Computer Communications 142–143 (2019) 95–123

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

A survey of Internet of Things communication using ICN: A use case perspective

Boubakr Nour [a], Kashif Sharif [a,*], Fan Li [a,*], Sujit Biswas [a], Hassine Moungla [b,c], Mohsen Guizani [d], Yu Wang [e]

[a] *School of Computer Science, Beijing Institute of Technology, Beijing, China*
[b] *LIPADE, University of Paris Descartes, Sorbonne Paris Cite, Paris, France*
[c] *UMR 5157, CNRS, Institute Mines Telecom, Telecom SudParis, Nano-Innov CEA Saclay, France*
[d] *College of Engineering, Qatar University, Doha, Qatar*
[e] *Department of Computer Science, University of North Carolina at Charlotte, Charlotte, USA*

ARTICLE INFO

Keywords:
Information-centric networking (ICN)
Named-data networking (NDN)
Content-centric networking (CCN)
Internet of things (IoT)

ABSTRACT

Internet of Things (IoT) has gained extensive attention from industry and academia alike in past decade. The connectivity of each and every piece of technology in the environment with Internet, has opened many avenues of research and development. Applications, algorithms, trust models, devices, all have evolved to accommodate the demands of user needs in the most optimal way possible. However, one thing still remains constant: host-centric communication. It is the most predominant way of communication in Internet today. With evolution of everything else, host based communication has been stretched to limits, and exploration of new models have been underway for sometime. Information Centric Networking (ICN) is a major contender for the future Internet architecture, where content is the basic element regardless of its location (host). It intends to offer in-network caching, inherent mobility, multicast support, and content based security as part of design and not add-on functionality. In recent years, numerous efforts have been made to integrate IoT with ICN as the communication model. In this paper, we provide a detailed and systematic review of IoT–ICN research. We investigate ICN as communication enabler for IoT domain specific use cases, and the use of ICN features for the benefit of IoT networks. These include IoT device & content naming, discovery, and caching. We also survey synchronization, interoperability, publish/subscribe communication, quality of service, security, and mobility of IoT devices with ICN perspectives. The paper also presents challenges and possible research directions for the benefit of community.

Contents

[*] Corresponding authors.
E-mail addresses: n.boubakr@bit.edu.cn (B. Nour), kashif@bit.edu.cn (K. Sharif), fli@bit.edu.cn (F. Li), sujitedu@bit.edu.cn (S. Biswas), hassine.moungla@parisdescartes.fr (H. Moungla), mguizani@ieee.org (M. Guizani), yu.wang@uncc.edu (Y. Wang).

https://doi.org/10.1016/j.comcom.2019.05.010
Received 31 October 2018; Received in revised form 13 May 2019; Accepted 15 May 2019
Available online 17 May 2019

1. Introduction

In the coming decade, there will be tens of billions of connected devices such as sensors, smart phones, cars and data centers. Fig. 1 shows the growth projection of devices in use until 2025 globally which will be exponential. These connected devices with sensing and decision making capabilities are usually small in size and potentially mobile. This ecosystem makes up the *Internet of Things* (IoT) [1] that can be deployed with sensing and intelligence capabilities so that they can not only communicate, but also collect data, negotiate, collaborate, and exchange the collected values. On the other hand, the current Internet model was developed many decades ago to allow connectivity between specific end-points or devices. Using unique IP addresses, most of the Internet communication happens between a client and well-known server based on addresses. However, user's needs have since changed, where they are more related to content sharing rather than the connectivity [2]. Peer-to-peer (P2P) model is one example which primarily aims at content sharing and not on connectivity to a specific server. Nonetheless, the communication is still among specific devices sharing the content. Moreover, this device or host-centric model lacks mobility and security as part of its design. Hence, various add-ons and patches have been developed to support them. This makes the model and the system more complex and can impact the communication performance.

IoT addresses a wide range of real life business functions and applications, such as the following. Smart Cities [3]: smart parking systems, traffic monitoring & control, bike sharing, and smart bus, etc. Smart Homes: automated home control devices such as Alexa and Google Home, etc. Smart Grids: distributed renewable energy generation and advanced metering infrastructure, etc. Smart Transportation: including vehicle safety, traffic efficiency, support for autonomous driving [4]. Smart Health: for remote health monitoring and people with disabilities. All of these applications share many common characteristics such as energy efficiency, interactivity, real-time data connection & analyses, and non-intrusive monitoring systems. The main goal of IoT [5] by interconnecting devices, collecting, and processing data is to enable applications, machines, humans, and things to better understand their surrounding environments. This enables services and applications to make intelligent decisions, and to respond to dynamic changes of the environment in order to improve our lives in different aspects such as reduced human efforts, efficient resource utilization, real-time marketing, and data analysis. However, various challenges need to be addressed in this context such as heterogeneous nature

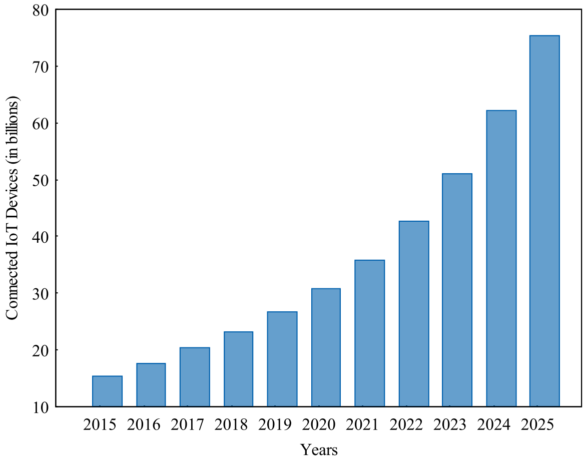


Fig. 1. IoT device connectivity global statistics [7].

of devices and sensors, efficient data retrieval, energy and memory limitations, power consumption, mobility, scalability, security, and dynamic network topology [6].

In light of these changing dynamics, new approaches [8] have been proposed for Internet communication. The objective is to address the challenges and limitations of existing systems at design level. *Information-Centric Networking* (ICN) [9] has been proposed as a new network paradigm for the future Internet. The key element in ICN is the use of data/content name rather than the network address. A content name should be unique, persistent and location-independent. A consumer requests the content by its name instead of the address of the provider. Hence, in-network caching can be applied during the communication by storing the content more closer to consumers to improve data retrieval and reduce network traffic. As content is independent from the location, ICN natively handles the mobility, simply by re-issuing any unsatisfied requests. Furthermore, ICN provides easy data retrieval based on request–reply exchange model, content-based security by attaching all security-related information within the content itself, and a native support of multicast, which can be especially useful in the Internet of Things.

To achieve the goal of ICN, many research projects have been proposed in literature [10] such as Data-Oriented Network (DONA) [11], Publish–Subscribe Internet (PURSUIT) [12], Network of Information (NetInf) [13], Content-Centric Networking (CCN) [14], and Named Data Networking (NDN) [15]. Although these projects have different architectures, they share the same concept which is addressing the content by its name, rather than the network address of hosting device.

On the other hand, most of IoT applications (and their communication) inherently follows content-oriented paradigm [16]. IoT users or things ask for the content and consume the generated data from the network instead of communicating with a specific host or device, such as retrieval of sensed values from a sensor, update mobile application with recently published content (e.g., weather notification), or monitoring the status of patient in their home. In fact, ICN design can facilitate large-scale IoT deployment [17], by improving network performance & scalability, enhance security & mobility, and optimize energy consumption of devices.

1.1. Related literature

A number of publications are available which address ICN and IoT independently. We summarize these efforts below for the benefit of reader. Sheng et al. [5] presented different communication standards by giving an overview of IoT solutions in both industry and academic perspective, highlighting key technical challenges in large-scale IoT networks. While Fuqaha et al. [1] summarized the most relevant protocols and applications that can be used to enable IoT technologies, by discussing relationships between IoT and emerging technologies such as big data analytics, cloud and fog computing. The authors also presented detailed use cases using different protocols and applications in order to provide reliable IoT smart services. A recent study in [18] discussed the IoT from system architecture, technologies, security and privacy viewpoints. The work also presented existing solutions to integrate IoT with fog and edge computing by demonstrating their implementations for real-word IoT applications. It is important to note that all of these solutions are focused only on IoT.

Choi et al. [2] surveyed content naming and name-based routing in Content-Oriented Networking and compared the existing routing protocols and their effects in publish–subscribe communication and the existence of in-network caching. They also discussed technical issues and identified future research challenges in the context of name-based routing. Ahlgren et al. [10] compared different ICN architectures and discussed their components, design choices, and features such as naming, routing, transport, security and caching. In a similar fashion, Bari et al. [19] focused on the naming and routing solutions in ICN architectures, and provided an in-depth comparison and discussion about these two aspects. They discussed these primarily for DONA, PSIRP, and NDN. Vasilakos et al. [20] focused on the existing research progress in ICN, by discussing different ICN aspects such as naming, routing, caching, etc., highlighting the advantages of implementing ICN as future Internet architecture, and providing research challenges and opportunities for both in-network caching and security.

Various other surveys have focused on specific ICN aspects. Tyson et al. [21] provided a short survey on mobility support in ICN, and discussed the advantages of deploying ICN in a mobile environment. The authors explored key challenges that should be addressed (i.e. names, mobility, and security), and provided future research directions. Xylomenos et al. [22] identified the core ICN functionalities and described/compared the existing ICN proposals by highlighting similarities and differences among different networking perspectives. Abdullahi et al. [23] studied in-networking caching in some of ICN architectures (i.e. CCN, DONA, PSIRP, and NetInf). They compared the implementation and deployment of different cache replacement strategies and placement policies in terms of bandwidth consumption and content delivery. Abdallah et al. [24] surveyed different attacks related to ICN architectures. The authors in this survey classified attacks based on ICN aspects such as naming attacks, routing, caching and other. At the end, they provided security requirements to ensure confidentiality, integrity, availability, and privacy. Tourani et al. [25] addressed the security, privacy and access-control issues in ICN, by studying the existing security/privacy mechanisms based on ICN aspects (i.e. naming, caching, etc.), drawbacks, and proposed future research directions.

Focusing on NDN, Saxena et al. [26] provided a comprehensive survey on NDN by making a new taxonomy to facilitate the study, presenting NDN system architecture and working principles, and covering the existing NDN applications. The authors also identified different challenges and issues that should be addressed in NDN. Zhang et al. [27] studied the mobility support in NDN, and classified existing solutions based on their commonalities. The survey also provided key challenges from mobility perspectives and future research directions to provide an effective and efficient mobility support over NDN. Khelifi et al. [28] surveyed the applicability and the feasibility of NDN architecture in vehicular environment only.

There have been two efforts to survey ICN solutions for IoT networks. Amadeo et al. [9] studied the opportunities to deploy ICN for IoT, by mapping IoT challenges with ICN features and how ICN can become a suitable solution for IoT communication. The authors showed a precursory ICN-only design to face some IoT requirements and listed the major challenges toward this goal, without discussing IoT–ICN merger in depth. However, the survey is very limited and only serves as an introduction to the two technology. Work in [29] reviewed existing

ICN solutions that can match with IoT requirements, and provided open research challenges. However, it does not cover works from past few years, or consider IoT application specific ICN solutions.

In addition, an IRTF's Information-Centric Networking Research Group (ICNRG) has many active works (RFC 7927 [30] and RFC 7476 [31]), which discuss the research challenges of ICN, the requirements and challenges for IoT over ICN, and propose design choices toward this goal. However, with the current development in ICN and especially in NDN architecture, newer issues and challenges have emerged.

1.2. Motivation & main contributions

In contrast to the above-listed surveys, this survey focuses on ICN (i.e. NDN and CCN architectures) from IoT applications & use cases perspective, and ICN as a communication enabler for IoT. In comparison to [29], our work provides an extensive and comprehensive up-to-date review of not only IoT–ICN but also NDN/CCN for IoT applications, such as smart cities, smart home, smart healthcare, smart grids, and smart transportation. This work also covers ICN features for IoT including naming and forwarding schemes, caching placement and replacement policies, synchronization, interoperability with IP-based networks, publish–subscribe communication, Quality of Service (QoS) support, security, mobility, and wireless IoT on top of ICN. Finally, we provide issues and open research challenges for the research community to explore.

In this regard, the major contributions are summarized as follows:

- Provide an overview of Internet of Things, communication models, physical layer connectivity, and application requirements.
- Present an in-depth explanation of ICN as well as its different aspects and features.
- Discuss different IoT challenges and how ICN and its implementation can be applied to IoT as a suitable solution.
- Discuss the realization of IoT using ICN as communication enabler in different domain-specific applications.
- Provide a comprehensive survey on ICN solutions for IoT, classified by ICN components and aspects.
- Highlight various research challenges and future directions related to ICN based IoT.

1.3. Organization of the paper

The rest of the paper is structured as shown in Table 1. Section 2 provides literature review about IoT, with a list of challenges faced by IoT realization. Section 3 introduces the ICN paradigm by highlighting its different aspects and components, with an overview of NDN architectures. In section Section 4, we provide a discussion about the mapping of ICN with IoT, and the benefits that can be gained. In section Section 5, we present a review of the available ICN/NDN/CCN solutions for IoT domain-specific applications such as Smart Cities and Smart Homes, Healthcare, Smart Grid, and Smart Transportation. In section Section 6, we discuss ICN issues from IoT perspectives. We present state-of-the-art IoT–ICN aspects, targeting the main ICN elements including content naming, routing and forwarding, caching, synchronization, and interoperability and adoption. Section 7 discusses the existing efforts to enable Publish–Subscribe communication in ICN. While Section 8 presents existing schemes to ensure quality of service in IoT-based ICN networks. Similarly, Section 10 discusses the mobility issues for IoT, and its perspective solutions with ICN. Next, we discuss Wireless IoT from ICN perspective in Section 11. We present open challenges and research directions in section Section 12. Finally, section Section 13 concludes the paper.

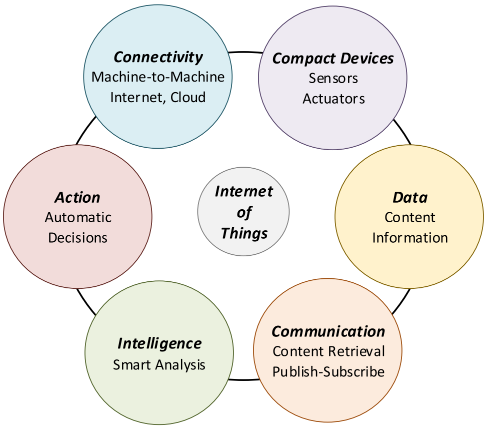


Fig. 2. IoT characteristics & benefits.

2. Internet of Things (IoT)

The basic idea of Internet of Things (IoT) [18] is to connect every object around us with Internet, and enable intelligence feature on it. Thus, various technologies are combined, in order to allow sensors and actuators to sense and collect desirable data, interact and collaborate, provide smart data analytics, and take decisions without human intervention. Fig. 2 represents the main IoT benefits.

2.1. IoT characteristics

IoT is a complex network that represents convergence of many real-world domains, where each domain has its own characteristics. Here we list the major characteristics:

- *Sensing:* The sensing characteristics can be utilized in a vast number of IoT use cases, such as: smart mobile devices, healthcare, industrial control, climate monitoring, etc. Sensors allow measurement, in a context aware manner, of environmental parameters, and enable the device to communicate with the physical world and people around.
- *Connectivity:* Different technologies are used to build connectivity between IoT devices or the Internet, enable service accessibility, global information exchange, and communication among different infrastructures.
- *Intelligence:* IoT devices facilitate the data sensing and collecting. They may also incorporate different algorithms which can enable smart data analysis and take decisions accordingly.
- *Heterogeneity:* Various hardware platforms and operating systems are involved in enabling IoT. This complex ecosystem must allow an interconnection among heterogeneous devices and services in a way to provide seamless data exchange.
- *Dynamic changes:* IoT networks are characterized by the dynamic changes in topology, since they can connect or disconnect according to their battery level or mobility. Moreover, the growing number of IoT devices and their usage makes the network topology more dynamic.
- *Scale:* A tremendous amount of data is generated by a huge number of IoT devices. This makes the network management and data analysis more challenging and requires scalable IoT schemes and solutions.

2.2. IoT stack and operating systems

The Internet of Things covers a large number of industries and use cases scaling from a single constrained device up to big cross-platform deployments of embedded technologies and cloud systems

Table 1
Structure of this article.

Section number	Section title	Description
2	Internet of Things (IoT)	Introduction of IoT. Elaboration of its characteristics, technologies, communication models, and requirements.
3	Information-Centric Networks (ICN)	Introduction to Information Centric paradigm and working principle. Overview of ICN projects and NDN architecture.
4	Why ICN for IoT?	Mapping between IoT applications and Information Centric model. Benefits of deploying ICN as a communication model in IoT. Existing IRTF ICNRG efforts to integrate ICN in IoT.
5	Domain specific IoT–ICN solutions	Review of available solutions for IoT application utilizing ICN communication model.
6	General IoT–ICN issues	Review of solutions which address specific IoT–ICN challenges.
7	Publish–subscribe communication	Review of publish–subscribe communication solutions of IoT.
8	Quality of service	Review of QoS solutions for IoT networks using ICN.
9	IoT security in ICN	Review of security & privacy mechanisms to secure IoT using ICN communication.
10	Mobility in IoT and ICN	Review of ICN mobility solutions in mobile IoT networks.
11	Wireless IoT networks	Review of specific wireless (sensor and IoT) networks using ICN paradigm.
12	What is next?	Open research challenges and issues for different aspects in ICN based IoT environment.
13	Conclusion	Paper conclusion and final remarks regarding IoT–ICN solutions.

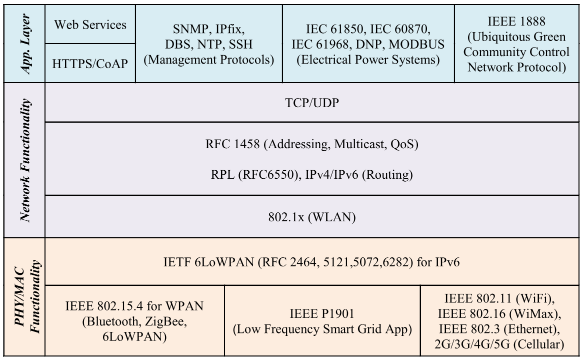

App. Layer
Web Services
HTTPS/CoAP
SNMP, IPfix, DBS, NTP, SSH (Management Protocols)
IEC 61850, IEC 60870, IEC 61968, DNP, MODBUS (Electrical Power Systems)
IEEE 1888 (Ubiquitous Green Community Control Network Protocol)
Network Functionality
TCP/UDP
RFC 1458 (Addressing, Multicast, QoS)
RPL (RFC6550), IPv4/IPv6 (Routing)
802.1x (WLAN)
PHY/MAC Functionality
IETF 6LoWPAN (RFC 2464, 5121,5072,6282) for IPv6
IEEE 802.15.4 for WPAN (Bluetooth, ZigBee, 6LoWPAN)
IEEE P1901 (Low Frequency Smart Grid App)
IEEE 802.11 (WiFi), IEEE 802.16 (WiMax), IEEE 802.3 (Ethernet), 2G/3G/4G/5G (Cellular)

Fig. 3. IoT technology stack and protocols.

interconnected in real-time. The layered IoT stack, shown in Fig. 3, presents the standards, technologies, and protocols used in such systems. Application layer specifies all the shared communication protocols and interface medium used by IoT devices. Network layer specifies communication path over the network (IP address). Physical/Media Access Control (PHY/MAC) layer specifies communication path between adjacent nodes and data transfer.

On the other hand, several operating systems (OS) have been designed to enable smart IoT services on resource-constrained devices [32], which can work with low processing, memory, size, and power capabilities. IoT device operating systems are mostly embedded OS, which enable data collection and communication over the Internet.

Tiny OS [33]: is a flexible, application-specific open source operating system designed specifically for low-power wireless devices, e.g., sensor networks, ubiquitous computing, personal area networks, smart buildings, and smart meters. It can run efficiently in low memory requirements with low-power operation. Tiny OS has three computational abstractions: commands, events, and tasks. Commands and events are tools for inter-component communication, while tasks are used to display intra-component concurrency.

Contiki [34]: is an open source, lightweight, and highly portable operating system with an event-driven kernel that supports multitasking. Contiki has been designed for memory-efficient networked embedded systems, and wireless sensor networks constrained in processing, memory, power, and communication bandwidth. Contiki provides three network stacks: uIP TCP/IP stack for IPv4 networking, uIPv6 stack for IPv6, and Rime stack for low-power wireless networks.

RIOT [35]: also referred to as Linux of the Internet of Things, is an open-source operating system that enables developers to write IoT applications using C and C++ programming languages, supports multi-threading, modularity, uniform API access, and real-time capabilities. RIOT OS is a microkernel-based operating system, that takes minimal resources into consideration such as energy-efficiency and small memory.

Ubuntu Core [36]: is a tiny and lightweight version of Ubuntu OS, designed specifically for IoT devices and large-scale deployments. Ubuntu Core uses the same Ubuntu kernel to enable secure application development and deployment in a friendly way. It can be run on a broad array of computationally constrained devices.

2.3. IoT physical layer technologies

Various applications fall under the umbrella of IoT, that use different technologies as the main communication enabler [5,37]. The most commonly used physical layer technologies, as shown in Fig. 3, are:

ZigBee (IEEE 802.15.4) [38]: Specifies the physical layer and media access control for low-rate wireless personal area networks. It has been designed to run on low-power devices enabling machine-to-machine (M2M) communication. It provides low-power consumption and low duty cycle to maximize battery life. ZigBee can also be used in mesh networks, and supports a large number of devices over long distances with many different topologies, connected all together through multiple pathways.

WiFi (IEEE 802.11) [39]: Allows local communication between two or more devices using radio waves, it is the most used technology to connect the Internet gateway to devices. WiFi utilizes both 2.4 GHz UHF and 5 GHz SHF ISM radio bands. WiFi networks operate in the unlicensed 2.4 radio bands, where the access point and the mobile stations share the same channel and communicate in half duplex mode.

Bluetooth & Bluetooth Low Energy (IEEE 802.15.1) [40]: Are used to transfer data over short distances using 2.4 GHz ISM band and frequency hopping, and up to 3 Mbps data rate with 100 m as maximum range. The technology is mostly used to connect user phones and small devices with each other.

6LoWPAN [41]: 6LowPAN is a networking technology that combined the Internet Protocol (IPv6) with Low-power Wireless Personal Area Networks (LoWPAN), which is one of the most suitable technology for IoT deployment. It is a good choice for the smaller devices that are limited in processing and transmission capabilities.

5G [42]: The fifth-generation wireless is the newest iteration of cellular technology that is based on the IEEE 802.11ac wireless networking standard in order to improve data rate and reduce latency. Both Long-Term Evolution (LTE) and Multiple-Input Multiple-Output (MIMO) are used as a foundation in 5G network, as well as network slicing.

2.4. IoT communication models

IoT devices aim to cooperate, exchange, and process data between each other. They are able to communicate with their domain gateway, or with the Internet. Hence, we can broadly classify IoT communication models into the following classes:

Device-to-Device Communication Model: Two or more Wireless IoT devices may directly connect and communicate with each other instead of going through an intermediate service (e.g., smart watch communicates directly with mobile phone). Different protocols can be used for device-to-device (D2D) communication such as Bluetooth and ZigBee.

Device-to-Gateway Communication Model: This model is also known as Device-to-Application-Layer Model, where a wireless IoT device connects with an associated service or gateway that acts as a go-between IoT network and Internet, to access the Internet or Cloud services. For example, a local home gateway connects with various smart home sensors, and allows user's access to these sensors through a smartphone application via Internet/Cloud.

Device-to-Internet Communication Model: In this model, Wireless IoT devices can directly connect to an Internet cloud service (e.g., Application Service Provider) to exchange data and receive control messages. Users through the cloud service, are able to obtain remote access to sensor devices using smart phone applications. For example, they may monitor their Smart TV for shows, and take control over certain channels. Users may also export their desirable data from cloud services, merge data source for aggregation purposes and deep analysis, for example analyzing the home energy consumption.

2.5. IoT application requirements

Despite the fact that IoT has been integrated into most of the environments, various challenges need to be addressed. Below, we outline the most critical challenges in IoT-based applications.

- *Addressing:* Billions of IoT devices can interconnect and collaborate for different tasks, create, and exchange content between each other. Each IoT device should have a unique and persistent address. Furthermore, users and sensors are more concerned about the created content, and less about the address of sensors. Hence, addressing the content is as important as addressing the devices in IoT context. A large space IoT addressing scheme is required with less processing, a simple header, and persistent abilities during the whole content lifetime and mobility across different networks. Moreover, IoT addresses should be secure and related to the application semantic to resist against different application and network layer attacks.
- *Heterogeneity:* The heterogeneous nature of IoT devices and the deployed architectures and technologies, require various middlewares to collaborate and share the content between devices and across IoT networks. The existence of these middlewares makes the communication complex and prone to performance issues, where establishing secure data sharing becomes a complicated task. Therefore, designing a clean Internet architecture that processes the content regardless of the nature of the hosting device or the requesting application may overcome the heterogeneity issue.
- *Security & Privacy:* Most of the data is generated and collected by IoT devices and analyzed for monitoring purposes and decisions. Thus, the network layer should treat the content by its name rather than its network address or the availability of the original producer. Also, the content may face different attacks and privacy issues during the generation (application layer perspective) and transmission (communication layer perspective). Therefore, IoT-based smart applications must adopt serious security mechanisms to ensure the data security, privacy, access control, reliability, and confidentiality, regardless of the type of channel used. Hence, keeping this data safe and reducing the risk, requires developing different trust models among content providers and consumers that work with different application requirements. Mainly, all IoT-based applications should treat security and privacy as a top priority.
- *Mobility:* IoT-based applications may cause some reliability issues, due to the patient mobility in healthcare systems, or vehicle mobility in smart transportation systems. Providing anytime anywhere connectivity, and content availability in IoT requires serious design choices especially in a highly dynamic mobile environment. Hence, seamless mobility support in IoT is needed to provide fast data retrieval in a reliable and secure manner.
- *Network Scalability:* Millions of distributed IoT devices generate a large amount of data, analyze, and transfer it with each other or with the Internet service. Also, new devices may connect to the network, disconnect, or move from one network to another, e.g., a dynamic connection/disconnection of sensors in healthcare environment, or dynamic mobility for vehicles in smart transportation systems. This has major impact on the communication reliability and quality of services. Hence, ensuring a scalable IoT network is an important aspect for the IoT ecosystem that may handle the computation of data and communication of device.
- *Resource Constraints:* Most of IoT devices are considered as resource-constrained with limitations in power, memory, computing capabilities, and bandwidth. Providing IoT applications that deal with these constraints is required to satisfy the user experiences and provide a continuous service availability during high mobility and network outage.

3. Information-Centric Networks (ICN)

Information-Centric Networking [22] has been proposed as a new architecture for the future Internet, addressing many issues in the current IP-based networks, such as routing process, scalability issue, and content sharing performance [43]. ICN integrates all network functionalities around the name of content rather than the address of the network, in a way to ensure efficient data dissemination and access.

Formerly, different concepts such as P2P and CDN (Content Distribution Network) have been developed to improve the content sharing and distribution in the Internet [44]. However, ICN in contrast to P2P and CDN, is a standardized protocol that works at the network layer. P2P is an application-specific protocol, whereas CDN is a proprietary solution working at the application layer. Moreover, P2P content is delivered from end-users, while in CDN proprietary infrastructure is used. However, in ICN content can be delivered from the network infrastructure itself.

This redesign from "*where* the content is located" to "*what* is the content" will improve the network performance, facilitate the content retrieval and replication using in-network content caching, and support native multicast delivery & mobility.

Fig. 4 illustrates the difference between IP and ICN communication. Content retrieval is shown in red and blue color respectively. Assuming that all consumers are requesting the same content D provided by the producer, IP-based communication requires that each consumer (consumer 1 and 2) individually knows the address of the content producer, and then independently fetches the content through an IP routed path. However, in ICN-based communication the consumers should specify only the requested content name (without knowing the host IP). The request is forwarded based on name-based routing rules until it reaches a device which has the content. In Fig. 4 consumer 3's demand is satisfied by the producer (first demand), during which router (e.g., R3) can cache the content. When consumer 4 requests the same content, the request is satisfied by the cache store at R3, thus eliminating the need to reach the original producer.

Many research works have focused on different ICN functionalities such as naming, in-network caching, mobility, and security. In the following sub-sections, we highlight the key features of ICN, and the historical evolution to its current state.

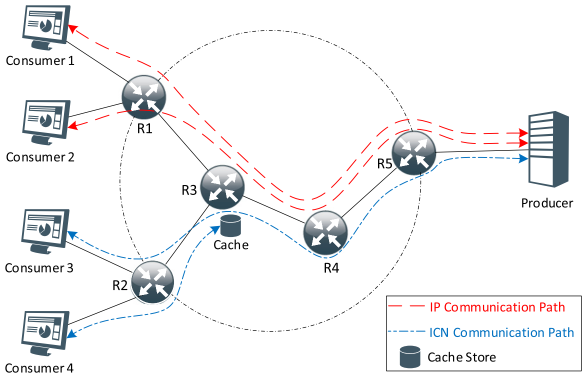


Fig. 4. Content retrieval: IP-based vs. ICN-based networks. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

3.1. *ICN features*

ICN promises to replace the current host-centric communication model by leveraging the content name as the key network elements.

3.1.1. *Content naming*

The content name [19] is the key element in ICN, which uniquely identifies the content itself. It should be compact, persistent, and be able to validate the content. The used naming scheme must be scalable and should allow name aggregation. Four main types of naming schemes have been proposed in ICN.

- *Hierarchical Names:* They consist of multiple components [45] to identify the content and describe the application/services. It has a similar structure to current *Uniform Resource Identifiers* (URIs) and can create user-friendly and meaningful names for users. Hierarchical naming enhances the scalability since name prefixes can be aggregated, but may also be lengthy.
- *Flat Names:* They are typically obtained through hash algorithms applied to content [46]. There is no structure to the name. Hence it is not human-friendly and can hardly be assigned to dynamic content that is not published yet. Flat naming has scalability issues since it does not support routing aggregation.
- *Attribute-Value based Names:* Attribute-value based naming scheme [47] has a collection of attributes, where each attribute has a name, a type, and a set of possible values (creation date/time, content type, location, version, etc.). Collectively, they represent a single content and its properties. This naming scheme supports an easy searching process by using known content keywords. However, it is hard to ensure naming uniqueness, as many unique contents may have the same properties.
- *Hybrid Names:* A hybrid naming scheme [48] combines at least two of the previously discussed schemes or all of them. It attempts to use the best features provided by the base scheme to improve the network scalability & performance, and enhance the security & privacy. For example, taking advantage of name aggregation to enhance the lookup process, fixed length of flat names to save space, and attribute values to provide keyword searching and security/privacy.

Moreover, ICN can use Name Resolution System (NRS) instead of providing hop-by-hop name-based routing. The interest packet is forwarded to NRS server to provide a resolution of the requested name and forward the request to content provider/producer.

3.1.2. *Routing and forwarding*

The use of names to identify the content introduces name-based routing [19] to discover and deliver the content to the requester. Due to the receiver-driven design, a consumer triggers a request asking for content by specifying its name. The discovery process starts searching for the content based only on name. The request is forwarded hop-by-hop using forwarding/routing table until it reaches the original or a replica node that has the requested content, after which the content is delivered to the requester.

3.1.3. *In-network caching*

As the content names are location-independent and each data packet is self-consistent, in-network caching [23] can be applied during ICN communication. Each ICN node can cache the content, and serve it for future requests, as shown in Fig. 4. Caching improves the network performance by reducing the delay and facilitates content retrieval.

However, deciding what kind of content should be cached in ICN involves treating content based on various metrics including popularity and freshness. Hence, studying the network topology with analysis on consumer traffic demands is required, while taking into consideration device capabilities such as the cache memory and processing. In addition, removing old cached content and replacing it with new content introduces the need for replacement algorithms and strategies to keep the most used content with less changes in the cache store [49–51].

3.1.4. *Content-based security*

ICN emphasis content-based security [52], where security mechanisms are applied to content itself rather than the communication process. Different trust models have been developed based on network services. Also, each data packet is self-authenticating based on the original contents security-related information (e.g., the publisher public/secret keys and signature) [53–55].

3.1.5. *Mobility*

From ICN perspective [21], the content is independent from its original location, and only the desirable content name is used to discover and forward it back to the consumer. When a node moves from a network to another, it can re-issue any unsatisfied requests, and the producer replies with the requested data without any need to request a new address during the movement.

Due to the variety of features offered by the native ICN paradigm to solve the complex Internet design and functionalities, the research community has started developing and implementing different architectures using the ICN perspective. In the following, we present an overview of such architectures.

3.2. *Overview of ICN proposed architectures*

In the following, we review some representative ICN architectures including Data-Oriented Network (DONA) [11], Scalable and Adaptive Internet Solutions (4WARD/SAIL) [56] [57], Publish–Subscribe Internet Routing Paradigm (PSIRP/PURSUIT) [12], Content-Centric Networking (CCN) [14], COMET [58], CONVERGENCE [59], Mobility-First [60], and Named Data Networking (NDN) [61]. In this work, we mostly focus on research relevant to CCN & NDN, as they have received more attention from the research community in the past, and continue to be favored as architectures of choice. Fig. 5 summaries these ICN projects, funding, life-time, and different components such as naming, routing/forwarding, and working concept.

3.2.1. *Data-oriented network architecture*

It is one of the first ICN architectures, and uses persistent flat names to identify information objects. In particular, names are in the form $P : L$, where P is the ciphered hash of the public key of the content owner, and L uniquely identifies one of the contents with respect to the same owner. The content publisher uses a cryptographic hash as an object identifier, where subscribers can verify the content integrity easily by hashing it and comparing the results.

3.2.2. Scalable and adaptive internet solutions

SAIL and its predecessor 4WARD (Architecture and Design for the Future Internet) [56,57], is a general architecture because it inherits aspects both from PURSUIT and from NDN. SAIL uses self-certifying flat names with possible explicit aggregation in the form $ni : //A/L$, where A is the authority part, and L is the local part with respect to the authority, each part can by any type of string, from an URL to a hash value.

3.2.3. Publish–subscribe internet technology

This project is based on its predecessor Publish–Subscribe Internet Routing Paradigm (PSIRP) [12]. It adopts a complete clean-state approach in designing its ICN architecture, by using publish/subscribe stack instead of IP protocol stack. It uses self-certifying flat names consisting of scope and rendezvous parts (scopes organized hierarchically).

3.2.4. Convergence

This solution inherits a number of features from the NDN architecture. Names can be self-certifying & flat in the form $namespaceID : name$, resembling the $P : L$ pair of DONA, or they can be hierarchical as in NDN.

3.2.5. MobilityFirst

This project mainly focuses on the mobility issue. The naming scheme adopted is self-certifying & flat which has a global unique identification (GUID). The GUID is detached with its location, i.e. IP address for URI. Although GUID and network address are separated from each other, the MobilityFirst architecture still maintains a mapping between the two, therefore it implements two routing schemes, GUID and network address based.

3.2.6. Named data networking & content centric networking

Currently, NDN [61] is one of the most active architectures in ICN research that has been forked from CCN architecture in 2010. NDN uses two types of packets: interest and data. Both interest and data packets carry the name of the requested content. NDN is a named-based network where the routing is achieved by using names. NDN uses hierarchical, human-readable, and structured URL-like names. Moreover, NDN maintains three data structures: Cache Store (CS), Pending Interest Table (PIT), and Forwarding Information Base (FIB).

Fig. 6 shows interest and data forwarding planes in NDN. When an NDN node receives an interest packet, it checks in its local CS. If the requested data already exists in the cache, it means this node is a replica node. In such case a data packet will be sent using the same face where the interest has been received. Otherwise, it will check in PIT if a match for similar request has already been forwarded upstream. In this case, NDN will append the face where the interest has been received to the PIT entry (interest aggregation), otherwise, a new PIT entry will be created that has the name of the requested content and the name of the face. Then it checks FIB to find the next hop toward the content provider.

In reverse path, when an NDN node receives a data packet, it checks its PIT. If no match is found, which means there is no request that has been sent before, the node discards the data packet by considering it as an unsolicited packet. Otherwise, it will forward the data packet to all the faces saved in the PIT table. At the same time, based on cache policy, the nodes along data path may cache content.

4. Why ICN for IoT?

The information produced by IoT smart devices can be regarded as content [62]. Consumers in the network request data in IoT context without the need to know the location of the sensors or the actuators. There is no end-to-end session requirement for content retrieval, and ICN targets the content in the network by its name rather than its address. For example, asking for humidity value for a specific place, or query some information, or data monitoring.

ICN nodes can act as replica-nodes by using content stores. Content can be cached and served for future requests regardless of the original producer's reachability. This caching improves the data retrieval, and reduces the latency. In such scenarios, ICN is more suitable for IoT than IP [63], not only for the rapid content delivery, but also for its receive-driven design and request aggregation. Moreover, multicast and mobility support of ICN is an additive point, where multicast can be done from the network layer, and any unsatisfied requests during mobility can be re-issued without the need for complex handover solutions like those of IP. Furthermore, by using global unique names, ICN provides content-based security and encryption, and ensures content integrity and authenticity, as part of its design.

IoT can be combined with different daily user routines, by enabling seamless integration and interaction with applications, sensors, and actuators. Daily personal monitoring, industrial processes control are some real examples of IoT applications. By using content-based naming and Name Resolution System (NRS), the addressing issue in IoT can be solved. This will also help in removing any restriction on the type of content and the nature of producer device [64]. Moreover, decoupling the content from its original location, and using the name as the main element to identify the content, the heterogeneous nature of IoT sensors becomes irrelevant [65].

From security perspective, securing the communication channel in ICN is not required as the latter follows a content-based mechanism by encrypting the content itself and applying different trust models in the application layer. Furthermore, since IoT devices are resource-constrained, in-network caching, forwarding strategies, caching placement/replacement policies, interest aggregation, and session-less concepts improve the energy efficiency and reduce power consumptions.

Overall, all these features contribute to make ICN an efficient alternative solution for IoT in terms of scalability and reliability [66].

4.1. IETF efforts

Currently, various drafts from IRTF ICNRG research group are focusing on IoT–ICN. Work in [67] identifies the requirements to develop a unified IoT architecture that addresses IoT traffic, mobility, and management issues. Also, it elaborates the benefits of using ICN on top of IoT (i.e. naming, security, and caching) and lists major ICN challenges (i.e. standard naming, scalability, caching & storage, etc.), by discussing the current IP-based IoT solutions and how to overcome the different disadvantages in order to build a suitable IoT–ICN framework. [68] describes the potential modifications of ICN and more specifically CCN architecture, and different design choices that should be taken into consideration in order to integrate ICN in IoT. These include an appropriate naming scheme for IoT content, immutable data by leveraging meta-data files decoupling the consumers from the content publisher, and combining Pull and Push-based traffic with the ICN communication model using name-based routing. The modification should consequently improve the efficiency and scalability of the overall IoT network and its applications by using a simple communication model with less processing overhead.

A recent draft [69] discusses the motivation and the needs of IoT–ICN architecture to connect heterogeneous IoT devices. The work proposes an IoT–ICN architecture combined with a middle-ware. It has various functionalities to ensure device onboarding and discovery, naming service, services discovery, and publish–subscribe management. Also, co-existence with heterogeneous networks such IP-based has been discussed by using name-to-name primitives and introducing a named protocol bridge to forward the message through different core networks.

Broadly speaking, ICN opens new opportunities to implement a native content-oriented view of IoT [70]. However, most of the current proposed ICN solutions and architectures did not take IoT principles in their design [71]. Thus, enabling ICN in IoT environments needs a careful design of different IoT network components, applications and services [72].

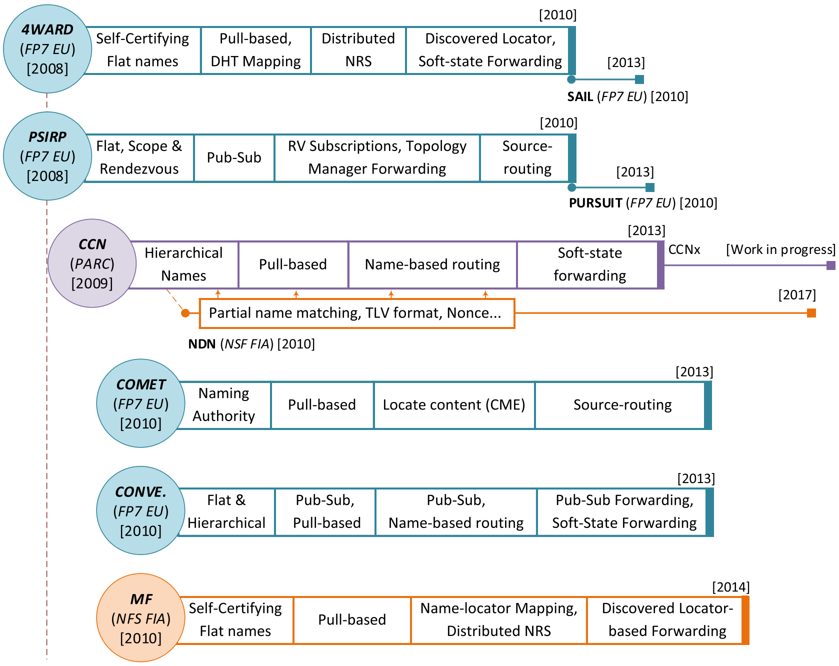
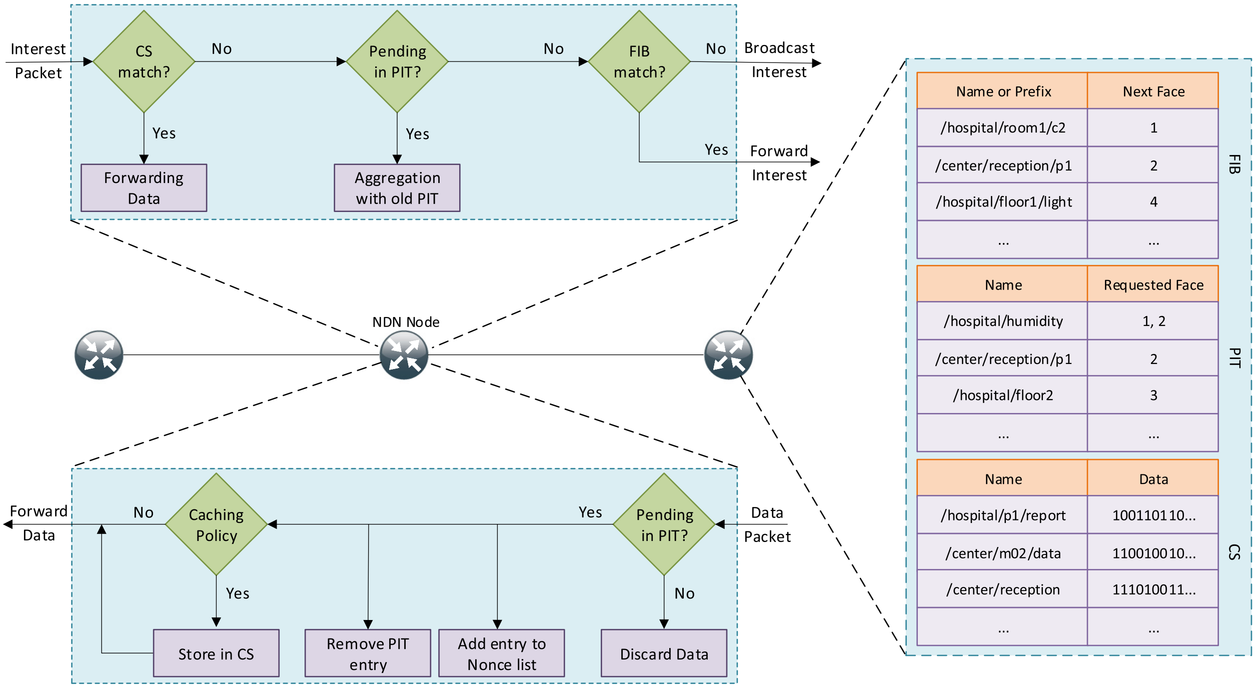


Fig. 5. ICN projects time line overview.



Name or Prefix	Next Face
/hospital/room1/c2	1
/center/reception/p1	2
/hospital/floor1/light	4
...	...

Name	Requested Face
/hospital/humidity	1, 2
/center/reception/p1	2
/hospital/floor2	3
...	...

Name	Data
/hospital/p1/report	100110110...
/center/m02/data	110010010...
/center/reception	111010011...
...	...

Fig. 6. NDN operational logic and table structure.

5. Domain specific IoT-ICN solutions

Internet of Things is involved in different applications. These domain-specific use cases have a common vision, but still, have different characteristics. In order to reap the benefits of merged IoT–ICN technology, it is important to address these characteristics of domain-specific applications. In the following, we present a review of different IoT applications using ICN as their communication model. Table 2 summaries the ICN proposed solutions in IoT domain-specific applications.

5.1. Smart city systems

Smart Cities [94] comprise of many interconnected ubiquitous services. Sensor and IoT networks are used to improve citizens' quality of life, and support other systems such as remote power usage monitoring, integrated parking and security services, etc. In fact, smart cities face all the challenges discussed earlier in section Section 2.5, as it includes smart homes, smart parking, weather systems, vehicular traffic, surveillance systems, smart energy, and smart grids. Providing a large naming space with interoperability between different ecosystems, devices, protocols and applications, and high security and privacy schemes are indispensable in such environments.

Table 2
ICN solutions for IoT domain specific use cases.

Scope	Ref.	ICN area	Summary	Year
Smart cities	[73]	Communication model, Naming, Content discovery, Service management, Security	NDN-based IoT platform for smart cities to ensure secure and reliable smart services.	2014
	[74]	Research directions	The feasibility of brining NDN into smart cities and future NDN requirements in this context.	2017
	[75]	Naming	A naming scheme which utilizes deep learning to predict the used name components in a weather monitoring system.	2017
	[76]	Content caching	A periodic caching scheme to enhance content delivery in smart cities.	2018
Smart homes	[77]	Naming, Discovery and service management	A proof of concept for ICN-based home network and compared it with IPv6-based IETF proposal.	2013
	[78]	Security	An NDN-based security architecture for light control scenario in Building Automation Systems.	2013
	[79]	Naming, Communication Model and Strategies	Adapting NDN for smart homes to identify different services and tasks, and satisfy communication and services requirements.	2015
Smart healthcare	[80]	Naming, service	Benefits of NDN naming and clean design to improve the IoT-AAL performance.	2015
	[81]	Naming, Security	Design and implementation for a distributed mobile health based on NDN.	2016
	[82]	Naming, Mobility, Publish–Subscribe	Distributed architecture for AAL that support mobility, management and publish–subscribe communications.	2017
	[83]	Forwarding, Publish–Subscribe	Design and verification of NDN-based smart health using M2M and publish/subscribe paradigm.	2017
Smart grid	[84]	Security, Publish–subscribe	Secure group communication in home energy management systems.	2012
	[85]	M2M communication	Smart grid machine-to-machine communication challenges.	2014
	[86]	Challenges	Challenges and requirements to achieve a secure ICN communication in smart grid environment.	2016
Smart transportation systems	[87]	Challenges & Research directions	Study the applicability of ICN in vehicular networks by showing the opportunities of ICN to address the current challenges.	2016
	[88]	Security	Different security challenges and attacks when applying NDN in vehicular environment.	2016
	[89]	Naming, Forwarding	Implementation and study of the performance of various IP-based forwarding schemes on top of NDN in real vehicular testbed.	2017
	[90,91]	Security	NDN-based scheme for anonymous authentication and pseudonym-renewal scheme in VANET by using Certificate Issuing Proxy and pseudonyms vehicle names.	2017
	[92]	Research directions, Architecture	Discuss ITS requirements and challenges and provide a unified NDN-based architecture to address different issues.	2017
	[93]	Security	A study on security and attacks in vehicular cyber–physical systems running on top of NDN.	2018

ICN use case scenario: A huge amount of distributed devices are used in smart cities, including houses, vehicles, buildings, and public environments, as well as a massive number of services and applications. IoT-based smart cities aim to enhance citizens' services. For example, finding an available parking spot gets harder due to the growing number of cars, and the limitation of parking spaces. Today's smart parking may use different IoT sensors to detect the availability of free space and facilitate parking asset management. Vehicles willing to get into the parking can subscribe for Parking Services, whenever a new space is available, all vehicles get notifications according to their GPS position. In such a scenario, a *content-oriented paradigm* is the perfect communication model, where subscribers are interested only in the data they need (e.g., available spot). Moreover, video surveillance solutions can be integrated to facilitate the public parking management. Another scenario, where distributed sensors are implemented in different city locations to monitor the pollution levels. People may get notifications and warnings about pollution levels over time, and at different locations in real-time. These services can be integrated with deep learning modules to predict situations in users' workplaces, schools, and open public spaces.

Current ICN efforts: Piro et al. [73] proposed an ICN-based platform for smart cities on top of NDN to take advantages of content-centric features. Secure communication model based on discovery and content delivery have been discussed. In the first phase, a consumer should find the content provider through service discovery, establish a secure communication channel by including both consumer name, and provide name in the interest name field. Different use cases have been illustrated where hierarchical naming schemes have been used. The use of hierarchical naming is motivated by its efficiency to support various kinds of services used in smart cities, with simple routing operations and aggregation capabilities. The major limitation of this solution, is the use of both consumer and provider names in the content name, that takes the ICN paradigm back to the host-centric model. Moreover, it uses long names which translate to larger overhead in the lookup processing. Further, this method ignores the use of in-network caching. Ahmed et al. [74] discussed the feasibility of bringing NDN into smart cities. They have presented different concepts and scenarios that contribute to smart cities such as wireless sensor networks, smart grids, and vehicular networks where NDN can fit well. The authors also discussed different NDN aspects for future smart cities such as content naming, data exchange and forwarding process, and content discovery. Mochida et al. [75] presented the case of a weather monitoring system in a smart city, where a network of weather sensors and cameras generates large volume of content. The authors used deep learning approaches to predict the components of the used naming scheme for such data. Although the scheme is shown to be very useful in generating names specific to the context of content, it tends to generate lengthy names. This may create overhead for resource constrained IoT devices. Naeem et al. [76] aimed at improving content delivery with reduced latency and producer load, by distributed content caching. The distributed nature of caches across the city may allow a higher number of connected devices and satisfy their demands with better service quality.

Due to lack of complete solutions in this domain, integrating ICN in smart cities requires more investigation. Flexible trust models are required to address secure data dissemination and data privacy. Also, developing smart caching schemes to decide where content should be cached at a city-wide scale is needed.

5.2. Smart home systems

Smart Home services [95] are used to enhance personal lifestyle, and make it easier and simpler. These include smart home security systems, fire detection, lighting control, and temperature monitoring, etc. Moreover, these services may also provide home appliances remote monitoring systems, by collecting the environment conditions and send the collected data to home controllers, which provides continuous monitoring and best control actions.

ICN use case scenario: Nowadays, various home control gateways and solutions are available. These solutions may provide complete control of the home automation, i.e. switching on the lights automatically when someone enters the room, or off when someone leaves it, intelligent face recognition at the home entrance, and managing heating systems by tracking data from outdoor and indoor temperature. All of these features and others enhance quality of life & improves home energy efficiency. From both communication and application perspective, there is no need to know the address of the hosted sensors or the service. All what is required is information about the service. Furthermore, it is more feasible to apply access control mechanism and authorization based on the content name regardless of the physical position. Hence, leveraging ICN as a communication model may help their fast deployment and management.

However, various challenges can be found in smart home applications including:

- Smart home systems must take decisions on how to collect data, transmit it among different IoT devices, control it and take decisions based on context.
- Home heterogeneous devices need to operate and adapt to conventional naming between different offered data and services, with high trust strategies and control among them.
- Handle movement and mobility of sensors, data producers and consumers.
- Accommodate guest and untrusted devices, by controlling user permissions and shared data privacy.

Current ICN efforts: Ravindran et al. [77] compared the IPv6 IETF proposal for home networks with ICN-based approach from different perspectives such as service, control, and data plane as well as complexity. The authors discussed various challenges faced for such implementation and how to use ICN features to realize a unified IoT–ICN platform that is able to handle the heterogeneity of IoT devices, services and user needs by using ICN naming scheme and in-network caching for content distribution and native support of mobility. Only by using names, the authors proposed a service discovery protocol and content-based policy on top of ICN to enable user interaction with devices in infrastructure or non-infrastructure mode. Burke et al. [78] addressed the security in lighting control for Building Automation Systems (BAS). The authors identified the security requirements and built an NDN-based security architecture by combining a trust model with key attributes and access-control policies just by using the name of content. The application creates and signs the desired commands that are described using names. The sensor checks the command signature, executes it, and replies with a data packet as execution acknowledgment. Amadeo et al. [79] proposed a tailored ICN framework for smart homes, by using hierarchical naming scheme to identify various services and tasks. They have modeled different services for push and pull-based traffic by unsolicited data packets. However, this violates the primitives of interest-response mechanism. Also, a multi-party forwarding strategy has been used to allow data retrieval from multiple producers in home environment based on sharing of a common name prefix among consumers.

Although the previous works are focusing on the integration of ICN in smart homes, more efforts are needed to provide a scalable publish–subscribe communication model in ICN. The use of unsolicited data violates the interest-data exchange model, while persistent interest is not sufficient to handle the growing number of subscribers. Also, providing secure data sharing on top of such models is indispensable to allow only the legitimate subscribers to consume the data. Moreover, as smart homes are directly connected to people, privacy of user needs to be addressed as a primary objective.

5.3. Smart healthcare systems

Smart Healthcare [96] represents one of the most attractive IoT application, due to its potential for remote diagnostics and examinations, patient tracking and monitoring, and treatment and surgery. Several technologies are used in IoT-based healthcare environments, such as sensors and actuators, heterogeneous wireless networks, medical applications, portable/wearable devices, and personal computers. Medical sensors are able to collect data from physiological signals (e.g., electrocardiogram and electromyogram, heart rate, and oxygen consumption) or data reflecting the body movements (e.g., accelerometer). Personal mobile devices, such as smart phones are also used as motion and location sensors (e.g., accelerometer and GPS). Moreover, many environmental sensors can be used to determine if the environmental conditions are fit for patient's health (e.g., temperature, light, humidity, and carbon dioxide levels).

ICN use case scenario: Deploying different health sensors on patient's body and surrounding is one promising solution to facilitate healthcare services, where patients are not required to stay in the hospital. Doctors and nurses may keep monitoring the patients situation based on the collected data from attached on-body and environmental sensors just by specifying the patient name and/or the target sensor/service. Also, when a patient comes to a hospital, it will recognize him automatically, hence all its reports and available data will be loaded and synchronized with medical professionals. Further, third party member such as family members and assurance companies may have the ability to keep monitoring the patients health based on their permission levels. These reports and information can be cached at any network level (home's access point, hospital database, clinical access point, etc.) to facilitate its distribution and increase its availability. Also, data and report sharing among different entities can be done using the name of patient or information that will enhance its access and distribution. Finally, all security and access control rules may be deployed based on the name of users, which is much easier and efficient than using the address of the host node/sensor.

Different challenges face smart healthcare systems, including:

- Health applications must provide real-time data, and reliable communication with no network failures.
- Due to the heterogeneity if sensors, protocols, and applications, interoperability among them is required to provide highly sophisticated health-care systems.
- Be resilient against different network and application attacks, securely transmitted users data, and preserve privacy during the processing between different health-care entities.

Current ICN efforts: Hail et al. [80] proposed an IoT architecture for Ambient Assisted Living (AAL) over NDN, that may improve the overall service by using caching and simple NDN design. They proposed a specific naming structure for AAL to solve the heterogeneous devices and integrate different services between them without the need for middle ware. However, the work is mostly an abstraction and does not address various AAL scenarios, has a highly expressive naming scheme, and does not address patient mobility or secure publish–subscribe communication. Similarly, Nour et al. [82] presented a distributed NDN architecture for AAL applications, that supports different IoT traffic models with a service management process. The authors also proposed a persistent interest with Subscription Table to support publish–subscribe communications. Although the architecture supports producer and cache-replica mobility using mapping-based and hand-off mechanisms, the exchanged data still can be accessed by any node in the network. Hence, secure group communication is required. Zhang et al. [81] designed and implemented NDNFit which is a distributed mobile health platform running on top of NDN. NDNFit collects and shares mobile health data using cloud-enabled mobile architecture, and allows users to take control directly to their data deciding which application and user are allowed to use and manipulate such data. Also, data is named using hierarchical names and all security mechanisms are applied on the data itself that make it self-secure and independent from the producer. However, the proposed solution has different components to allow IoT data storage, process and visualization. Saxena et al. [83] proposed NHealthIoT which is an NDN-based smart health IoT. A pure NDN M2M communication is used to capture and transmit data from sensors to the home server, and detect emergency events using Hidden Markov Model. The proposed solution uses a context-aware adaptive forwarding strategy to send events to the cloud server, and periodically pulls other information data using a publish/subscribe paradigm.

Due to different user access levels that can be integrated into one health-care application (i.e. patient, doctor, nurse, family members, etc.), an adequate trust management scheme with data privacy must be developed with name-based access control, that defines access for each member. Also, providing quality of service support is necessary to allow emergency and event-based traffic. Moreover, the mobility factor is an important aspect (i.e. mobility of patient with attached on-body sensors) that should support reliable data delivery.

5.4. Smart grid systems

Smart Grids [97] use IoT to provide smart management and control of energy distribution. Smart Grid systems aim to improve and enhance the energy consumption of homes and building. The concept consists of collecting, analyzing, controlling, monitoring, and managing resources in order to reduce the potential of failures, increase efficiency, and improve quality of services.

ICN use case scenario: Smart grids aim to contribute in the economy, and improve environmental health through moving the available energy in an optimized and reliable manner. The use of IoT devices in cities, homes, and grids may transmit the electricity in an efficient, secure, and scalable way, quickly run restoration and backup solutions after power disturbances, reduce the peak demand, and enhance lower electricity rates. Considering the communication layer of smart grids, we find that it is independent from the host point of view, and is related only to the requested information. The use of caching will enhance the communication between smart grids entities without end-to-end device communication. Even if it is the case, the communication is still optimized and secure in nature by leveraging content-based security. Similarly, using content name to allow data retrieval can enhance the multi-source content delivery in an optimized manner.

Some of the current smart grid challenges are:

- Within a large number of heterogeneous devices, smart grids must manage device scalability.
- Perform real-time data collection, processing, control, and analyses.
- Deal with hardware, software, and networking failures.
- As grids are critical infrastructures, protecting the ecosystem against malicious attacks and intrusion detection is indispensable.

Current ICN efforts: Zhang *et at.* [84] proposed an ICN-based architecture to secure the communication in home energy management systems. The idea consists of collecting the measurement information from household elements, performing data aggregation and analysis for future intelligent decisions. To this aim, the authors adopted two different layers: publish–subscribe communication layer, and security layer which is responsible to share the encryption key along the subscribers. Although the architecture provides secure data sharing, it cannot scale with the dynamic increase of subscribers, and only addresses the data collection. Katsaros et al. [85] used real grid topologies in Netherlands to study the feasibility of using ICN solutions to address different machine-to-machine communication challenges in smart grid, and compared the performance gained by ICN against host-centric solutions. The authors found that ICN may address various emerging challenges in smart grids including multi-rendezvous points selection and in-network processing. E. Oh [86] discussed network mechanics and requirements for smart grid using an IoT system. Author highlighted the design choices and strategies for a secure smart grid using ICN, to enable reliable and efficient communications, and to decrease the system and computational complexity. However, the paper is limited to design only. Future work may include implementation and experimentation.

Machine-to-machine communication is a dominant model in smart grids. However, defining M2M model on top of content names needs more investigation. Similarly, securing the publish–subscribe data flow among the active subscribes requires new and flexible key exchange protocols.

5.5. Smart transportation systems & vehicular networks

Smart Transportation [98] couples computation and communication to monitor and control the transportation networks. IoT may play an important rule in such context, i.e. traffic control systems to monitor vehicular traffic in cities, deploy services to manage traffic routing and avoid congestion, or using sensors in smart parking systems to improve mobility in urban areas. All these and other smart services are used to achieve better reliability, efficiency, availability, and safety of the transportation infrastructure.

ICN use case scenario: Public transportation has significant impact on daily life of commuters, and vehicles exchange large volume of data with other vehicles (V2V communication) like warning messages, or between infrastructure (V2I communication) for navigation or downloading files. The exchanged data may cause network congestion and affect hundreds of vehicles in network. Thus, ICN caching can improve the data availability regardless of producer reachability (get the data from near cache store at the vehicle level). This may gain time for both citizens and public transport companies, and increase safety especially for children and elderly people. Another scenario, where passengers may subscribe to public transport services to better monitor bus routes and delay. These services may combine both real-time information with the personal needs to fetch the content, and fulfill its demands. Here, passengers are not interested in the bus address, the communication will be related to the name of the offered services. In such cases, the subscription may be satisfied by any subscriber in the same direction.

Moreover, smart transportation faces the following challenges:

- Deal with a large number of mobile vehicles and nodes interconnected with different infrastructure elements using different communication models.
- Operate in real-time and remain resilient against any failures and attacks.
- Deal with end-to-end latency by providing in-network computing.
- Provide simple interoperability with heterogeneous devices and protocols.

Current ICN efforts: Bouk et al. [92] discussed the integration of NDN in intelligent transportation system from the smart cities perspective. They elaborated on securing and enabling reliable communication among mobile devices, by benefiting from NDN features such as naming, in-network caching, and content-based security. The authors highlighted various research directions aiming to enhance the merger of NDN and transportation system, but excluded the mapping of NDN and VANET. Similarly, Amadeo et al. [87] discussed the applicability of ICN in vehicular environments, by elaborating different ICN functionalities from VANET perspectives. Although authors debated the different opportunities used by ICN naming, caching and support of multicast and mobility to overcome critical challenges in vehicular networks, they did not cover recent efforts in such context.

Saxena et al. [89] studied the performance of NDN-based forwarding schemes in VANET in term of content retrieving and disseminating data, by implementing different IP-based forwarding schemes such as Epidemic [99], Spray & Wait [100], and Adaptive Forwarding [101] on top of NDN in a real vehicular testbed. However, the proposed solution does not address duplicate requests and forwarding loops, nor it considers vehicle's mobility. Chowdhury et al. [90,91] proposed an anonymous authentication and pseudonym-renewal scheme for VANET on top of NDN. The authors divided the network elements into three entities: Vehicle, Manufacturer, and a Root Organization. By benefiting from NDN naming and security, they presented a trust model and Certificate Issuing Proxy (CIP) for authentication, where vehicles use pseudonyms rather than real names to prevent tracking. They used Raspberry Pi-based miniature cars for implementation and evaluation. Signorello et al. [88] addressed the security challenges in NDN by focusing on vehicular environments, and different vulnerabilities that may be created when applying NDN on top of VANETs. They focus on interest flooding attacks, and cache poisoning attacks. This work did not cover security in other ICN components such as naming, caching, mobility, etc. Similarly, Bouk et al. [93] discussed various security vulnerabilities and attacks in vehicular cyber–physical systems, and highlighting various issues and challenges. Based on their discussion, the authors proposed NDN-based cyber-resilient architecture, which contains an NDN forwarding daemon with threat aversion, detection, and resilience capabilities. However, the authors did not discuss in detail how their architecture will be implemented, nor any results have been presented.

The high mobility of cars is a critical issue in smart transportation that effects the data dissemination and quality of service. Smart collaborative caching schemes must be developed with the integration of edge computing to overcome such issues. Also, there is a need to develop adequate forwarding schemes that can deal with broadcast nature of traffic and take benefit of in-network caching.

5.6. Summary & insights

In light of the efforts discussed in this section, there is a dire need to work on comprehensive solutions along with implementations for each of the IoT application domains. We find that either the existing works are too broad in nature, or too narrow and specific. In either case, the different use cases present unique requirements of IoT–ICN system. Standardizing the content/service naming is still an open issue, while defining what type of content should be cached to reap the benefits of in-network caching. Finally, as most of IoT traffic follows publish–subscribe model, a secure and scale publish–subscribe protocol is required in the core ICN layer rather than at the application level.

6. General IoT-ICN issues

Continuing from earlier discussion, IoT communication follows data oriented concept very closely [102]. Hence, ICN connectivity and principles must be adapted to IoT paradigm. In the following sub-sections, we review the existing ICN solutions tailored for IoT network. Tables 3 and 4 provide classifications and comparative summaries of different aspects.

6.1. Data/content naming

The content name is the main component to build an ICN network, request, and deliver data. The performance and the working principles of other aspects such as security, mobility and caching are based on the efficient working of naming. Hence, designing a flexible and custom-based naming scheme with a broad name-space in ICN is an important task, especially for scalability of networks.

ICN naming solutions: Bari et al. [19] discussed various naming solutions in ICN architectures such as DONA, NetInf, PURSUIT, and NDN; and presented a qualitative comparison of their naming/routing schemes. Then, different requirements and design alternatives based on the study have been proposed to achieve an efficient content naming/routing model. Adhatarao et al. [103] presented a qualitative and quantitative comparison on hierarchical and flat names. Different metrics have been taken into account such as lookup efficiency, aggregate-ability, semantics, and manageability. The study shows that a higher lookup complexity can be achieved using hierarchical names due to the parse and lookup for each name component to determine the next interface. However, hierarchical names can reduce the FIB table size by using name aggregation compared to flat name that has non structure/semantic features but no aggregation can be applied. Mochida et al. [75] earlier discussed from its use case perspective, also presented an interesting approach which may be applicable in other IoT use cases in general. In this scheme, names are assigned automatically at the monitoring camera using deep learning algorithm (Conditional Random Field) to generate a model of the predicted name sequence. With context awareness of other use cases, same can be extended to other IoT devices, however, the length of the name generated can become a bottleneck.

Hierarchical naming schemes: Burke et al. [78] used NDN hierarchical names to secure the control in Building Automation Systems (BAS). Their goal is to benefit from having a hierarchical structure to name all system components including authentication using the following */namespace/commad/randomizer/auth-tag*. Although they added security aspect to naming, long hierarchical name is still an issue, that effects the lookup process. Also, the used algorithm (i.e. RSA and HMAC) requires more processing and energy. Amadeo et al. [79] designed an NDN framework for smart homes, by proposing a namespace for the home with two classes: *config* and *task*. For each class, they defined the *task type* and its associated *sub-types*, such as */action/light/on* and */sensing/movement*, the last component in the name is the location of the sensors such as *kitchen, bedroom, etc.* This naming scheme can support rule aggregation to reduce the number of sent requests. However, it is designed for a specific use case, and requires more efforts from the application layer to understand the naming semantic. Similarly, the used hierarchical unbounded name may effect the lookup and forwarding performance. Bracciale et al. [104] introduced an abstract Lightweight Named Object (LNO) scheme for IoT devices. The motivation behind such naming is to provide programming, simplicity, and extended functionalities to physical devices. The proposed solution uses NDN hierarchical names in order to represent physical IoT objects in a derived name-space. However, the used names are very long as they include device name, function, and a list of parameters. Although the functionality is light weight, the storage and matching of long names may be a limiting factors in some IoT scenarios. Moreover, such topological naming is not recommended in high mobility IoT networks where device connectivity often changes.

Hybrid naming schemes: Ascigil et al. [47] proposed a keyword-based naming scheme in ICN for IoT applications that allows data retrieval from multiple sources without breaking the One-Interest One-Data rule. The proposed naming is a hybrid scheme, and mainly has three parts: *(i) Hierarchical part* that follows the native NDN hierarchical names and usually describes the IoT domain, *(ii) Function part* that consists of a single tag and defines the used function to allow multiple data retrievals and node local processing, and *(iii) Hashtags* is the last component which is, in fact, hashtag-like keywords separated by ' / ' and describes the needed IoT data to be retrieved. The main drawback of the proposed scheme is the length of name and the number of allowed keywords that may have impact on the content reliability. Also, processing in-network aggregation without providing any trust model can directly effect the data privacy. Nour et al. [48] represented a Multilayer Multi-component Hierarchical Attribute-Value naming scheme (M2HAV), which combines prefix-labeling with variable-length encoding methods to represent the hierarchical location of data. The authors tested the naming with decimal classification and Fibonacci encoding

Table 3
IoT–ICN existing research for Naming, Routing, Content Discovery, Caching, and Synchronization.

Aspect		Ref.	Summary	Architecture	Year
Data/Content naming	*Basic*	[19]	Comparison of requirements and design choices of different naming scheme in ICN projects.	ICN	2012
		[103]	Qualitative and quantitative comparison of hierarchical and flat names.	NDN, MF	2016
		[75]	Use of deep learning approach to assign names to sensors and monitoring systems.	ICN	2017
	Hierarchical	[78]	Secure names by appending authentication tag in hierarchical structure.	NDN	2013
		[79]	Design of a wide name space for smart home applications by defining the class and task.	NDN	2015
		[104]	Design of a lightweight hierarchical naming scheme for physical IoT devices.	NDN	2019
	Hybrid	[47]	Multi-source data retrieval using keyword-based naming scheme.	NDN	2017
		[48]	Multilayer multi-component naming scheme using prefix-labeling with variable-length encoding methods.	NDN	2017
		[105]	Hybrid multi-parts naming scheme that combines hierarchical, attribute and flat components.	NDN	2017
		[106]	Convert long content-prefix names to small prefix-codes that can be used in local IoT commun.	NDN	2017
Forwarding & Content discovery	*Forwarding*	[47]	Hybrid routing: NDN forwarding between domains, and tag-based routing for local IoT network.	NDN	2017
		[107]	Intelligent context-based forwarding strategy for resource-constrained devices based on request content and corresponding application.	NDN	2016
		[108,109]	Design of a Bloom Filter-based Routing scheme to support pull traffic in NDN applications.	NDN	2018
		[110]	Design of a Bloom Filter-based forwarding scheme to forward flat names.	PURSUIT	2018
		[111]	Adaptive forwarding strategy for Persistent Interest using probing results.	NDN	2017
		[112]	Divide large-scale network into sub-networks and perform fixed-length Bloom-filter.	ICN	2016
		[113]	Address the forwarding speed and analyze False-Positive-Free Bloom-filter design.	ICN	2015
		[114]	Adopt Bloom-filter based forwarding to mitigate brute force and denial-of-service attacks.	ICN	2013
		[115]	Focus on Bloom-filter size security and propose a mechanism to decrease the attack probability.	PURSUIT	2014
	Discovery	[116]	Flexible and less-complex semantic matching-based discovery mechanism.	ICN	2016
		[117]	Opportunistic coordination approach to locate the cached content using EFIB table and budget-based multicast forwarding strategy to track the recent directions.	ICN	2017
In-network caching	*Placement*	[118]	A freshness-based caching scheme based on extended CS table with a freshness field.	NDN	2014
		[119]	Caching metrics from IoT perspectives and how to decide the cache-possibility of content.	ICN	2014
		[120]	Harmony Search based content caching and updating algorithm based on content freshness and IoT device energy.	ICN	2018
		[121]	Select optimal cache to minimize both content delivery cost and caching cost based on IoT traffic.	ICN	2018
		[76]	A periodic cache scheme that caches the most frequent content in smart city use case.	ICN	2018
		[122]	A cooperative caching scheme based on content lifetime and access rate.	NDN	2018
		[123,124]	Verification scheme to secure cache content and prevent verification attack in cache store.	NDN	2017
	Replacement	[125]	A popularity based replacement scheme to keep only popular content in the cache store.	NDN	2013
		[126]	Integrated Bloom filter to capture content popularity in a continuous way.	NDN	2014
		[127]	Use of content freshness to decide the cache replacement rule in IoT networks.	NDN	2019
Synchronization	*Sync*	[128]	Surveying multi-party data-centric solutions.	NDN	2017
		[129]	iSync protocol using two-level Invertible Bloom Filter structure.	NDN	2014
		[130]	Distributed dataset sync protocol with dataset state vectors, and leader-based group membership mechanism for security operations.	NDN	2017
		[131,132]	Improved version of RoundSync by reducing messages exchanged and packet loses.	NDN	2017

scheme. They also used different attributes in each level with a set of properties. The proposed naming consumes less memory and time for lookup and routing process as compared to the generic hierarchical names. However, the names are not user friendly. Similarly, Arshad et al. [105] proposed a hybrid naming scheme for IoT that addresses smart campus use case. The authors used four parts in the name: *(a) Primary Root Prefix*: to indicate the application type e.g., smart cities (SC), Smart Transport (ST), Smart Home (SH). *(b) Hierarchical Components*: to combine campus information in a hierarchical NDN format, information such as campus location, content originator ID, and content type are listed at this level. *(c) Attribute Components*: to describe details information about the content itself such as content properties and task type. *(d) Flat Components*: to provide a secure and signed names by using hash function. Although this scheme has a lot of information about the content and its properties, reaching a scalable and fast lookup process is a challenging issue, due to its length.

Local IoT communication support: Yang et al. [106] proposed a Local Naming Service (LNS) to perform a local communication in resource-constrained IoT environment. The idea consists of making an inter-conversion between a sensor and a network sink, and convert the content-prefix to prefix-code. The sink node maintains a *Prefix Code Table* (PCT) to map the content-prefix with the prefix-code. If the communication is local, only the code prefix is used in name, and to ensure global communication, the sink converts the prefix-code with the original content-prefix. The major issue with this mechanism is that the node has to update all nodes with the new prefix-code whenever new data has been created. This, will significantly decrease the network performance, and effect the communication.

Summary: Hybrid naming schemes are gaining more attention and efforts from researchers as they can provide benefits from many schemes. The benefit includes name-aggregation rules, better scalability supports, overcome the long names provided by hierarchical names,

Table 4
Comparison of ICN naming in IoT.

Naming scheme	Friendly	Short-length	Fast lookup
Ascigil *et al.* [47]	✓	✗	✗
Nour *et al.* [48]	✗	✓	✓
Bracciale *et al.* [104]	✓	✗	✗
Arshad *et al.* [105]	✓	✗	✗
Yang *et al.* [106]	✗	✓	✓

and save more space in IoT resource-constrained devices with a fast name lookup operation. However, they increase the complexity of name, which may impact the lookup process at each node.

6.2. Forwarding & content discovery

From ICN perspective, the routing plane is used to set and update the network topology, handle their long-term changes, and update the intermediate node's forwarding tables. NDN and CCN architectures also uses the forwarding plane to rank and probe faces used in the routing/forwarding process. The substantial difference between the routing and forwarding is that the former is used to decide about route/path availability, while the latter is used to decide about the preferences to use best path based on different metrics.

6.2.1. Routing solutions

Different routing algorithms are used in the current Internet on top of IP protocol (link-state & distance-vector algorithms). They can be extended with slight modification and be used in ICN. The major modification in the route calculation process is to distribute name-prefix instead of IP addresses. A name-based OSPF version for NDN (OSPFN) has been proposed in [133]. OSPFN builds an Opaque Link State Advertisements (OLSA) as each name-prefix needs to be announced in the network through flooding. When OSPF Daemon (OSPFD) receives an OLSA, it updates its local OSPFN. If the packet contains a new name-prefix, then the name is extracted with its associated Router-ID and stored in the name-prefix table. To find next-hop, OSPFN queries OSPFD that by return checks for path cost, and replies with a query message containing next-hop(s) to reach the original router that has the requested name-prefix. OSPFN prepares and maintains FIB entries to keep it updated with best routes. Link-State Routing Protocol for NDN (NLSR) has been proposed in [134]. NLSR uses Link-State Advertisement (LSA) to build network topology and distribute name-prefixes. Where each NLSR node maintains Link State Database (LSDB). Two types of LSA are used in NLSR: (a) *Adjacency LSAs* that are used to advertise the active links to all node neighbors, and (b) *Prefix LSAs* that are used to advertise the registered name-prefixes. Each NLSR is signed by its original advertiser to support network authentication.

6.2.2. Forwarding solutions

The forwarding plane is responsible to detect failures, perform recovery, and act as a control plane. NDN Forwarding plane may have different forwarding strategies that perform all decisions needed for each interest and data packet, and use multiple forwarding options to choose the best face toward the content provider in an efficient manner. Also, network developers can develop different strategies based on the used network environments and context. Ascigil et al. [47] used a hybrid naming scheme by combining both NDN hierarchical names with hashtag-like keywords. A hybrid routing process has been introduced in the same work. The authors proposed to use generic NDN forwarding scheme to route the interests between Internet domains, and a modified version of TagNeT [135] to achieve local IoT routing. They used tags included in the name and exclude the hierarchical part in local routing, which is used only outside the local network. Melvix et al. [107] focused on the forwarding strategy in NDN-based IoT applications, where context-based forwarding has been proposed. This strategy determines the context of the requested content, the corresponding application's tolerance, and uses of the cached data to make an intelligent forwarding decision. By enabling all these features, the forwarding process will reduce the node's power consumption.

Marandi et al. [108,109] proposed a Bloom Filter-based Routing scheme to support pull traffic in NDN. The content publishers advertise only the demanded content names in the network that helps to utilize fewer memory resources. Pull communication can be extremely beneficial in IoT, as many of the use cases require specific updates at desired intervals. However, the scalability of IoT can be a concern, as the scheme does not directly addresses large scale systems. Rodrigues et al. [110] studied the network performance using Bloom Filter-based forwarding on top of flat names. The authors defined a Bloom Filter-based packet flow model using Bayesian Network to determine the probability of forwarding decision. The study points that aggressive aggregation may lead to excessive incorrect forwarding decisions compared to exact match, and proposes a Bloom Filter scheme to overcome negative impact. Although the scheme has been designed for generic communication, but its applicability at IoT gateways may be useful. Antikainen et al. [112] introduced XBF, an Extensible-Bloom-filter scheme for large-scale intra-domain multicast networks. XBF partitions the network to a set of sub-networks according to the network topology and traffic patterns, and performs a separate fixed-length Bloom-filter to each one. Each sub-network comprises of three entities: (a) *Topology manager:* a centralized entity similar to a SDN controller that creates Bloom-filters, (b) *Popper switches:* are boundary switches between different sub-networks, and (c) *Forwarder switches:* are normal switches that perform Bloom-filter forwarding operations. The main drawback of this scheme is the use of fixed-length Bloom-filter which may affect the network scalability. To address forwarding speed, state, and scalability issues using Bloom-filter, Tapolcai et al. [113] proposed and analyzed a False-Positive-Free Bloom Filter design. The authors used arbitrary size trees based on flat routing approach (i.e., tree encoding-based), and multistage Bloom filters to decide the optimal-length varying-size instead of using a fixed-size. Simulation results show the effectiveness of the proposed solution.

Focusing on secure forwarding plane, Alzahrani et al. [114] proposed a Bloom-filter based forwarding scheme to mitigate brute force and distributed denial-of-service attacks. The authors analytically studied the required time to launch a distributed denial-of-service, and then proposed a solution to mitigate it. The overall idea aims at increasing the safe window, which refers to the required time for a malicious user to find a valid filter with a certain probability, hence securing the system against brute force and denial-of-service attacks. Similarly, work in [115] studies the Bloom filter size and maximum fill factor from security perspective. Then, the authors proposed to enhance the header length and consequently increase the safe window and decrease the attack probability.

As NDN packets exchange follows pull-based model, pushing the data from the consumer without an interest is not possible, and the data packets will be considered unsolicited and dropped immediately. Persistent interest [82,136] has been proposed to keep interest for a longer time in PIT table, and establish a long-lived path. Hence, data packets can flow from producer without continuous interest requests. Moll et al. [111] proposed an adaptive forwarding strategy for persistent interest, by using information from the FIB table such as reachable status, corresponding face, costs, and probing results. The idea is that the consumer sends a probing interest to calculate the delay and loss, in order to rate and evaluate the performance of the different paths through the network.

The forwarding plane has been proposed to overcome routing scalability and stability issues in IP-based networking. The NDN forwarding concept aims to forward the data without continuous updates in FIB table. More investigation is required to provide scalable and efficient forwarding schemes that support both IoT push and pull traffic.

6.2.3. Content discovery mechanisms

The structure of the generated and shared data between IoT devices is still a challenge due to the heterogeneous nature of devices and naming schemes. To overcome this issue, Quevedo et al. [116] proposed an ICN-based discovery mechanism that uses semantic matching [137] to provide a flexible and less-complex discovery process. In addition to *Clients* and *Service Providers*, the authors defined *Discovery Brokers*, which are responsible to manage information regarding the available services and incoming queries. Semantic Matching Engine is used to keep track of registered services by Service Providers and matches incoming queries with available services. Similarly, Ascigil et al. [117] addressed the content discovery in cache-enabled nodes, by using opportunistic coordination approach that does not require any further signaling or update protocols to locate the cached content. It uses a new data structure on each router namely, *Ephemeral Forwarding Information Base* to keep track of the recent direction of the data chunks. Moreover, a budget-based multicast forwarding strategy has been used that consists of giving a forwarding budget to every interest packet to forward the interest toward on-path replica-node and/or the original content provider.

Summary: Forwarding strategies in NDN are one of the most important aspects in networking. However, there is a lack of research in this area that focuses on IoT environments. IoT devices are resource-constrained, and most of the current routing algorithms may consume more resources and energy. Hence, a more focused view of IoT application from ICN perspective is needed. Further, optimization forwarding techniques that take IoT traffic and device metrics into consideration, need to be designed to facilitate path adaptation and improve device performance. Finally, it is important to take wireless sensor network characteristics into consideration while designing efficient solutions for fast discovery of working paths and maximization through multi-path utilization.

6.3. In-network caching

In-network caching is one of the fundamental features to support content-centric data-delivery model in ICN. Using in-network caching either on or off path will improve the data availability in the network, without requiring the content producer and consumer to be connected. Hence, any node in the network can serve the content requested [138]. The main advantages of using in-network caching in ICN are: (a) dissociate the content from its original provider, (b) by making multiple copies of the content in the network, requests can be served by any replica node in the network, and may reduce the overhead at the provider side and avoid a single point of failure, (c) facilitate multicasting and retransmission due to packet loss, and (d) improve content retrieval and reduce the network delay and latency.

Abdullahi et al. [23] surveyed caching in different ICN architectures and projects, by discussing cache deployment strategies perspectives like proxy, reverse proxy, caching, adaptive, and active caching. Further, the authors highlighted various research issues in recent ICN solutions (e.g., CCN, DONA, PURSUIT, etc.) in order to achieve the caching goal by minimizing the overall bandwidth consumption, and improve content delivery. Meddeb et al. [138] presented a comparative study among different NDN caching schemes and caching replacements targeting IoT environments. However, this work is general in nature and not comprehensive. In the sections below, we divide caching strategies into two groups i.e. content caching and placement strategies, and cache replacement schemes.

Cache content & placement strategies: ICN nodes need to decide whether the processed content (data packet) should be cached in the intermediate node or not. Hence, various cache placement schemes have been proposed such as: *Leave Copy Everywhere* (LCE) [15], *Copy with Probability* (LCE-Prob) [139]. LCE is an in-built NDN scheme that consists of caching and keeping a copy of the content in all the routers in the path from provider to consumer. The main drawback of LCE is that the same content is cached many times, which by consequence reduces the cached content diversity. To overcome this issues, LCE-Prob caches the content with a given probability $p = 1/(hopcount)$. Keeping IoT content characteristics and devices limitations into consideration, Quevedo et al. [118] focused on the content characteristics side, especially the content freshness, by proposing a freshness-based caching scheme. This scheme consists of adding a new field in Cache Store table for content freshness value, and checks it before serving that request. Consumers from their side may specify the freshness threshold of the requested content (totally fresh or not), whereas the content producers set the content freshness value in the data packets.

Vural et al. [119] also discussed the in-network caching from IoT perspective. Because of the nature of IoT data, caching cannot be applied in similar ways as that of Internet traffic. Hence, the authors considered different metrics (data popularity) to decide if IoT data content should be cached or not. Further, they discussed trade-off between retrieving freshly generated content from the original provider that is at multiple hops from the consumer, or fetching the cached (not as fresh) content from replica-node with less hops. Different metrics are used in the study such as content lifetime, time range of incoming requests, and hop distance to the content source and requesters. However, this work focuses on electrically powered and static devices ignoring the resource-constrained characteristics. Xu et al. [120] studied the content caching and updating in IoT networks. The authors formulated the content caching and cache store updating as a mixed 0–1 integer non-convex optimization problem, and proposed a Harmony Search based content caching and updating algorithm. The proposed algorithm takes content freshness and device energy into consideration. The main limitation of this study is that the authors ignored other parameters of wireless devices, such as mobility and topological changes. Nour et al. [121] proposed a near ICN cache placement scheme based on IoT traffic class. The algorithm selects the optimal cache placement by minimizing the data movement from the original content producer to the cache store, the minimum cost of caching the data in the cache store, and the minimum cost of delivering the data from the cache store to consumers. Although the proposed algorithm improves the cache utilization and provides a fast data delivery, it processes it in a centralized manner. Naeem et al. [76] designed a periodic caching scheme for smart cities where each node has a Distinctive Statistics Table. This table is used to find out the most frequently requested content based on a set of metrics (e.g., content name, frequency count, recently requested time, etc.). The use case assumed in this work is that of smart cities, however, within a smart city other use cases may be integrated, such as smart grid and transportation systems. It is not clear, if the solution can be utilized across the board or will suffer from limitations due to different use case characteristics. Zhang et al. [122] proposed a cooperative IoT caching scheme, based on data lifetime and content access rate to enhance content dissemination & reduce energy consumption. The authors introduced a slide time window to measure the request rate, and a local threshold to cache content. However, the selection of threshold value is an open question, and may be different for different types of content/traffic. Moreover, this scheme is not applicable for content generated for single use. Kim et al. [123,124] discussed the cache poisoning attacks, and suggested a verification scheme to minimize the unnecessary verification. The authors proposed to verify only the served content and favors already-verified content in the content cache store. From NDN perspective, the original content provider signs its data content, and consumers verify it. Hence, each and every data packet contains a digital signature. By using this mechanism, the intermediate router will discard poisoned content if they perform signature verification, however providing verification process in each router is expensive in terms of processing and decreases the overall performance.

Cache replacement schemes: Due to the space limitation of the cache store, some content should be removed to make room for new content. Hence, the cache replacement scheme consists of deciding on which content should be removed from the cache store [140]. *Least Recently Used* (LRU) scheme is well-known in NDN and most used. LRU consists of keeping the most recently used content used and removes the least recently accessed from the CS. *Least Frequently Used* (LFU) consists of removing the less frequently used contents from the CS, hence only the most frequently used content is kept in the store.

From caching perspectives and to increase its benefits, only popular contents should be cached. This may improve the network performance, especially in highly dynamic networks such as IoT. A content popularity based caching scheme has been proposed in [125], where authors created a new data structure that cooperates with *Content Popularity Table* (CPT), to store information about the cache hit, and content's previous & current popularity associated with its name. Their experiments show better results as compared to LRU and LFU schemes in term of cache hit ratio, network capacity, and load. However, the scheme consumes more CPU that may not be suitable for large-scale network and resource-constrained devices. This issue has been addressed in [126], by proposing a line speed Bloom filter-based method to capture the content popularity in a continuous manner, and at the same time minimize the memory usage and overall resource consumption. However, the proposed method has a major issue with the storage cost. Meddeb et al. [127] designed Least Fresh First cache replacement scheme for IoT applications that integrates content freshness as the main element. The authors adopted Auto-regression Moving Average model [141] to predict the content freshness. However, using the freshness parameters is not enough in IoT context, other metrics (e.g., content popularity) must be taken into consideration.

Summary: ICN caching schemes may help IoT networks by improving network performance and data dissemination. However, caching IoT content based on its popularity is not enough. IoT devices are limited in resources and energy. Hence, node properties should be taken into consideration to decide at which device the caching should be applied. Also, due to the diversity of the IoT traffic, some of them follow 1-usage pattern (used one time), and may not benefit from the caching. So, deciding what kind of traffic should be cached is another issue, especially for publish–subscribe traffic. Finally, most of the existing cache replacement schemes are designed for general Internet traffic without considering IoT networks. Future research needs to explore IoT-based replacement strategies to ensure data diversity with less memory and resource consumption.

6.4. Synchronization

Multi-party data-centric communication is an important communication model in today's Internet, where applications such as group messaging and Dropbox-style file sharing require a distributed dataset synchronization mechanisms. In the IoT environment, various applications require to be synchronized, for example, the home gateway device, user mobile phone, and cloud repository. Similarly, in a smart hospital, doctors, nurses, family member, and monitoring applications in the Internet can synchronize with all patient's statistics and reports.

Several protocols have been proposed in the literature [128], with different design choices, but share the same idea of using content name to sync the dataset among members. iSync protocol [129] uses a two-level Invertible Bloom Filter structure to support an efficient data synchronization and reconciliation between different nodes. While VectorSync [130] which is a distributed synchronization protocol, has two processes: (1) a mechanism to maintain the synchronization state of the dataset by using state vector (version vector), and (2) a leader-based group membership mechanism to facilitate data authentication, access control among participants. Similarly, iRoundSync protocol [131] has been developed as an improved variant of RoundSync [132], to allow participating nodes to detect, propagate, and reconcile all changes in a resilient way toward packet losses with fewer messages exchange in multiple-change scenarios.

Summary: To the authors' best knowledge, most of synchronization solutions have been designed from a regular Internet point of view. There is a lack of research efforts in terms of IoT–ICN synchronization part which is an important point. In e-health scenario, where a patient is monitored by multiple doctors, all reports and information must be synchronized in time to avoid any critical issues. For example, when a doctor changes the medicine or its dosage, other doctors' and nurses' databases must be synchronized to provide the suitable medicine to the patient.

6.5. Interoperability & adoption

Real world deployment and adoption of ICN for large-scale Internet communication is a challenging process. A clean slate implementation of ICN across the board is highly improbable. Primary reason being the immature nature of ICN solutions and the high economic impact on service providers. Hence, the solutions which aim at coexistence of both IP and ICN architectures will be favorable in future.

Coexistence can be done in two ways: (a) Overlay & Underlay, or (b) Packet translation. In the first method, ICN packets travel over IP networks or vice versa, essentially creating tunnels for each other. In the later, gateways or proxies are used to extract data from packets, and encapsulate it into new packets which can travel over the subsequent networks. In either of the case, the biggest challenge is translation of names into addresses and vice versa. Usage of either solution will have tremendous economic value attached to it, which demands that service providers carefully choose the migration and adoption policies for future Internet. Below we present solutions from literature, which have addressed these three elements in detail, and Table 5 provides a summary of these solutions.

Underlay/overlay solutions: Shailendra et al. [142] proposed an Overlay Information Centric Networks (O-ICN) architecture that consists of separating the data plane from the control plane activities. Although not specific to IoT, the authors proposed that naming and routing to be included in the control plane functionalities, whereas in-network caching is in the data plane. This can be useful in IoT networks, where control plane can be implemented at gateways. The proposal utilizes an ICN Manager Module which is an extended version of Domain Name System (DNS), that can be used for name resolution. Small isolated IoT networks can benefit from this work. Shannigrahi et al. [143] designed a tunneling protocol (IPoC) to allow IP-based applications to utilize ICN networks in a transparent manner. The authors included the IP address in the naming scheme, including two layers IPoC Client and Gateway to allow encapsulation and re-sequencing during the communication. Moiseenko et al. [144] proposed co-existence of TCP and ICN, by allowing applications to use TCP and carry packet over an ICN instead of using IP over ICN. The authors designed a TCP/ICN proxy that carries traffic between two TCP/IP users over an ICN network. Extending and implementing it in IoT networks still needs evaluation and analysis for placement of proxy at access points.

POINT project (IP-over-ICN networking) [154] aims to run IP protocol over ICN for an individual operator, and hence improves IP-based service offered to end-users. POINT project has been derived from PURSUIT architecture [12] by combining both ICN core with Network Attachment Points (NAPs) with no changes in end-user equipment or IP routers. Initial efforts have demonstrated efficient video streaming [155] and Internet Protocol Television (IPTV) [156] services using POINT architecture. Within the POINT project, Trossen et al. [145] presented a publisher–subscriber communication mechanism to place IP-based services on top of ICN-driven networks. The proposed architecture supports different IP-based protocols such as HTTP, Constrained Application Protocol (CoAP), and TCP, as well as various data structures of the underlying protocols within the ICN network. Evaluation and implementation for IoT networks will be interesting in this regard. As different IoT use cases have different topological sizes, hence large vehicular networks may benefit from it. Similarly, Fotiou et al. [146] designed a proxy-based solution to encode CoAP traffic over an ICN network. The authors used a Publish–Subscribe Internet model and a

Table 5
Interoperability and adoption solutions.

Aspect	Ref.	Summary	Architecture	Method	Year
Underlay & Overlay	[142]	Overlay ICN architecture that separates the control from data plane.	NDN	ICN over IP	2015
	[143]	Tunneling protocol to allow IP-based traffic utilize ICN networks transparently.	ICN	IP over ICN	2018
	[144]	Carry traditional application traffic over ICN network using TCP.	TCP	TCP over ICN	2016
	[145]	ICN publisher–subscriber communication style to replace IP and compatible with IoT protocols.	ICN	IP over ICN	2015
	[146]	A proxy-based solution to encode CoAP traffic over an ICN network using publish–subscribe model.	ICN	CoAP over ICN	2017
	[147]	Use of Network Attached Point to provide transparent CoAP services on top of ICN network.	ICN	CoAP over ICN	2019
Packet conversion	[148]	Use of SDN to install ICN forwarding state without any previous knowledge of ICN concept	ICN	ICN-SDN controller	2013
	[149]	IP-to-NDN gateway to fetch content between two networks without re-formatting packets.	NDN	IP ↔ NDN	2017
	[150]	Translate TCP/IP packet into NDN format using content name and new type of interest packets.	NDN	TCP/IP → NDN	2018
	[151]	Coexistence of NDN and IP-based MQTT in IoT scenarios by using conversation points for content mapping and discovery.	NDN	IP ↔ NDN	2017
Migration cost	[152]	Study of expected economic benefits of migrated to ICN. Proposed a near-optimal Randomized Rounding heuristic to compute the node migration and object allocation cost.	ICN	Heuristic algorithm	2014
	[153]	Study ICN content-aware network-planning problem in budget-constrained scenario, and proposed a greedy heuristic algorithm to find an optimal migration strategy for operators.	ICN	Greedy heuristic	2015

collection of attributes to aggregate requests and transmit update notifications via the proxy. However, the authors did not explain in detail the implementation of multicast communication and access-control management in the publish–subscribe model. Recently Islam et al. [147] introduced an ICN-based CoAP [157] using Network Attached Point in order to improve and provide transparent services. The overall idea consists of receiving requests from CoAP clients running IP protocol and then translate message to ICN. The response message generated by the CoAP server is forwarded to clients using the reverse process. The authors demonstrate that deploying CoAP over ICN network improves the performance and reduces overhead and complexity.

Packet conversion solutions: Vahlenkamp et al. [148] discussed how to enable ICN on existing IP networks. The authors proposed to use the Software-Defined Networking (SDN) paradigm. The idea consists of enabling SDN controllers to install the appropriate forwarding state for ICN requests. Thus, nodes have to support only IP forwarding without any previous knowledge of ICN concept. However, this concept requires the SDN protocol to handle different packet header format. Refaei et al. [149] proposed an IP-to-NDN gateway scheme to model the IP client–server applications into NDN networks. IP-based applications can fetch content from NDN network without the need of re-formatting or re-designing packets. The idea consists of creating a configuration file (JSON format) at the gateway level to translate both IP and NDN headers. The major limitation of this solution is that the configuration file should include explicitly all kind of applications and their mapping which is not a feasible solution in large-scale IoT networks. Luo et al. [150] proposed a set of migration mechanisms at the Internet, TCP, and the Application layer in order to translate TCP/IP packets into NDN, and thus run them in NDN-based networks. The main idea is to include all information in the content names. In particular, the IP address is used as a component in the content name, while IP header is encoded into a new type of interest namely NotifyInterest (in order to minimize network traffic). Finally, the authors used a hierarchical naming convention to include application-related information in the naming scheme. The major issue with this scheme is that it produces large names. Quevedo et al. [151] presented a new mechanism to provide interoperability between NDN-based IoT and IP-based Message Queue Telemetry Transport (MQTT) devices, in order to allow coexistence of the two paradigms. To ensure the interaction between two types of communications, the authors proposed an entity namely *Future Internet eXchange Point* (FIXP) that converses messages, content mapping, and available resources discovery.

Migration Cost: The previous section discusses a number of solutions for adopting ICN as a mainstream architecture. However, a major factor for service providers is the migration or adoption cost. This factor alone may become a deciding point for the scale of adoption in future, regardless of the efficiency gain of ICN. There has been very limited work on economic analysis of migration from pure host centric to a hybrid or pure content centric network.

In this regard, Mangili et al. [152] focused on the expected economic benefits that an operator may gain if migrated to ICN, including the infrastructure change required. The authors formulated migration costs into a content-aware network-planning model and proposed a near-optimal Randomized Rounding heuristic algorithm to compute node migration and object allocation cost efficiently. The authors extended their content-aware network-planning work in [153]. Considering a budget-constrained scenario, ICN traffic routing and content caching, the authors demonstrated that the problem is NP-hard, and further proposed a greedy heuristic algorithm to find an optimal migration strategy for operators. The authors concluded that migrating only few nodes to ICN model may help the operator to reduct traffic costs compared to IP-based model, and when the content popularity increases, migrating to ICN is more preferable (because of in-network content caching) to offload the content distribution from provider side to the network level.

Summary: Deploying a clean-slate ICN network requires more efforts and time. Thus, an overlay mode is a preferable mechanism in the first ICN deployment phase. Also, we believe that ICN can outperform IP in the local IoT network, while IP still exists between networks. Hence, mapping solutions or network function virtualization may be used to achieve this. Finally, a critical element will be to understand the effect of new network stack on existing IoT applications. Ultimately, the adoption will rely on economic factors of replacing the infrastructure, and providing migration support for legacy applications.

7. Publish–subscribe communication

Publish–Subscribe model is widely used in IoT applications, where a group of users subscribe to a topic or content offered by a publisher. For each newly generated data element, the publisher pushes the data toward these subscribers. Moreover, in case of new events triggered at the publisher side, an event report is sent toward the subscribers. However, due to the communication model used in NDN which is

Table 6
IoT–ICN publish-subscribe solutions.

Aspect	Ref.	Summary	Architecture	Year
Persistent PIT	[158]	Propose of different strategies to deliver push-based IoT traffic: Interest notification, Unsolicited data, or Virtual interest polling.	NDN	2014
	[82]	Use of persistent interest and Subscriber Table to support push-based model and track active subscription sessions.	NDN	2017
	[159]	Use of subscribe/publish message and Rendezvous Point to receive subscribed content.	NDN	2016
	[136]	Customize semi-persistent interest packets with channel information to create session-like communication.	NDN	2011
	[111,160]	Study the use of persistent interests to support pull traffic in NDN architecture.	NDN	2018
Generic Pub/Sub	[161–163]	Support of push-traffic in VANET by allowing unsolicited packets, beacon messages, or dynamic PIT lifetime timer.	NDN	2017
	[164]	A distributed publisher-driven architecture to share IoT data in a secure manner using a set of attributes.	ICN	2017
	[165]	Use of content proxy node to cache content persistently where consumer may pull data.	ICN	2018

based on Interest-Data exchange with 1-to –1 rule, pushing of data from publisher (without interest packet) is impossible, hence requiring innovative and efficient solutions. Table 6 lists the solutions discussed in this section. The classification is based on the persistent nature of PIT entries. It is important to note, that traditional IP networks implement topic subscription system at the application level. Same can be used in ICN, however, each message under a topic is considered as independent content with a unique name. Hence, the ICN-IoT solutions available in literature usually focus on content-based pub/sub model, where each piece of content when updated, has to be delivered to consumers.

Persistent interest solutions: Deploying publish–subscribe communication in NDN is challenging. Various solutions have been proposed either by proposing long-lived persistence interest to allow flow of multiple data packets for one interest or adding an exception in the forwarding by allowing unsolicited data packet to be forwarded without any previous interest.

Amadeo et al. [158] proposed three different strategies to deliver push-based IoT traffic: (a) the publisher sends an interest packet for periodical and event-triggered notification, that includes the data in interest name components, (b) by sending unsolicited data without any interest, and intermediate nodes validate the content signature rather than checking the PIT table, and (c) use Virtual Interest polling, where PIT entry has a long lifetime.

Unfortunately, these schemes violate the NDN primitives, and produce an overload at different NDN nodes. Furthermore, any nodes in the network can subscribe to such content and receive it without any access control mechanism. Nour et al. [82] proposed a push-based model in NDN to support publish–subscribe communication in an AAL environment. The authors introduced persistent interest and a new data structure namely Subscriber Table (ST) to track active subscription sessions in each intermediate node, while the persistent value in PIT table allows push data. A publisher can send data packet upon its creation using the reverse path created by the persistent interest. Similarly, when the publisher generates an event or condition based traffic, a reverse interest packet is initialized by the publisher. However, this solution lacks security perspective, where any subscriber can send interest and receive data without being authenticated.

Tagami et al. [159] proposed a Content-Oriented pub–sub system in fragmented networks by introducing subscribe/publish messages in the network, and a Rendezvous Point that allows subscribers to receive generated content even if they were off-line. Further, intermediate nodes maintain a subscription state similar to IP Multicast to allow multicast forwarding. IoT can benefit from this solution, as many use cases of IoT are small networks.

Tsilopoulos et al. [136] proposed the use of two customized types of interest packets to support different type of information, by introducing a channel concept which is a TCP like session created by network to deliver data. Then, a reliable notification is initialized by the publisher upon content creation, and a semi-persistent interest packet that is stored in PIT table to satisfy multiple data packet. It cannot be removed until the subscriber removes it explicitly. The channel forwards each packet belonging to this session, and follows Stop and Wait Automatic Repeat Request algorithm. Moll et al. [160] studied the use of persistent interests to support push-based communication in Interest-based ICN architectures, while using their earlier work [111] on forwarding. The authors proposed an adaptive persistent interest forwarding scheme to overcome the long-lived path, and extend the hierarchical naming scheme by adding the sequence number at the end of the name. A persistent entry is refreshed only when another persistent interest is received. As persistence in PIT is not the generic working of NDN or CCN, hence the adoption of such mechanism requires large scale deployment and standardization.

Other pub–sub solutions: Different solutions have been proposed in [161–163] to support push-traffic in VANETs. The authors in [161] allowed vehicles to produce and process unsolicited packet to forward emergency messages to the network without any previous interest. While [162] proposed that a vehicle sends one-hop beacon message that is a special interest packet. Neighbor vehicles create a temporary PIT entry when receiving the beacon and cache the incoming unsolicited data instead of discarding it. A dynamic PIT entry lifetime scheme has been proposed in [163] that calculates entry lifetime timer dynamically based on the hop count and interest satisfaction rate. Li et al. [164] proposed a distributed publisher-driven architecture targeting secure data sharing among IoT devices. The authors suggested creating for each content a set of attributes (i.e. attribute manifest and data manifest) that can be cached in the network and retrieved from distributed set of nodes. The authors also proposed Automatic Attribute Self-update Mechanism to update the already published attributes. However, this scheme lacks a mechanism to handle the short-life duration of IoT content. Gundougan et al. [165] designed a robust and resilient publish–subscribe model for IoT applications. The authors suggested selecting the stable nodes as Content Proxies to act as a persistent cache point. Publisher nodes push the content to the Context Proxies where subscribers can fetch it with lesser delay. However, this model has various issues with the mobility of subscribers or even the content proxy. Also, content encryption and access control have not been addressed.

Summary: Most of publish–subscribe solutions focus on semi-persistent interest and modifying NDN forwarding. Persistent interest may have some issues related to PIT table and its management as well as others network attacks. Hence, more optimized publish–subscribe solutions are needed which can be used with different IoT solutions. Also, ensuring security and access control on top of publish–subscribe, and pushing content only to authorized consumers needs more investigation.

Table 7
ICN-based solutions for quality of service in IoT.

Aspect	Ref.	Summary	Architecture	Year
Forwarding strategies	[166]	Multi-constraint QoS forwarding strategy based on Particle-Swarm Optimization.	NDN	2017
	[167]	QoS forwarding strategy based on Ant Colony Optimization to select the best forwarding path.	NDN	2016
	[168]	QoS-aware multi-path forwarding strategy using Ant Colony Optimization problem with real-time parameter measurements.	NDN	2017
Other solutions	[169]	Push–Pull Traffic algorithm that improves QoS provisioning using traffic sorting and classifying.	NDN	2017
	[170]	IoT traffic classification and prioritization and Markov Decision Process forwarding scheme to improve QoS.	NDN	2018
	[171]	Control protocol for named data networks to enhance overall network performance, monitoring, and maintenance.	NDN	2018

8. Quality of service

Quality of Service support is an essential feature in IoT, due to the nature of application requirements and user needs, such as low latency, better scalability, high reliability, and data availability. It is important to note that by using NDN on top of IoT, the data delivery path is the same as interest forwarding path in the reverse direction (symmetric). Thus, providing QoS in both communication phases is a challenging issue as resource reservation is not unidirectional. Moreover, IoT applications may generate different type of traffic such as queries, time-constrained, and event-triggered traffic, thus QoS guarantees must be different from one type to another. Table 7 presents a comparative summary of solutions discussed in this section.

QoS-based forwarding strategies: These strategies are focused on providing QoS during the forwarding phase. A multi-constraint QoS forwarding strategy based on Particle-Swarm Optimization (PSO) has been developed in [166] that aims to use forwarding experiences of data elements (particles) to maintain forwarding probability of each FIB entry. The authors defined a new table namely *PSO Information Table* to record different pieces of information about available prefixes with their faces, and different metrics used in forwarding such as position and velocity vectors. The proposed algorithm forwards the interest based on these vectors and cost functions that take into consideration bandwidth and delay. The algorithm has been simulated and evaluated against Ant-Colony Optimization (ACO) and random strategy, where it performs better. Huang et al. [167] presented a forwarding strategy that supports QoS by using Ant Colony Optimization to select a path that meets the QoS requirement with an optimal strategy. Two additional tables are used in the solution, Neighbor Cache Table (NCT) and Pheromone Table (PT). The former is used to record information about the cached content on neighbor nodes, while the latter is used in the forwarding plane to store delay and cost pheromones with their associated forwarding probability. In a similar way, Kerrouche et al. [168] designed a QoS-aware multi-path forwarding strategy that uses Ant Colony Optimization problem. It consists of monitoring and estimating the bandwidth and round-trip time (RTT) by using ants to measure the real-time QoS parameters of the traversed path from the consumer toward the data provider. It uses the measurements to calculate the pheromone in order to determine which interface the interest packet should be forwarded on.

These solutions may improve the QoS, but it is still not clear how they will fair in resource constrained IoT devices.

Other QoS solutions: A Push–Pull Traffic algorithm has been proposed in [169] that aims to improve QoS provisioning in IoT–NDN network by supporting both Push and Pull traffic. The algorithm consists of sorting and classifying the IoT traffic either as Pull (query-based) or Push (time-based or event-based) traffic. It uses a traffic-based caching concept in NDN cache at router level to decide the content caching. The proposed algorithm has been evaluated in a Building Management System and benchmarked against IPv6. The simulation experiments showed that the proposed algorithm can achieve better results than the traditional IPv6. Similarly, Muralidharan et al. [170] focused on application requirements from quality of service perspective. The authors classified IoT traffic for prioritization purposes, and proposed a Markov Decision Process based interest scheduling scheme to satisfy latency requirements for delay-intolerant applications. Both interest and data packets have been extended by adding traffic class field that is used in the forwarding decision. However, the solution relies solely on RTT for selection of forwarding interface, and adds some overhead to NDN packets and data structures. Nour et al. [171] designed a control protocol for named data networks similar to Internet control messaging protocol. This protocol can be utilized to relay different network errors, information, notification, and service messages to improve the performance and management of the overall system.

Summary: As NDN does not have a dedicated transport layer, most of QoS efforts are developed at forwarding level during the data discovery phase without taking the data delivery phase into account. Whereas QoS provisioning and resource allocation in IoT is as important as routing. Also, some of IoT traffic needs to be delivered with high QoS, support such as emergency and alert messages.

9. IoT security in ICN

ICN performs content-based security [172], where all security-related mechanisms are applied to content rather than the communication channel. In addition to security, various privacy and access control solutions based on name of content have been well-surveyed in [24,25]. However, these are generic solutions for Internet and not specific to IoT. Table 8 provides a summary of the existing content centric security solutions in the context of IoT.

Content security: Each data packet in NDN is signed with its original provider's public key, and verified by any consumer in the network. NDN can support both symmetric and asymmetric encryption algorithms. An encrypted data content using public key, can be decrypted using its associated private key, if symmetric keys are used for encryption, then consumers need to fetch the secret key.

Compagno et al. [173] presented an authentication and authorization protocol for resource-constrained devices in IoT–ICN system. The proposed protocol combines Protocol Authentication for Network Access (PANA) with Extensible Authentication Protocol (EAP) to authenticate and authorize device join operation in an untrusted network, and bootstrap the required keys to secure the communication. The simulation shows that the proposed protocol reduces the energy consumption in comparison to EAP-PANA deployed in IP networks. Mick et al. [174] proposed a secure and scalable framework for lightweight authentication, secure on-boarding, and hierarchical routing in NDN-based IoT networks. Every node in the network is required to be authenticated by the gateway before joining the network or initiating the routing process. The authors used asymmetric cryptography to overcome nodal resource limitations, based on pre-shared keys. This may also be viewed as a weak point in the system. Moreover, node mobility has not been addressed in this work and its impact on the authentication overhead. Frey et al. [175] studied the potential integration of

ICN to provide a secure solution for resource-constrained controllers in industrial safety systems. Toward this, the authors compared IP-based solutions (e.g, MQTT and CoAP) with NDN-based solutions from different viewpoints (e.g, secure network infrastructure, secure data access, denial-of-service resistance, etc.). The authors claimed that the use of content-based security helps ICN to overcome common attacks in the current Internet. Zhu et al. [176] reviewed security attacks in named data IoT networks from different perspectives, e.g., content retrieval and data caching. The authors also provided an initial design for Blockchain based architecture to secure IoT network from different attacks. However, the mentioned attacks are not specific to the IoT networks, and the merger of Blockchain with NDN requires more investigation. Liu et al. [177] designed a distributed low rate denial of service attack mitigation scheme for NDN taking IoT networks into consideration. Each NDN node maintains an extra data structure, namely Malicious Request Table to store malicious name prefix, using which malicious interest requests are dropped. Although this scheme prevents the attacks, it requires changes in the NDN forwarding process, and creates scalability issues for new tables. Adhikari et al. [178] designed a secure CCN framework for IoT applications with a certificate-less public key infrastructure to support the processing limitations. In addition, the authors used elliptic curve cryptography to design a lightweight crypto-system. However, the designed system is centralized and based on the security of trusted authentication server, in which the system may not handle the mobility of IoT devices.

Access control schemes: As soon as the content is cached by replica-nodes in the network, the original provider loses the control on who can access the content. The replica may reply to requests regardless of requester privileges for accessing it. Various Access Control schemes have been proposed in the literature for ICN. Li et al. [179] proposed an ICN access control enforcement, by using a trusted third party entity in the network that may define and manage different content attributes and anthologies. The authors benefit from flat names to preserve content privacy and prevent unauthorized access. During the content creation, a random symmetric key is generated and used to encrypt the content. Only the encrypted version of the content is disseminated in the network with its associated meta-data to allow authorized users to decrypt it. However, in IoT networks, depending on use case, the existence of third party may not be possible.

An Attribute-Based Encryption (ABE) scheme for resource-constrained sensors has been proposed in [180,181]. The idea consists of caching an encrypted version of the content in CS. The encryption is based on a set of attributes that a collection of users have. These different users are allowed to decrypt and access the content based on their access credentials. By using ABE scheme, the content producer will encrypt the content once rather than encrypting it separately for each user using their public key. Managing the users list and actively changing keys based on user join and leave in challenging, especially in highly dynamic IoT networks. Zhu et al. [182] proposed an edge re-encryption-based access control, where the main idea is encryption of content using a symmetric key, while the key used to encrypt the content is encrypted twice, by the content producer as well as by the edge router. The scheme allows the user to fetch the content key from the network rather than the original producer, hence the trust on edge router is critical in the system and may be considered as a weak design point. Moreover, the authors did not discuss how access control rules may be updated after publishing content.

Privacy preservation: Privacy issues and attacks may target all of ICN devices such as providers, consumers, intermediate, and replica nodes. Work in [25] provided a comprehensive survey about various attacks. However, it is observed that very little research work in the area of IoT is available. Sicari et al. [183] proposed a secure IoT–ICN architecture, as a way to guarantee security and privacy in different ICN phases such as device discovery, naming, and content delivery. In the proposed architecture, a suitable trust model has been discussed based on different IoT entities and relationships. Also, secure content delivery for sensitive content with access control has been defined in the proposed architecture. However, the authors did not show any implementation, evaluation, or validation details.

Further, in contrast to IP address where it is easy to track *what* content has been requested and by *whom*, in NDN, only tracking *what* content is requested is possible. Hence, to provide high privacy level, encrypting both content and its name is needed. Dibenedetto et al. [184] proposed an anonymous application design on top of NDN, by borrowing features from the Tor project [185], providing both asymmetric and session-based privacy and anonymity for NDN traffic. Although the idea is interesting if implemented, more efforts are needed to show the effectiveness of the solution with realistic privacy-based scenarios, and the performance in real/large scale IoT networks.

Summary: Security and privacy are one of the most critical topics in the whole networking area. Various solutions have been proposed addressing ICN security issues. Most of solutions and algorithms are not suitable for IoT devices due to their limitation in processing and memory. Future research needs to explore IoT security and privacy, proposing suitable crypto-system that may be more efficient for IoT environments.

10. Mobility in IoT and ICN

In ICN, mobile users have better data access compared to mobile IP users, as they are not required to repeatedly acquire a new IP address when connecting in a new network [21,27,186]. The desired data may be readily available in the new network [187–190]. Combining the NDN receiver-driven model and the content-location independence, the mobile node can simply re-issue the lost requests during mobility, and can benefit from distributed network caching. In the following, we detail IoT specific mobility solutions.

Data producer mobility: When a consumer moves from a network to another, it can simply re-ask for the missed content during the mobility. However, the mobility of the content provider is a challenging issue. Jiang et al. [191] addressed the producer mobility, where they proposed a DNS-based technique to map the content and locator. They extended interest packet by adding a *Locator* tag and use it in the forwarding strategy, while using the content name as an identifier in the CS/PIT matching processes. Kite [192] has designed a data producer mobility mechanism by leveraging state in PIT table to reach mobile nodes. The correspondent node contacts an anchor node which is not mobile, that could be the home agent of the mobile producer node via an interest. To reach the anchor node, the interest packet follows the requesting faces recorded in PIT table. Due to the use of a pre-defined anchor, the mechanism requires significant overhead to build and maintain the traces especially when the number of mobile nodes increases. Also, by using public accessible PIT entries, the solution opens more security risk such as flooding attacks. Authors in [193,194] proposed a locator-based mobility approach. The approach consists of assigning a unique locator to each access router, enabling in-network caching, and adding additional information (e.g., outgoing face, mobility status, locator) to each FIB entry. Data packet is extended by adding an outgoing FIB interface in order to keep track of the provider mobility status and force the interest requests to be delivered to the original provider rather than fetching an old content version from cache stores. Lehmann et al. [195] combined in-network caching and NDN forwarding strategy to push different version of the content proactively in the network. By using the distributed in-network caching, any node in the network may reply with content request and solve the producer reachability during mobility. However, the main drawback of this mechanism is related to the nature of real-time/dynamic data generation, and in case of replica node mobility.

Nour et al. [82] addressed the producer and replica sensors mobility in an AAL environment. The authors proposed to track the node movement or unavailability in Local Node Table (LNT) by different timers. Also, they incorporated in-network caching to enhance the edge node

Table 8
Security solutions using ICN in IoT.

Aspect	Ref.	Summary	Architecture	Year
Content security	[173]	Authentication and authorization scheme for resource-constrained devices using PANA and EAP protocols.	ICN	2016
	[174]	A secure and scalable framework for lightweight authentication, secure onboarding, and hierarchical routing using asymmetric cryptographic.	NDN	2018
	[175]	Compared MQTT and CoAP vs. NDN from the perspective of network/data security and attacks in IoT applications.	NDN	2018
	[176]	Design an initial Blockchain-based architecture to secure IoT network from different attacks in Named Data Networks.	NDN	2018
	[177]	A distributed low-rate denial-of-service attack mitigation scheme for resource-constrained devices.	NDN	2019
	[178]	A secure CCN framework for IoT applications with a certificate-less public key infrastructure.	CCN	2019
Access control	[179]	An ICN access control enforcement mechanism using a trusted third party with benefits of flat names.	ICN	2016
	[180,181]	An attribute-based encryption scheme for resource-constrained devices, where all attributes must be defined by the user.	ICN	2017
	[182]	An edge re-encryption-based access control scheme, where the content is encrypted using symmetric double-encrypted keys.	NDN	2019
Privacy	[183]	A secure IoT–ICN architecture to guarantee security and privacy in different ICN communication phases.	ICN	2017
	[184]	An anonymous application design on top of NDN to provide anonymous communication, inspired from Tor project.	NDN	2011

mobility, by caching the received data and sending it back to the new edge node. All edge things are connected through a backbone network. In a similar way, all information about the subscription and management will be transferred to the new node in case of edge thing/node mobility. Compagno et al. [196] focused on security in mobility. They proposed a prefix-attestation mechanism to secure producer mobility. Instead of using name-based approach, the moved producer is authenticated by a Registration Server, that verifies the announced prefix's ownership by the mobile node, after that the server decides either to validate the prefixes or not. Hence, consumer cannot be sure if content is coming from a legitimate entity or not. Meddeb et al. [197] proposed an adaptive forwarding scheme to handle the link recovery and thus support producer mobility in IoT environment. The idea consists of updating the forwarding information in the intermediate nodes after producer mobility, and thus recover the request paths. However, this scheme may producer extra overhead in high mobility situations such as vehicular networks. An et al. [198] designed a light-weight content delivery scheme for IoT to handle the producer/gateway mobility. The authors proposed to learn forwarding information from the control packets and embed it in each packet before transmission. However, the applicability of such a scheme in real and large-scale scenarios has not been investigated.

Summary: ICN provides a new perspective on mobility support in IoT environments, while most of research is focused on producer mobility part. However, naming and routing are also related to the mobility, where scalable naming and routing schemes are needed to support large-scale IoT networks. Furthermore, handling both consumer and provider mobility requires a management solution that may discover the mobile content and deliver it to the mobile consumer with short delay.

11. Wireless IoT networks

The wireless technology plays an important role in IoT communication. Most of IoT devices have wireless capabilities. However, due to the native design of wireless network, using ICN in wireless IoT is not similar to regular ICN. In the following, we discuss the existing efforts in wireless IoT–ICN.

Abidy et al. [199] proposed data collection and aggregation mechanism in wireless sensor networks using CCNx protocol. They implemented the proposed solution in Contiki operating system, using hierarchical names with no limitation in length or number of components. Also, no naming structure is used, and the application developer has the ability to design its own naming semantic and conventions. The main benefits are to reduce the duplicate packets while broadcasting the interest, and provide less overhead. However, the work considers only static nodes with high complexity in the matching process. Amadeo et al. [200] addressed the problem of content retrieval from different IoT producers in a wireless sensor environment. To answer the question of reliability and duplicated content generated by one interest, a one-hop far node from the consumer performs a multi-source content retrieval, which is achieved by using a common name prefix in the interest name. Further, the data packets include an additional name component to identify the producer, while the PIT entry will not be removed after satisfying the first interest, rather it is kept active until the lifetime expires. This allows forwarding of multiple data packets. Hail et al. [201] proposed a distributed probabilistic caching strategy namely pCASTING. It considers a multi-hop wireless loT system, and takes the data freshness parameter, wireless node characteristics such as energy level and storage capabilities into consideration. By using these metrics, it computes a distributed caching probability, without any need of signaling information from nodes. The simulation experiments show that the proposed strategy decreases the energy usage with low content retrieval delays compared to other NDN strategies. Abane et al. [202] presented NDN-over-ZigBee design aiming to integrate IoT. Running NDN over ZigBee may provide better support for wireless IoT applications with low power consumption. However, the proposed design introduces a considerable time to deliver the content.

Wireless technologies aim to integrate the real IoT devices with the digital world, while ICN aims to provide communication between devices and services. Merging wireless IoT with ICN is an important topic especially in the earlier design of IoT–ICN. Similarly, hybrid IoT networks using wired and wireless communication require careful designing and optimization. Consequently, more research efforts must be carried in such areas.

12. What is next?

ICN has been designed on the premise of content centric nature of modern applications in Internet. Although there has been significant research done in various aspects of ICN, real world deployment is yet to begin. It is important to note that, many of the communication properties proposed in literature, should be integrated into the core design, rather than implemented as add-on protocols. Similarly, it is equally important to identify the challenges across the different ICN components, from the perspective of IoT. In the following, we discuss

Table 9
Summary of future IoT–ICN research directions.

Aspect	Challenges	Future research possibilities
Naming & Name resolution	How to monitor and manage IoT devices. Distinction between distributed services running on many devices. Long name compared to content size. Dynamic content naming. Preserve content ownership and copyrights.	Naming IoT device/sensor. Naming IoT services, that allow one-request to many-services. Use variable length naming schemes. Use of blockchain to build NRS to handle security, content identification, copyright and ownership.
In-network caching	What content should be cached? Content manipulation in cache store. On which node the cache should be enabled?	Traffic class-based caching strategy. Energy-saving replacement strategy. Weight function-based caching performance.
Mobility	Critical data delivery process in case of producer mobility. Data delivery in case of closer replica-node movement. Streaming and subscription delivery in mobility scenarios.	Synchronize the name resolution system with the new location of producer, or update the intermediate routers. Optimal near-caching selection based on node stability.
Publisher–Subscriber	Native push-based communication support without changing architecture primitives or overhead. Secure group communication among active subscribers.	Developing semi-persistent communication model. Deployment of efficient group key mechanism over the pub–sub protocol. Efficient solutions of topic-based and content-specific subscriptions systems at application level.
Security	Thing/content authentication. Public key cryptography on resource constrained devices.	Content-based authentication mechanisms. Designing lightweight crypto-systems.
Scalability	Optimization of large routing and caching tables. Optimizing time consuming lookup operation due to long names.	Lightweight/scalable heuristic naming lookup methods. Use of variable length naming scheme.
Deployment & Adoption	Transition from IP-based network to ICN-based network. Queries transiting on IP networks.	Running ICN on top of TCP/IP protocol suite. Running IP over an ICN access network. Translation between IP addresses and content names.
Business models	Developing new business models for ICN network. Improve the revenue of different network actors. Preserving the copyright and ensuring money flow.	Use of Blockchain technology to design a distributed and effective business model. Integrate smart contract concept to ensure auto-code execution.

major challenges for ICN over IoT, and highlight different guidelines and research directions. Table 9 provides a summary of these research directions.

12.1. Naming

One of the most crucial design choices for ICN in IoT architecture is the naming, not only because its the identifier of the content but it is the foundation for other functionalities such as forwarding, caching, mobility, security as well as scalability. NDN uses hierarchical, human-readable English-language names. But, developers are able to choose the naming model and scheme for their applications. In addition, NDN project recommended naming conventions [203] to enable interoperability at network and application layers.

Naming the IoT devices/sensors is also necessary in IoT environment, especially in monitoring and management context. As far as the data is concerned in IoT, naming the service that offers the content is also necessary to distinguish between different services running on one or many devices. Moreover, the size of data generated by IoT services is often smaller than the naming itself. This creates overhead, requiring better optimization solutions. Finally, naming dynamic content is also a challenging issue in the context of IoT–ICN. Solutions based on hash-based content name are suitable for large content where the content verification is important but not suitable for dynamic content in IoT–ICN.

In large-scale IoT networks, the same content may be published multiple times, thus multiple names will be assigned to each version. Consequently, the routing tables will have many entries with different names for the same content, and the cache store may end up caching different content which is in fact the same content (just with a different name). For this, an efficient mechanism to bind the name with the content is needed to avoid such problems.

12.2. Name resolution system

In addition to naming challenges, a name resolution system is required to handle naming with high scalability features. Since IoT environment comprises of billions of things, data, and services, mapping a name with the appropriate content/service is also required with a high level of trust and interoperability with the existing ICN/IP-based solutions. Furthermore, different IoT applications require specific features to be embedded in the naming resolution system. We find that *Smart Cities and Smart Home* resolution system requires privacy and access-control supports over different content and services with services and resources ownership identification. Smart grids require real-time control, while smart transportation systems requires a system able to handle extreme node mobility with short latency. Smart healthcare needs real-time interaction features within different applications and patients.

Hence, name and name resolution has to be either specialized but interoperable, or standardized but highly efficient for all.

12.3. In-network caching

Various caching strategies have been proposed for ICN, but none of them address IoT requirements in detail. Mostly, in an IoT environment, some data has short lifetime, whereas some data is used only once. Hence, an adequate caching policy based on traffic class is needed to decide which data should be cached. An optimal replacement strategy that should not affect the node energy and performance is also desired. Moreover, which node should be allowed to cache data needs to be addressed since most IoT devices are considered resources-constrained with limitation in memory, computations, and energy. Hence, a weight function that takes into consideration different factors such as CPU, energy, and memory can be used to evaluate the caching possibility on a node.

12.4. Mobility

An IoT environment mostly comprises of mobile devices, including vehicular devices and health sensors attached to human body. Mobility supports in IoT–ICN is a key requirement toward a stable and reliable architecture. The native design of ICN supports mobility by simply re-issuing any unsatisfied requested. However, this is a challenging question in case of both producer and consumer mobility. In case of data producer mobility, a scalable naming resolution system is required with an efficient mechanism to update the entire system, or updating intermediate forwarder with the new location of node. Moreover, when a cache store moves, probabilistic and optimization caching mechanisms are needed to select the nearest and stable caching node to consumers. Finally, handling consumer mobility with re-sending interests is not an optimal solution, as it ends up with interest looping and overhead. Thus, mapping and management mechanisms are required with efficient data structures and inter-node communication to support streamed and subscribed data.

12.5. Publisher/subscriber

The receiver-driven data transmission mechanism in NDN does not natively support the push-based communication, while most IoT applications and scenarios require it. Many NDN research efforts propose push-based support either by changing the NDN's Interest-Data exchange model or initializing the subscribers request by consumers which leads to a huge overhead. Hence, an efficient Publish/Subscribe communication model is required with support for both *periodic* and *event triggered* communication such as semi-persistent communication model, with a critical security design to ensure user authentication and secure data communication among members. Another important direction is to have efficient topic-specific and content specific solutions at application level, which can capitalize on one-interest on-data model. Topic may have many different individual contents, where each content may update over time. Hence, this dual challenge will be an interesting issue for IoT networks.

12.6. Security

IoT services are not open to public users to access and fetch information. Hence, authenticated consumer interests should be applied in this context, by leveraging access-control over the thing. Furthermore, most of devices in IoT environments are resources constrained with low CPU and memory capabilities, and it is hard to use public key cryptography. Thus, flexible and lightweight crypto-systems are required, with low cost trust models.

12.7. ICN scalability (in IoT perspective)

Considering the increasing number of IoT devices that produce huge amount of content, a scalable ICN architecture for IoT ecosystem is mandatory where all things over the network produce and consume content regardless of its location. In this regard, large routing tables will be produced with many replacement operations in the cache store. Hence, to accelerate the look-up process and reduce the table size, lightweight and scalable naming look-up methods are needed, with variable length naming scheme. Similarly, to avoid content adding/evicting on different cache stores, an optimized/energy-saving caching placement strategy and replacement policy are required.

12.8. Deployment & adoption

The deployment of ICN with/over IP-based networks has four modes: (1) A clean-state mode: only ICN protocol is deployed, (2) Overlay mode: running ICN on top of IP/TCP/UDP, (3) Underlay mode: running IP-over-ICN, or (4) Co-existence: where the network stack should support both IP and ICN. Each deployment mode has its pros and cons, the overlay mode limits the performance of ICN and limits it to the performance of the under-running protocol. Whereas, the co-existing mode requires re-implementing of the networking stack. IP-over-ICN design is a potential deployment solution especially for access networks such as IoT and sensor networks. In this case, the edge network can use ICN to locate content, while the legacy application can still operate on IP. Whereas, an ICN-over-IP solution may be for large scale networks, where infrastructural changes may not be possible. Transitioning to ICN requires a careful design and structuring of ICN sockets, with additional services to support the interoperability.

12.9. Business models

In the current host-centric model, all requests must be satisfied by the original content producer that has full control over the content. However, in ICN, the network layer can cache and serve the content transparently to different requests regardless of the availability of the producer. This decoupling of content and its location provides open content distribution. Whereas, all revenue generation is based on content. Thus, new application design conventions are required to adapt ICN with the business model. In addition to content producer and consumers, active and revue generating elements for dedicated cache stores and content discoverers may be beneficial. A completely distributed platform to manage the content revenue is highly desired, which can track content consumption with high degree of granularity. Content ownership and copyright should be respected during the different phase of content publishing, delivery, and consumption. However, this should not be at the cost of consumer privacy.

13. Conclusion

The current host-centric model faces various challenges, such as, scalability, mobility, addressing, security, etc., primarily due to the sharp increase in number of devices and application in the Internet. The other factor that has triggered re-thinking of host-centric model is the nature of applications and the demand for content by the users. The content-centric paradigm gives a fresh perspective to communication, by eliminating the need to find a specific destination machine in the network. Internet of Things is a major driving force behind content based applications, with billions of devices and large scale data generation. In this survey, we present and discuss the use of ICN as a communication enabler for IoT. The core focus is to analyze different solutions available in literature which utilize ICN-based communication for specific IoT use cases. The requirements of different IoT scenarios vary to a great degree, hence solutions which work in one environment are rendered useless in another. High mobility of vehicular networks compared to static nature of weather monitoring systems requires drastically different solutions, even if they are part of a single smart city network. The survey also focuses on different ICN specific perspective, such as, naming, caching, security, etc., and discusses how these individual elements effect ICN communication. In conclusion, we believe that significant research is still required in individual aspects, as well as from a holistic use case perspective, to reap the benefits of content centric communication in IoT. We have identified a number of research directions and challenges in this regard which can guide the community toward better ICN-based IoT solutions.

Acknowledgments

The work of F. Li is partially supported by the National Natural Science Foundation of China No. 61772077, 61370192, and the Beijing Natural Science Foundation No. 4192051. We would like to thank the editors and reviewers for their comments and suggestions, which helped us to improve the quality, content, and presentation of this article.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: A survey on enabling technologies, protocols, and applications, IEEE Commun. Surv. Tutor. 17 (4) (2015) 2347–2376, http://dx.doi.org/10.1109/COMST.2015.2444095.

[2] J. Choi, J. Han, E. Cho, T. Kwon, Y. Choi, A survey on content-oriented networking for efficient content delivery, IEEE Commun. Mag. 49 (3) (2011) http://dx.doi.org/10.1109/MCOM.2011.5723809.

[3] Smart Nation Singapore Project, http://www.smartnation.sg, 2018, Accessed: 2018-05-18.

[4] Qualcomm and Ford: C-V2X Global Initiative, https://www.qualcomm.com/news/releases/2018/01/09/qualcomm-and-ford-collaborate-c-v2x-global-initiative-improve-vehicle, 2018, Accessed: 2018-05-18.

[5] Z. Sheng, S. Yang, Y. Yu, A.V. Vasilakos, J. Mccann, K. Leung, A survey on the IETF protocol suite for the internet of things: standards, challenges, and opportunities, IEEE Wirel. Commun. 20 (6) (2013) 91–98, http://dx.doi.org/10.1109/MWC.2013.6704479.

[6] E.T. Chen, The internet of things: Opportunities, issues, and challenges, in: The Internet of Things in the Modern Business Environment, IGI Global, 2017, pp. 167–187, http://dx.doi.org/10.4018/978-1-5225-2104-4.ch009.

[7] Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions), https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, 2018, Accessed: 2018-05-18.

[8] J. Pan, S. Paul, R. Jain, A survey of the research on future internet architectures, IEEE Commun. Mag. 49 (7) (2011) http://dx.doi.org/10.1109/MCOM.2011.5936152.

[9] M. Amadeo, C. Campolo, J. Quevedo, D. Corujo, A. Molinaro, A. Iera, R.L. Aguiar, A.V. Vasilakos, Information-centric networking for the internet of things: challenges and opportunities, IEEE Network 30 (2) (2016) 92–100, http://dx.doi.org/10.1109/MNET.2016.7437030.

[10] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, B. Ohlman, A survey of information-centric networking, IEEE Commun. Mag. 50 (7) (2012) http://dx.doi.org/10.1109/MCOM.2012.6231276.

[11] T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K.H. Kim, S. Shenker, I. Stoica, A data-oriented (and beyond) network architecture, in: ACM SIGCOMM Comput. Commun. Rev., Vol. 37, 2007, pp. 181–192, http://dx.doi.org/10.1145/1282427.1282402.

[12] N. Fotiou, P. Nikander, D. Trossen, G.C. Polyzos, Developing information networking further: From PSIRP to PURSUIT, in: Conference on Broadband, Springer, 2010, pp. 1–13, http://dx.doi.org/10.1007/978-3-642-30376-0_1.

[13] C. Dannewitz, D. Kutscher, B. Ohlman, S. Farrell, B. Ahlgren, H. Karl, Network of information (netinf) - an information-centric networking architecture, Comput. Commun. 36 (7) (2013) 721–735, http://dx.doi.org/10.1016/j.comcom.2013.01.009.

[14] F. Oehlmann, Content-centric networking, Seminar FI & IITM: Network Archit. Serv. 43 (2013) 11–18, http://dx.doi.org/10.2312/NET-2013-02-1_06.

[15] L. Zhang, D. Estrin, J. Burke, V. Jacobson, J.D. Thornton, D.K. Smetters, B. Zhang, G. Tsudik, D. Massey, C. Papadopoulos, Named Data Networking (NDN) Project, Technical Report NDN-0001, Xerox Palo Alto Research Center-PARC, 2010.

[16] O. Waltari, J. Kangasharju, Content-centric networking in the internet of things, in: IEEE Annual Consumer Communications & Networking Conference (CCNC), 2016, pp. 73–78, http://dx.doi.org/10.1109/CCNC.2016.7444734.

[17] M. Amadeo, C. Campolo, A. Iera, A. Molinaro, Named data networking for iot: An architectural perspective, in: European Conference on Networks and Communications (EuCNC), IEEE, 2014, pp. 1–5, http://dx.doi.org/10.1109/EuCNC.2014.6882665.

[18] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications, IEEE Internet Things J. 4 (5) (2017) 1125–1142, http://dx.doi.org/10.1109/JIOT.2017.2683200.

[19] M.F. Bari, S.R. Chowdhury, R. Ahmed, R. Boutaba, B. Mathieu, A survey of naming and routing in information-centric networks, IEEE Commun. Mag. 50 (12) (2012) http://dx.doi.org/10.1109/MCOM.2012.6384450.

[20] A.V. Vasilakos, Z. Li, G. Simon, W. You, Information centric network: Research challenges and opportunities, J. Netw. Comput. Appl. 52 (2015) 1–10, http://dx.doi.org/10.1016/j.jnca.2015.02.001.

[21] G. Tyson, N. Sastry, I. Rimac, R. Cuevas, A. Mauthe, A survey of mobility in information-centric networks: Challenges and research directions, in: ACM Workshop on Emerging Name-Oriented Mobile Networking Design-Architecture, Algorithms, and Applications, 2012, pp. 1–6, http://dx.doi.org/10.1145/2248361.2248363.

[22] G. Xylomenos, C.N. Ververidis, V.A. Siris, N. Fotiou, C. Tsilopoulos, X. Vasilakos, K.V. Katsaros, G.C. Polyzos, A survey of information-centric networking research, IEEE Commun. Surv. Tutor. 16 (2) (2014) 1024–1049, http://dx.doi.org/10.1109/SURV.2013.070813.00063.

[23] I. Abdullahi, S. Arif, S. Hassan, Survey on caching approaches in information centric networking, J. Netw. Comput. Appl. 56 (2015) 48–59, http://dx.doi.org/10.1016/j.jnca.2015.06.011.

[24] E.G. AbdAllah, H.S. Hassanein, M. Zulkernine, A survey of security attacks in information-centric networking, IEEE Commun. Surv. Tutor. 17 (3) (2015) 1441–1454, http://dx.doi.org/10.1109/COMST.2015.2392629.

[25] R. Tourani, S. Misra, T. Mick, G. Panwar, Security, privacy, and access control in information-centric networking: A survey, IEEE Commun. Surv. Tutor. (2017) http://dx.doi.org/10.1109/COMST.2017.2749508.

[26] D. Saxena, V. Raychoudhury, N. Suri, C. Becker, J. Cao, Named data networking: a survey, Comput. Sci. Rev. 19 (2016) 15–55, http://dx.doi.org/10.1016/j.cosrev.2016.01.001.

[27] Y. Zhang, A. Afanasyev, J. Burke, L. Zhang, A survey of mobility support in named data networking, in: IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2016, pp. 83–88, http://dx.doi.org/10.1109/INFCOMW.2016.7562050.

[28] H. Khelifi, S. Luo, B. Nour, H. Moungla, Y. Faheem, R. Hussain, A. Ksentini, Named data networking in vehicular ad hoc networks: State-of-the-art and challenges, IEEE Commun. Surv. Tutor. (2019) http://dx.doi.org/10.1109/COMST.2019.2894816.

[29] S. Arshad, M.A. Azam, M.H. Rehmani, J. Loo, Recent advances in information-centric networking based internet of things (ICN-iot), IEEE Internet Things J. (2018) http://dx.doi.org/10.1109/JIOT.2018.2873343.

[30] D. Kutscher, S. Eum, K. Pentikousis, I. Psaras, D. Corujo, D. Saucez, T.C. Schmidt, R.. Matthias Waehlisch, Information-Centric Networking (ICN) Research Challenges, 2016.

[31] K. Pentikousis, B. Ohlman, D. Corujo, G. Boggia, G. Tyson, E.B. Davies, A. Molinaro, S. Eum, Information-Centric Networking: Baseline Scenarios, RFC 7476, 2015.

[32] O. Hahm, E. Baccelli, H. Petersen, N. Tsiftes, Operating systems for low-end devices in the internet of things: a survey, IEEE Internet Things J. 3 (5) (2016) 720–734, http://dx.doi.org/10.1109/JIOT.2015.2505901.

[33] P. Levis, S. Madden, J. Polastre, R. Szewczyk, K. Whitehouse, A. Woo, D. Gay, J. Hill, M. Welsh, E. Brewer, et al., Tinyos: An operating system for sensor networks, in: Ambient Intelligence, Springer, 2005, pp. 115–148, http://dx.doi.org/10.1007/3-540-27139-2_7.

[34] A. Dunkels, B. Gronvall, T. Voigt, Contiki-a lightweight and flexible operating system for tiny networked sensors, in: Annual IEEE International Conference on Local Computer Networks (LCN), IEEE, 2004, pp. 455–462, http://dx.doi.org/10.1109/LCN.2004.38.

[35] E. Baccelli, O. Hahm, M. Gunes, M. Wahlisch, T.C. Schmidt, RIOT OS: Towards an OS for the internet of things, in: IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2013, pp. 79–80, http://dx.doi.org/10.1109/INFCOMW.2013.6970748.

[36] Ubuntu Core, https://www.ubuntu.com/core, 2018, Accessed: 2018-05-18.

[37] C. Withanage, R. Ashok, C. Yuen, K. Otto, A comparison of the popular home automation technologies, in: Innovative Smart Grid Technologies-Asia (ISGT Asia), IEEE, 2014, pp. 600–605, http://dx.doi.org/10.1109/ISGT-Asia.2014.6873860.

[38] T. Kivinen, P. Kinney, IEEE 802.15.4 Information Element for the IETF, RFC 8137, 2017, https://rfc-editor.org/rfc/rfc8137.txt.

[39] C. Shao, D. Hui, R. Pazhyannur, F. Bari, R. Zhang, IEEE 802.11 Medium Access Control (MAC) Profile for Control and Provisioning of Wireless Access Points (CAPWAP), RFC 7494, 2015, https://rfc-editor.org/rfc/rfc7494.txt.

[40] J. Nieminen, T. Savolainen, M. Isomaki, B. Patil, Z. Shelby, C. Gomez, IPv6 over BLUETOOTH(R) Low Energy, RFC 7668, 2015. https://rfc-editor.org/rfc/rfc7668.txt.

[41] Z. Shelby, C. Bormann, 6LoWPAN: The wireless embedded Internet, Vol. 43, John Wiley & Sons, 2011.

[42] T.S. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G.N. Wong, J.K. Schulz, M. Samimi, F. Gutierrez, Millimeter wave mobile communications for 5g cellular: It will work!, IEEE Access 1 (2013) 335–349, http://dx.doi.org/10.1109/ACCESS.2013.2260813.

[43] D.P. Arjunwadkar, Introduction of NDN with comparison to current internet architecture based on TCP/IP, Int. J. Comput. Appl. 105 (5) (2014) 31–35, http://dx.doi.org/10.5120/18376-9536.

[44] A. Passarella, A survey on content-centric technologies for the current internet: Cdn and p2p solutions, Comput. Commun. 35 (1) (2012) 1–32, http://dx.doi.org/10.1016/j.comcom.2011.10.005.

[45] S. Arshad, B. Shahzaad, M.A. Azam, J. Loo, S.H. Ahmed, S. Aslam, Hierarchical and flat based hybrid naming scheme in content-centric networks of things, IEEE Internet Things J. 5 (2) (2018) 1070–1080, http://dx.doi.org/10.1109/JIOT.2018.2792016.

[46] M. Baugher, B. Davie, A. Narayanan, D. Oran, Self-verifying names for read-only named data, in: IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2012, pp. 274–279, http://dx.doi.org/10.1109/INFCOMW.2012.6193505.

[47] O. Ascigil, S. Ree, G. Xylomenos, I. Psaras, G. Pavlou, A keyword-based ICN-iot platform, in: ACM Conference on Information-Centric Networking (ICN), 2017, pp. 22–28, http://dx.doi.org/10.1145/3125719.3125733.

[48] B. Nour, K. Sharif, F. Li, H. Moungla, Y. Liu, M2hav: A standardized ICN naming scheme for wireless devices in internet of things, in: International Conference on Wireless Algorithms, Systems, and Applications (WASA), Springer, 2017, pp. 289–301, http://dx.doi.org/10.1007/978-3-319-60033-8_26.

[49] I.U. Din, S. Hassan, M.K. Khan, M. Guizani, O. Ghazali, A. Habbal, CaChing in information-centric networking: Strategies, challenges, and future research directions, IEEE Commun. Surv. Tutor. 20 (2) (2018) 1443–1474, http://dx.doi.org/10.1109/COMST.2017.2787609.

[50] C. Bernardini, T. Silverston, A. Vasilakos, Caching Strategies for Information Centric Networking: Opportunities and Challenges, arXiv preprint arXiv:1606.07630, 2016.

[51] C. Bernardini, T. Silverston, O. Festor, A comparison of caching strategies for content centric networking, in: IEEE Global Communications Conference (GLOBECOM), 2015, pp. 1–6, http://dx.doi.org/10.1109/GLOCOM.2015.7417007.

[52] Z. Zhang, Y. Yu, H. Zhang, E. Newberry, S. Mastorakis, Y. Li, A. Afanasyev, L. Zhang, An overview of security support in named data networking, IEEE Commun. Mag. 56 (11) (2018) 62–68, http://dx.doi.org/10.1109/MCOM.2018.1701147.

[53] Y. Yu, A. Afanasyev, D. Clark, V. Jacobson, L. Zhang, et al., Schematizing trust in named data networking, in: ACM International Conference on Information-Centric Networking, 2015, pp. 177–186, http://dx.doi.org/10.1145/2810156.2810170.

[54] P. He, Y. Wan, Q. Xia, S. Li, J. Hong, K. Xue, LASA: Lightweight, auditable and secure access control in ICN with limitation of access times, in: IEEE International Conference on Communications (ICC), 2018, pp. 1–6, http://dx.doi.org/10.1109/ICC.2018.8422829.

[55] N. Fotiou, B.A. Alzahrani, Rendezvous-based access control for information-centric architectures, Int. J. Netw. Manag. 28 (1) (2018) 1–11, http://dx.doi.org/10.1002/nem.2007.

[56] 4WARD, http://www.4ward-project.eu/, 2008, Accessed: 2018-05-18.

[57] FP7 SAIL Project, http://www.sail-project.eu/, Accessed: 2018-05-18.

[58] G. Garcia, A. Beben, F.J. Ramon, A. Maeso, I. Psaras, G. Pavlou, et al., COMET: Content mediator architecture for content-aware networks, in: Future Network Mobile Summit, 2011.

[59] N.B. Melazzi, S. Salsano, A. Detti, G. Tropea, L. Chiariglione, A. Difino, et al., Publish/subscribe over information centric networks: A standardized approach in convergence, in: Future Network Mobile Summit, 2012.

[60] I. Seskar, K. Nagaraja, S. Nelson, D. Raychaudhuri, Mobilityfirst: Future internet architecture project, in: Asian Internet Engineering Conference, ACM, 2011, http://dx.doi.org/10.1145/2089016.2089017.

[61] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, P. Crowley, C. Papadopoulos, L. Wang, B. Zhang, et al., Named data networking, ACM SIGCOMM Comput. Commun. Rev. 44 (3) (2014) 66–73, http://dx.doi.org/10.1145/2656877.2656887.

[62] A. Rayes, M. Morrow, D. Lake, Internet of things implications on ICN, in: International Conference on Collaboration Technologies and Systems (CTS), IEEE, 2012, pp. 27–33, http://dx.doi.org/10.1109/CTS.2012.6261023.

[63] W. Shang, Y. Yu, R. Droms, L. Zhang, Challenges in IoT networking via TCP/IP architecture, Technical Report, NDN Project, Tech. Rep. NDN-0038, 2016.

[64] 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: IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI), 2016, pp. 117–128, http://dx.doi.org/10.1109/IoTDI.2015.44.

[65] E. Baccelli, C. Mehlis, O. Hahm, T.C. Schmidt, M. Wählisch, Information centric networking in the iot: Experiments with NDN in the wild, in: International Conference on Information-Centric Networking, ACM, 2014, pp. 77–86, http://dx.doi.org/10.1145/2660129.2660144.

[66] A. Lindgren, F.B. Abdesslem, B. Ahlgren, O. Schelén, A.M. Malik, Design choices for the iot in information-centric networks, in: IEEE Consumer Communications & Networking Conference (CCNC), 2016, pp. 882–888, http://dx.doi.org/10.1109/CCNC.2016.7444905.

[67] Y. Zhang, D. Raychadhuri, L.A. Grieco, E. Baccelli, J. Burke, R. Ravindran, G. Wang, A. Lindgren, B. Ahlgren, O. Schelen, Design Considerations for Applying ICN to IoT, Internet-Draft, Internet Engineering Task Force, 2017, https://datatracker.ietf.org/doc/html/draft-zhang-icnrg-icniot-01, Work in Progress, Accessed: 2018-05-18.

[68] A. Lindgren, F.B. Abdesslem, B. Ahlgren, O. Schelen, A.M. Malik, Proposed Design Choices for IoT over Information Cen- tric Networking, Internet-Draft, Internet Engineering Task Force, 2015. URL: https://datatracker.ietf.org/doc/html/draft-lindgren-icnrg-designchoices-00, Work in Progress, Accessed: 2018-05-18.

[69] Y. Zhang, D. Raychadhuri, L.A. Grieco, S. Sabrina, H. Liu, S. Misra, R. Ravindran, G. Wang, ICN based Architecture for IoT, Internet-Draft, Internet Engineering Task Force, 2017. URL: https://datatracker.ietf.org/doc/html/draft-zhang-icnrg-icniot-architecture-01, Work in Progress, Accessed: 2018-05-18.

[70] A. Rao, O. Schelén, A. Lindgren, Performance implications for iot over information centric networks, in: ACM Workshop on Challenged Networks, 2016, pp. 57–62, http://dx.doi.org/10.1145/2979683.2979686.

[71] D. Corujo, R.L. Aguiar, I. Vidal, J. Garcia-Reinoso, K. Pentikousis, Research challenges towards a managed information-centric network of things, in: European Conference on Networks and Communications (EuCNC), IEEE, 2014, pp. 1–5, http://dx.doi.org/10.1109/EuCNC.2014.6882681.

[72] J. Quevedo, D. Corujo, R. Aguiar, A case for ICN usage in iot environments, in: IEEE Global Communications Conference (GLOBECOM), 2014, pp. 2770–2775, http://dx.doi.org/10.1109/GLOCOM.2014.7037227.

[73] G. Piro, I. Cianci, L.A. Grieco, G. Boggia, P. Camarda, Information centric services in smart cities, J. Syst. Softw. 88 (2014) 169–188, http://dx.doi.org/10.1016/j.jss.2013.10.029.

[74] S.H. Ahmed, S.H. Bouk, D. Kim, M. Sarkar, Bringing Named Data Networks into Smart Cities, John Wiley & Sons, Inc. Hoboken, NJ, USA, 2017, pp. 275–309, http://dx.doi.org/10.1002/9781119226444.ch10.

[75] T. Mochida, D. Nozaki, K. Okamoto, X. Qi, Z. Wen, T. Sato, K. Yu, Naming scheme using NLP machine learning method for network weather monitoring system based on ICN, in: International Symposium on Wireless Personal Multimedia Communications (WPMC), 2017, pp. 428–434, http://dx.doi.org/10.1109/WPMC.2017.8301851.

[76] M. Naeem, R. Ali, B.-S. Kim, S. Nor, S. Hassan, A periodic caching strategy solution for the smart city in information-centric internet of things, Sustainability 10 (7) (2018) 2576, http://dx.doi.org/10.3390/su10072576.

[77] R. Ravindran, T. Biswas, X. Zhang, A. Chakraborti, G. Wang, Information-centric networking based homenet, in: IFIP/IEEE International Symposium on Integrated Network Management (IM), IEEE, 2013, pp. 1102–1108.

[78] J. Burke, P. Gasti, N. Nathan, G. Tsudik, Securing instrumented environments over content-centric networking: the case of lighting control and NDN, in: IEEE Conference on Computer Communications Workshops (INFOCOM Wkshps), 2013, pp. 394–398, http://dx.doi.org/10.1109/INFCOMW.2013.6970725.

[79] M. Amadeo, C. Campolo, A. Iera, A. Molinaro, Information centric networking in iot scenarios: The case of a smart home, in: IEEE International Conference on Communications (ICC), 2015, pp. 648–653, http://dx.doi.org/10.1109/ICC.2015.7248395.

[80] M.A. Hail, S. Fischer, Iot for AAL: An architecture via information-centric networking, in: IEEE Global Communications Conference Workshops (GLOBECOM Wkshps), 2015, pp. 1–6, http://dx.doi.org/10.1109/GLOCOMW.2015.7414020.

[81] H. Zhang, Z. Wang, C. Scherb, C. Marxer, J. Burke, L. Zhang, C.F. Tschudin, Sharing mhealth data via named data networking, in: ACM Conference on Information-Centric Networking (ICN), 2016, pp. 142–147, http://dx.doi.org/10.1145/2984356.2984379.

[82] B. Nour, K. Sharif, F. Li, H. Moungla, A distributed ICN-based iot network architecture: An ambient assisted living application Case study, in: IEEE Global Communications Conference (IEEE GLOBECOM), 2017, http://dx.doi.org/10.1109/GLOCOM.2017.8255022.

[83] D. Saxena, V. Raychoudhury, Design and verification of an NDN-based safety-critical application: A Case study with smart healthcare, IEEE Trans. Syst. Man Cybern.: Syst. (2017) http://dx.doi.org/10.1109/TSMC.2017.2723843.

[84] J. Zhang, Q. Li, E.M. Schooler, Ihems: An information-centric approach to secure home energy management, in: IEEE International Conference on Smart Grid Communications (SmartGridComm), 2012, pp. 217–222, http://dx.doi.org/10.1109/SmartGridComm.2012.6485986.

[85] 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, http://dx.doi.org/10.1109/MNET.2014.6843233.

[86] E. Oh, Secure information network design strategies for information-centric future smart grid, in: Applied Science and Engineering for Better Human Life, 2016, http://dx.doi.org/10.3390/s17112512.

[87] M. Amadeo, C. Campolo, A. Molinaro, Information-centric networking for connected vehicles: a survey and future perspectives, IEEE Commun. Mag. 54 (2) (2016) 98–104, http://dx.doi.org/10.1109/MCOM.2016.7402268.

[88] S. Signorello, M.R. Palattella, L.A. Grieco, Security challenges in future NDN-enabled VANETs, in: IEEE Trustcom/BigDataSE/ISPA, 2016, pp. 1771–1775, http://dx.doi.org/10.1109/TrustCom.2016.0272.

[89] D. Saxena, V. Raychoudhury, C. Becker, Implementation and performance evaluation of name-based forwarding schemes in v-NDN, in: International Conference on Distributed Computing and Networking, ACM, 2017, p. 35, http://dx.doi.org/10.1145/3007748.3007766.

[90] M. Chowdhury, A. Gawande, L. Wang, Secure information sharing among autonomous vehicles in NDN, in: IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), IEEE, 2017, pp. 15–26.

[91] M. Chowdhury, A. Gawande, L. Wang, Anonymous authentication and pseudonym-renewal for VANET in NDN, in: ACM Conference on Information-Centric Networking (ICN), 2017, pp. 222–223, http://dx.doi.org/10.1145/3125719.3132111.

[92] S.H. Bouk, S.H. Ahmed, D. Kim, H. Song, Named-data-networking-based ITS for smart cities, IEEE Commun. Mag. 55 (1) (2017) 105–111, http://dx.doi.org/10.1109/MCOM.2017.1600230CM.

[93] S.H. Bouk, S.H. Ahmed, R. Hussain, Y. Eun, Named data networking's intrinsic cyber-resilience for vehicular CPS, IEEE Access 6 (2018) 60570–60585, http://dx.doi.org/10.1109/ACCESS.2018.2875890.

[94] A. Zanella, N. Bui, A. Castellani, L. Vangelista, M. Zorzi, Internet of things for smart cities, IEEE Internet Things J. 1 (1) (2014) 22–32, http://dx.doi.org/10.1109/JIOT.2014.2306328.

[95] N. Komninos, E. Philippou, A. Pitsillides, Survey in smart grid and smart home security: Issues, challenges and countermeasures, IEEE Commun. Surv. Tutor. 16 (4) (2014) 1933–1954, http://dx.doi.org/10.1109/COMST.2014.2320093.

[96] S.R. Islam, D. Kwak, M.H. Kabir, M. Hossain, K.-S. Kwak, The internet of things for health Care: A comprehensive survey, IEEE Access 3 (2015) 678–708, http://dx.doi.org/10.1109/ACCESS.2015.2437951.

[97] Y. Yan, Y. Qian, H. Sharif, D. Tipper, A survey on smart grid communication infrastructures: Motivations, requirements and challenges, IEEE Commun. Surv. Tutor. 15 (1) (2013) 5–20, http://dx.doi.org/10.1109/SURV.2012.021312.00034.

[98] S.-h. An, B.-H. Lee, D.-R. Shin, A survey of intelligent transportation systems, in: IEEE International Conference on Computational Intelligence, Communication Systems and Networks (CICN), 2011, pp. 332–337, http://dx.doi.org/10.1109/CICSyN.2011.76.

[99] A. Vahdat, D. Becker, Epidemic routing for partially connected ad hoc networks, Technical Report CS-200006, Duke University, 2000.

[100] T. Spyropoulos, K. Psounis, C.S. Raghavendra, Spray and wait: an efficient routing scheme for intermittently connected mobile networks, in: ACM SIGCOMM Workshop on Delay-Tolerant Networking, 2005, pp. 252–259, http://dx.doi.org/10.1145/1080139.1080143.

[101] F. Hou, X. Shen, An adaptive forwarding scheme for message delivery over delay tolerant networks, in: IEEE Global Telecommunications Conference, 2009, pp. 1–5, http://dx.doi.org/10.1109/GLOCOM.2009.5425746.

[102] G.C. Polyzos, N. Fotiou, Building a reliable internet of things using information-centric networking, J. Reliab. Intell. Environ. 1 (1) (2015) 47–58, http://dx.doi.org/10.1007/s40860-015-0003-5.

[103] S.S. Adhatarao, J. Chen, M. Arumaithurai, X. Fu, K. Ramakrishnan, Comparison of naming schema in ICN, in: IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), 2016, pp. 1–6, http://dx.doi.org/10.1109/LANMAN.2016.7548856.

[104] L. Bracciale, P. Loreti, A. Detti, R. Paolillo, N.B. Melazzi, Lightweight named object: an ICN-based abstraction for iot device programming and management, IEEE Internet Things J. (2019) 1, http://dx.doi.org/10.1109/JIOT.2019.2894969.

[105] S. Arshad, M.A. Azam, S.H. Ahmed, J. Loo, Towards information-centric networking (ICN) naming for internet of things (iot): the case of smart campus, in: International Conference on Future Networks and Distributed Systems (ICFNDS), ACM, 2017, p. 30, http://dx.doi.org/10.1145/3102304.3102345.

[106] Y. Yang, T. Song, Local naming service for named data networking of things, in: ACM Conference on Information-Centric Networking (ICN), 2017, pp. 190–191, http://dx.doi.org/10.1145/3125719.3132104.

[107] L. Melvix, V. Lokesh, G.C. Polyzos, Energy efficient context based forwarding strategy in named data networking of things, in: ACM Conference on Information-Centric Networking (ICN), 2016, pp. 249–254, http://dx.doi.org/10.1145/2984356.2988520.

[108] A. Marandi, T. Braun, K. Salamatian, N. Thomos, BFR: a bloom filter-based routing approach for information-centric networks, in: IFIP Networking Conference (IFIP Networking) and Workshops, IEEE, 2017, pp. 1–9, http://dx.doi.org/10.23919/IFIPNetworking.2017.8264842.

[109] A. Marandi, T. Braun, K. Salamatian, N. Thomos, Pull-based Bloom Filter-based Routing for Information-Centric Networks, arXiv preprint arXiv:1809.10948.

[110] A. Rodrigues, P. Steenkiste, A. Aguiar, Analysis and improvement of name-based packet forwarding over flat id network architectures, in: ACM Conference on Information-Centric Networking (ICN), ACM, 2018, http://dx.doi.org/10.1145/3267955.3267960.

[111] P. Moll, J. Janda, H. Hellwagner, Adaptive forwarding of persistent interests in named data networking, in: ACM Conference on Information-Centric Networking (ICN), 2017, http://dx.doi.org/10.1145/3125719.3132091.

[112] M. Antikainen, L. Wang, D. Trossen, A. Sathiaseelan, XBF: scaling up bloom-filter-based source routing, arXiv preprint arXiv:1602.05853, 2016.

[113] J. Tapolcai, J. Bíró, P. Babarczi, A. Gulyás, Z. Heszberger, D. Trossen, Optimal false-positive-free bloom filter design for scalable multicast forwarding, IEEE/ACM Trans. Netw. 23 (6) (2015) 1832–1845, http://dx.doi.org/10.1109/TNET.2014.2342155.

[114] B.A. Alzahrani, V.G. Vassilakis, M.J. Reed, Mitigating brute-force attacks on bloom-filter based forwarding, in: Conference on Future Internet Communications (CFIC), IEEE, 2013, pp. 1–7, http://dx.doi.org/10.1109/CFIC.2013.6566320.

[115] B.A. Alzahrani, V.G. Vassilakis, M.J. Reed, Selecting bloom-filter header lengths for secure information centric networking, in: International Symposium on Communication Systems, Networks & Digital Sign (CSNDSP), IEEE, 2014, pp. 628–633, http://dx.doi.org/10.1109/CSNDSP.2014.6923904.

[116] J. Quevedo, M. Antunes, D. Corujo, D. Gomes, R.L. Aguiar, On the application of contextual iot service discovery in information centric networks, Comput. Commun. 89 (2016) 117–127, http://dx.doi.org/10.1016/j.comcom.2016.03.011.

[117] O. Ascigil, V. Sourlas, I. Psaras, G. Pavlou, A native content discovery mechanism for the information-centric networks, in: ACM Conference on Information-Centric Networking (ICN), 2017, pp. 145–155, http://dx.doi.org/10.1145/3125719.3125734.

[118] J. Quevedo, D. Corujo, R. Aguiar, Consumer driven information freshness approach for content centric networking, in: IEEE Computer Communications Workshops (INFOCOM WKSHPS), 2014, pp. 482–487, http://dx.doi.org/10.1109/INFCOMW.2014.6849279.

[119] S. Vural, P. Navaratnam, N. Wang, C. Wang, L. Dong, R. Tafazolli, In-network caching of internet-of-things data, in: IEEE International Conference on Communications (ICC), 2014, pp. 3185–3190, http://dx.doi.org/10.1109/ICC.2014.6883811.

[120] C. Xu, X. Wang, Transient content caching and updating with modified harmony search for internet of things, Dig. Commun. Netw. (2018) http://dx.doi.org/10.1016/j.dcan.2018.10.002.

[121] B. Nour, K. Sharif, F. Li, H. Moungla, A.E. Kamal, H. Afifi, NCP: A near ICN Cache placement scheme for iot-based traffic class, in: IEEE Global Communications Conference (GLOBECOM), 2018.

[122] Z. Zhang, C.-H. Lung, I. Lambadaris, M. St-Hilaire, Iot data lifetime-based cooperative caching scheme for ICN-iot networks, in: IEEE International Conference on Communications (ICC), IEEE, 2018, pp. 1–7, http://dx.doi.org/10.1109/ICC.2018.8422100.

[123] D. Kim, S. Nam, J. Bi, I. Yeom, Efficient content verification in named data networking, in: ACM Conference on Information-Centric Networking (ICN), 2015, pp. 109–116, http://dx.doi.org/10.1145/2810156.2810165.

[124] D. Kim, J. Bi, A.V. Vasilakos, I. Yeom, Security of Cached content in NDN, IEEE Trans. Inf. Forensics Secur. 12 (12) (2017) 2933–2944, http://dx.doi.org/10.1109/TIFS.2017.2725229.

[125] J. Ran, N. Lv, D. Zhang, Y. Ma, Z. Xie, On performance of cache policies in named data networking, in: International Conference on Advanced Computer Science and Electronics Information, 2013, pp. 668–671, http://dx.doi.org/10.2991/icacsei.2013.160.

[126] H. Dai, Y. Wang, H. Wu, J. Lu, B. Liu, Towards line-speed and accurate on-line popularity monitoring on ndn routers, in: International Symposium of Quality of Service (IWQoS), IEEE, 2014, pp. 178–187, http://dx.doi.org/10.1109/IWQoS.2014.6914318.

[127] M. Meddeb, A. Dhraief, A. Belghith, T. Monteil, K. Drira, H. Mathkour, Least fresh first cache replacement policy for NDN-based iot networks, Pervasive Mob. Comput. 52 (2019) 60–70, http://dx.doi.org/10.1016/j.pmcj.2018.12.002.

[128] W. Shang, Y. Yu, L. Wang, A. Afanasyev, L. Zhang, A Survey of Distributed Dataset Synchronization in Named Data Networking, Technical Report, Technical Report NDN-0053, NDN, 2017.

[129] W. Fu, H. Ben Abraham, P. Crowley, Isync: a high performance and scalable data synchronization protocol for named data networking, in: ACM Conference on Information-Centric Networking (ICN), 2014, pp. 181–182, http://dx.doi.org/10.1145/2660129.2660161.

[130] W. Shang, A. Afanasyev, L. Zhang, Vectorsync: distributed dataset synchronization over named data networking, in: ACM Conference on Information-Centric Networking (ICN), 2017, pp. 192–193, http://dx.doi.org/10.1145/3125719.3132106.

[131] A.Z. Hindi, M. Kieffer, C. Adjih, C. Weidmann, NDN Synchronization: iroundsync, an improved roundsync, in: ACM Conference on Information-Centric Networking (ICN), 2017, pp. 194–195, http://dx.doi.org/10.1145/3125719.3132108.

[132] P. de-las Heras-Quirós, E.M. Castro, W. Shang, Y. Yu, S. Mastorakis, A. Afanasyev, L. Zhang, The Design of RoundSync Protocol, Technical Report, NDN Project, Technical Report NDN-0048, 2017.

[133] L. Wang, A. Hoque, C. Yi, A. Alyyan, B. Zhang, OSPFN: An OSPF based routing protocol for named data networking, University of Memphis and University of Arizona, Tech. Rep., 2012.

[134] A. Hoque, S.O. Amin, A. Alyyan, B. Zhang, L. Zhang, L. Wang, NLSR: named-data link state routing protocol, in: ACM SIGCOMM Workshop on Information-Centric Networking, 2013, pp. 15–20, http://dx.doi.org/10.1145/2491224.2491231.

[135] M. Papalini, A. Carzaniga, K. Khazaei, A.L. Wolf, Scalable routing for tag-based information-centric networking, in: ACM Conference on Information-Centric Networking (ICN), 2014, pp. 17–26, http://dx.doi.org/10.1145/2660129.2660155.

[136] C. Tsilopoulos, G. Xylomenos, Supporting diverse traffic types in information centric networks, in: ACM Conference on Information-Centric Networking (ICN), 2011, pp. 13–18, http://dx.doi.org/10.1145/2018584.2018588.

[137] M. Antunes, D. Gomes, R. Aguiar, Semantic features for context organization, in: International Conference on Future Internet of Things and Cloud (FiCloud), IEEE, 2015, pp. 87–92, http://dx.doi.org/10.1109/FiCloud.2015.103.

[138] M. Meddeb, A. Dhraief, A. Belghith, T. Monteil, K. Drira, How to cache in ICN-based iot environments?, in: IEEE/ACS International Conference on Computer Systems and Applications (AICCSA), 2017, pp. 1117–1124, http://dx.doi.org/10.1109/AICCSA.2017.37.

[139] G. Zhang, Y. Li, T. Lin, CaChing in information centric networking: A survey, Comput. Netw. 57 (16) (2013) 3128–3141, http://dx.doi.org/10.1016/j.comnet.2013.07.007.

[140] A. Seetharam, On Caching and routing in information-centric networks, IEEE Commun. Mag. 56 (3) (2018) 204–209, http://dx.doi.org/10.1109/MCOM.2017.1700184.

[141] R.J. Hyndman, G. Athanasopoulos, Forecasting: Principles and Practice, OTexts, 2018.

[142] S. Shailendra, B. Panigrahi, H.K. Rath, A. Simha, A novel overlay architecture for information centric networking, in: National Conference on Communications (NCC), IEEE, 2015, pp. 1–6, http://dx.doi.org/10.1109/NCC.2015.7084921.

[143] S. Shannigrahi, C. Fan, G. White, Bridging the ICN deployment gap with ipoc: An IP-over-ICN protocol for 5g networks, in: Workshop on Networking for Emerging Applications and Technologies, ACM, 2018, pp. 1–7, http://dx.doi.org/10.1145/3229574.3229575.

[144] I. Moiseenko, D. Oran, TCP/icn: Carrying TCP over content centric and named data networks, in: ACM Conference on Information-Centric Networking (ICN), 2016, pp. 112–121, http://dx.doi.org/10.1145/2984356.2984357.

[145] D. Trossen, M.J. Reed, J. Riihijärvi, M. Georgiades, N. Fotiou, G. Xylomenos, IP Over ICN - the better ip?, in: European Conference on Networks and Communications (EuCNC), IEEE, 2015, pp. 413–417, http://dx.doi.org/10.1109/EuCNC.2015.7194109.

[146] N. Fotiou, G. Xylomenos, G.C. Polyzos, H. Islam, D. Lagutin, T. Hakala, E. Hakala, ICN Enabling coap extensions for IP based iot devices, in: ACM Conference on Information-Centric Networking, ACM, 2017, pp. 218–219, http://dx.doi.org/10.1145/3125719.3132105.

[147] H.M.A. Islam, D. Lagutin, A. Ylä-Jääski, N. Fotiou, A. Gurtov, Transparent coap services to iot endpoints through ICN operator networks, Sensors 19 (6) (2019) 1339, http://dx.doi.org/10.3390/s19061339.

[148] M. Vahlenkamp, F. Schneider, D. Kutscher, J. Seedorf, Enabling ICN in IP networks using SDN, in: IEEE International Conference on Network Protocols (ICNP), IEEE, 2013, pp. 1–2, http://dx.doi.org/10.1109/ICNP.2013.6733634.

[149] T. Refaei, J. Ma, S. Ha, S. Liu, Integrating IP and NDN through an extensible IP-NDN gateway, in: ACM Conference on Information-Centric Networking (ICN), 2017, pp. 224–225, http://dx.doi.org/10.1145/3125719.3132112.

[150] S. Luo, S. Zhong, K. Lei, IP/NDN: A multi-level translation and migration mechanism, in: IEEE/IFIP Network Operations and Management Symposium (NOMS), IEEE, 2018, pp. 1–5, http://dx.doi.org/10.1109/NOMS.2018.8406213.

[151] J. Quevedo, R. Ferreira, C. Guimarães, R.L. Aguiar, D. Corujo, Internet of things discovery in interoperable information centric and IP networks, Internet Technol. Lett. 1 (1) (2018) 1–6, http://dx.doi.org/10.1002/itl2.1.

[152] M. Mangili, F. Martignon, A. Capone, F. Malucelli, Content-aware planning models for information-centric networking, in: IEEE Global Communications Conference (GLOBECOM), 2014, pp. 1854–1860, http://dx.doi.org/10.1109/GLOCOM.2014.7037078.

[153] M. Mangili, F. Martignon, A. Capone, Optimal design of information centric networks, Comput. Netw. 91 (2015) 638–653, http://dx.doi.org/10.1016/j.comnet.2015.09.003.

[154] POINT Project (IP-over-ICN networking), [Online] https://www.point-h2020.eu/, 2019, Accessed: 2019-02-01.

[155] G. Xylomenos, Y. Thomas, X. Vasilakos, M. Georgiades, A. Phinikarides, I. Doumanis, S. Porter, D. Trossen, S. Robitzsch, M.J. Reed, et al., IP Over ICN Goes Live, arXiv preprint arXiv:1804.07511, 2018.

[156] G. Xylomenos, A. Phinikarides, I. Doumanis, X. Vasilakos, Y. Thomas, D. Trossen, M. Georgiades, S. Porter, IPTV Over ICN, 2018, arXiv preprint arXiv:1804.07509.

[157] N. Fotiou, H. Islam, D. Lagutin, T. Hakala, G.C. Polyzos, Coap over ICN, in: IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2016, pp. 1–4, http://dx.doi.org/10.1109/NTMS.2016.7792438.

[158] M. Amadeo, C. Campolo, A. Molinaro, Internet of things via named data networking: The support of push traffic, in: International Conference and Workshop on the Network of the Future (NOF), IEEE, 2014, pp. 1–5, http://dx.doi.org/10.1109/NOF.2014.7119766.

[159] A. Tagami, T. Yagyu, K. Sugiyama, M. Arumaithurai, K. Nakamura, T. Hasegawa, T. Asami, K. Ramakrishnan, Name-based push/pull message dissemination for disaster message board, in: IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), IEEE, 2016, pp. 1–6, http://dx.doi.org/10.1109/LANMAN.2016.7548855.

[160] P. Moll, S. Theuermann, H. Hellwagner, Persistent interests in named data networking, in: IEEE Vehicular Technology Conference (VTC Spring), 2018, pp. 1–5, http://dx.doi.org/10.1109/VTCSpring.2018.8417861.

[161] G. Arnould, D. Khadraoui, Z. Habbas, A self-organizing content centric network model for hybrid vehicular ad-hoc networks, in: ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications (DIVANet), 2011, pp. 15–22, http://dx.doi.org/10.1145/2069000.2069004.

[162] M.F. Majeed, S.H. Ahmed, M.N. Dailey, Enabling push-based critical data forwarding in vehicular named data networks, IEEE Commun. Lett. 21 (4) (2017) 873–876, http://dx.doi.org/10.1109/LCOMM.2016.2642194.

[163] S.H. Bouk, S.H. Ahmed, M.A. Yaqub, D. Kim, M. Gerla, DPEL: Dynamic PIT entry lifetime in vehicular named data networks, IEEE Commun. Lett. 20 (2) (2016) 336–339, http://dx.doi.org/10.1109/LCOMM.2015.2508798.

[164] R. Li, H. Asaeda, J. Li, A distributed publisher-driven secure data sharing scheme for information-centric iot, IEEE Internet Things J. 4 (3) (2017) 791–803, http://dx.doi.org/10.1109/JIOT.2017.2666799.

[165] C. Gündoğan, P. Kietzmann, T.C. Schmidt, M. Wählisch, HoPP: Robust and Resilient Publish-Subscribe for an Information-Centric Internet of Things, arXiv preprint arXiv:1801.03890, 2018.

[166] R. Hou, Y. Chang, L. Yang, Multi-constrained qos routing based on PSO for named data networking, IET Commun. (2017) http://dx.doi.org/10.1049/iet-com.2016.0783.

[167] Q. Huang, F. Luo, Ant-colony optimization based qos routing in named data networking, J. Comput. Methods Sci. Eng. 16 (3) (2016) 671–682, http://dx.doi.org/10.3233/JCM-160648.

[168] A. Kerrouche, M.R. Senouci, A. Mellouk, T. Abreu, AC-Qos-FS: Ant colony based qos-aware forwarding strategy for routing in named data networking, in: IEEE International Conference on Communications (ICC), 2017, pp. 1–6, http://dx.doi.org/10.1109/ICC.2017.7996960.

[169] S. Muralidharan, B.J. Sahu, N. Saxena, A. Roy, PPT: A push pull traffic algorithm to improve qos provisioning in iot-NDN environment, IEEE Commun. Lett. 21 (6) (2017) 1417–1420, http://dx.doi.org/10.1109/LCOMM.2017.2677922.

[170] S. Muralidharan, A. Roy, N. Saxena, MDP-Iot: MDP based interest forwarding for heterogeneous traffic in iot-NDN environment, Future Gener. Comput. Syst. 79 (2018) 892–908, http://dx.doi.org/10.1016/j.future.2017.08.058.

[171] B. Nour, K. Sharif, F. Li, H. Moungla, H. Khelifi, NNCP: A named data network control protocol for iot applications, in: IEEE Conference on Standards for Communications and Networking (CSCN), 2018, http://dx.doi.org/10.1109/CSCN.2018.8581844.

[172] C. Ghali, G. Tsudik, C.A. Wood, When encryption is not enough: privacy attacks in content-centric networking, in: ACM Conference on Information-Centric Networking (ICN), 2017, pp. 1–10, http://dx.doi.org/10.1145/3125719.3125723.

[173] A. Compagno, M. Conti, R.E. Droms, Onboardicng: a secure protocol for on-boarding iot devices in ICN, in: ACM Conference on Information-Centric Networking (ICN), 2016, pp. 166–175, http://dx.doi.org/10.1145/2984356.2984374.

[174] T. Mick, R. Tourani, S. Misra, Laser: Lightweight authentication and secured routing for NDN iot in smart cities, IEEE Internet Things J. 5 (2) (2018) 755–764, http://dx.doi.org/10.1109/JIOT.2017.2725238.

[175] M. Frey, C. Gündoğan, P. Kietzmann, M. Lenders, H. Petersen, T.C. Schmidt, F. Shzu-Juraschek, M. Wählisch, Security for the Industrial IoT: The Case for Information-Centric Networking, arXiv preprint arXiv:1810.04645, 2018.

[176] K. Zhu, Z. Chen, W. Yan, L. Zhang, Security attacks in named data networking of things and a blockchain solution, IEEE Internet Things J. (2018) http://dx.doi.org/10.1109/JIOT.2018.2877647.

[177] G. Liu, W. Quan, N. Cheng, H. Zhang, S. Yu, Efficient ddos attacks mitigation for stateful forwarding in internet of things, J. Netw. Comput. Appl. (2019) http://dx.doi.org/10.1016/j.jnca.2019.01.006.

[178] S. Adhikari, S. Ray, A lightweight and secure iot communication framework in content-centric network using elliptic curve cryptography, in: Recent Trends in Communication, Computing, and Electronics, Springer, 2019, pp. 207–216, http://dx.doi.org/10.1007/978-981-13-2685-1_21.

[179] B. Li, D. Huang, Z. Wang, Y. Zhu, Attribute-based access control for ICN naming scheme, IEEE Trans. Dependable Secure Comput. (2016) http://dx.doi.org/10.1109/TDSC.2016.2550437.

[180] A.M. Malik, J. Borgh, B. Ohlman, Attribute-based encryption on a resource constrained sensor in an information-centric network, in: ACM Conference on Information-Centric Networking (ICN), 2016, pp. 217–218, http://dx.doi.org/10.1145/2984356.2985229.

[181] J. Borgh, E. Ngai, B. Ohlman, A.M. Malik, Employing attribute-based encryption in systems with resource constrained devices in an information-centric networking context, in: Global Internet of Things Summit (GIoTS), IEEE, 2017, pp. 1–6, http://dx.doi.org/10.1109/GIOTS.2017.8016277.

[182] Y. Zhu, R. Huang, Y. Tao, X. Wang, An edge re-encryption-based access control mechanism in NDN, Trans. Emerg. Telecommun. Technol. (2019) e3564, http://dx.doi.org/10.1002/ett.3565.

[183] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, A secure ICN-iot architecture, in: International Conference on Communications Workshops (ICC Wkshps), IEEE, 2017, pp. 259–264, http://dx.doi.org/10.1109/ICCW.2017.7962667.

[184] S. DiBenedetto, P. Gasti, G. Tsudik, E. Uzun, Andana: Anonymous named data networking application, in: Annual Network & Distributed System Security Symposium, 2011.

[185] The Tor Project, https://www.torproject.org/, 2018, Accessed: 2018-05-18.

[186] Z. Zhu, A. Afanasyev, L. Zhang, A new perspective on mobility support, Named-Data Networking Project, Tech. Rep, 2013.

[187] A. Azgin, R. Ravindran, G. Wang, Location-driven mobility support architecture for information centric networks, in: IEEE International Conference on Computing, Networking and Communications (ICNC), 2018, pp. 905–911, http://dx.doi.org/10.1109/ICCNC.2018.8390268.

[188] Z. Yan, G. Geng, S. Zeadally, Y.-J. Park, Distributed all-IP mobility management architecture supported by the NDN overlay, IEEE Access 5 (2017) 243–251, http://dx.doi.org/10.1109/ACCESS.2016.2639008.

[189] V. Sivaraman, B. Sikdar, Hop-count based forwarding for seamless producer mobility in NDN, in: IEEE Global Communications Conference (GLOBECOM), 2017, pp. 1–6, http://dx.doi.org/10.1109/GLOCOM.2017.8254709.

[190] H. Nakazato, S. Zhang, Y.J. Park, A. Detti, D. Bursztynowski, Z. Kopertowski, I. Psaras, On-path resolver architecture for mobility support in information centric networking, in: IEEE Global Communication Workshops (GLOBECOM Wkshps), 2015, pp. 1–6, http://dx.doi.org/10.1109/GLOCOMW.2015.7413979.

[191] X. Jiang, J. Bi, Y. Wang, P. Lin, Z. Li, A content provider mobility solution of named data networking, in: IEEE International Conference on Network Protocols (ICNP), 2012, pp. 1–2, http://dx.doi.org/10.1109/ICNP.2012.6459937.

[192] Y. Zhang, H. Zhang, L. Zhang, Kite: a mobility support scheme for NDN, in: ACM Conference on Information-Centric Networking (ICN), 2014, pp. 179–180, http://dx.doi.org/10.1145/2660129.2660159.

[193] Y. Rao, D. Gao, H. Luo, NLBA: A novel provider mobility support approach in mobile ndn environment, in: IEEE Consumer Communications and Networking Conference (CCNC), 2014, pp. 188–193, http://dx.doi.org/10.1109/CCNC.2014.6866569.

[194] R. Ying, L. Hongbin, G. Deyun, Z. Huachun, Z. Hongke, LBMA: A novel locator based mobility support approach in named data networking, China Commun. 11 (4) (2014) 111–120, http://dx.doi.org/10.1109/CC.2014.6827573.

[195] M.B. Lehmann, M.P. Barcellos, A. Mauthe, Providing producer mobility support in NDN through proactive data replication, in: IEEE/IFIP Network Operations and Management Symposium (NOMS), 2016, pp. 383–391, http://dx.doi.org/10.1109/NOMS.2016.7502835.

[196] A. Compagno, X. Zeng, L. Muscariello, G. Carofiglio, J. Augé, Secure producer mobility in information-centric network, in: ACM Conference on Information-Centric Networking (ICN), 2017, pp. 163–169, http://dx.doi.org/10.1145/3125719.3125725.

[197] M. Meddeb, A. Dhraief, A. Belghith, T. Monteil, K. Drira, S. Gannouni, AFIRM: Adaptive forwarding based link recovery for mobility support in NDN/iot networks, Future Gener. Comput. Syst. 87 (2018) 351–363, http://dx.doi.org/10.1016/j.future.2018.04.087.

[198] D. An, D. Kim, ICN-Based light-weighted mobility support in iot, in: International Conference on Computer Communication and Networks (ICCCN), IEEE, 2018, pp. 1–2, http://dx.doi.org/10.1109/ICCCN.2018.8487384.

[199] Y. Abidy, B. Saadallahy, A. Lahmadi, O. Festor, Named data aggregation in wireless sensor networks, in: IEEE Network Operations and Management Symposium (NOMS), 2014, pp. 1–8, http://dx.doi.org/10.1109/NOMS.2014.6838364.

[200] M. Amadeo, C. Campolo, A. Molinaro, Multi-source data retrieval in iot via named data networking, in: ACM Conference on Information-Centric Networking (ICN), 2014, pp. 67–76, http://dx.doi.org/10.1145/2660129.2660148.

[201] M.A. Hail, M. Amadeo, A. Molinaro, S. Fischer, CaChing in named data networking for the wireless internet of things, in: International Conference on Recent Advances in Internet of Things (RIoT), IEEE, 2015, pp. 1–6, http://dx.doi.org/10.1109/RIOT.2015.7104902.

[202] A. Abane, M. Daoui, S. Bouzefrane, P. Muhlethaler, NDN-Over-zigbee: A zigbee support for named data networking, Future Gener. Comput. Syst. (2017) 1–7, http://dx.doi.org/10.1016/j.future.2017.09.053.

[203] Y. Yingdi, A. Alexander, Z. Zhenkai, Z. Lixia, Naming Conventions, Technical Report,, NDN Project, Tech. Rep. NDN-0023, 2014.