

Information Centric Services in Smart Cities

G. Piro, I. Cianci, L. A. Grieco, G. Boggia, P. Camarda

*Department of Electrical and Information Engineering (DEI), Politecnico di Bari
v. Orabona, 4 - 70125, Bari, Italy.*

Email: {g.piro,i.cianci,a.grieco,g.boggia,camarda}@poliba.it

Abstract

A “Smart City” is intended as an urban environment which, supported by pervasive ICT systems, is able to offer advanced and innovative services to citizens in order to improve the overall quality of their life. In this context, the present contribution formulates a pioneering proposal, by drawing an advanced information centric platform for supporting the typical ICT services of a Smart City. It can easily embrace all available and upcoming wireless technologies, while enforcing, at the same time, ubiquitous and secure applications in many domains, such as, e-government and public administration, intelligent transportation systems, public safety, social, health-care, educational, building and urban planning, environmental, and energy and water management applications. All the details of the proposed approach have been carefully described by means of pragmatical use-cases, such as the management of administrative procedures, the starting of a new business in a given country, the navigation assistance, the signaling of an urban accident aimed at improving the public safety, the reservation of a medical examination, the remote assistance of patients, and the management of waste in a city. This description makes evident the real effectiveness of the present proposal in future urban environments.

Keywords: Information Centric Networking, Smart Cities, NDN, Services in urban environment.

Acronyms

CCN Content-Centric Networking

CS Content Store

DONA Data-Oriented Network Architecture
EU European Union
FIA Future Internet Assembly
FIB Forwarding Information Base
GPS Global Positioning System
ICN Information-Centric Network
ICNRG ICN Research Group
ICT Information & Communication Technology
IoT Internet of Things
IRTF Internet Research Task Force
ITS Intelligent Transport System
LFU Least Frequently Used
LRU Least Recently Used
LTE Long Term Evolution
LTE-A LTE Advanced
NDN Named Data Networking
PIT Pending Interest Table
PURSUIT Publish Subscribe Internet Technology
QoS Quality of Service
SAIL Scalable and Adaptive Internet Solutions
VANET Vehicular Ad-Hoc Network
WAVE Wireless Access in Vehicular Environments
WiMAX Worldwide Interoperability for Microwave Access

1. Introduction

While we are still waiting for an exact theoretical definition of the concept of *Smart City*, real urban agglomerations are already putting in place pragmatical attempts to win the race with their incumbent future, dominated by a steadily increase of the demographic pressure [1]. At the present stage, such actions head toward six main innovation axes [2][3], including: smart economy, smart mobility, smart environment, smart people, smart living, and smart governance. In this way, a Smart City can become a business-competitive and attractive environment, aimed at the well-being of its citizens. In future urban contexts, people will be surrounded by an ubiquitous digital eco-system made by internet-connected vehicles, smart buildings, and a myriad of other equipments, like computer, tablet, smartphone, Global Positioning System (GPS) navigation devices, sensors, and so on, willing to interact to each other (see for example Fig. 1). Accordingly, Information & Communication Technology (ICT) platforms became the ground floor of the Smart City foundation, thanks to their capability to offer advanced services in Intelligent Transport System (ITS), environmental and energy monitoring, building management, healthcare, public safety and security, remote working, and e-commerce domains [4, 5]. In other words, ICT plays a key role by interconnecting all the actors of a Smart City [6] and by supporting the provision of seamless ubiquitous services [7].

At the time of this writing, we are assisting to a radical change of the way digital resources are used. Nowadays, in fact, users are interested to share contents rather than to interconnect themselves to remote devices [8]. Without loss of generality, we cannot neglect the imminent possibility that this trend will affect also how enhanced services will be offered and exploited in future Smart Cities. Accordingly, ICT infrastructure should be deployed taking into account this important aspect. From a technological point of view, the present is very rich of possibilities to create wireless communication systems, based, for example, on the Internet of Things (IoT) paradigm [9], Long Term Evolution (LTE) and LTE Advanced (LTE-A) specifications [10], Worldwide Interoperability for Microwave Access (WiMAX) standard [11], and the Wireless Access in Vehicular Environments (WAVE) protocol stack [12]. Unfortunately, despite the current Internet architecture already supports the communication among all of these technologies, it will not be able to offer a highly scalable and efficient distribution of contents. Moreover, it manifests a set of issues related to: (i) the decoupling of contents from the

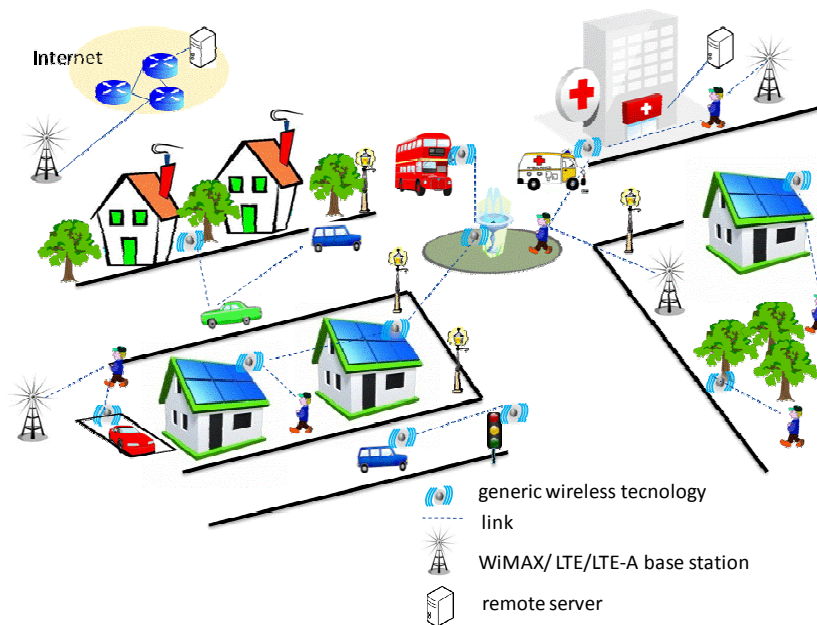


Figure 1: Example of a Smart City.

knowledge of their location, (ii) security aspects, (iii) the mobility of users, (iv) the services scalability, and (v) the tolerance to system failures (see Sec. 2 for more details).

All of these challenges has fostered the definition of the Information-Centric Network (ICN) paradigm, which proposes new networking primitives for the Future Internet [13].

Based on these considerations, a change of perspective is required; in fact, ICT platforms should be information-centric rather than host-centric as in today Internet and, at the same time, should be able to embrace the wide availability of cutting-edge wireless communication systems.

The ICN approach is currently investigated and developed in several projects, such as Data-Oriented Network Architecture (DONA) [14], Publish Subscribe Internet Technology (PURSUIT) [15], Scalable and Adaptive Internet Solutions (SAIL) [16], CONVERGENCE [17], and Named Data Networking (NDN) [18]. Despite all the proposed architectures differ in some aspects (e.g., naming scheme, data integrity, data granularity, routing strategy for both requests and data [19]), all of them assume a receiver-driven data exchange model based on content names. As a consequence, all theoretical

aspects, related to the management of services in urban environments discussed in this work, will remain valid (to a large extent) for all ICN proposals. Among the many ICN proposals, the one designed within the NDN project is gaining an increasing interest from the scientific community [20]. Hence, since a complete and unique definition of ICN is still a work in progress at ICN Research Group (ICNRG) of the Internet Research Task Force (IRTF), we will adopt in our work, for the sake of clarity and without loss of generality, the NDN terminology.

While the adoption of Future Internet architectures in Smart Cities has been preliminarily introduced in [4, 5], some ICN-based solutions have been recently formulated in [21], [22], [23], and [24] for offering enhanced services in urban environments. In particular, a secure publish-subscribe system based on ICN to support home energy management has been discussed in [23]. The main goal of this proposal is the collection of measurements and status information from household elements, the aggregation and the analysis of collected data, and the proposal of intelligent control decisions for actuations. In [22], authors present an efficient mechanism for distributing Internet services in a Smart City. It is based on a geo-localized lookup of resources carried out through a distributed hash table. The work discussed in [24], instead, studies the possibility of offering smart services through the interaction among sensors, moving vehicles, and cloud computing systems. Moreover, the adoption of named-data networking in vehicle-to-vehicle communications systems has been proposed in [21]. These interesting contributions solve specific problems of a smart city using an ICN approach, but they require to be integrated in a unifying architecture with standardized interfaces in order to exploit their maximum potential and to avoid a fragmentation of service-specific solutions.

Noticeable, in [25] it is proposed an extension of CCNx, i.e., the open source implementation of the protocol stack designed within the NDN project [26], which defines how a NDN node can implement a specific service after the reception of a given user request. This contribution represents a first step towards the definition of a more complete platform enabling enhanced services in urban environments.

The idea of exploiting a NDN-oriented service platform for Smart Cities has been already discussed (but only in a preliminary formulation) in [27] by the same authors of this work.

In this paper, we significantly extend our previous contribution by detailing how each smart service can be really handled in future urban environments through a NDN-oriented platform.

In particular, the main goals of this contribution can be summarized as it follows:

- the development of a complete and efficient platform enabling enhanced services in Smart Cities, based on the emerging NDN network paradigm.
- The definition of the service execution through three consecutive phases: (i) the *Discovering Phase*, useful to find specific remote content publishers; (ii) the *Security Initialization Phase*, exploited to setup a secure communication channel; and (iii) the *Service Usage Phase*, during which the user benefits from a service by exchanging messages with the network.
- The design of a hierarchical and flexible structure of the *name space*, in order to efficiently support several kind of services and, at the same time, to simplify routing operations.
- A clear illustration of the relevance of the proposed platform in realistic urban scenarios by means of many use-cases, embracing government and public administration, intelligent transportation systems, *life-events*, public safety, social, healthcare, and urban planning application fields, which represent very significant activities of Smart Cities widely investigated in several European projects working in this area (see Sec. 2).

It is worth to mention that our proposal is not an alternative to the one discussed in [25], but the two works should be considered complementary to each other. If, from one side, in [25] a way for implementing a service on a NDN node is discussed, from another hand our paper focuses the attention on the entire NDN architecture and presents a service platform, which embraces security aspects and an efficient name space, that can be used to design and to implement any kind of services in future urban scenarios.

We wish that the proposed platform could become a reference architecture in favor of a smart growth of future urban agglomerations, entailing the well being of our progeny.

The rest of the paper is organized as follows: in Sec. 2 the background on Smart City and Future Internet is presented. Sec. 3 provides a brief review of the NDN rationale. Sec. 4 describes the service platform that we envisage in this contribution and discusses also significant practical examples

and use cases about smart services which it can enable. Finally, Sec. 5 draws conclusions and forecasts future research.

2. Smart Cities and Future Internet

Despite the term *Smart City* is very common in everyday speaking, its exact definition is still not well-established [28]. In literature, some interesting definitions can be found, as:

- “*a city connecting the physical infrastructure, the ICT infrastructure, the social infrastructure, and the business infrastructure to leverage the collective intelligence of the city*” [29].
- “*A city that invests in human and social capital and traditional and modern (ICT) communication infrastructure in order to sustain the economic growth and a high quality of life, with a wise management of natural resources, through participatory governance*” [1].
- “*A city whose community has learned to learn, adapt and innovate. People need to be able to use the technology in order to benefit from it*” [30].
- “*A city that reflects a particular idea of local community, one where city governments, enterprises and residents use ICTs to reinvent and reinforce the community’s role in the new service economy, create jobs locally and improve the quality of community life*” [31].

It is evident that, without loss of generality, a metropolitan area can be classified as *smart* when safety, enhanced public services, healthcare monitoring, green sustainability, intense social interaction, and efficient transportation systems become available to any citizen wherever he is located [32, 33]. All this requires to design, develop, deploy, and maintain public and private infrastructures, based on advanced and integrated materials, sensors, electronics, computer systems, and databases [34].

In this direction, the European Union (EU) is devoting constant efforts to conceive sustainable strategies for a *smart* urban growth for its metropolitan areas [1]. This is demonstrated by the presence of still active or recently concluded projects on Smart Cities [35]-[53].

In Fig. 2, the most investigated *use-cases* by EU projects are grouped in several macro categories (i.e., government and public administration, intelligent transportation systems, public safety, social, health-care, educational, building and urban planning, environmental, and energy and water management). We note that the proposed services classification is in line with those envisaged by the IBM company¹ and in other scientific works recently presented in literature, like [54, 55, 33].

More recently, the concept of *life-events*, which identifies any kind of event that generate a change of circumstance in the citizen's life, is also gaining in popularity. These events lead to the execution of a number of administrative procedures that, very often, are handled by different societies and/or public administration entities and, at the same time, are not perfectly known by the citizen itself [56]. To simplify their execution, several efforts have been dedicated to the formalization of a number of proposals aimed at defining interactive Web portals and architectural models (see for example those discussed in [57, 58, 59, 60]) able to manage *life-event* services in a Smart City. To shed some lights on this aspect, valid examples of *life-events* are the looking for a job, the applying for a drivers license (or the renewing of an existing one), the buying of building, car, or any kind of movable, the change of the address, the request for a passport, the start of new business in another country, the reporting of a crime, the declaration of income taxes, and so on [61]. It is very easy to understand how all these events require the execution of several services summarized in Fig. 2 under an orchestrated coordination.

ICT platforms are widely considered the key-enabling factor of a Smart City because of their ability to support a huge amount of services for citizens.

In this regard, we note that in a Smart City a very huge number of devices will coexist; they (equipped by heterogeneous technologies) will interact among them to execute, join, and participate to a myriad of services. As a consequence, the following challenges will arise [62]:

1. *availability issue*: users need to fetch contents in a fast, reliable, and effective way;
2. *location-dependence issue*: it is no more necessary for many services to identify the location of a given data (i.e., no need for IP addresses);

¹See http://www.ibm.com/smarterplanet/us/en/smarter_cities/overview/ for more details.

		SMARTSANTANDER [35]	ELLIOT [36]	TEFIS [37]	FIREBALL [38]	IOE [39]	SAFECITY [40]	OUTSMART [41]	RELYORIT [42]	FINEST [43]	DIGITAL CITIES [44]	MOBINCITY [45]	HOBNET [46]	CITYSDK [47]	LIVE CITY [48]	IES CITIES [49]	PERIPHERIA [50]	iCITY [51]	TV-RING [52]	SMARTFREIGHT [53]	
Transportation	Traffic monitoring in emerging situations			X					X												
	Limited parking management	X																			
	Loading and unloading of areas	X																			
	Logistic		X							X											X
	Trip optimization				X						X	X									X
	Transport services (train, bus, plane, etc)	X	X	X			X				X	X				X	X				X
	Parking for people with disabilities	X																			
Diagnosis and Prediction of Traffic	X							X													
Government and public administration	Automatic and optimized administrative procedures				X						X										
	Document search				X																
	Tax payment				X																
	Election accessibility for people with disabilities problems.																X				
Public safety	Management of road accidents						X														
	Crime prevention						X														
	Monitoring of public places						X														
	Prediction of climate change effects																X				
Social	Tourism assistance	X	X										X		X	X					
	Identification of point of interest	X																			
	Location based services	X											X				X				
	Media distribution	X												X							X
	Retail services and shops discovering		X																		
	Content sharing			X																	X
	Socially sustainable campus																X				
Health-care	Dissemination of data about pollution and temperature for patients		X																		
	Remote patients assistance	X	X																		
	Remote coordination of surgeries			X																	
	Media trasmission for hospitals and doctors													X							
	Generic health-care services															X					
Education	Distribution of multimedia contents in a school														X						
Smarter building and urban planning	Building monitoring and control							X					X								
	Monitoring of electrical devices												X								
	Management of emergency situations												X								
	People and resource tracking												X								
	Park irrigation	X											X								
	Waste management						X														
Environmental	Environmental monitoring	X	X	X															X		
	Luminosity Measurement	X																			
Energy and water	Efficient management of artificial light	X	X				X														
	Efficient management of heating and air conditioning		X	X				X													
	Water distribution						X														
	Optimized energy distribution				X																

Figure 2: Use-cases investigated by the most important EU research projects.

3. *security issue*: in line with the previous requirement, it is necessary to trust contents independently from the location and the identity of who is providing them;
4. *mobility issue*: it is necessary to guarantee the seamless support of mobile users which should not experience any service interruption when moving across different access networks;
5. *scalability issue*: the problems related to limited storage, bandwidth, and computational capabilities that affect service providers when handling a huge number of users should not influence the behavior and the quality of services;
6. *fault-tolerance issue*: for all the application fields there is the need to increase the resilience of ICT services to system failures.

Unfortunately, it is widely recognized that the current Internet architecture is not able to efficiently face all of the aforementioned challenges [8, 63, 64]. In fact, the Future Internet Assembly (FIA)² has identified its fundamental limitations, classifying them in four main areas [65]: (i) the impossibility to process and handle, in real-time, data packets exchanged within the network according to the information stored within them; (ii) the lack of content/context aware caching and storage capabilities in network routers; (iii) the inefficient transmission of content-oriented data; and (iv) the lack of flexibility and adaptive control mechanisms that could react in an autonomous manner to external events.

To overcome such obstacles, novel network architectures are being conceived, based on radically different Internet primitives (a summary of the most important proposals can be found in [66]).

Among them, particular interest has been achieved by the emerging ICN paradigm which quickly gained into popularity, thanks to its inherent ability to afford all the issues argued before.

With respect to the classical TCP/IP architecture, the ICN approach introduces the following novel and useful features [64]:

- addressing of contents through names that do not more contain any reference to their location.
- In-network caching strategies that would make faster and faster the

²See www.future-internet.eu.

distribution of contents among users, as well as reduce the traffic load at the server side.

- Delivering of user demands towards the closest device that may satisfy the request by adopting *routing-by-name* approaches.
- Simplified management of mobility (e.g., users that modify the point of access does not perform again the initialization of the connection, but they can continue to ask consecutive portion of the requested content).
- Native support to security features (e.g., in ICN it is possible to encrypt and authenticate directly names and contents, without relaying to sophisticated schemes conceived instead for protecting the communication among nodes).
- Simplified support to peer-to-peer communications.
- Possibility to implement lean Quality of Service (QoS) aware strategies for handling the routing of requests and the delivery of data packets.
- Native support to multicast communications.

Despite ICN represents a promising architecture for the Future Internet in general, we believe that its adoption in the context of Smart City could give enormous advantages for the improvement of the quality of services offered to all the citizens and for the diffusion of such smart services. In line with this opinion, some of EU projects are already developing their proposals according to Future Internet guidelines. On the other hand, also the ICNRG working group has identified in a Smart City an important base line scenario where designing, evaluating, and optimizing ICN-based solutions [67].

Our contribution would complement all of these activities by proposing a complete service platform enabling Smart City services through the ICN architecture devised within the NDN project.

In conclusion, the Future Internet can offer solutions to many challenges that Smart Cities have to face; but, contrariwise, also a Smart Cities can provide an excellent experimental environment for probing pros and cons of Future Internet architectures in a variety of application domains [4].

3. Named Data Networking

The ICN architecture conceived within the NDN project, known with the name Content-Centric Networking (CCN), is based on a “data-centric” approach: all contents are identified by a unique name, allowing users to retrieve information without having any awareness about the physical location of servers (e.g., IP address). Furthermore, it targets receiver-driven communications, based on the exchange of content chunks, name-based routing, and self-certifying packets [63, 20].

A NDN network can be deployed by adopting a “clean-state” approach or considering an “overlay” layer. In the first case, the entire system is redesigned from scratch, thus connecting the NDN architecture directly to the lower technological layer [68]. In the other case, instead, it is considered a feasible solution that allows to quickly design, experiment, and deploy the proposed novel architecture on top of the current Internet structure [69]. Anyway, in both cases, NDN introduces in the protocol suite two novel layers: the *strategy* layer, which is in charge of disseminating messages within the network [70], and the *security* layer, which handles all security aspects [71].

NDN communications are driven by the consumer of data and only two kinds of messages are exchanged: *Interests* and *Data*. The main fields³ of such messages are reported in Tab. 1. An user may ask for a content by issuing an *Interest*, routed towards the nodes in posses of the required information; these nodes are triggered to reply with *Data* packets.

Each content is uniquely identified by the *Content Name*. NDN adopts a hierarchical structure for names; therefore a *name tree* is introduced. It is formed by several components, each one made by a number of arbitrary octets (optionally encrypted), so that every *name prefix* identifies a sub-tree in the name space. An *Interest* packet can specify the full name of the content or its prefix, thus accessing to the entire collection of elements under that prefix.

Other two novel aspects that characterize the behavior of a NDN network are the routing and the distributed caching mechanism. Routing operations are performed by the strategy layer only for *Interest* packets. *Data* messages, instead, just follow the reverse path to the requesting user, allowing every intermediate node to cache the forwarded content. Moreover, each node

³Herein, we consider the packet structure proposed with the CCNx implementation, available at www.ccnx.org.

Table 1: Main fields of NDN messages

Field	Description
<i>Interest</i> Packet	
<i>Content Name</i>	Specification of requested item. Formed by several components identifying a sub-tree in the name space.
<i>Min Suffix Components</i>	Access to a specific collection of elements according to the prefix stored in the <i>Content Name</i> field.
<i>Max Suffix Components</i>	Access to a specific collection of elements according to the prefix stored in the <i>Content Name</i> field.
<i>Publisher Public Key Digest</i>	It imposes that only a specific user can answer to this <i>Interest</i> .
<i>Exclude</i>	Set of components forming the content name that should not appear in the response to the <i>Interest</i> .
<i>Child Selector</i>	When in the presence of multiple answers, it expresses a preference for which of these should be returned.
<i>Answer Origin Kind</i>	Several bits that alter the usual response to <i>Interest</i> (i.e., answer can be “stale” or answer can be generated).
<i>Scope</i>	Limit on <i>Interest</i> propagation.
<i>Interest Life time</i>	Approximatively, after this time interval <i>Interest</i> is considered deprecated.
<i>Nonce</i>	Randomly-generated byte string for detecting duplicates.
<i>Data</i> Packet	
<i>Content Name</i>	Identification of requested item.
<i>Signature</i>	Guarantee on publisher authentication.
<i>Publisher Public Key Digest</i>	Identification of users that generated data.
<i>Time Stamp</i>	Generation time of the content.
<i>Type</i>	Type of <i>Data</i> packet (i.e., data, encrypted data, public key, link, and NACK with no content).
<i>Freshness Seconds</i>	Lifetime of the carried payload. Used to schedule caching operations (eventually prohibited).
<i>Final Block ID</i>	Identifier of the final block in a sequence of fragments.
<i>Key Locator</i>	Specification about where to find the key for content verification.
<i>Content</i>	Content with an arbitrary length.

receiving a *Data* packet decides to cache it, according to the adopted caching technique. In this way, the contents diffusion process is simplified, with a significant reduction both of server computational load and bandwidth consumption. In addition, since content exchange is based on content names themselves, multiple users interested to a particular content can share it using multicast suppression techniques over a broadcast medium [72].

To accomplish the aforementioned activities, a NDN node exploits three main structures:

- the Content Store (CS), that is a cache memory implementing different replacement policies, such as Least Recently Used, Least Frequently Used or Random, where some received contents can be stored.
- The Forwarding Information Base (FIB), which is similar to a classical IP FIB except for the possibility to have a list of faces for each content name entry; in this manner, *Interest* packets can be forwarded towards many potential sources of the required *Data*.
- The Pending Interest Table (PIT), which is a table used to keep track of the *Interest* packets previously forwarded upstream towards content sources; it saves information about the arrival faces. In this way, backward *Data* packets can be properly delivered to the right requesters.

To provide a further insight on the NDN paradigm, Fig. 3 reports an example highlighting its main functionalities. In such an example, it is supposed that a consumer wants to download a content identified by the name */domain/content*. Hence, it expresses an *Interest* packet that will be forwarded by NDN routers according to information stored in FIB tables towards the device that has the requested content in its CS. In this operation, an intermediate NDN router stores all the forwarded requests in the PIT table, thus avoiding to send multiple *Interest* packets asking for the same content. Once the *Interest* packet reaches a node that can satisfy such a request, a corresponding *Data* packet will be generated and delivered to the consumer towards the reverse path. Any intermediate router, as shown in figure, may cache the content; in this manner it is able to satisfy future requests for the same data.

Some optional fields stored into both *Interest* and *Data* packets may modify the execution of the NDN protocol in each node. For example, a device may prohibit that its generated contents are cached into the network, as well

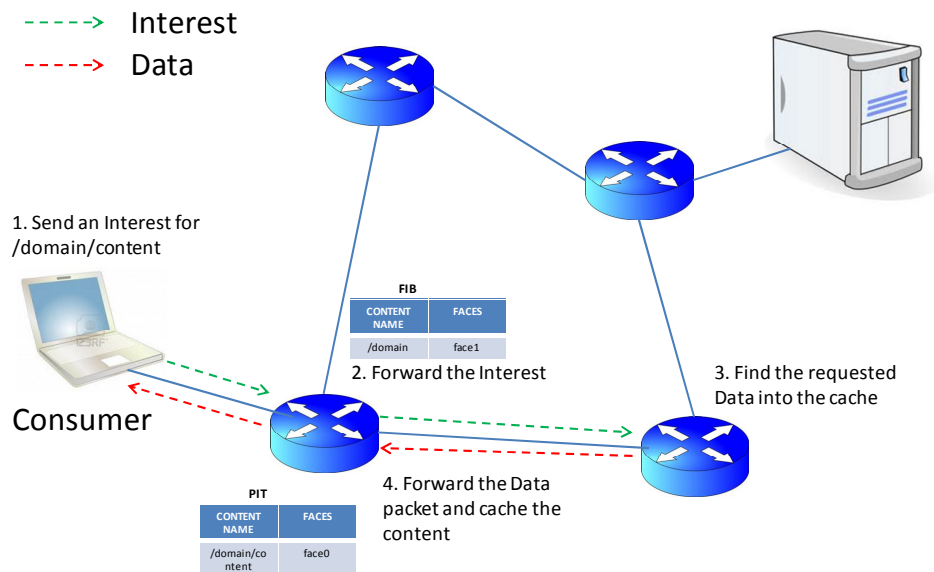


Figure 3: An example showing NDN functionalities.

as a device sending the *Interest* packet could impose that the answer should be necessary generated by the publisher, thus bypassing any intermediate caches.

Since a *Data* packet is sent only as answer to a given *Interest* packet, NDN guarantees the flow balance. Moreover, the suppression of duplicated *Data* transmissions is achieved by using a *nonce* within the *Interest* packet. When the requested content is not received until a given timeout, the client could trigger the retransmission of the *Interest* packet; this provides a minimum level of reliability to the communication. Finally, NDN supports also some security features, such as the encryption and the authentication of both *content name* (or a part of it) and the content stored into the *Data* packet [63][71].

4. The envisaged service platform

The service platform proposed in this work is built on two levels: the *service* layer and the *technology* layer, both interacting through a NDN interface (see Fig. 4).

A strength of our proposal is that it is fully compatible with both *clean-state* [68] and *overlay* approaches [69]. In fact, in the case that the Future

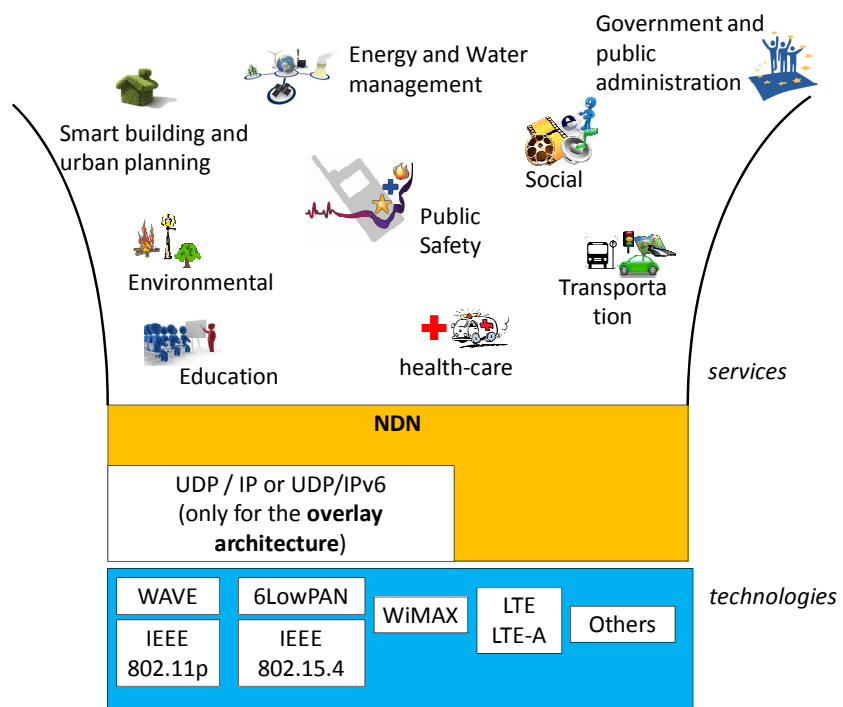


Figure 4: The NDN-oriented service platform.

Internet architecture will be redesign from scratch (i.e., the *clean-state* solution), the NDN interface, which is exploited for enabling enhanced services, can be directly installed on top of the technology level. On the other hand, if the *overlay* approach will be adopted for a graceful transition to the Future Internet, the service platform, including the NDN layer, can be deployed, without any difficulties, on top of the existing TCP/IP protocol suite.

In the rest of this section, all details of this new architecture will be described, as well as its applications and pragmatical *use-cases*.

In order to accommodate the multi-faceted requirements of Smart City scenarios, three consecutive phases are conceived in service provisioning: (1) the *Discovering* phase, (2) the *Security Initialization* phase, and (3) the *Service Usage* phase.

Moreover, the *name space* is designed to classify and map all the services in an ordered and hierarchical fashion, with consequent enormous advantages for routing operations and packet processing.

In the proposed platform, a user could exploit, in an ubiquitous fashion, a given service by using a device connected to the rest of the world with a specific wireless technology. We assumed that a dedicated software, properly developed and configured to perform one or more services, is installed on the considered device and that it is able to execute all features and tasks expected for each phase of the service execution. The user may interact with this software with a graphical interface for selecting the type of service he/she is interested to, as well as the set of its preferences. Anyway, we would like to remark that the definition of the software is beyond the scope of this contribution.

4.1. Services Management

As stated before, the execution of a service is articulated in three consecutive steps that will be clarified herein.

During the first optional *Discovering* phase, it is possible to find remote publishers that could satisfy user requests. Generally, this phase is performed when the requested content cannot be found in the cache memories of intermediate nodes, or in the case a secure communication with the publisher has to be initialized.

The *Security Initialization* phase allows a user to retrieve some security information, like the key exploited for encrypting the content, the public key adopted for authenticating the *Data* packet, and so on. In addition, it enables the possibility to setup the secure communication channel, i.e.,

by negotiating a security key, between user and publisher. Similarly to the discovering process, also this task is not mandatory and has to be carried out only when exchanged data need to be protected.

After the user has found the remote publisher and initialized with it a secure mechanisms for exchanging *Interest* and *Data*, she/he can enjoy the service by sending/receiving some *Interest/Data* packets to/from the network. This *Service Usage* phase represents the only mandatory step in our proposal.

Sometime, the *Service Usage* phase may overlap with the *Discovering* phase. This happens when the *Data* packet generated by the publisher during the discovering procedure already contains all the information that the user would like to obtain.

4.2. Designing the name space

The definition of the *name tree* is a key aspect of a NDN network because the *Content Name* field strongly influences the way *Interest* and *Data* packets are treated. Moreover, an optimized name space could give enormous advantages for routing operations and packet processing.

The definition of the *name space* is based on both *contractable names* and *on-demand publishing* concepts, firstly proposed in [73]. The former one supposes that each user is able to construct the name of a desired content through specific algorithms (e.g., it knows the structure of the name tree and the value that each field of the *Content Name* may assume). The latter one, instead, describes the ability to request a content that has not yet been published in the past, but it has to be created in answer to the received request.

Without loss of generality, we can assume that a given service can be offered by a specific entity (which can be the public administration or a private company) and that it can be offered within a specific coverage area of a city. In addition, we suppose also that the same service can be managed by multiple providers, thus allowing the user to select one of them according to its preferences.

Therefore, the following *name tree* structure will be adopted hereafter:

/domain/main-service/sub-categories-of-services/type-of-question/additional-info

Starting from the the root tree, which is identified with “/”, we introduced the *domain* field in order to explicitly indicate that a given service

may be offered by a specific entity (whether public or private) and within a specific coverage area of a city. The *main – service* field specifies the macro category which the service belongs to, i.e., one of the main applications reported in Tab. 2. Then, the set of components listed in the *sub – categories – of – services* field allows to pick out a specific service in a hierarchical structure of sub-categories. The *type – of – question* field explicits the user demand. Just to make few significant examples, it can be set equal to the value *discover*, *reserve*, *query*, and *communicate* in the case the user wants to discover a node offering a given service, reserve a service, interrogate a remote node, and communicate somethings to another device, respectively. Finally, components belonging to the *additional – info* field are used for appending to the *Content Name* specific optional values that can be exchanged among nodes during the negotiation and the execution of the service itself.

Generally, the part of the *Content Name* before the *additional – info* field serves for routing purposes, i.e., for delivering the *Interest* packet to a node that is able to satisfy the user request. The *additional – info* field could provide further details useful for the publisher to elaborate and generate a more specific answer to be included into the *Data* packet.

Starting from the list of services envisioned in Fig. 2, we have pictured in Fig. 5 an example of the *name tree* generated by adopting the proposed hierarchical structure. In our design, security functionalities are considered a possible sub-category of services. However, due to the lack of space, we reported in the figure this service only for public administration applications, implying that it can be adopted in to all of the macro categories.

Obviously, the *name tree* shown in Fig. 5 have to be considered as a possible starting point for conceiving more complete *names space* structures, which would encompass a very large number of smart services that, probably, have not been yet conceived nor envisaged. Thanks to its high flexibility, in fact, it is possible to extend the *name tree* by introducing new categories and sub-categories of services, as well as different kind of questions and additional details to append at the end of the name. Moreover, since the *names space* enables all the services that should be executed during the management of *life-event*, it fully supports the development of any kind *life-event* strategy properly devised for Smart Cities.

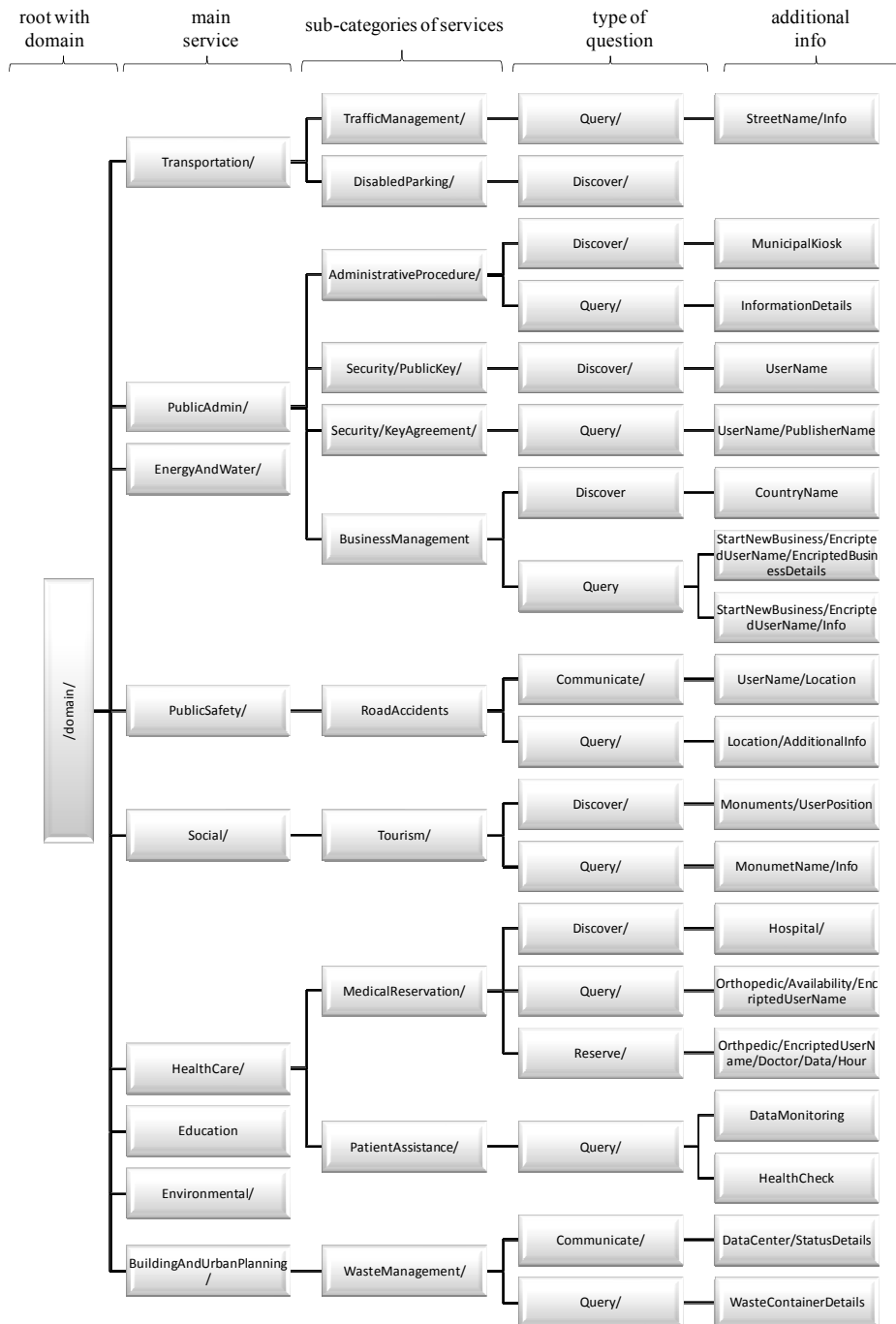


Figure 5: Example of *name tree* structure.

4.3. Key exchange mechanisms

Security requirements are mandatory for a wide range of services. The encryption of contents, as well as the authentication of a *Data* packet, cannot be faced without the adoption of a security key.

The basic NDN architecture does not specify neither an encryption algorithm nor a separate mechanism for distributing the key [63]. Regarding the protection of the *Data* packet, a node may use its preferable scheme for encrypting the content that it has generated. It has only to communicate to the client the algorithm and the the type of key used for doing this (to this aim, the *Key Locator* field in Tab. 1 can be added in the *Data* packet). As suggested in [71], the distribution of a key can be handled like any other data by using the communication mechanism based on the exchange of *Interest* and *Data* packets. In this way, the encryption of contents, or even names or name components, becomes completely transparent to the NDN network.

With the aim of better characterizing the *Security Initialization* phase introduced before, we present herein some simple schemes that can be adopted for exchanging and/or negotiating the security materials (i.e., key, parameters, algorithms, and so on). Besides these suggestions, however, more complex solutions, such as those proposed in [74, 75, 76, 77, 78] can be simply implemented within our framework.

As a starting point, we focus the attention on the possibility to authenticate messages generated by nodes in the network. We suppose that a publisher can exploit a couple of keys (i.e., the *PrivateKey* and the *PublicKey*) for authenticating the content of its *Data* packets. We note that such a feature has been already conceived within the NDN architecture: the *Signature* field of the *Data* packet (see Tab. 1) is just used to authenticate the whole message. In particular, the publisher can obtain the *Signature* by encrypting, through its *PrivateKey*, a hash digest of the *Data* packet it has generated.

A generic node that needs to verify the authenticity of a *Data* packet, should possess the publisher *PublicKey*. We propose in Fig. 6 a scheme for its retrieving in a NDN network. The user sends an *Interest* packet with the *Content Name* equal to

/domain/main-service/Security/PublicKey/Discover/PublisherName

where, the name has been built by following the *name tree* described in Sec. 4.2.

Any nodes having this data into the cache may answer to the user by replying with a *Data* packet containing the public key, the adopted cryptography algorithm, and eventually other security related information.

We suggest also to consider an authority for authenticating the *PublicKey* of each node, thus preventing that a malicious user may simulate to be a given publisher and modify the correct execution of a service. In that case, the answer to the aforementioned *Interest* packet will contain a certificate of the publisher *PublicKey* signed by the authority (the ITU-T X.509 standard [79] can be used for this purpose).

The previous example has an important limitation: all users/nodes of the network are able to decipher any things sent by a given publisher. This poor security level may be acceptable when, for example, the publisher wants only to guarantee the authenticity of data packet and the correct correspondence between *Content Name* and content.

However, sometimes it is required to establish a secure link between client and publisher, thus preventing that any third part could understand their communication. In this specific case, it is necessary to negotiate a key by means of well-known key agreement mechanisms, e.g., RSA algorithm, Diffie-Hellman, use of certificates, and so on. As shown in Fig. 7, the computation of a key can be done after the exchange of a couple of *Interest* and *Data* packets.

4.4. Use Cases

To describe the main details of the architecture we are proposing, we present herein a set of significant *use-cases* depicting some important services that can be handled in future urban environments. We remark that application fields we will investigate in what follows reflect those studied and suggested within EU research projects. Moreover, for sake of clarity, we will present very basic scenarios composed by a limited number of devices (e.g., we suppose to have only one intermediate NDN router in the network), but it is easy to extend them to more complex topologies.

4.4.1. Government and public administration services: starting of a new business in a foreign country and retrieving of a document from a municipal kiosk.

Empowering businesses means providing an environment, which fosters competitiveness and good business practice. In this context, governments in Europe have been urged to streamline bureaucratic procedures to ensure that

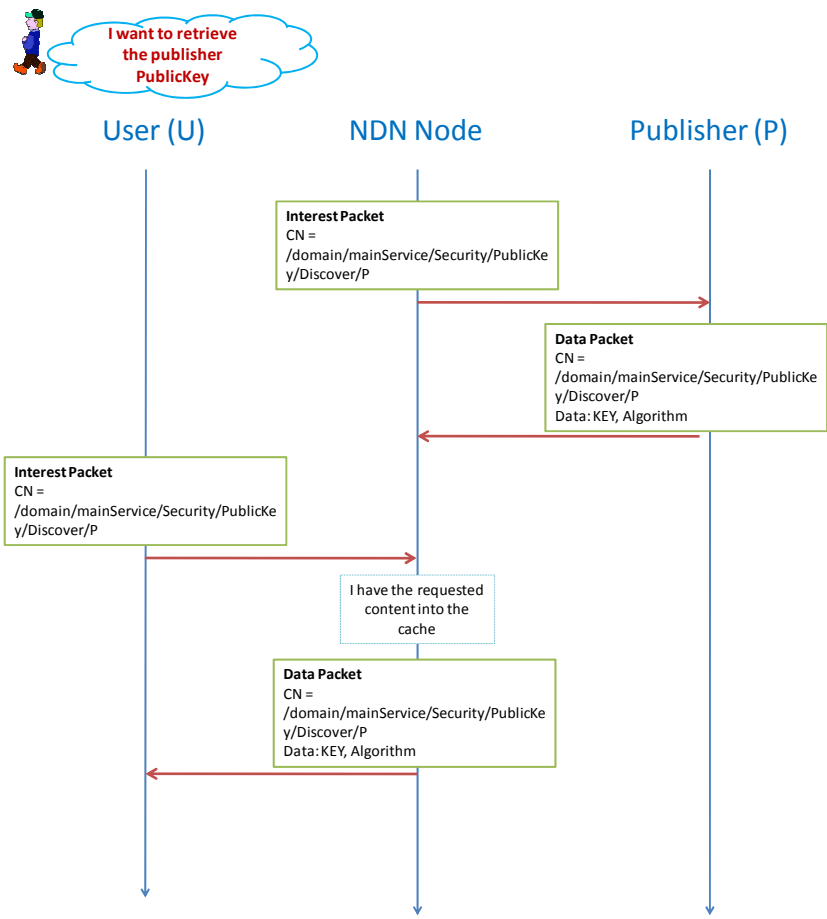


Figure 6: Scheme for retrieving the publisher *PublicKey*.

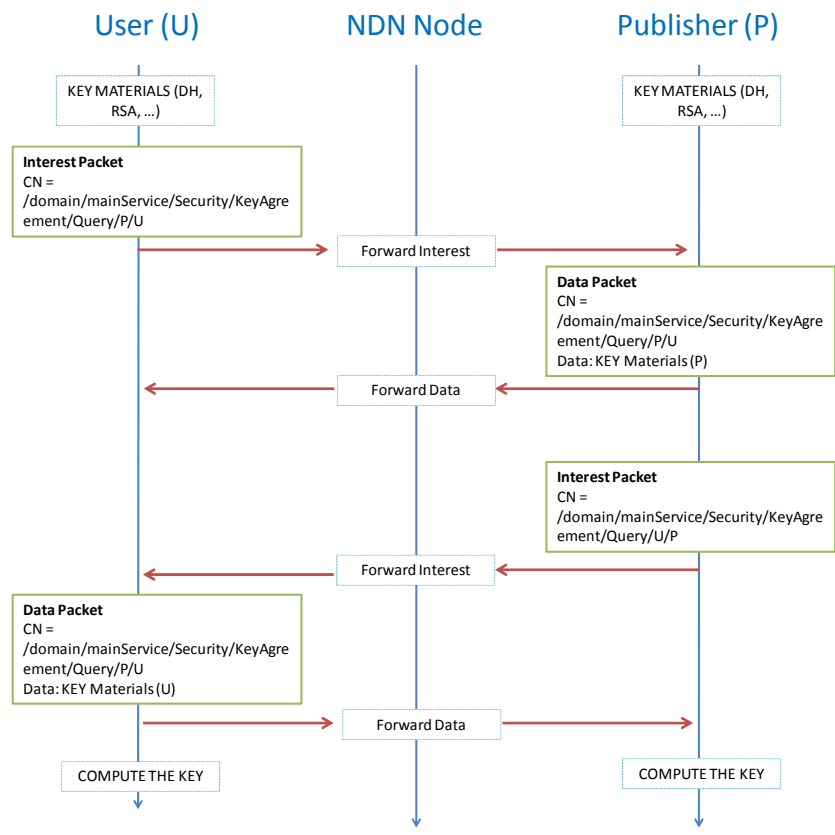


Figure 7: Key agreement procedure.

all procedures and formalities relating to access to a service activity and to the exercise thereof may be easily completed at a distance and by electronic means through the relevant “Point of Single Contact” [58]. Bearing in mind this consideration, the first *use-case* presented is related to the management of an important *life-event*: it depicts a citizens who would like to start a new business in a foreign country (this example has been proposed in [58]). This *use-case* has been proposed to demonstrate that our platform can be useful as the foundations for robust, streamlined, and sustainable eGovernment services.

Fig. 8 shows all the steps that should be performed during the execution of the service.

In line with one of the main properties of a *life-event* strategy (i.e., the user does not know perfectly which entity should be contacted to start administrative procedures), the *Discovery* phase is exploited to collect information about possible portals that can support administrative procedures required to reach the aforementioned goal. Supposing that the user wants to start a business in *CountryY*, it will discover a portal by diffusing an *Interest* packets with the *Content Name* set to

/domain/PublicAdmin/BusinessManagement/Discover/CountryY.

This message is received by an intermediate router that is able to provide requested information by generating a specific *Data* packet. When all details about the remote eGovernment portal are received by the citizen, the *Secure Initialization* phase is handled to create a secure communication between them. To this end, the key agreement scheme reported in Fig. 7 could be used.

Now, the user can initiate the procedure to start-up a business by sending an *Interest* packets whose *Content Name* stores all the details need to accomplish this task:

/domain/PublicAdmin/BusinessManagemnt/

Query/StartNewBusiness/EncryptedUserName/EncryptedBusinessDetails.

To ensure that this request will be handled by only the discovered portal, the *PublisherPublicKeyDigest* and *AnswerOriginKind* fields of the *Interest* packet contain the hash function of the public key of the portal and the numerical value 3, respectively. Moreover, all the *additional – info* fields of the name have been encrypted by using the key negotiated during the *Secure Initialization* phase previously concluded.

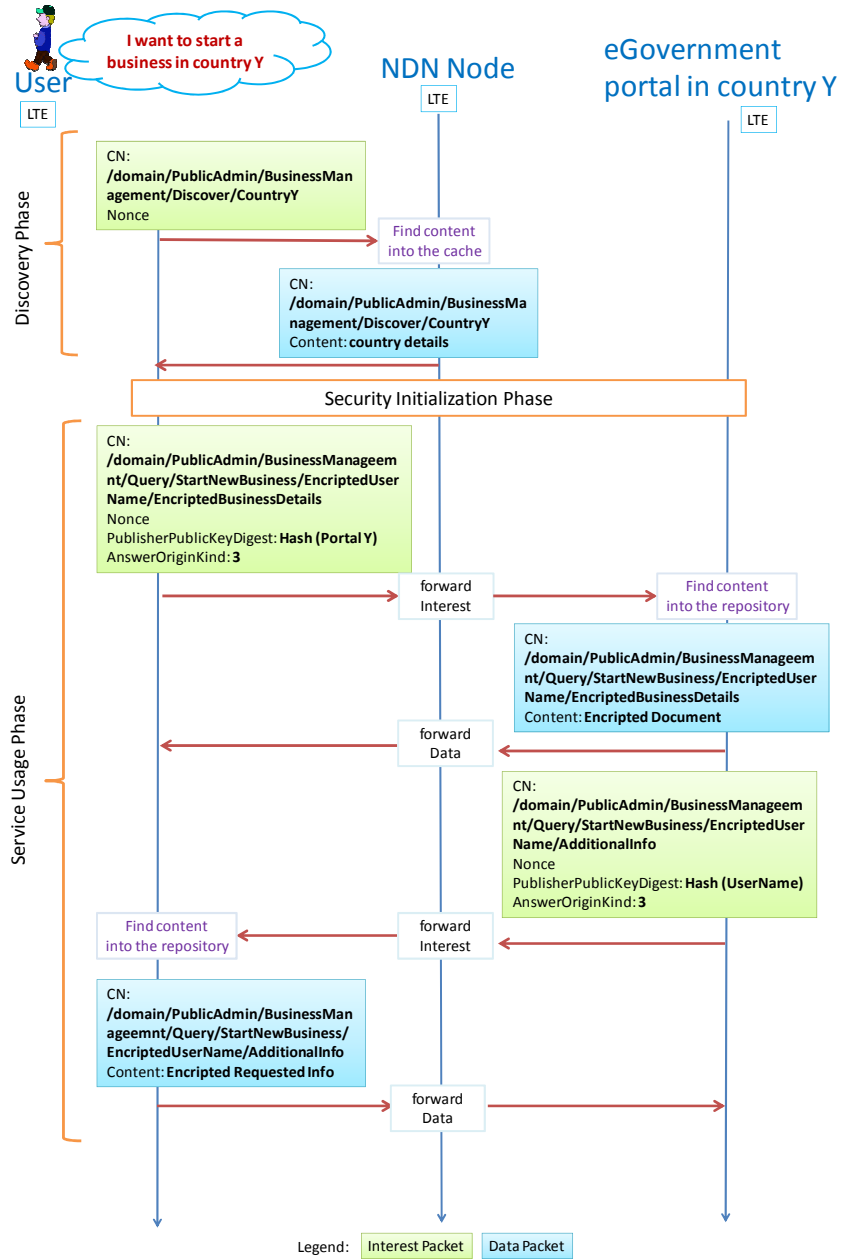


Figure 8: Use case 1: starting a new business in a foreign country (*life-event* service belonging to the government and public administration application field).

Answering to this request, the eGovernment portal will formalize the administrative procedure and generate a *Data* packet containing the document (e.g., a receipt) to feedback to the citizen.

To make the example more realistic as possible, we can also suppose that the portal may requires for additional information to complete the administrative procedure. To this aim, a new request can be forwarded to the citizen with *Content Name* set as

*/domain/PublicAdmin/BusinessManagemnt/
Query/StartNewBusiness/EncryptedUserName/AdditionalInfo.*

In this case, the *PublisherPublicKeyDigest* field of the *Interest* packet contains the hash of the public key of the citizen, i.e., the only user allowed to satisfy such a request.

After the reception of this *Interest* packet, the citizen will generate the corresponding *Data* packet to deliver to the remote portal.

Besides the previous significant example, there is the vision of a Smart City conceived in the FIREBALL project [38], according to which a smart governance could be reached by exploiting municipal kiosks providing open information to citizens for accelerating any kind of administrative procedure and for reducing, at the same time, the useless latencies at dedicated offices. Following such an idea, we devised another *use-case* where our proposal is used by a citizen to retrieve an administrative document.

In the scenario depicted in Fig. 9 is showed that the communication is handled by using the WiMAX technology, that represents the wireless interface common to every devices in the considered network.

For security purposes, it is preferable that all messages exchanged between user and municipal kiosk are encrypted by using a negotiated session key. For this reason, the service starts with the mandatory *Discovering* phase, during which the user try to discover municipal kiosk in its neighborhood, thus recovering all the information required to perform the *Security Initialization* phase (e.g., the name associated to the municipal kiosk). To this aim, she/he sends an *Interest* packets with the *Content Name* set to

/domain/PublicAdmin/DocumentSearch/Discover/MunicipalKiosk.

The user request reaches an intermediate NDN router that, having the requested information in its cache, generates a *Data* packet storing all the details about the handy municipal kiosk.

The secure communication between user and municipal kiosk is then created by using the key agreement scheme reported in Fig. 7.

Now, the user can ask for a specific document by issuing an *Interest* packet having the following *Content Name*:

/domain/PublicAdmin/DocumentSearch/

Query/MunicipalKioskName/EncryptedUserName/DocumentName.

Similarly to the previous example, *PublisherPublicKeyDigest* and *AnswerOriginKind* fields of the *Interest* packet are properly set for ensuring that only the selected municipal kiosk generate the answer.

In response to the user demand, the municipal kiosk sends a *Data* packet with an encrypted payload storing the requested document. The *Freshness Second* of the last generated message is set to zero in order to prohibit any caching procedures.

4.4.2. Transportation services: disabled parking and navigation assistance

Transport is one of the pillars of modern society and ITS integrates different technological components in order to offer solution of general transport control and transport information services provision [80, 81, 82, 83]. For this reason it has to be enormously supported and ameliorated in future urban environments.

We are aware that the adoption of mobile terminals is prohibited for a lot of countries worldwide. Anyway the execution of these services does not violate laws because we assume that such services are handled by devices, like satellite navigation systems, that are already widely used at the driving. Once the application installed on that device has been properly configured by the user (e.g., at the beginning of the trip), she/he will execute the service without requiring an active interaction with her/him, thus avoiding to compromise the safety of the driving.

The first *use-case* we present in the area of *ITS* applications is related to the management of parkings for people with disabilities, which has been studied within the SMART SANTANDER project [35]. The scenario described in Fig. 10 supposes that an user with disabilities wants to reach a dedicated parking where leaving its car. With the aim of discovering available parkings at that time instant, the user generates an *Interest* packet with the *Content Name* equal to:

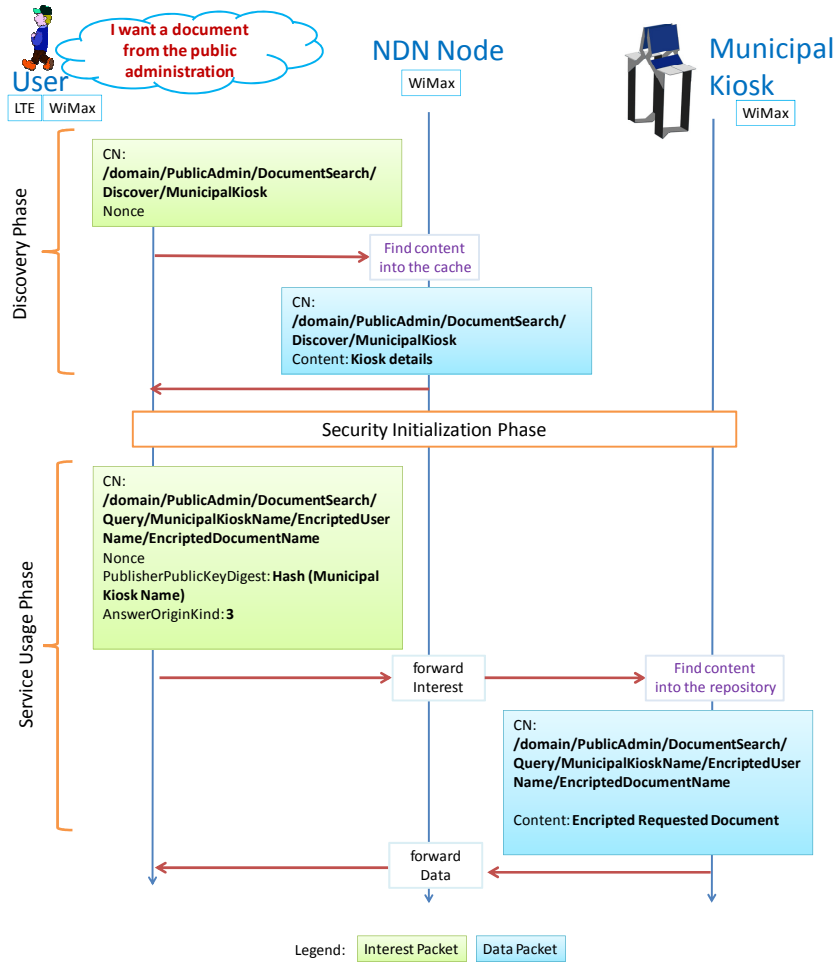


Figure 9: Use case 2: discovering of a document from a municipal kiosk (government and public administration service).

/domain/Transportation/DisableParking/Discover/

In this example, any cached data could not be more useful because they could be out of date. For this reason, the value of the *AnswerOriginKind* field of the aforementioned *Interest* packet is properly set to ensuring that the answer has to be necessarily generated by the publisher (i.e., a generic parking). The request will reach two different parkings, i.e., *DisableParkingA* and *DisableParkingB*, that will provide a *Data* packet containing the address and the status (i.e., free or busy). Once these messages will be received by the user, she/he can decide to drive towards the closest and free disabled parking (i.e., the *DisableParkingB* in Fig. 10).

We highlight that in this example the *Discovering* phase and the *Service Usage* phase are overlapped.

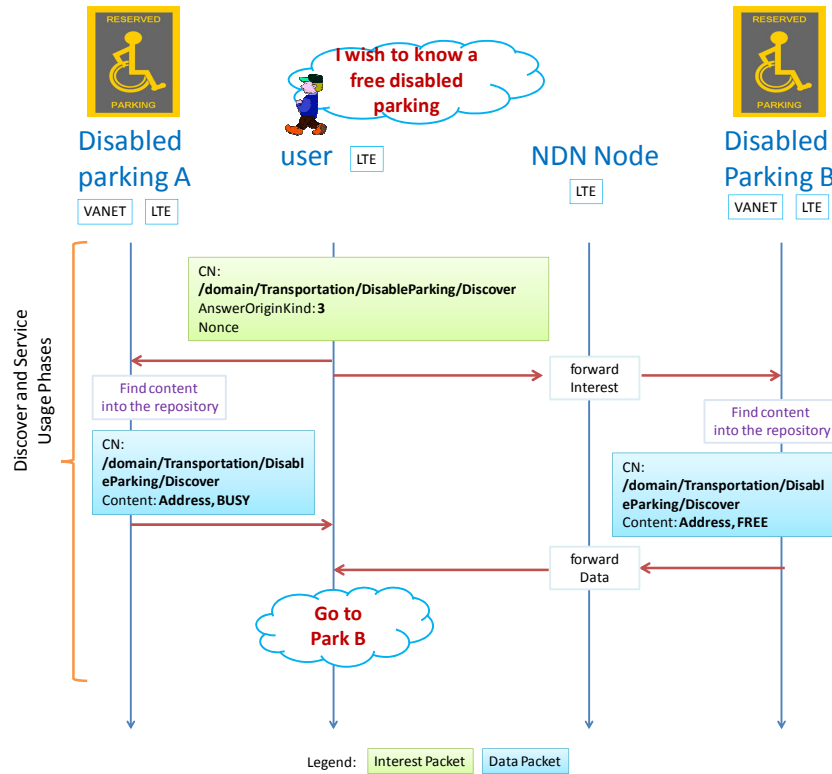


Figure 10: Use case 3: disabled parking (transportation service).

Another important *use-case* in this category of services focused on the

navigation assistance, which is a topic worth of investigation for the most of EU research projects. Generally, it requires the execution of the only *Service Usage* phase, but there is the possibility to enhance the service with additional features (like those related to the security).

Focusing the attention on a Vehicular Ad-Hoc Network (VANET) composed by a number of vehicles and fixed objects (such as a traffic light), each one equipped with a GPS device, we assume that each node enjoying the ITS service has in its repository the information related to the street it is in (e.g., average walking time, any work in progress, accidents, and so on). Other ones, instead, could store some information within their cache. Like in all the aforementioned *use-cases*, intermediate NDN routers are in charge of forwarding both *Interest* and *Data* packets. In the example shown in Fig. 11, the User-1, which is reaching an intersection, has to choose which street to take, i.e., *StreetA* or *StreetB*. She/he diffuses two *Interest* packets asking for

/domain/Transportation/TrafficManagement/Query/StreetA/Info

and

/domain/Transportation/TrafficManagement/Query/StreetB/Info.

User-2 and User-3 will answer to these requests by generating their specific *Data* packets providing information about *StreetA* and *StreetB*, respectively. We note that all nodes among the reverse path to User-1 can cache the status of considered streets. In this way, the information exchange (including emergency alert) becomes faster and more efficient.

Received information are finally interpreted by satellite navigation system in order to select the best suitable path to choose.

4.4.3. *Public safety services: signaling of a road accident*

In a Smart City it is necessary to foster the spontaneous participation of people in episodes concerning the urban environment [84]. For example, they can cooperate to notify the presence of proper anomalies, inefficiencies, and danger situations to the competent authorities. Among all the possibilities, this features can be really exploited to improve the public safety, as it has been highlighted in the SAFECITY project [40].

In this regard, we propose an *use-case* in which an user reports a road accident to the police (see the scenario depicted in Fig. 12).

Due to the receiver-driven communication model of NDN, if a citizen wants to report a given episode that may influence the safety of other peoples,

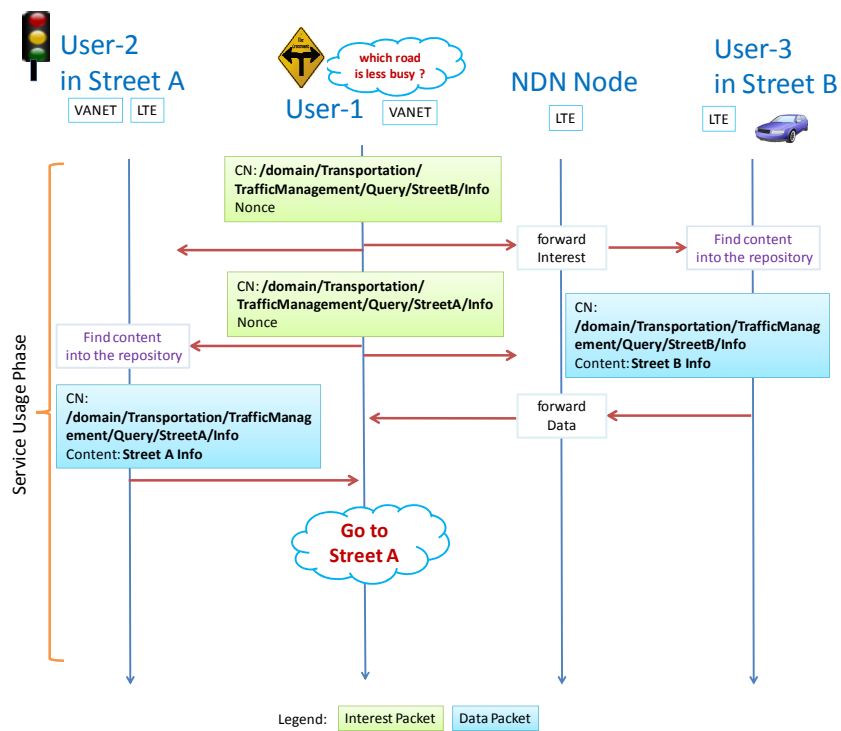


Figure 11: Use case 4: navigation assistance (transportation service).

she/he has to diffuse an *Interest* packet with *Content Name* set to

/domain/PublicSafety/RoadAccident/Communicate/UserName.

This message will be forwarded by intermediate NDN nodes towards the closest police car, which will reply with a *Data* packet of confirmation.

In addition, the police may also ask to the user additional details about the accident (e.g., a photo of the road). To this end, she/he generates a new *Interest* packet whose *Content Name* is set to

/domain/PublicSafety/RoadAccident/Query/UserName/AdditionalInfo/Photo.

Such a message will be forwarded towards the user that will reply with a *Data* packet storing the requested content.

The proposed *use-case* is composed by the only *Service Execution* phase, but it can be further improved by introducing security features.

4.4.4. *E-Healthcare services: reservation of a medical examination and remote assistance of patients*

The remote assistance of patient is an important healthcare application that is obtaining more and more attention in our society. This justify the reason why some projects, such as ELLIOT and TEFIS, are developing sophisticated solutions and services in this field to enhance the quality of the citizen life in future urban environments [36, 37].

In this context, we propose in Fig. 13 a reference *use-case* conceived by the ELLIOT project, which has been revised in the context of ICN. In this example, a medical device interacts with sensors diffused on the body of a patient to collect information about its life parameters (such as pressure, ECG, pulse measurement, and so on) and communicates them to remote medical center if some anomalies are detected.

As reported in Fig. 13, the medical device and sensors exchange messages through the IoT technology, whereas the communication with a remote medical center, i.e., an ambulance in our example, is done by means of the LTE infrastructure.

The medical device periodically asks body sensors to generate a report on life parameters, by issuing an *Interest* packet with the *Content name* set to:

/domain/HealthCare/PatientAssistance/Query/DataMonitoring/TypeOfData.

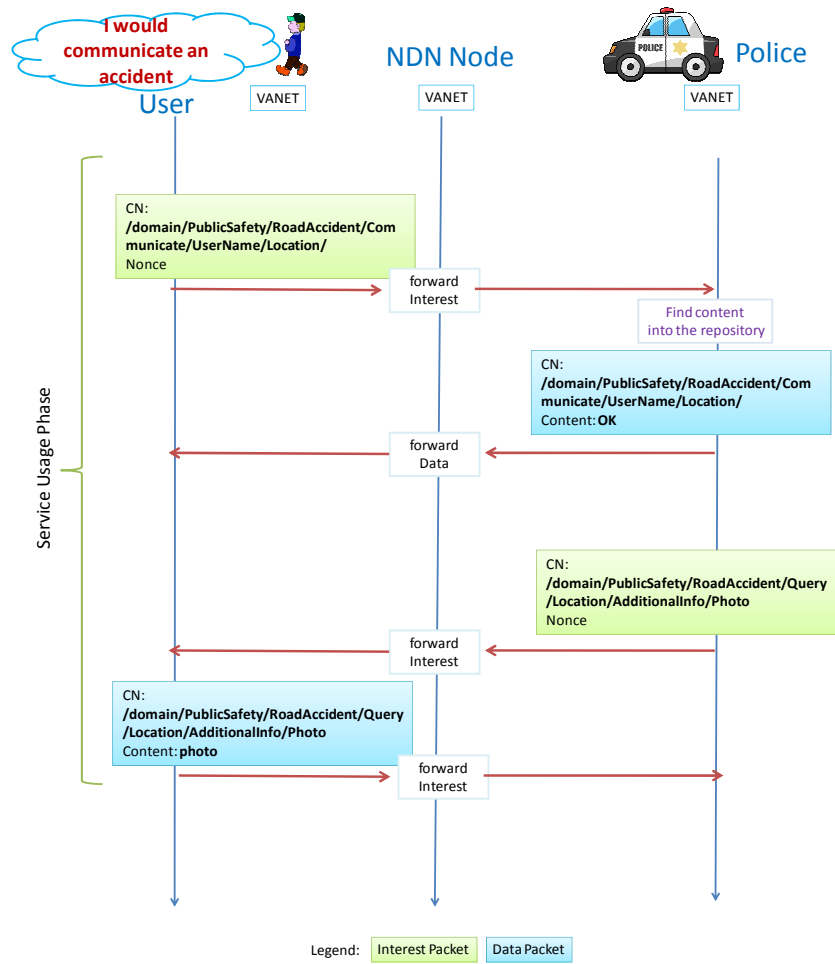


Figure 12: Use case 5: signaling of a road accident (public safety service).

By collecting all the information stored within all the received *Data* packets, it could identify the presence of an anomaly. If so, it will immediately contact the closest medical entity, thus triggering it to provide an urgent assistance to the patient. To this end, an *Interest* packet having the following *Content Name* is generated and sent by the LTE interface

/domain/HealthCare/PatientAssistance/Query/HealthCheck/PatientDetails/Data,

This request will reach a remote ambulance that will replay with a *Data* packet of confirmation and will reach the patient to provide her/him assistance.

Another interesting service in the health-care application field is related to the reservation of a medical examination. It is constituted by a user wants to book an orthopedic examination in a public hospital of his town. Moreover, we assume that she/he is connected to the Internet by using a cellular network based on the LTE technology. The execution of the service is reported in Fig. 14.

In order to be aware about healthcare structures able to satisfy the request, the user begins the *Discovery* phase by diffusing an *Interest* packet with the *Content Name* equal to

/domain/HealthCare/MedicalReservation/Discover/Hospital.

Several NDN nodes (e.g., hospitals and NDN devices having the content stored into the cache) can answer to the request. Thus, the user could received multiple *Data* packets; she/he will choose her/his preferred hospital, i.e., *HospitalName*.

The *Security Initialization* phase is performed for creating the secure communication and guarantee the respect of the privacy, which represents one of the most important requirement for the considered use case. We suppose to negotiate the key by adopting the approach shown in Fig. 7. The negotiated session key will be used to encrypt *additional – info* fields of *Interest* packets and the content of *Data* packets that will be exchanged from this moment on.

At this point, the user is ready for handling the *Service Usage* phase: a new *Interest* packet is sent asking for the remote hospital dates and doctors available for the request examination. The *Content Name* is set to

/domain/HealthCare/MedicalReservation/

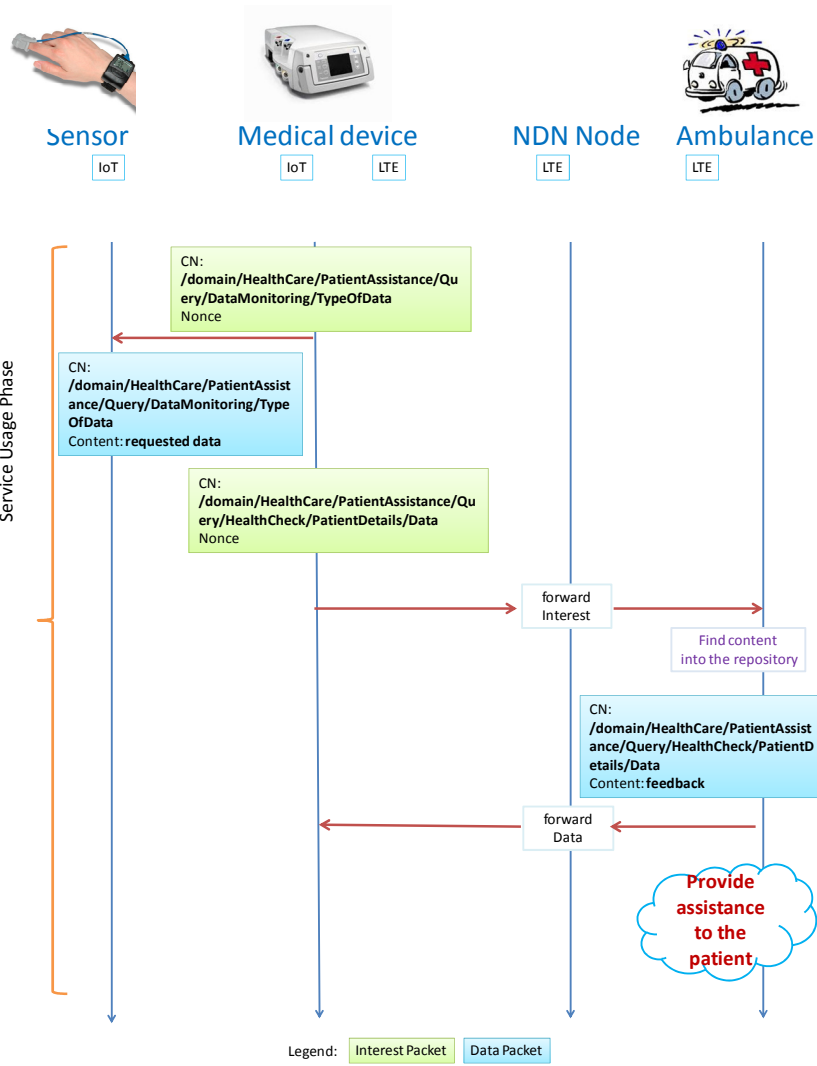


Figure 13: Use case 6: remote patient assistance (e-healthcare service).

Query/HospitalName/Orthopedic/Availability/UserEncryptedName.

Whereas maintaining unchanged components of the name adopted during the discovering procedure, both *type-of-question* and *additional-info* have been updated in order to better report the user request. Furthermore, *PublisherPublicKeyDigest* and *AnswerOriginKind* fields of the *Interest* packet have been properly set for ensuring that only the selected hospital will generate the answer. In response to the user demand, the hospital will send a *Data* packet with an encrypted payload. The *Freshness Second* will be set to zero to prohibit any caching procedures.

Finally, the user will generate another *Interest* packet for reserving the examination. Now, additional information stored into the *Content Name* is used to explicit the choice performed by the user:

/domain/HealthCare/MedicalReservation/Reserve/

HospitalName/Orthopedic/UserEncryptedName /Doctor/Data/Hour,

The hospital will confirm the reservation by sending a new *Data* packet.

4.4.5. *Urban planning service: waste management in a urban environment*

An efficient urban planning can, without any doubts, improve the quality of the life of all the citizens. One emerging issue that is affecting modern urban areas is the management of waste (this aspect is highly studied in the OUTSMART project [41]).

The last *use-cases* we would describe in this paper is related to a smart management of waste in a city. The scenario in Fig. 15 depicts an user that wants to know the waste container in which she/he can throw her/his trash. To this end, she/he releases an *Interest* packet having the *Content Name* equal to

/domain/BuildingUrbanPlanning/WasteManagement/Query/WasteContainerDetails.

Note that the *additional – info* field is properly built to ask not only for the position of the waste container, but also to understand if it is empty or not. These details will be provided by the waste container within the generated *Data* packet.

In addition, the waste container may also communicate to a remote data center its filling level. Such an information is directly stored within the *Content Name* of the *Interest* packet:

/domain/BuildingUrbanPlanning/WasteManagement/Communicate/DataCenter/StatusDetails.

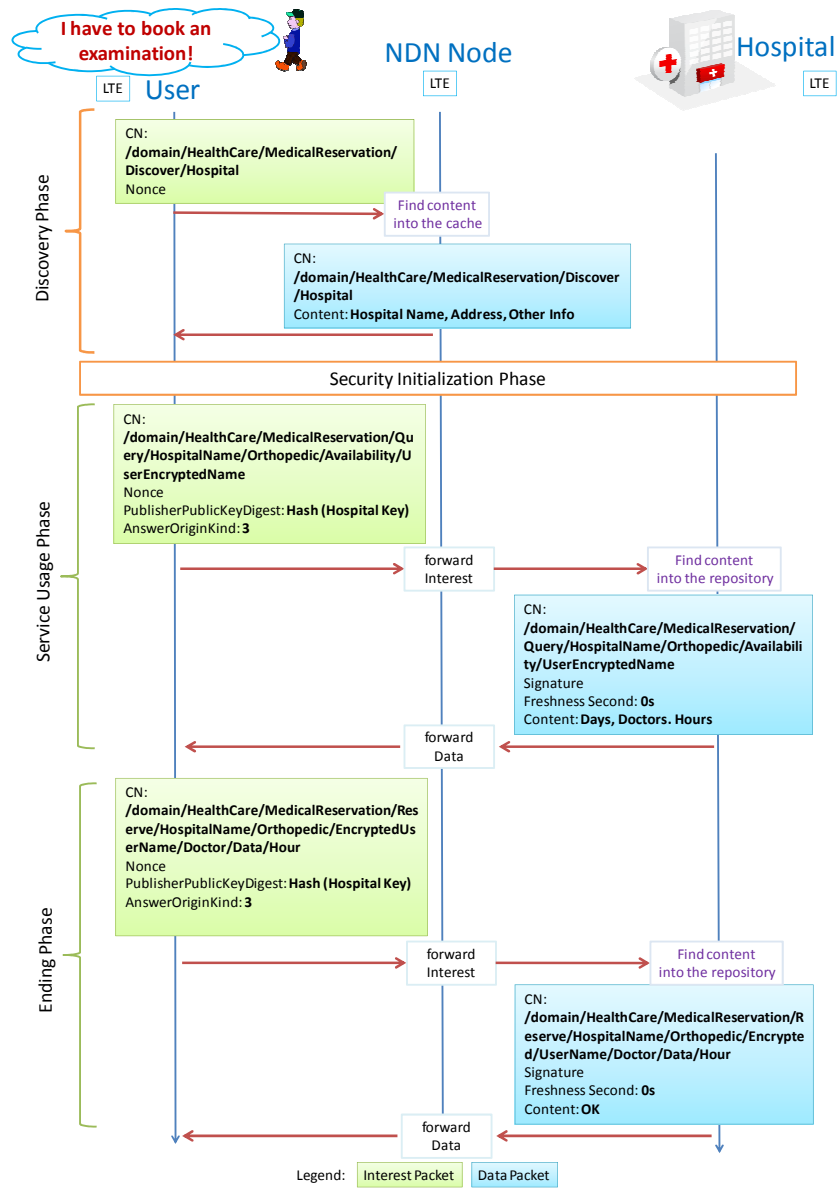


Figure 14: Use case 7: the reservation of a medical examination (e-healthcare service).

The waste management data center replies with a *Data* packet of confirmation and then properly react to the received message (i.e., by planning to empty the waste container).

5. Conclusions

How to cope with ICT services in Smart Cities? This paper has proposed a possible approach to the problem by highlighting its relevance in real-life use cases, taken from government and public administration, intelligent transportation systems, public safety, social, health-care, educational, and building and urban planning application domains. At its foundation, the ICN rationale has been adopted to improve the efficiency of communication networks, to ease mobility, to support security, and to exploit all the potentials of next generation wireless technologies.

Main goal of our work can be summarized as in the sequel: (i) the design of a complete and efficient platform enabling enhanced services in Smart Cities, (ii) the exploitation of the NDN architecture as a connection point between the service layer and the technological layer, (iii) the definition of the execution of a service through four consecutive phases, (iv) the design of the structure of the *name tree*, and (v) the demonstration of the utility and the behavior of the devised platform by means of a set of significant *use-cases*, which reflect the most common examples investigated by EU research projects working in this field.

Despite all the theoretical details discussed in this work, several issues still remain uncovered. Among them, we can identify the design and optimization of protocols and algorithms related to caching and routing operations, as well as those handling the generation of users' requests during the time. Future works will further explore such aspects to better discover the benefits that could derive from wide deployment of the conceived platform and to finely scavenge possible drawbacks. At the same time, we plan to test our platform with real experiments and to implement prototype software applications that can be exploited to execute conceived services in a real urban scenarios.

6. Acknowledge

This work was supported by the PON projects (RES NOVAE, ERMES-01-03113, DSS-01-02499 and EURO6-01-02238) funded by the Italian MIUR and by the European Union (European Social Fund).

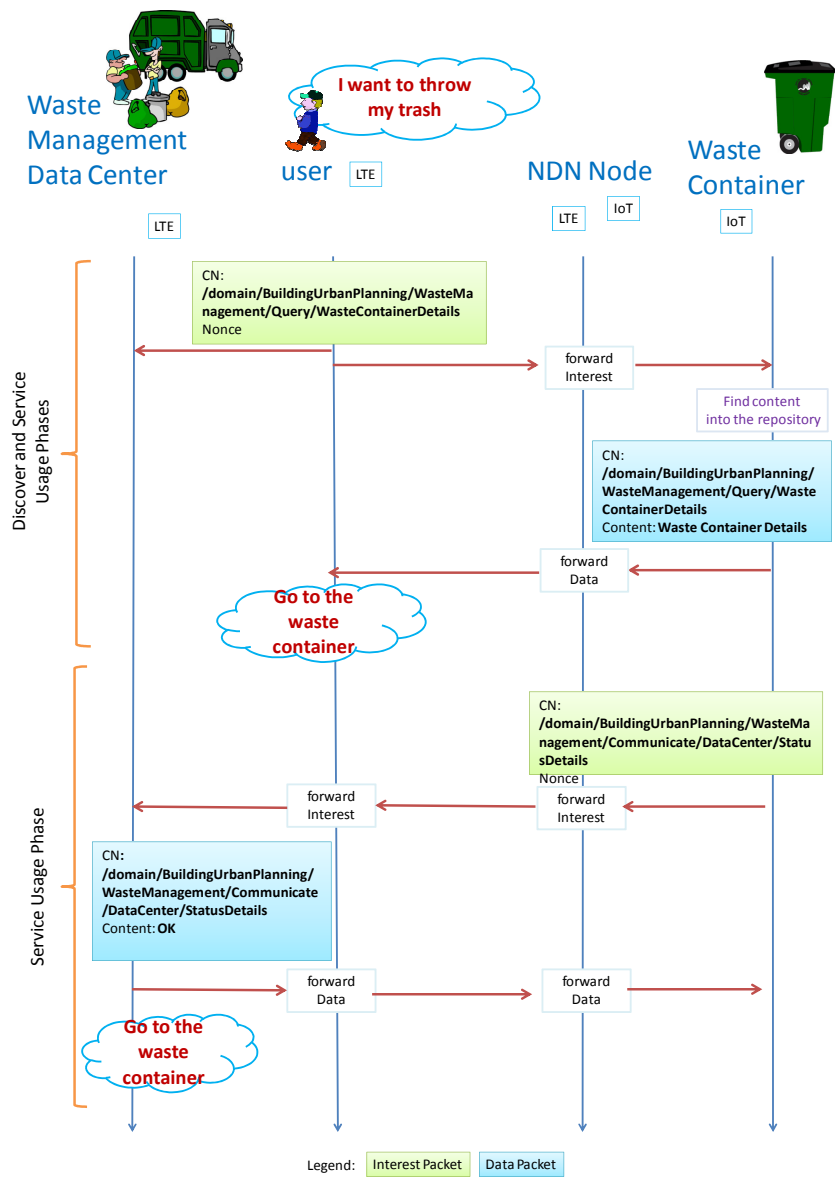


Figure 15: Use case 8: waste management in a urban environment (urban planning service).

7. Vitae

Giuseppe Piro is a postdoctoral researcher at Politecnico di Bari, Italy. His main research interests include quality of service in wireless networks, network simulation tools, 4G cellular systems, and Information Centric Networking. Piro has a PhD in electronics engineering from Politecnico di Bari. He founded the LTE-Sim project and is a developer of Network Simulator 3.

Ilaria Cianci is a PhD student at Politecnico di Bari, Italy. Her main research interests include the study of ICN solutions for the Future Internet, congestion control in NDN, real time video streaming in wireless environment. Cianci received the master degree com laude in telecommunication engineering from Politecnico di Bari in 2010. From November 2012 to August 2013 she collaborated with the Diana team - INRIA, at SOPHIA ANTIPO-LIS (France) as a visiting PhD student. She developed CCN-Joker, an open source experimental platform for NDN.

Luigi Alfredo Grieco is an assistant professor of telecommunications at Politecnico di Bari, Italy. His main research interests include congestion control in computer networks, quality of service in wireless networks, Internet of Things, Machine to Machine systems, Internet multimedia applications, Internet measurements, Information Centric Networking. Grieco has a PhD in information engineering from Università di Lecce, Italy. Hes an editor for IEEE Transactions on Vehicular Technology and an Executive Editor for the Transactions on Emerging Telecommunications Technologies (Wiley).

Gennaro Boggia is an associate professor in the department of "Ingegneria Elettrica e dell'Informazione" at the "Politecnico di Bari", Italy. His research interests include wireless networking, cellular communication, protocol stacks for industrial applications and smart grids, Internet measurements, and network performance evaluation. Boggia has a PhD in electronics engineering from Politecnico di Bari.

Pietro Camarda is currently a Professor of Telecommunications in the department of "Ingegneria Elettrica e dell'Informazione" at the "Politecnico di Bari", Italy. He was visiting scholar from October 1986 to December 1987 at Computer Science Department of the University of California, Los Angeles, with the supervision of Prof. Mario Gerla. He has been involved in

various research areas. In the past few years he focused mainly on wireless networks (cellular networks, wireless LANs, Ad Hoc Networks), developing topics that include Resource Allocation based on Neural Networks, Header Compression Schemes for Wireless Networks, Authentication Protocols in Wireless Networks, Bandwidth Allocation and Quality of Service in WLANs, MAC protocols for Ad Hoc networks, etc.

References

- [1] A. Caragliu, C. del Bo, P. Nijkamp, Smart cities in europe, in: Proc. of Central European Conf. in Regional Science, CERS, Kaschau, Slovak Republic, 2009.
- [2] R. Giffinger, Smart cities - ranking of european medium-sized cities, Tech. Rep. Centre of Regional Science, Vienna UT (10 2007).
- [3] C. Balakrishna, Enabling Technologies for Smart City Services and Applications, in: Proc. of IEEE Int. Conf. on Next Generation Mobile Applications, Services and Technologies, NGMAST, Paris, France, 2012.
- [4] J. M. Hernandez-Muoz, J. B. Vercher, L. Muoz, J. A. Galache, M. Presser, L. A. H. Gmez, J. Pettersson, Smart cities at the forefront of the future internet, in: The future internet, Springer-Verlag, 2011, pp. 447–462.
- [5] H. Schaffers, N. Komninos, M. Pallot, B. Trousse, M. Nilsson, A. Oliveira, Smart cities and the future internet: towards cooperation frameworks for open innovation, in: The future internet, Springer-Verlag, 2011, pp. 431–446.
- [6] L. Anthopoulos, P. Fitsilis, From digital to ubiquitous cities: Defining a common architecture for urban development, in: Proc. of IEEE Int. Conf. on Intelligent Environments (IE), Kuala Lumpur, Malaysia, 2010.
- [7] O. Kwon, J. Kim, A Methodology of Identifying Ubiquitous Smart Services for U-City Development, in: Proc. of Int. Conf. on Ubiquitous Intelligence and Computing (UIC), Hong Kong, China, 2007.
- [8] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, B. Ohlman, A survey of Information-centric Networking, IEEE Communication Magazine 50 (7) (2012) 26–36.

- [9] O. Hersent, D. Boswarthick, O. Elloumi, *The Internet of Things: Key Applications and Protocols*, 2nd Edition, Wiley, 2012.
- [10] E. Dahlman, S. Parkvall, J. Skold, *4G LTE/LTE-Advanced for Mobile Broadband*, Academic Press, 2011.
- [11] B. H. Walke, S. Mangold, L. Berlemann, *IEEE 802 Wireless Systems*, John Wiley and Sons, 2006.
- [12] IEEE, *Wireless Access in Vehicular Environments (WAVE): IEEE 1609 Standards Series*, IEEE Std. 1609 (2009).
- [13] D. Matsubara, T. Egawa, N. Nishinaga, V. Kafle, M.-K. Shin, A. Galis, *Toward future networks: A viewpoint from ITU-T*, *IEEE Communication Magazine* 51 (3) (2013) 112–118.
- [14] T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, I. Stoica, *A data-oriented (and beyond) network architecture*, in: *Proc. of ACM Conf. on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM)*, Kyoto, Japan, 2007.
- [15] N. Fotiou, P. Nikander, D. Trossen, G. C. Polyzos, *Developing Information Networking Further: From PSIRP to PURSUIT*, in: *Proc. of Int. Conf. on Broadband Communications, Networks, and Systems (BROADNETS)*, Athens, Greece, 2010.
- [16] C. Dannewitz, D. Kutscher, B. Ohlman, S. Farrell, B. Ahlgren, H. Karl, *Network of Information (NetInf), An information-centric networking architecture*, *Computer Communications* 36 (7) (2013) 721 – 735.
- [17] N. Melazzi, S. Salsano, A. Detti, G. Tropea, L. Chiariglione, A. Difino, A. Anadiotis, A. Mousas, I. Venieris, C. Patrikakis, *Publish/subscribe over information centric networks: A Standardized approach in CONVERGENCE*, in: *Proc. of Future Network Mobile Summit (FutureNetw)*, Berlin, Germany, 2012.
- [18] NDN, *The named data networking project*, <http://www.named-data.net/>.

- [19] M. Bari, S. Chowdhury, R. Ahmed, R. Boutaba, B. Mathieu, A survey of naming and routing in information-centric networks, *IEEE Communication Magazine* 50 (12) (2012) 44–53.
- [20] L. Zhang, D. Estrin, J. Burke, V. Jacobson, J. D. Thornot, D. Smatters, B. Zhang, G. Tsudik, D. Krioukov, D. Massey, C. Papadopoulos, T. Abdelzaher, L. Wang, P. Crowley, E. Yeh, Named data networking (NDN) project, PARC Tech. Rep. TR-2010-02, 2010.
- [21] L. Wang, A. Afanasyev, R. Kuntz, R. Vuyyuru, R. Wakikawa, L. Zhang, Rapid traffic information dissemination using named data, in: *Proc. of ACM workshop on Emerging Name-Oriented Mobile Networking Design - Architecture, Algorithms, and Applications*, Hilton Head, SC, USA, 2012.
- [22] F. Andreini, F. Crisciani, C. Cicconetti, R. Mambrini, A scalable architecture for geo-localized service access in smart cities, in: *Proc. of Future Network Mobile Summit (FutureNetw)*, Warsaw, Poland, 2011.
- [23] J. Zhang, Q. Li, E. Schooler, iHEMS: An information-centric approach to secure home energy management, in: *Proc. of IEEE 3th Int. Conf. on Smart Grid Communications (SmartGridComm)*, Vancouver, Canada, 2012.
- [24] S. Idowu, N. Bari, A Development Framework for Smart City Services, Master’s thesis, Lulea University of Technology, Lulea, SWEDEN (2012).
- [25] S. Srinivasan, A. Singh, D. Batni, J. Lee, H. Schulzrinne, V. Hilt, G. Kunzmann, CCNxServ: Dynamic service scalability in information-centric networks, in: *Proc. of IEEE Int. Conf. on Communications (ICC)*, Ottawa, Canada, 2012.
- [26] CCNx, The Content-Centric Networking Implementation, available at <https://www.ccnx.org/>.
- [27] I. Cianci, G. Piro, L. A. Grieco, G. Boggia, P. Camarda, Content Centric Services in Smart Cities, in: *Proc. of Int. workshop on technologies and applications for smart cities (I-TASC)*, Paris, France, 2012.

- [28] H. Chourabi, T. Nam, S. Walker, J. Gil-Garcia, S. Mellouli, K. Nahon, T. Pardo, H. Scholl, Understanding smart cities: An integrative framework, in: Proc. of Hawaii Int. Conf. on System Science (HICSS), Grand Wailea, Maui, Hawaii, 2012.
- [29] C. Harrison, B. Eckman, R. Hamilton, P. Hartswick, J. Kalagnanam, J. Paraszczak, P. Williams, Foundations for smarter cities, IBM Journal of Research and Development 54 (4) (2010) 1–16.
- [30] A. Coe, G. Paquet, J. Roy, E-governance and smart communities: a social learning challenge, Journal on Social Science Computer Review 19 (1) (2001) 80–93.
- [31] A.-V. Anttiroiko, P. Valkama, S. Bailey, Smart cities in the new service economy: building platforms for smart services, Journal of AI and SOCIETY 28 (1) (2013) 1–12.
- [32] N. Komninos, H. Schaffers, M. Pallot, Developing a policy roadmap for smart cities and the future internet, in: Proc. of eChallenges Conference (e-2011), Florence, Italy, 2011.
- [33] K. Su, J. Li, H. Fu, Smart city and the applications, in: Proc. of Int. Conf. on Electronics, Communications and Control (ICECC), Ningbo, China, 2011.
- [34] R. E. Hall, The vision of a smart city, in: Proc. of Int. Life Extension Technology Workshop, Paris, France, 2000.
- [35] L. Sanchez, J. A. Galache, V. Gutierrez, J. Hernandez, J. Bernat, A. Gluhak, T. Garcia, Smartsantander: The meeting point between future internet research and experimentation and the smart cities, in: Proc. of IEEE Future Network and Mobile Summit (FutureNetw), Warsaw, Poland, 2011.
- [36] ELLIOT website, Experiential living lab for the internet of things, <http://www.elliott-project.eu/>.
- [37] J. Leguay, A. Sällström, B. Pickering, E. Borrelli, F. Benbadis, Travel eCommerce experiment - through TEFIS, a single access point to different testbed resources, in: Proc. of the 4th European conference on Towards a service-based internet, Poznan, Poland, 2011.

- [38] FIREBALL website, Smart cities as innovation ecosystems sustained by the future internet, <http://www.fireball4smartcities.eu/>.
- [39] IOE website, Internet of energy for electric mobility, <http://www.artemis-ioe.eu/>.
- [40] SafeCity website, Future internet applied to public safety in smart cities, <http://www.safecity-project.eu/>.
- [41] OUTSMART website, Outsmart, <http://www.fi-ppp-outsmart.eu/>.
- [42] RELYonIT website, Research by experimentation for dependability on the internet of things, <http://www.relyonit.eu/>.
- [43] FINEST website, Future internet enabled optimization of transport and logistics business networks, <http://www.finest-ppp.eu/>.
- [44] DigitalCities website, Digital cities, <http://www.digital-cities.eu/>.
- [45] Mobincity website, Smart mobility in smart city, <http://www.mobincity.eu/>.
- [46] HOBNET website, Holistic platform design for smart buildings and the future internet, <http://www.hobnet-project.eu/>.
- [47] CitySKD website, City Service Development Kit, <http://www.citysdk.eu/>.
- [48] LiveCity website, Live video-to-video supporting interactive city infrastructure, <http://www.livecity-ppp.eu/>.
- [49] IES website, Internet-enabled services for the city across europe, <http://iescities.eu/>.
- [50] PERIPHERIA website, Smart Peripheral Cities for Sustainable Lifestyles, <http://www.periphedia.eu/>.
- [51] iCITY website, icity, <http://www.icityproject.com/>.
- [52] TV-RING website, Testbeds for connected tv services using hbbtv, <http://cordis.europa.eu/fp7/ict/fire/connected-smart-cities/factsheets/tv-ring-sep12.pdf>.

- [53] G. Stefansson, J. Woxenius, The Concept of Smart Freight Transport Systems the road hauliers perspective, in: Proc. of the 19th NOFOMA Conference, Reykjavik, Island, 2007.
- [54] B. David, Y. Chuantao, Z. Yun, X. Tao, Z. Bingxue, J. Huiliang, R. Chalon, SMART-CITY: Problematics, techniques and case studies, in: Proc. of IEEE Int. Conf. on Computing Technology and Information Management (ICCM), Berlin, Germany, 2012.
- [55] A. Elmangoush, H. Coskun, S. Wahle, T. Magedanz, Design aspects for a reference M2M communication platform for Smart Cities, in: Proc. of IEEE Int. Conf. on Innovations in Information Technology (IIT), Al Ain, UAE, 2013.
- [56] M. Wimmer (Ed.), Knowledge Management in Electronic Government, Lecture Notes in Computer Science, Springer, Enschede, Netherlands, 2003.
- [57] M. Castelli, M. Comerio, M. Cremaschi, Towards the Definition of Value-added Services for Citizens: a New Model for the Description of Public Administration Services, International Journal of Management & Information Technology 4 (1) (2013) 166–173.
- [58] D. G. European Commission, Digitizing Public Services in Europe: Putting ambition into action , Tech. rep. (Dec. 2010).
URL http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display\&\#38;doc_id=747
- [59] A. Leben, M. Bohanec, Architecture of an active life-event portal: A knowledge-based approach., in: Proc. of 5th IFIP International Conference (KMGov2004), Krems, Austria, 2004.
- [60] N. Odendaal, Information and communication technology and local governance: understanding the difference between cities in developed and emerging economies., Computers, Environment and Urban Systems 27 (6) (2003) 585–607.
- [61] C. . T. European Commission, DG Communications Networks, eGovernment Benchmark Framework 2012-2015, Tech. rep. (Jul. 2012).
URL <https://ec.europa.eu/digital-agenda/sites/>

digital-agenda/files/eGovernment\%20Benchmarking\%20method\%20paper\%20published\%20version_0.pdf

- [62] G. Piro, L. A. Grieco, G. Boggia, P. Chatzimisios, Information-centric networking and multimedia services: present and future challenges, ETT, Transactions on Emerging Telecommunications Technologies, To be published.
- [63] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, R. L. Braynard, Networking named content, in: Proc. of ACM Int. Conf. on emerging Networking Experiments and Technologies (CONEXT), Rome, Italy, 2009.
- [64] N. B. Melazzi, L. Chiariglione, The Potential of Information Centric Networking in Two Illustrative Use Scenarios: Mobile Video Delivery and Network Management in Disaster Situations, IEEE COMSOC MMTC E-letter (2013) 17–20.
- [65] FIArch Group, Fundamental Limitations of Current Internet and the path to Future Internet, in: White Paper, 2010.
- [66] J. Pan, S. Paul, R. Jain, A survey of the research on future internet architectures, IEEE Communication Magazine 49 (7) (2011) 26–36.
- [67] K. Pentikousis, B. Ohlman, D. Corujo, G. Boggia, G. Tyson, E. Davies, P. Mahadevan, S. Spirou, A. Molinaro, D. Gellert, S. Eum, ICN Baseline Scenarios and Evaluation Methodology, draft-pentikousis-icn-scenarios-04, expires on Jan. 16, 2014 (7 2013).
- [68] A. Feldmann, Internet clean-slate design: what and why?, ACM SIGCOMM Computer Communication Review 37 (3) (2007) 59–64.
- [69] D. Clark, B. Lehr, S. Bauer, P. Faratin, R. Sami, J. Wroclawski, Overlay networks and future of the internet, Journal of Communications and Strategies 63 (1) (2006) 1–21.
- [70] M. Tortelli, L. A. Grieco, G. Boggia, K. Pentikousis, COBRA: Lean Intra-domain Routing in NDN, in: Proc. of IEEE Consumer Communications and Networking Conference, CCNC, Special Session on Research and Case Study for Designing and Deploying Information-centric Networks, Las Vegas, NV, USA, 2014.

- [71] D. K. Smetters, V. Jacobson, Securing network content, PARC Tech. Rep. TR-2009-1, 2009.
- [72] B. Adamson, C. Bormann, M. Handley, J. Macker, RFC 5401 - Multicast Negative-Acknowledgment (NACK) Building Blocks (Nov. 2008).
- [73] V. Jacobson, D. K. Smetters, N. H. Briggs, M. F. Plass, P. Stewart, J. D. Thornton, R. L. Braynard, VoCCN: voice-over content-centric networks, in: Proc. of the workshop on Re-architecting the internet (ReArch), Rome, Italy, 2009.
- [74] J. Kim, M. wuk Jang, B.-J. Lee, K. Kim, Content centric network-based virtual private community, in: Proc. of IEEE Int. Conf. on Consumer Electronics (ICCE), Las Vegas, USA, 2011.
- [75] K. Lei, Z. Wang, A CA-based scheme of user authentication over Content-Centric Networking, in: Proc. of IEEE Int. Conf. on Computer Science Education (ICCSE), Melbourne, Australia, 2012.
- [76] A. Martinez-Balleste, P. Perez-Martinez, A. Solanas, The pursuit of citizens' privacy: a privacy-aware smart city is possible, IEEE Communication Magazine 51 (6) (2013) 136–141.
- [77] P. Martinez-Julia, A. Gomez-Skarmeta, Secure identity-to-identity communications over content-centric networking, in: Proc. of IEEE Int. Conf. on Internet Multimedia Services Architecture and Application (IMSAA), Bangalore, India, 2010.
- [78] X. Zhang, K. Chang, H. Xiong, Y. Wen, G. Shi, G. Wang, Towards name-based trust and security for content-centric network, in: Proc. of IEEE Int. Conf. on Network Protocols (ICNP), Vancouver, Canada, 2011.
- [79] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Tech. rep. (May 2008).
- [80] C. Barba, M. Mateos, P. Soto, A. Mezher, M. Igartua, Smart city for VANETs using warning messages, traffic statistics and intelligent traffic lights, in: Proc. of IEEE Symposium on Intelligent Vehicles (IV), Alcal de Henares, Spain, 2012.

- [81] B. Drilo, D. Saric, R. Filjar, The role of telecommunications in development of new-generation intelligent transport systems, in: Proc. of Int. Conf. on Wireless VITAE, Aalborg, Denmark, 2009.
- [82] J. Ferreira, J. Afonso, Mobi_System: A personal travel assistance for electrical vehicles in smart cities, in: Proc. of IEEE Int. Symposium on Industrial Electronics (ISIE), Gdask, Poland, 2011.
- [83] G. Khekare, A. Sakhare, A smart city framework for intelligent traffic system using VANET, in: Proc. of IEEE Int. Conf. on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), Kerala, India, 2013.
- [84] G. Cardone, L. Foschini, P. Bellavista, A. Corradi, C. Borcea, M. Tallasila, R. Curtmola, Fostering participation in smart cities: a geo-social crowdsensing platform, IEEE Communication Magazine 51 (6) (2013) 112–119.