizing the physical (PHY) and medium access control (MAC) layers. There are three families facilitating low-power short-range IoT operation, i.e. IEEE 802.15.4 (as used by ZigBee); IEEE 802.15.1 (as used by Bluetooth); and IEEE 802.15.11 (as used by Wi-Fi). We subsequently briefly discuss their role in the capillary Smart City M2M ecosystem.

1) IEEE 802.15.4.: IEEE 802.15.4 [4] [5]is maintained by the IEEE 802.15 working group. IEEE standard 802.15.4 intends to offer the fundamental lower network layers of a type of wireless personal area network (WPAN) which focuses on low-cost, low-speed ubiquitous communication between devices. The emphasis is on very low cost communication of nearby devices with little to no underlying infrastructure, intending to exploit this to lower power consumption even more. Important features include real-time suitability by reservation of guaranteed time slots, collision avoidance through CSMA/CA and integrated support for secure communications. Devices also include power management functions such as link quality and energy detection. IEEE 802.15.4 is the basis for the ZigBee, WirelessHART, and ISA 100.11a specification, each of which further attempts to offer a complete networking solution by developing the upper layers which are not covered by the standard. The following list summarizes the stable and currently evolving versions:

- **IEEE 802.15.4-2006.** It consists today of several different PHY layers, all tailored to low power operation. There are two different MAC layers, i.e. the non-beacon-enabled mode for low traffic and the beacon-enabled mode for medium and high traffic. The link layer is generally very secure, accept that the acknowledgements are sent in clear thus constituting a very serious security hole which has been greatly underestimated by many real-world deployments, including those using ZigBee.
- **IEEE 802.15.4e.** The IEEE 802.15.4e task group is in charge to modify the MAC sub-layer of IEEE 802.15.4 to meet the requirements of various industrial applications overcoming limitations of the current MACs. The application includes factory automation, process automation, intelligent building, asset tracking, and smart grid. This task group has emphasized three major elements: media management to minimize listening costs, improved

security mechanisms, and increased link level reliability through the use of multiple channels, especially in the narrow, lower frequency bands. Now, with the 4e standard approaching ratification, IP networks will be able to improve their performance. Security has been taken very seriously, where the loophole of the unsecured acknowledgement has been rectified.
- **IEEE 802.15.4f.** It has been chartered to define new wireless PHYs and MAC enhancements required to support active RFID system for bi-directional and location determination applications. An active RFID tag is a device which is typically attached to an asset or person with a unique identification and the ability to produce its own radio signal not derived from an external radio signal. Currently, three PHY layers are under discussion.
- **IEEE 802.15.4g.** The role of IEEE 802.15 Smart Utility Networks (SUN) Task Group 4g is to create a PHY amendment to 802.15.4 to provide a global standard that facilitates very large scale process control applications such as the utility smart-grid network capable of supporting large, geographically diverse networks with minimal infrastructure, with potentially millions of fixed endpoints. It is currently under development.
- **IEEE 802.15.4k.** It addresses applications such as critical infrastructure monitoring. It defines an alternate PHY and only those MAC modifications needed to support its implementation. It is fully concentrated on ultra-low power operation, thus allowing for connectivity where no permanent energy sources are available.

2) IEEE 802.11.: In 1997 the IEEE adopted IEEE Standard 802.11-1997 [4], the first wireless LAN (WLAN) standard. This technology is promoted from WiFi Alliance that is a trade association in charge of certifies products if they conform to certain standards of interpretability. Wifi has had a tremendous success in recent years and has also technically been advanced through various amendments. As such, IEEE 802.11 networks are not suitable to low-power networking designs; however, latest developments into low-power solutions may yield some surprises. Notably, if low-power Wifi really takes off, the problem of coverage which IEEE 802.15.4 networks try to overcome by means of multihop will automatically be eliminated.

- **IEEE 802.11 Low Power.** With the growing market for smart objects and wireless sensors, several companies have developed application specific integrated circuits that are optimized for sensing applications. These products achieve a similar power profile as above low power architectures whilst leveraging the huge installed base of over 2 billion Wifi certified devices; a vibrant standard and industry alliance of close to 300 members; well proven encryption, authentication and end to end network security; mature network management systems; etc. Among one of the first companies promoting the concept of low power Wifi was Ozmo Devices. They tune the .11 protocol stack as well as introduce aggressive power saving operations.
- **Security Issues.** The Wifi Protected Access (WPA) security protocol has become the industry standard for securing .11 networks. Using a pre-shared encryption key (PSK) or digital certificates, the WPA algorithm Temporal Key Integrity Protocol (TKIP) securely encrypts data and provides authentication to said networks. TKIP was designed to be a transition between old hardware and new encryption models. The IEEE 802.11i protocol improved upon the WPA algorithm (TKIP) to the new WPA2 [6] that uses a better encryption algorithm: Advanced Encryption Standard (AES). As a major step forward, the protocol also specifies more advanced key distribution techniques, which result in better session security to prevent eavesdropping.

B. IETF Standards Solutions

The Internet Engineering Task Force (IETF) is actually not an SDO since not approved by the US government. It is composed of individuals, not companies. It meets about three times a year, and gathers an average of 1,300 individuals. It enjoys more than 120 active working groups organized into various areas. The general scope of the IETF is *above the wire/link and below the application*. However, layers are getting fuzzy (MAC & APL influence routing) and we lately hence experience a constant exploration of edges. There are three working groups pertinent to capillary M2M where we will concentrate on two, i.e. IETF 6LoWPAN (establishing gateway to Internet); and IETF ROLL (facilitating routing in low-power network). We subsequently briefly discuss their role in the capillary M2M ecosystem.

1) IETF 6LoWPAN.: IPv6 over Low power WPAN (6LoWPAN) acts as a simplified gateway between the low power embedded network and the Internet. It facilitates neighborhood discovery, header compression with up to 80% compression rate, packet fragmentation (1260 byte IPv6 frames → 127 byte IEEE 802.15.4 frames), and thus direct end-to-end Internet integration. However, it does not provide routing. Security is also catered for [7].

2) IETF ROLL.: Routing Over Low power and Lossy networks (ROLL) deals with the design of a routing protocol for wireless low power mesh networks. It is in its final stage of standardization. It is based on a gradient routing protocol where nodes acquire a rank based on the distance to the collecting node and the messages follow the gradient of ranks to reach the destination. Again, security is currently being catered for [8].

VI. Cellular Smart City M2M Solutions – IoT of the Future

Cellular Smart City M2M technology developments are commencing to take momentum, with many companies and various SDOs envisioning future IoT applications to run over such networks. From a rate and range point of view, current cellular systems already meet the M2M requirements; however, from a power consumption point of view, many issues remain open. We will thus briefly discuss various cellular M2M initiatives that are studied for Smart City scenario.

A. ETSI M2M

ETSI M2M is composed by various manufacturers, operators and service providers, among others. ETSI typically provides the framework, requirements and architecture, whereupon technologies such as 3GPP or IEEE can be used to populate the developed architecture. The work is organized in stages:

- **Stage 0: Use cases documents.** Several use case documents have been developed in parallel, such as M2M requirements for smart metering, health applications, etc.
- **Stage 1: Services requirements.** The thus resulting service requirements have then been developed which aims to unify the requirements of the different use case documents.
- **Stage 2: Architecture.** Here, capabilities and interfaces are developed, as well as message flows, etc.
- **Stage 3: Refinement.** In this stage, the architecture is refined to meet the prior outlined user requirements.

ETSI M2M currently (Q1 2011) also works on security requirements which influence the entire M2M architectural design.

B. 3GPP LTE-M

The concept of M2M has been born out from 2G cellular systems and, early adopters of GSM/GPRS data plans, clearly demonstrated the its value. 3GPP thus naturally issued in January 2007 a technical report TR 22.868 “Study on Facilitating Machine to Machine Communication in 3GPP Systems” which identified that a huge market potential for M2M beyond the current market segment. However, due to CDMA-based 3G systems not being suitable to low power operations, there have been little developments until recently. With OFDM-based LTE on the horizon, cellular M2M has suddenly become of interest again and a set of further documents has been issued lately, e.g. TS 22.368 “Service Requirements for Machine-Type Communications (MTC)” and TR 23.888 “System Improvements for MTC”.

Not all MTC applications have the same characteristics and not every optimization is suitable to all applications; therefore, features are defined to provide some structure to the customer and the network is then tuned accordingly to needs. These features are offered on a per subscription basis and include items such as Low Mobility, Time Controlled, Time Tolerant, Packet Switched only, Small Data Transmissions, Mobile originated only, Infrequent Mobile Terminated, MTC Monitoring, Priority Alarm Message (PAM), Secure Connection, Location Specific Trigger, Network Provided destination for Uplink Data, Infrequent transmission, Group Based Policing, Group Based Addressing, etc.

VII. Conclusions

The concept of Smart Cities gained importance in the last years, as a means of enabling services and applications available to the citizens, companies and authorities that are part of a city’s system. It aims at increasing citizens’ quality of life, and improving the efficiency and quality of the services provided by governing entities and businesses. This perspective requires an integrated vision of a city and of its infrastructures, in all its components: it has to incorporate a number of dimensions that are not related to technology, e.g., the social and political ones. As a critical infrastructure element of future society, Smart City requires the highest levels of security. A comprehensive architecture with security built in from the beginning is necessary. In order to achieve user consent, trust in, and acceptance of Smart Cities, integration of security and privacy-preserving mechanisms must be a key concern of future research.

Overall research challenges can be classified into the following aspects: identity and privacy management, where, e.g., pseudo-nomination must be applied throughout the whole system, in order to separate the data collected about a user from the user’s real identity; integration into systems of security technologies, e.g., advanced encryption and access control, and intelligent data aggregation techniques; handling of the increasing complexity of distributed systems from the security perspective is required; a number of security services have to be defined just to provide high security level; availability needs to be guaranteed because services delays and DoS attacks don’t have to affect daily life of citizens; security emergency plan is fundamental because Smart City will implement a great number of new solutions that cannot be tested in properly way; finally, key management is necessary to provide reliable and efficient mechanisms of re-keying just to complete cyber Security with low energy costs.

Acknowledgment

This work has in part been supported by a France Telecom research contract on M2M security as well as the EU project ICT-258512 EXALTED.

References

[1] (2009) Smart grid cyber security strategy and requirements. [Online]. Available: www.nist.gov

[2] A. Bartoli, H. J., M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, “Secure lossless aggregation for smart grid m2m networks,” in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, oct. 2010, pp. 333 –338.

[3] A. Bartoli, J. Hernandez, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, “Secure lossless aggregation over fading & shadowing channels for smart grid m2m networks,” *IEEE Transactions on Smart Grids*, 2010 November.

[4] (2010) The ieee 802.x website. [Online]. Available: http://www.ieee802.org/11/

[5] J. Lopez, R. Roman, and C. Alcaraz, “Analysis of security threats, requirements, technologies and standards in wireless sensor networks,” in *Foundations of Security Analysis and Design V*, ser. Lecture Notes in Computer Science, A. Aldini, G. Barthe, and R. Gorrieri, Eds. Springer Berlin / Heidelberg, vol. 5705, pp. 289–338.

[6] J.-C. Chen, M.-C. Jiang, and Y. wen Liu, “Wireless lan security and ieee 802.11i,” *Wireless Communications, IEEE*, vol. 12, no. 1, pp. 27 – 36, 2005.

[7] R. Barker, “Security aspects in 6lowpan networks,” in *Design, Automation Test in Europe Conference Exhibition (DATE), 2010*, 2010, p. 660.

[8] *A Security Framework for Routing over Low Power and Lossy Networks*, IETF Std. ROLL, Work in progress.