Using Information Centric Networking in Internet of Things: A Survey

Dorra Mars, Sonia Mettali Gammar, Abdelkader Lahmadi, Leila Azouz Saidane

Using Information Centric Networking in Internet of Things: A survey

Dorra Mars[a,1], Sonia Mettali Gammar[a,2], Abdelkader Lahmadi[b,3], Leila Azouz Saidane[a,4]

[a] *National School of Computer Science, CRISTAL Lab, University of Manouba, Tunisia*
[b] *Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France*

Abstract

Internet of Things (IoT) is increasingly deployed in different domains and environments including smart homes, smart cities, healthcare, industry 4.0, and smart agriculture, by connecting a large number of physical objects to deliver a new class of applications. The rising number of these connected objects and their heterogeneity have raised new research directions and challenges regarding their communications, scalability and the large amount of data that generate. As a result, new communication technologies have been proposed to be applied in these environments and applications, mainly to consider their main inherent properties which are the information that generate and handle, and the content that disseminate. Among the adopted techniques and recently integrated into the IoT is the ICN (Information Centric Networking) paradigm. The choice of integration of ICN in the context of IoT is mainly motivated by all the advantages it represents, in particular content caching and decoupling senders and receivers. In this paper, we provide a detailed analysis of the motivations behind using ICN in IoT environments and a survey of existing research work that have already applied ICN as a communication support for IoT applications.

Keywords: Internet of Things (IoT), Information Centric Networking (ICN), Applications.

[1] dorram@live.fr
[2] sonia.gammar@ensi.rnu.tn
[3] abdelkader.lahmadi@loria.fr
[4] leila.saidane@ensi-uma.tn

1. Introduction

The evolution of Internet to support the connection of different devices, as well as their associated methods that allow online content manipulation, has created a set of new challenges, enabling technologies, protocols and applications. The integration of low-cost sensors, actuators, and the development of wireless technologies allowing the connection of small devices to the Internet has led to an increasing deployment of Internet of Things (IoT), where everyday physical objects are transformed into communicating and smart objects. Several networking solutions have been proposed to foster the emergence of IoT and its associated applications. Besides the traditional Internet protocol (IP) host-based approach [1], other solutions such as Information Centric Networking (ICN) have been proposed [2]. ICN is defined as a new paradigm for naming content and placing information at the center of its architecture [3] instead of relying on IP host identifiers. The main goal is to transform the current Internet to a simpler and more generic architecture. Several ICN instances and approaches have been proposed. Content Centric Networking (CCN) was proposed in 2009[4] and it was followed by other paradigms such as the Network of Information architecture (Netinf)[5] and the Publish Subscribe Internet Technology (PURSUIT)[6]. In particular, Named Data Networking (NDN) approach has been widely adopted because of its simple communication model, scalability, light configuration and management operations[7]. It offers a naming scheme without topology and provides routing for better forwarding mechanism. Moreover, NDN specifies an easy and robust receiver-driven communication model based on the exchange of two packets types, Interest and Data, which consider hierarchical and application-specific content names.

Today ICN has emerged as a new solution to overcome identified constraints and support various IoT scenarios by taking benefit from its advantages and characteristics to deploy applications in different environments including Smart home, Smart Health, Smart cities and manufacturing [2]. Moreover, ICN is used as a communication framework by Machine-to-Machine (M2M) technologies to connect devices, equipped with sensors and actuators, operating autonomously, and allowing the building of several services in the IoT context. It has been also applied as a support for the communications between the gateway and the constrained devices[8]. The employment of ICN and in particular NDN addresses the issue of energy saving in IoT environments. In [9], authors have shown that we can reach up to 90 % reduction in energy consumption while using different NDN content caching strategies of IoT contents. It is also easy to notice the increasing number of research work dealing with ICN and IoT [10]. Several works have tried to adopt ICN in the context of IoT in order to improve the communication within the network and to have more significant and promising results. Therefore, we find ICN applied by researchers as a communication medium by adopting properties such as naming, routing, caching, etc as stated in [11][12][13]. Other studies have tried to take advantage of the available features of ICN and integrate them into different IoT applications[14] [15]. In particular, ICN has been applied in multiple environment domains such as smart city-specific applications including intelligent transport[16], smart health [17] [18], smart home[19], and smart grid[20].

Until now, however, existing work on ICN and IoT remains limited when compared to other areas. To the best of our knowledge, this is the first work providing a survey of existing approaches integrating both ICN and IoT within different IoT application domains.

The paper is organized as follows. In section 2, we present the characteristics and the most popular application domains of IoT. In section 3, we explain the benefits of using ICN in the context of IoT. In section 4, we present a survey of applications using ICN in the context of IoT while comparing their characteristics. Finally, we provide conclusions of the study carried in this paper.

2. Overview of Internet of Things

The Internet of Things (IoT) is a term that has recently emerged and introduced by Kevin Ashton in 1999. The main idea of the IoT focuses on the massive deployment of a set of objects (things) such as radio frequency identification (RFID), sensors, actuators and mobile phones. These objects have the ability to interact with each other and cooperating with their neighbors in order to achieve common goals[10]. However, there is no exact definition for the Internet of Things, since the term has been constantly changing as a result of progress and new perspectives. The IoT European Research Cluster (IERC), a research group whose work involves defining a common vision and expressing the challenges of technological research and development that IoT faces at the European level, defines IoT as follows: *a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual things have identities, physical attributes, and virtual personalities and use smart interfaces, and are seamlessly integrated into the network information.*

2.1. IoT characteristics

Iot relies on the following set of characteristics [21]:

- Interconnectivity: with IoT, everything can be interconnected with the global information and communication infrastructure.
- Object-related services: IoT provides object-related services by considering the constraints of a thing such as privacy and semantic consistency between physical things and their associated virtual objects.
- Heterogeneity: IoT devices are heterogeneous on the basis of different hardware platforms and networks. Interaction with other platforms or services is done via different networks.
- Dynamic changes: device status with IoT changes dynamically, for example, location, speed, sleeping and waking, connected and/or disconnected.

Therefore, the number of devices can change dynamically.

- Large scale: with IoT the number of devices is increasing while they must be managed and the communication interactions will be of order of magnitude greater than the devices connected to the current Internet.

- Safety and security: safety is one of the most important characteristics that must be taken into consideration when developing and deploying IoT devices since they may affect the physical world. Also, securing the nodes, networks and data transfered through them requires creating security mechanisms able to spread out across them.

- Connectivity: it allows IoT devices to access the network to consume and produce data.

2.2. IoT applications

The services provided by IoT and its ability to connect multiple heterogeneous devices makes it able to cover a large number of application domains within multiple environments. The emergence of smart objects and their locations everywhere contributes in developing a better quality of life [22] by enabling multiple applications. Several domains have leveraged IoT technologies to provide new applications. We detail four application domains that have been impacted by IoT.

Healthcare domain. The benefits of the IoT technologies in the healthcare field are numerous. Based on intelligent objects that can be integrated either in the body or in the environment, it becomes possible to perform several tasks, namely[23]:

- Ensuring the monitoring of the location and movements of patients, for faster interventions in emergency cases.

- Reducing the incidence of harmful accidents thanks to a clear identification system. Generally, identification and authentication are used to meet the requirements relating to safety procedures.

- Collecting automated data, by allowing processing time reduction and process automation.
- Detecting patient status based on sensors.

Smart environment (home, office, plant) domain. Smart environments allow us to think in a comfortable environment equipped with a set of intelligent embedded objects in houses, offices, industries, places of entertainment, etc. The smart home can be one of the IoT applications by the use of RFID technologies. Various intelligent home services can be created such as washing programs, shopping, cooking, energy consumption monitoring and healthcare of the elderly [24].

Transportation and logistics domain. Intelligent Transportation includes cars, buses, bikes and trains and all means of transportation that are equipped with sensors conducted with a capacity of treatment equipment. Moreover, the transported goods are equipped with sensors to monitor and assist depot management operations [25].

Social domain. Social domain includes applications allowing the user to interact with other people in order to build relationships. Among the applications, we mention social networks[26]. The IoT applications in social and personal networks, such as Facebook and LinkedIn, give the individual the possibility to stay connected and interact with the world. Nowadays, the personal and social domain is constantly developing thanks to many tools that rely on IoT. This increasing connectivity brings to light the importance of accounting for the security and protection of personal information. The integration of ICN in these IoT enabled application domains is justified by a set of advantages that offer ICN to IoT.

3. Why ICN for IoT?

IoT is mostly based on the interconnection of several heterogeneous devices. Most IoT systems rely on TCP/IP protocols, in particular by using IPV6 protocol. Nevertheless, it may be inadequate in properly supporting IoT applications.

One of the main problems in IPv6, is the header length which is equal to 40 bytes, as well the IPv6 specification that requires that networks support a minimum MTU size of 1280 bytes. However, low power constrained links are often based on very small MTUs which have considered by the 6loWPAN layer. 6loWPAN is an adaptation layer between the network layer and the link layer, which offers a compression mechanism for the IPv6 header, extension and UDP headers. However, such layer relies on link layer fragmentation which introduces overhead and also increases the complexity of the network stack. Another problem in an IoT environment is the common lack of wired network infrastructure leading to the use of wireless mesh networks. Thus, to ensure communications between devices we have to rely on multi-link model. Due to the energy constraints, networks become vulnerable to multicast operations, which require that all nodes participating in a multicast communication to switch to the awake state instead of the sleeping state. Moreover, multicast communication usually deactivates the ACK of the link layer MAC protocols that cause lost of packets that could not be retrieved at the transport layer. Other problems are specific to the transport layer where IoT applications are faced with several communication models that TCP cannot support. Due to energy constraints, the devices can switch to standby mode, which disrupts the connection mode of IoT applications. Some issues are related to the application layer where the service discovery mechanism for traditional IP networks is based on DNS, and requires a more general approach to better identify heterogeneous resources. IoT communication can be either synchronous or asynchronous when constrained devices have to save energy while TCP/IP communication requires the client and server nodes to wake up at the same time. Furthermore, among the requirements of IoT is security, which is justified by the continuous interaction with the physical world. Indeed, the IP security model is based on the security of the communication channel. But this alternative is not suitable for the IoT environment for several reasons. First the TLS (Transport Layer Security) [27] and DTLS (Datagram Transport Layer Security) [28] protocols used by IP need long processing times for authentication and verification operations. Channel-based security does not check the request/response security when the application data leaves the channel. Similarly, both channel ending points must maintain the channel states until it is closed, which introduces a strong pressure on the use of the memory. It is therefore easy to see the need to apply a new architecture different from TCP/IP capable of supporting the different IoT requirements. In order to solve these problems, ICN is proposed as an alternative communication techniques for IoT applications [27].

3.1. The naming

The use of names for authentication and identification requires clear and accurate naming. Similarly, used names must be easily manageable and revocable. Thus, in IoT environments an expressive and personalized naming scheme arises. A name resolution system must take into account the mobility of objects and their connectivity. Data naming provides inherent support for delay tolerant networking (manages intermittent connectivity) unlike the Internet. Naming in IoT covers the naming of devices, data, and services. In [11], the authors proposed the following naming schemes:

Hash-based content name. This scheme relies on hash algorithms to name the content and makes it possible to verify that the content is the one requested. This method is adapted in the context of systems with a large number of objects.

Naming content based on Metadata. Metadata is used to generate a name for an object before it is created. This requires semantics to match the metadata. However, naming has some limitations. Assigning unique names to identify each object can raise problems at the naming mechanism level since here the name is the identification key. That's why methods for differentiating and selecting names are essential.

3.2. Caching

Caching has a set of benefits such as accelerating data retrieval and increasing the availability of the content being searched. Caching-related operations can be costly, leading to increased energy consumption. ICN provides solutions to answer questions related to the efficient retrieval of information compared to the traditional Internet communications [28]. Thus with ICN, clients and nodes are not concerned with the address of the home location, but focus on the demand for their interests. Also with ICN, the content is cached next to the interest for any additional request for similar data. ICN, has the advantage that the information is not automatically deleted like in the IP transfer, which allows the reduction of upstream bandwidth flows and makes information available to the users. Though caching is a main feature of ICN, occasionally the use of caching mechanisms is not beneficial in the case where a content is requested only once. In addition, distributed caching is less useful in ICN nodes when in a case with repository overlays such as a cloud or a data distribution network (CDN) or clients can retrieve the data (Clients in these situations can recover without the need for caching).

3.3. Decoupling sender and receiver

Decoupling the sender and the receiver is a useful mechanism provided by the ICN approach, particularly for retrieval of content delivered by devices with intermittent connectivity. However, in order to efficiently retrieve data, it must be possible for receivers to easily deduce the name of the data to be requested, without any direct contact with the sender. An important feature of the ICN is that it will allow responders (eg, IoT devices) to be sometimes inaccessible, for example, due to intermittent connectivity, low battery level, or because of duty cycles. Another advantage is that caching in ICN will ensure that data objects are normally delivered only once from IoT devices, regardless of the number of immediate requesters. However, decoupling is undesirable in the situation where authentication is necessary for management and actuation reasons.

3.4. Scalability

Assigning names to IoT content allows the structuring of information and users can request the content they really want. Name resolution at network layer level and name-based transfer reduces signaling overhead within IoT deployments. Also, ICN can identify requests for the same named information, which avoids the possibility of transmitting them differently on the same path. Content is cached in the intermediate nodes, allowing queries to be satisfied by the first available copy, which prevents over-querying and support in connectionless scenarios.

3.5. Energy efficiency

Deployed IoT devices have usually constraints since they are limited in terms of energy and computation. Embedded devices spend a large part of their life time in standby mode and only wake up when they need to exchange data. Therefore, the design of energy-efficient operation is crucial for multiple IoT networking solution. The communication model driven by the ICN receiver, coupled with anycast and caching mechanisms in the network, can help recover content even in networks constrained with low cycle service providers. In fact, a query can be satisfied by another node, maintaining a copy of the data, when the producer is in sleep mode. Also, distributed caching makes it possible to avoid massive access to the data of the constrained devices, which saves energy resources. In the same way, using multicast based communications makes it possible to achieve the goal of reducing the amount of traffic and the interactions with the nodes. Such approach reduces the energy consumption of IoT systems which are generally deployed on constrained devices that have energy efficiency and battery life requirements.

3.6. Mobility

Mobility is considered as a necessity (e.g., when IoT devices are moving on vehicles or are transported by humans). Existing IP mobility management solutions (for example, Mobile IP) are the subject of several research work due to the increase in the number of mobile terminals. However, they are facing scalability problems, leading to more efficient solutions (e.g. distributed mobility management), which have yet to be adopted by mobile operators, and proved valid in such scenarios. ICN supports the mobility of information consumers: when a consumer reinstates, he or she can simply re-issue any unsatisfied demand / subscription and be served by another node. In addition, ICN natively supports multi-homing, so that content or data requests can use any interface (or even all simultaneously) available on the device. However, mobility can be a limit in some cases. For some deployment scenarios, mobility requires updates in the transport intermediaries (in the case of NBR: Name Based Routing) or in the entities participating in the resolution of names. These mechanisms can lead to large delays and periods of disruption.

3.7. Heterogeneity

One of the properties of IoT is the presence of a variety of equipments and services. Using a traditional host-centric architecture only shows that the devices or their network interfaces are named at the network level, leaving the application layer to name the data and services. In several applications in IoT, data and services are the main primary objectives, while the specific communication between two devices remains secondary.

Content and data services can be offered by multiple devices, or a set of devices, which explains why naming data and services is often more important than naming devices. In this context, ICN appears to be a well-suited solution for IoT. Standardized naming is used to summarize services and content to mask the heterogeneity of underlying networks and devices and to facilitate interoperability between different actors. For example, ICN has the potential to allow entities to request content by its name, regardless of the type of service that provides it, and transmits it from the source. Moreover, by decoupling consumers and producers and providing coherent data packets, the ICN can interconnect information, devices and services in heterogeneous network scenarios.

3.8. Quality of service

With IoT, several applications may require various QoS. For example, while some of them need a timely reply, others may tolerate longer delivery delays.

ICN has the ability to promote the quality of content recovery and management of different QoS requests. Support for network caching, anycast and multicast mechanisms can increase data recovery and reduce traffic congestion.

3.9. Security

Activating security services is fundamental in IoT since most applications have the potential to be integrated into users daily lives. ICN offers security support at the network layer where it facilitates the sharing of content between nodes with local verification of authentication and data integrity which eliminates the need to trust intermediate nodes. In addition, by securing the content itself, ICN may restrict access to the data to a specific user or group of users[29].

4. IoT applications with ICN

Several approaches combining IoT and ICN have been proposed in literature. We classify them according to four application domains: smart grid, smart building, smart home and smart health.

4.1. Smart Grid

Existing Work with ICN support in smart grids are increasing, which is justified by the overall benefits of ICN in this application domain. ICN can be included in the intelligent network infrastructure to support distribution of data across heterogeneous entities. The broadcast mode in SG (Smart Grid) is mainly based on multicast, where a node sends data to many nodes, which explains the need for a well suited communication infrastructure. Mainly, the use of the publish/subscribe paradigm of ICN is capable of supporting communication between the entities in the intelligent network.

In this context, the C-DAX [30] project has a communication platform for a wide range of smart grid applications. C-DAX relies on the properties of ICN to provide network architectures that are more secure, resilient, scalable and flexible than the ones in conventional information systems [31]. C-DAX is tailored to the specific requirements of smart grids for effective support of the massive integration of renewable energy and a heterogeneous set of smart grid applications coexisting with multiple benefits for utilities. Intelligent networks should therefore support dynamic new active components, such as the distribution of energy resources and electric vehicles (EV).

ICNs ability to integrate the smart grid comes from the RP (rendezvous point) approach which is responsible for transmitting data to subscribers, storing and processing them. The management of data distribution in a topic is possible with multiple RP. In this case, each publisher who publishes a topic, always announces its data on one of RP determined by the resolver, while a subscriber can be connected to all or a subset of RP [20]. By focusing on network infrastructure with heterogeneous communication technologies, the use of an ICN-based approach is able to adapt to the available grid capabilities. This allows better selective communication technologies suitable for the specific requirements of the application.

- The results achieved by the researchers in this context showed that ICN was able to address emerging challenges and enable a series of design features such as multi-RP selection and network processing. By focusing on the topological characteristics of a power network in the Netherlands, they proved the ability of an ICN approach to address the above challenges through simulation based experiments.

Today, we find C-DAX to be present in real-world uses cases such as retail energy transactions, pervasive Synchrophasor deployment at MV Level, and RTU/IEDs at distribution substations [30].

Another case integrating ICN in smart grid is home networks. A home network (HOMENET) performs several important functions such as energy management, media sharing, lighting and climate control within a smart grid environment. Thus, there are requirements for security, mobility, and control of network traffic. These problems also belong to the fundamental questions that an IP network should prioritize. The integration of ICN in a HOMENET is justified by the following [32]:

First, ICN is based on a receiver oriented operation that allows HOMENET to provide an access method centered on content. Users in HOMENET focus on the content itself, rather than the location of the content. For example, when a user attempts to obtain a media file in HOMENET, it is not necessary to obtain the physical address of the file. ICN can meet this requirement with its paradigm of data of interest through the appointed route. Migrating from routing centered on the host to content centric routing also facilitates support for mobile clients.

Second, ICN supports caching in the network, which can effectively reduce the response time and the amount of traffic in transit. The data can be cached at each intermediate node from a source to a destination in ICN, so that users can retrieve the nearest router that stored the copied data instead of going back to the source.

- This feature of ICN can help HOMENET to provide better network traffic control capacity. Mobile devices in ICN do not need to recover data when reconnecting to the network, but rather to return the interest and get cached data. Similarly, temporarily disconnected devices can also benefit from caching in the network.

Third, the data security mechanism of ICN can help a HOMENET system to simplify the integration of security mechanisms. HOMENET has strong requirements regarding security, particularly confidentiality and integrity. ICN secures the data itself rather than protecting communication channels. It can help HOMENET to simplify the processing of security by providing confidentiality, integrity and authentication. In addition, the low power operation of ICN as well as the use of a publisher-subscriber oriented group mode is also beneficial for HOMENET.

Fourth, HOMENET has a high mobility requirement in order to ensure seamless media sharing when the user switches to another the network. Thus, ICN can help HOMENET systems to support mobility when devices are changing the home network. ICN focuses on content when customers want to access it regardless of its location. Mobile devices in ICN do not need to recover data when re-connecting to the network instead they re-send the interest and get the data that have been cached in the nearest router to obtain a copy. This fully meets the requirements in HOMENET system, since devices in an Advanced Metering Infrastructure (AMI) may be intermittent only because of their mobility.

Thus, it is clear that ICN meets the requirements of a HOMENET, namely: system security, mobility and a communication-oriented support group. It is therefore well-suited to provide better services for future HOMENET systems.

4.2. Building and Home Automation

In this section we discuss the integration of ICN in smart homes and smart buildings because they are two similar domains. Building smart homes relies on IoT technologies in order to monitor and control houses. Devices such as smart thermostats, sensors, security cameras, wireless light switches, and intelligent door locks have been introduced on the consumer market in the recent years. IoT therefore leads us to build architectures capable of supporting between 50 and 100 million connected objects. This requires several research efforts to obtain a single platform capable of supporting this new concept.

For this reason, the community of network research turned towards the paradigm of ICN as a potential communication solution for smart homes [19][33]. In fact, to provide data ICN uses a routing based on the names and an inherent multicast. Similarly, it allows developers a great flexibility on the name and security. It prevents the dependencies on separate protocols and middleware in different IoT networks. Many researchers studied the emergence of ICN in IoT based smart homes. The requirements that should be respected by ICN for the needs of a smart home are the following:

- ✔ Local and global connectivity: the data produced in the smart home can be used locally and displayed to the owner of the house on an application screen, or it can be processed to initiate actions, such as activating air conditioning if the temperature is higher than a specified threshold.

- ✔ Wireless network: the use of wireless technologies pose new opportunities regarding flexibility. Thus, robust transmission schemes shall be designed if the applications requires reliability.
- ✔ Security: smart home applications usually handle sensitive information, which requires confidentiality, integrity and authentication features. The same data may be requested by various consumers located in different administrative domains; so strong security support is needed to protect information regardless of the transmission channel.
- ✔ Service models: in smart homes, there are two basic service models which are pulling and pushing. A pull service concerns a wide range of (i) control applications, where enforcement action is required, and (ii) monitoring applications where data collection is required. A push service covers unsolicited data transmissions, such as alarm messages, usually in real time.
- ✔ Multi Communications: four possible transmission modes are encountered: (i) one single consumer and source (1C: 1S); (ii) individual consumers and multiple sources (1C: MS); (iii) many consumers and single source (MC: 1S); (iv) many consumers Sources (MC: MS); and a combination of (ii) and (iii).

To answer these challenges, ICN was integrated in smart homes in order to guarantee a more secure and dependable communication. NDOMUS [19] is one of the NDN-based architectures that was proposed in the context of smart homes. The researchers focused on three basic aspects of NDN: the naming scheme, the service model and the strategy for multiparty communications. For naming, two namespaces are identified:

- ❍ Configuration and management namespace: used for initialization of the home network, realization of configuration updates and management operations.
- ❍ Task namespace: used for the identification and activation of all supervision and surveillance operations.

Regarding the service model, smart home applications can be classified into three main categories: pull, periodic push, and event-triggered push. NDOMUS supports three models and provides routines for the retransmission of interests to ensure reliable delivery, as defined by the strategy function. Concerning multiparty communications, NDOMUS offers three modes:

- The multi-source communication (1C: MS) in NDN, which requires the transmission of separate interests to extract data from different producers by only consuming waiting interests.

- Multi-multi-source Consumer scenarios (MCMS) combines the two previous approaches.

In the local area, NDN is applied to the monitoring system which detects the presence of the homeowner back to work and sends a notification of interest to the home server which, in turn, confirms the receipt of the packet. Thus, the Home Server (HS) is programmed to check the status of the temperature in all rooms and adequately adjust the air conditioning. This is achieved on the basis of sensors and the multi-source communication (1C: MS). For example, if the temperature is too high in a room, the startup of air conditioning is initiated to adjust the temperature according to the preferences of the owner.

➩ ICN is an interesting solution for smart home applications. IoT was a popular solution for smart buildings by using IP networks, and several approaches have already been proposed. The intelligent building network has attracted a great attention in the academic community and industry. Like most smart devices, sensors and network devices are connected; a network of intelligent buildings can be very complex [1].

In the intelligent building, the devices have different ways of connecting to the Internet, often with severe resource constraints. The interactions between applications and devices are often real-time and dynamic, with strong security and privacy requirements. To meet these challenges, ICN is proposed in the context of effective services, which are safe and reliable in terms of network for intelligent buildings [34].

In order to take advantage of the benefits of ICN in smart buildings, the researchers proposed to integrate the naming property and embedding a specific naming structure. Regarding routing, ICN combined with smart building offers the following features:

- First, the push content is more important than the pull content in some intelligent building scenarios (e.g. emergency alerts triggered by fire alarm messages). Such content should be disseminated, even if there is no demand. Assuming that some sensors have a lack of storage capacity, data collected by the sensors are sent to the closest router periodically by wired or wireless channels to store them.
- A client uses packets of interest to request the network content. Following the naming scheme, the customer declares the content type in the name of interest. An interest packet is broadcasted to all neighboring routers. Different types of content do not influence the maintenance of the Pending Interest Table (PIT) and the transfer system, so that the architecture is compatible with other information centered architectures.
- To solve the problem of command messages, a new mechanism was also introduced. A control message generated by a control device is considered as a packet of interest. The name of the value is the name of the unit that intends to be controlled.

To better study the feasibility of integrating CCN in the field of smart buildings, several use cases are studied. Moreover, CCN has a better performance than IP based communications. In their future work, the authors propose to integrate other properties such as caching, mobility and security.

4.3. Smart Health

IoT based Health applications can reduce a lot of overhead, while allowing people to access health care services all the time (at any time) and everywhere (anywhere)[18]. However, in such applications where data exchange is based on IP introduces multiple issues regarding security-related vulnerabilities, privacy and mobility. A proposal for the integration of one of ICN based architectures is required, in particular (NDN) which is one of the last and substantial ICN approaches that uses named content to deliver the data. NDN is presented as an architecture supporting users mobility, that is well suited for mobile patients and caregivers. The use of NDN in projects for IoT based health care applications is justified by:

- NDN provides direct access to content using names in a peer-to-peer model rather than a client-server model using IP addressing. Thereby, NDN does not need to translate data names to IP addresses which allows a reduction of system overhead and increases efficiency.
- The content is distributed between the hosts which achieves a load balancing of the charge and the impact of a node failure is reduced.
- NDN supports user mobility, that is well suited for mobile patients and caregivers. NDN also ensures data security instead of the security of the channel [17]. Thus, each data packet is signed by the content provider in order to achieve a better data security.
- NDN enables a better access control by using encryption.

ICN, in particular NDN, presents a favorable environment to support user mobility and data security by using names to identify the content independently of their locations.

4.4. Smart Transport

ITS (intelligent transport system) is considered as one of the basic pillars of a smart city. ITS requires information sharing by all connected devices to provide all services to consumers. However, consumers are interested in small pieces of information, regardless of the location and identity of the suppliers. Generally, most communications take place on the move since consumers are moving when retrieving the required data. Current ITS relies on IP-based architecture as a communication medium between all devices, which cannot effectively deliver mobile content and also introduces several problems such as inefficient IP addresses allocation to mobile devices, intermittent connectivity and evolution of services. In order to overcome these problems, NDN is proposed as an alternative solution[35]. NDN, which is one of the architectures of ICN, is proposed as a potential solution that provides robust, secure, scalable and reliable communications between connected mobile devices. Many researchers have recognized the utility of NDN in several network scenarios ranging from wired networks to wireless ad hoc, sensors, vehicle networks and the Internet of Things (IoT). In [16],the authors have shown the utility of NDN in ITS for smart cities. where they proposed NDN-ITS architecture. The choice of using an NDN in this context is motivated by:

- ➢ The use of a hierarchical naming scheme to route and identify data. Such naming is used to know the traffic conditions as well as related information for a traveler.
- ➢ The caching feature allows each NDN node to serve the provider to effectively distribute device information in intermittent and disjointed network architectures.
- ➢ NDN transfer strategies allow to communicate priority data. Priority depends on the network including the number of satisfied interests, discarded messages, pending interests table size, vehicle speed, neighborhood change rate, and so on. Message transfer based on statistics can reduce message loss and provide timely and reliable information to consumers.

5. Comparaison of IoT-ICN applications

To better detail the role of ICN in IoT applications, we provide Table 1 which presents a comparison of the different characteristics of ICN regarding the studied application domains.

	Naming	Caching	Mobility	Routing	Service model	Security
Smart Grid [24] HOMENET [20] C-DAX [11]		Data can be cached at each intermediate node.	The routing host centric content facilitates support for mobile consumers (HOMENET).	The use of the publish,/subscribe paradigm (Project C-DAX).	-The RPs (rendez-vous point) allow the data to be transmitted to the subscribers and process (Project C-DAX).	Secure the data itself rather than protecting communication channels.
Smart Health [17]	Using the NDN naming convention to locate the healthcare services.		Support end-user mobility (Patient/Caregiver)	For the extensability of the network the NDN Cros algorithm is used.		

	Naming	Caching	Mobility	Routing	Service model	Security
Smart Building[34]	Using a naming strategy.			The use of PIT (Pending Interest Table) permit the aggregation of the requests.		
Smart Home [19]	The use of two namespaces : A name space for management and configuration and another namespace for tasks				- Adopt the Multi-Source communication., -The pull service is supported by NDN.	

	Naming	Caching	Mobility	Routing	Service model	Security
Smart Transport[16]	Use of a specific naming scheme to ask for a road traveler traffic conditions and related information for a traveler.					A security of the contents rather than the connections through the policy of encryption and signature of data.

Table 1: A comparison of IoT application domains regarding ICN features.

6. Conclusion

In this paper we firstly presented an overview of the inherent characteristics of IoT and ICN. Then we reviewed the benefits of using ICN features such as naming, mobility and caching in the context of IoT. Subsequently, we identified the most notable research work that combined IoT and ICN on multiple environments including smart home, smart grid, etc, while focusing on the contribution of ICN in each area. We have to note that Works related to the use of ICN in the context of IoT is not limited to these applications. These works have proposed extensions to improve the performance, the mobility and security of these applications and better exploit the characteristics of ICN. They mainly shown that ICN is a good candidate to replace IP based communications in IoT environments by focusing on the content instead of node identifiers.

More extensive work is still required to improve the coupling of ICN architectures and IoT environments as more connected devices and applications are massively deployed with different properties and requirements, mainly in the context of 5G networks. There is potential that ICN plays an important role in such networks by making easier the coupling of IoT devices with their access network, core networks and cloud computing platforms. However, challenges are still present to make this coupling information centric in a seamless manner while meeting QoS, security and mobility requirements.

References

[1] Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. Mccann, K. Leung, A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities, IEEE Wireless Communications 20 (6) (2013) 91–98.

[2] A. Lindgren, F. B. Abdesslem, B. Ahlgren, O. Schelén, A. Malik, Applicability and tradeoffs of information-centric networking for efficient iot (2015).

[3] A. V. Vasilakos, Z. Li, G. Simon, W. You, Information centric network: Research challenges and opportunities, Journal of Network and Computer Applications 52 (2015) 1–10.

[4] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, R. L. Braynard, Networking named content, in: Proceedings of the 5th international conference on Emerging networking experiments and technologies, ACM, 2009, pp. 1–12.

[5] 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.

[6] S. Sinha, Pursuit, http://www.fp7-pursuit.eu/PursuitWeb, an optional note (2013).

[7] L. Zhang, D. Estrin, J. Burke, V. Jacobson, J. D. Thornton, D. K. Smetters, B. Zhang, G. Tsudik, D. Massey, C. Papadopoulos, et al., Named data networking (ndn) project, Relatório Técnico NDN-0001, Xerox Palo Alto Research Center-PARC.

[8] M. Amadeo, O. Briante, C. Campolo, A. Molinaro, G. Ruggeri, Information-centric networking for m2m communications: Design and deployment, Computer Communications 89 (2016) 105–116.

[9] O. Hahm, E. Baccelli, T. C. Schmidt, M. Wählisch, C. Adjih, A named data network approach to energy efficiency in iot, in: IEEE GLOBECOM Workshop on Named Data Networking for Challenged Communication Environments, 2016.

[10] S. Li, L. Da Xu, S. Zhao, The internet of things: a survey, Information Systems Frontiers 17 (2) (2015) 243–259.

[11] A. Lindgren, F. B. Abdesslem, B. Ahlgren, O. Schelén, A. M. Malik, Design choices for the iot in information-centric networks, in: Consumer Communications & Networking Conference (CCNC), 2016 13th IEEE Annual, IEEE, 2016, pp. 882–888.

[12] M. A. Hail, M. Amadeo, A. Molinaro, S. Fischer, Caching in named data networking for the wireless internet of things, in: Recent Advances in Internet of Things (RIoT), 2015 International Conference on, IEEE, 2015, pp. 1–6.

[13] W. Shang, A. Bannis, T. Liang, Z. Wang, Y. Yu, A. Afanasyev, J. Thompson, J. Burke, B. Zhang, L. Zhang, Named data networking of things, in: Internet-of-Things Design and Implementation (IoTDI), 2016 IEEE First International Conference on, IEEE, 2016, pp. 117–128.

[14] T. Kurita, I. Sato, K. Fukuda, T. Tsuda, An extension of information-centric networking for iot applications, in: Computing, Networking and Communications (ICNC), 2017 International Conference on, IEEE, 2017, pp. 237–243.

[15] E. Baccelli, C. Mehlis, O. Hahm, T. C. Schmidt, M. Wählisch, Information centric networking in the iot: Experiments with ndn in the wild, in: Proceedings of the 1st international conference on Information-centric networking, ACM, 2014, pp. 77–86.

[16] S. H. Bouk, S. H. Ahmed, D. Kim, H. Song, Named-data-networking-based its for smart cities, IEEE Communications Magazine 55 (1) (2017) 105–111.

[17] D. Saxena, V. Raychoudhury, N. SriMahathi, Smarthealth-ndnot: Named data network of things for healthcare services., in: MobileHealth@ MobiHoc, 2015, pp. 45–50.

[18] S. P. Kumar, V. R. R. Samson, U. B. Sai, P. M. Rao, K. K. Eswar, Smart health monitoring system of patient through iot, in: I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2017 International Conference on, IEEE, 2017, pp. 551–556.

[19] M. Amadeo, C. Campolo, A. Iera, A. Molinaro, Information centric networking in iot scenarios: The case of a smart home, in: Communications (ICC), 2015 IEEE International Conference on, IEEE, 2015, pp. 648–653.

[20] K. Katsaros, W. Chai, N. Wang, G. Pavlou, H. Bontius, M. Paolone, Information-centric networking for machine-to-machine data delivery: a case study in smart grid applications, IEEE Network 28 (3) (2014) 58–64.

[21] O. Vermesan, P. Friess, Internet of things-from research and innovation to market deployment, River Publishers Aalborg, 2014.

[22] L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, Computer networks 54 (15) (2010) 2787–2805.

[23] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, G. Marrocco, Rfid technology for iot-based personal healthcare in smart spaces, IEEE Internet of Things Journal 1 (2) (2014) 144–152.

[24] M. Darianian, M. P. Michael, Smart home mobile rfid-based internet-of-things systems and services, in: Advanced Computer Theory and Engineering, 2008. ICACTE'08. International Conference on, IEEE, 2008, pp. 116–120.

[25] M. Zhang, T. Yu, G. F. Zhai, Smart transport system based on the internet of things, in: Applied mechanics and materials, Vol. 48, Trans Tech Publ, 2011, pp. 1073–1076.

[26] K. Smith, S. V. Ravulapati, Y. Daga, D. S. Naga, et al., The internet of things: The personal and social domain, Portuguese Journal of Management Studies 20 (1) (2015) 43–50.

[27] J. Garcia-Luna-Aceves, Adn: An information-centric networking architecture for the internet of things, in: Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, ACM, 2017, pp. 27–36.

[28] S. Wang, J. Bi, J. Wu, A. V. Vasilakos, Cphr: In-network caching for information-centric networking with partitioning and hash-routing, IEEE/ACM Transactions on Networking 24 (5) (2016) 2742–2755.

[29] S. Sicari, A. Rizzardi, L. A. Grieco, A. Coen-Porisini, A secure icn-iot architecture, in: Communications Workshops (ICC Workshops), 2017 IEEE International Conference on, IEEE, 2017, pp. 259–264.

[30] Cyber-secure data and control cloud for power grids, an optional note (2011).

[31] W. K. Chai, K. V. Katsaros, M. Strobbe, P. Romano, C. Ge, C. Develder, G. Pavlou, N. Wang, Enabling smart grid applications with icn, in: Proceedings of the 2nd International Conference on Information-Centric Networking, ACM, 2015, pp. 207–208.

[32] K. Yu, B. Davaasambuu, N. H. Nguyenand, Q. Nguyen, A. Mohammad, T. Sato, Cost-efficient residential energy management scheme for information-centric networking based home network in smart grid.

[33] U. De Silva, A. Lertsinsrubtavee, A. Sathiaseelan, K. Kanchanasut, Named data networking based smart home lighting, in: Proceedings of the 2016 ACM SIGCOMM Conference, ACM, 2016, pp. 573–574.

[34] Y. Jia, B. Lyu, M. Liang, J. Tu, Y. Yang, Context driven content centric networking for smart buildings, in: Fourth International Conference on

Wireless and Optical Communications, International Society for Optics and Photonics, 2016, pp. 99020D–99020D.

[35] Z. Yan, S. Zeadally, Y.-J. Park, A novel vehicular information network architecture based on named data networking (ndn), IEEE Internet of Things Journal 1 (6) (2014) 525–532.