Named data networking for IoT: An architectural perspective

Conference Paper · June 2014

DOI: 10.1109/EuCNC.2014.6882665

CITATIONS
16

READS
364

4 authors, including:

Marica Amadeo
Mediterranean University of Reggio Calabria
31 PUBLICATIONS **342** CITATIONS
SEE PROFILE

Claudia Campolo
Mediterranean University of Reggio Calabria
77 PUBLICATIONS **826** CITATIONS
SEE PROFILE

Antonio Iera
Mediterranean University of Reggio Calabria
272 PUBLICATIONS **4,455** CITATIONS
SEE PROFILE

This is the final submitted version of the paper published in: Proceedings of the EuCNC 2014 Conference, Year 2014, Pages: 1-5, DOI: 10.1109/EuCNC.2014.6882665

Named Data Networking for IoT: an Architectural Perspective

Marica Amadeo, Claudia Campolo, Antonio Iera, Antonella Molinaro
University "Mediterranea" of Reggio Calabria - DIIES Department
Email: {name.surname}@unirc.it

***Abstract*—The *Named Data Networking* (NDN) project is emerging as one of the most promising information-centric future Internet architectures. Besides NDN recognized potential as a content retrieval solution in wired and wireless domains, its innovative concepts, such as named content, name-based routing and in-network caching, particularly suit the requirements of *Internet of Things* (IoT), interconnecting billions of heterogeneous objects. IoT highly differs from today's Internet due to resource-constrained devices, massive volumes of small exchanged data, and traffic type diversity. The study in this paper addresses the design of a *high-level* NDN architecture, whose main components are overhauled to specifically meet the IoT challenges.**

***Index Terms*—Named Data Networking, Internet of Things**

I. Introduction

The proliferation of low-cost sensing and actuator devices together with the advancement in wireless communication technologies offer unprecedented opportunities for the support of applications that cut across many areas of modern day living (e.g., healthcare, smart home, sustainable transportation).

The urge for connecting and integrating such devices at a global scale has pushed towards the *Internet of Things (IoT)* vision. IETF working groups have proposed a suite of protocols and open IP-based standards to prevent wireless sensor and actuator networks (WSANs) to work *in isolation* by relying on Internet connections. The advantages of using IP are manifold: it is a well-defined open standard, enabling communication compatibility between entities in different domains. However, there are still open challenges to date in deploying IP-based IoT solutions on a large scale [1]. In addition to arising stringent application and device requirements (e.g., scalability, robustness, power efficiency) intrinsic to IoT, such solutions inherit issues strictly related to the *host-centric* IP paradigm that impact communication performance in the current (and future) Internet. The use of IP addresses, in fact, implies *(i)* the need of additional resolution systems to translate application-level requests (e.g., in the form of Uniform Resource Identifier), into IP addresses; *(ii)* connection-oriented end-to-end security; *(iii)* additional (burdensome) protocols to support mobility.

This is why the research community is currently exploring *cutting-edge* and *clean-slate* approaches to transform the Internet. The Information Centric Networking (ICN) paradigm [2] has been recently proposed to this purpose. Unlike the host-centric IP-based networking, in ICN the content is the first class network citizen: nodes specify *what* they search for and not *where* they expect it to be provided. Every data is a self-authenticating and self-identifying unit, which can be required by any interested authorized consumer by using a unique, persistent, location-independent name. In-network caching, multicasting and mobility are natively supported. In this research arena, the Named Data Networking architecture (NDN) [3] has rapidly gained consensus thanks to its simple communication model, scalable naming and lightweight configuration and management operations [4]. NDN features make it also a particularly promising solution to fit the peculiarities of the IoT ecosystem [1] (Section III), where applications spanning several domains may request the same data, regardless of their provenance, and billions of heterogeneous (constrained) nodes need to communicate.

Motivated by such unique challenges imposed by IoT, we take a top-down approach to develop a *high-level NDN architecture* for this domain and specify its main components (Section IV). At the heart of our design there is the clear identification of a *management and control plane* in the traditional NDN fabric. It accounts for the configuration and management of services and devices, for the types of IoT data exchange (e.g., on-demand sensing/action triggering, periodic monitoring, event-triggered alarms) and their demands (e.g., in terms of security, reliability, timeliness, local relevance), and it forges accordingly the *Strategy* layer, responsible for transport and forwarding routines. The work would also serve the purpose of incentiving the research community to contribute to a full-fledged *Future Named Data Internet of Things*.

II. NDN in a nutshell

The NDN architecture is based on the *Content Centric Networking* proposal, presented by Jacobson *et al.* in [5]. It defines a simple and robust receiver-driven communication model based on the exchange of two packets types, Interest and Data, which carry hierarchical, application-specific content names. NDN deals with content integrity and authenticity by piggybacking the data publisher's signature and other authentication information in each Data. Depending on local constraints and policies, a subset (or all) of the network nodes can cache contents in order to speed up data retrieval while reducing the network overhead.

As shown in Figure 1, NDN inherits the hourglass model of the IP architecture, but the narrow waist leverages names of

This work has been carried out within the national research project PON03PE_00050 DOMUS "Home automation systems for a cooperative energy brokerage service".

contents instead of IP addresses for data delivery. Each NDN node maintains three data structures: *(i)* a Content Store (CS) for temporary caching of incoming Data packets; *(ii)* a routing table named Forwarding Information Base (FIB) used to guide the Interests towards Data; and *(iii)* a Pending Interest Table (PIT), which keeps track of the forwarded Interest(s) that are not yet satisfied with a returned Data packet.

Each NDN node receiving an Interest acts as follows to make its forwarding decisions. First, it searches for a name prefix longest-match in its content store. If a match is found, then the node sends the Data back to the incoming interface of the processed Interest. Otherwise, if there is a matching PIT entry, the Interest is discarded because an equal request has been already forwarded. If it is not the case, a new PIT entry is created and the Interest is further forwarded to the interface stored in the FIB. Data packets follow the chain of PIT entries back to the requester(s). If a match is not found in the PIT, then the Data packet is considered *unsolicited* and it is dropped.

The NDN Strategy layer in Figure 1 permits to specify different transport and forwarding services, depending on the application requirements and the access network constraints.

III. NDN FOR IOT

The design of a networking architecture that interconnects a huge ecosystem, where things may be resource-constrained and/or mobile and also the traffic patterns are highly heterogeneous, poses great challenges. Agile network configuration and management, security, scalability, robustness, reliability are only a few of the requirements that IoT must support.

Main benefits. Due to its intrinsic features, we believe that NDN can address several IoT requirements by *directly managing* several functionalities (security, naming, data aggregation, etc.) at the network layer, as summarized in Table I.

Thanks to the use of hierarchical, application-specific namespaces and the smart forwarding fabric based on PIT and FIB structures, NDN can offer *easy, robust and scalable data retrieval*. The use of named contents coupled with named-based routing eliminates the IP address assignment procedures and facilitates content search and retrieval in large networks. Meaningful names related to the device's identity or function can be defined that also reflect access restrictions.

Interests aggregation performed by every PIT structure is specifically designed to deal with massive data access. Intermediate routers can identify multiple requests for the same content and forward a single Interest to the *thing*. At the same time, in-network caching natively supported by NDN nodes can make data available to different consumers also under intermittent connectivity, e.g., due to low-power operation. Moreover, by leveraging the natural aggregation properties of the hierarchical NDN namespace, NDN natively supports *many providers-to-one consumer* communication. This especially fits the case of a roadside station interested in gathering traffic road congestion information from many vehicles in a given area. This intrinsic *anycasting* feature of NDN can be particular helpful to overcome situations in which some nodes are currently unavailable (e.g., in sleep mode or out of range) and when the channel conditions are particular harsh and mine communication reliability. All these features clearly improve the *energy efficiency* of the overall network.

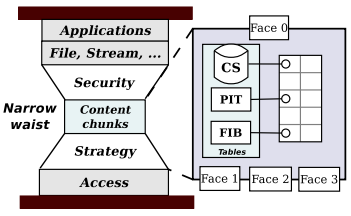

Fig. 1. NDN hourglass and node architecture.

Since IoT systems are not deployed in isolation but they are exposed to external controls on the Internet, security is also a primary concern. In NDN, per-packet signatures and optional encryption of Data offer inherent *security support* at the network layer.

IoT is expected to be a highly heterogeneous environment, but the NDN philosophy is open to several customizations which can match the miscellanea of devices and applications. NDN names have variable and unbounded lengths and they can be also user-friendly, even if it is not mandatory. Therefore, application developers are free to design a namespace that fits the constraints of their environment.

In addition, different transport and forwarding strategies can be implemented, including the opportunity to forward a request to different outgoing interfaces simultaneously; and different caching policies can be adopted, including the possibility of preventing caching at all for resource-constrained devices. Multipath routing and in-network caching also help to support a fundamental requirement of many IoT applications, which is *communication reliability*. This latter is also supported by Interest retransmission mechanisms, which usually involve the original consumer, albeit intermediate nodes may locally retry the Interest transmission in some cases. All in all, we argue that NDN is meant *to support the heterogeneity* of IoT.

Another requirement for some IoT applications is *mobility support* (e.g., data collection with a mobile sink; vehicle traffic monitoring), which involves the re-location of *things* (and users) in regards to their access network. Mobile IP patches have been criticized in the literature due to their inefficiencies in terms of forwarding overhead and delays. Vice versa, through the use of location-independent content names and receiver-driven connectionless communications, NDN *natively supports consumer mobility*. When a consumer re-locates, it can simply re-issue any unsatisfied Interest, without the need to perform any registration or configuration procedure. Mobility of producers requires routing updates but the possibility of multi-sourcing and distributed caching for consumers reduces the potential delays.

Background. So far, research about NDN for IoT is still at its infancy. The work in [6] targets stand-alone, generic content-centric WSANs. In [7], the initial design of a NDN based homenet is presented and the aspects of naming, node

and service discovery are discussed, with a comparison against an IPv6 architecture. The case of securing a building management system and a lighting control system running over NDN are discussed in [8] and [9], respectively. In [10], the concept of an information centric IoT platform is presented by discussing its main requirements and the possible advantages compared to overlay approaches built upon IP. Then, the work focuses on a specific ICN architecture, *MobilityFirst*, and builds a middleware layer for IoT services. Unlike [10], in this paper we specifically focus on the NDN architecture and analyse its applicability to the IoT world.

IV. The proposed NDN-IoT architecture

Although NDN principles match the expectations of the IoT world, there are many open aspects to address, as introduced in the following. IoT systems originate traffic patterns very different from the popular Internet applications (web browsing, video streaming, etc.) and require specific procedures for device/service discovery and management. Thereby, NDN should go beyond today's recognized scope, i.e., typically *large file transfers*. Unlike high-performing routers in the core network, IoT devices are mainly resource-constrained nodes (e.g., low power, low memory), the wireless medium is unreliable and data transfer performance may be very poor. NDN must be optimized in order to support such limitations.

To this aim, we devise a high-level architecture for NDN IoT systems, as depicted in Figure 2. At the bottom of the architecture, we put the *Thing* layer, that accounts for the multitude of devices of the IoT ecosystem. They can be equipped with heterogeneous communication interfaces and exhibit different mobility patterns and constraints (size, battery, cost, processing, storage). Some representative IoT applications, whose requirements should be satisfied, are summarized at the top of the stack. In such an architecture, NDN acts as a networking layer and is expected to hide to applications the complexity and diversity of the underlying things by adapting its modules to their features.

In the NDN box, we identified two main components: the *Data plane* and the *Management and Control plane*.

The former handles the individual packets (both Interest and Data are considered) and operations on top of them, i.e., naming, security, caching and strategy, that must be adequately overhauled to match IoT features. The latter re-engineers the existing NDN routing plane, to also account for device configuration and management operations, IoT data types and demands, crucial in the IoT domain to properly drive the Strategy layer decisions. Intuitively, naming and security will encompass *cross-plane functionalities* as it will be clear later.

The functionalities of the identified planes are presented in the following Subsections. Since the focus is on the high-level design philosophy, the details of conceived components are not specified. We argue instead how identified issues could be solved, by providing hints from preliminary related literature, whenever possible, and our own guidelines, otherwise.

A. Management and control plane

Service model. A wide range of control and monitoring applications can be classified as *pull*, where the consumers solicit the transmission of signed Data, e.g., the temperature in a room may be requested by a heating system. This is the standard operation mode of NDN. In NDN-IoT systems, in addition, nodes can use an Interest to trigger a device to perform a given task (e.g., to switch on a home appliance) and Data can be used to acknowledge the execution of the task and reporting the outcome of the action (e.g., success, failure, failure code). IoT applications may also originate *push* traffic, either for monitoring purposes (e.g., home appliances preconfigured to send measurements at fixed intervals to the utility company), or for high-priority real-time alarm propagation after the occurrence of an event (e.g., a fire-detection in a building). The NDN-IoT architecture must be overhauled with proper mechanisms that support both periodic and event-triggered content pushing, since unsolicited Data would be immediately discarded by the NDN forwarding fabric. The selection of such mechanisms mainly depends on the *scope* of the traffic (local or wide area traffic), the *requirements* of the application in terms of latency and reliability and the *data types*. The concept of *long-lived Interest* in [11] can be implemented to support both local and wide area push traffic in NDN with minimal effort. The idea is to use a single request to require more Data, like a subscription. The PIT entry is not consumed by the reception of a Data, but it remains active for a

TABLE I
IoT main requirements and native NDN support.

IoT requirement	NDN features
Scalability and robustness	hierarchical application-specific names, in-network caching, Interests aggregation, anycasting
Security	data integrity and origin authentication via per-packet signature, possibility of encryption
Energy efficiency	in-network caching, Interest aggregation, anycasting
Heterogeneity	unbounded application-specific namespaces, high customization of transport and forwarding strategies and caching policies
Mobility	location-independent names, receiver-driven connectionless communications, multi-source retrieval
Reliability	Interest retransmissions from original consumers and retries from intermediate nodes, in-network caching, multi-path routing

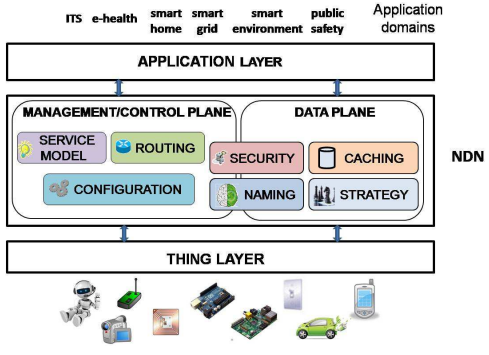

Fig. 2. NDN IoT architecture.

time interval, so more Data can be forwarded to the consumer. If the service requires reliability, an acknowledgement to the Data must be transmitted.

An even simpler approach for (only) local area networks is to allow *unsolicited Data* from authorized sources, provided that, during a preliminary configuration phase, data producer and consumer agree upon pushing periodic or event-triggered contents. On a wide scale, however, the use of unsolicited authorized Data is clearly unfeasible, due to scalability and forwarding issues.

In addition, in the presence of small contents, the Interest can be used to directly transfer a notification encoded in the name field. However, this strategy requires to build authenticated Interests and new prefix-match lookup mechanisms.

Configuration. An IoT system requires specific configuration procedures for the network (and applications) set-up and additional signaling for management purposes during the network lifetime, e.g., keep-alive messaging. These routines are usually developed in isolated domains, do not involve any remote control, and can be modelled with an Interest/Data exchange in a local network management namespace.

Device (and service) discovery and configuration protocols set the application namespace, identity and security rules of every device in the local domain. A preliminary neighbour discovery protocol (NDP) and a Service Publish and Discovery protocol (SPDP) in a NDN homenet are described in [7]. Both of them assume that nodes periodically express discovery Interests, which carry a prefix that identifies the protocol, */ndp* or */spdp*, and a unique device or service identifier. When a node receives this Interest, it sets a FIB entry and then forwards this information to its neighbours.

After the configuration of the local domain, global connectivity can take place thanks to the routing operation.

Routing. Name-based NDN routing appears extremely useful for global IoT communications. Content names, in fact, are unique and persistent and they are directly used to communicate, without the need to be resolved into network addresses, recognized as a cumbersome operation for constrained devices [1]. A data source could simply announce the name prefixes it can serve. A router that receives this information installs a local FIB entry for that prefixes and then floods this information to its neighbours.

The major challenge remains how to design efficient namespaces with robust names aggregation rules that cope with the enormous number of things on large scale. Routing performance is strictly related to the selected names, on which aggregation rules can be performed, but also to the scope of applications (e.g., locally relevant, globally relevant) and the time-validity of services/functions of IoT nodes. Current routing strategies developed for wide area networks (link-state, distance/path vector protocols) and wireless ad hoc and sensor networks (controlled flooding, proactive and reactive protocols) can be adapted to support named-based routing for IoT. It is expected that performance of such protocols can be even higher than their corresponding IP-based implementation because NDN can leverage an intelligent and adaptive forwarding strategy.

B. Data plane

Naming. The possibility to build application-specific naming schemes is a clear benefit to incentive customized NDN solutions for IoT. However, in the IoT domain the same information could be beneficial for more consumers, hence it is crucial to design naming structures that allow both the requests and information to be understood by entities spanning different application domains, to facilitate data sharing, while reducing in this way the traffic load.

It is reasonable that IoT names must identify the application, the task or the service offered by a device and other related attributes. In [8], for instance, the naming scheme for a Building Management System (BMS) is defined that reflects the physical location of the device and the hierarchy in the building structure. For example, the NDN name of a sensor data packet, e.g., */ndn/ucla.edu/bms/building/melnitz/studio/1/data/panel/J/voltage/timestamp*, indicates the application type, BMS, developed at the UCLA university, the location of the sensor (Panel J inside Studio 1, Melnitz Hall), the type of data (voltage) and the time when the data is acquired, expressed as a timestamp.

The definition of *thin* names should be pursued to accommodate them in small payloads, (e.g., ZigBee), for instance by keeping low the number of name components and their length.

Since NDN names are intuitive and user-friendly, their use as a clear text in Interests may cause security issues due to possible spoofing. It is therefore crucial to build proper security frameworks, as explained in the following.

Security. In addition to signed Data, in IoT systems there are applications that could benefit from authenticated Interests. This is the case of any remote control application: if an Interest is used to trigger an action, it is fundamental that requesters are only trusted and authorized people. Although the use of signatures prevents straightforward Interest aggregation, the adoption of authenticated Interest is recommended. It is already considered in the preliminary lighting control system in [9], where applications send Interests signed with a private key to command a task to the fixture. If the packet is successfully verified, the task can be performed and eventually the fixture sends a public verifiable ack. While per-Data/Interest signature is useful to guarantee security, the signing cost in terms of computation and delay may result very high for some entities such as simple sensors. Efficient trust models, access control policies and authorization mechanisms must be designed to minimize the burden of security support.

Caching. Caching strategies that operate in fully distributed mode are crucial to provide reliability, scalability and robustness to IoT ecosystems. Depending on the type of data exchanged, the network environments and the capabilities of IoT nodes, tens of caching schemes can be defined that range from *caching nothing* to *caching everything*. Some data may have a very short time validity, hence not requiring to be stored in traversed nodes, while other may serve the purposes of different applications, hence storing them is crucial.

Some devices with resource-sufficient capabilities can act as data mules and so move the content in an opportunistic fashion. For example, vehicles that capture Data from sensors on the road and transmit them to other vehicles along the way.

Moreover, in-network caching makes data available at *different granularities* to different applications, without the need to query the original device. As an example, a temperature sensor can send information every 20 seconds to the fire alarm system, every 5 minutes to the heating system, and a few times in a day to the house owner or other remote entities. It is reasonable to assume that in local area domains, like a house or a building, a single node, e.g., the home gateway, is in charge of caching the data originated by the set of devices under its control and answers to the requests of remote applications without involving the original producer.

Strategy Layer. The NDN Strategy layer encompasses forwarding and transport routines, to allow NDN to interact with the *Thing Layer*, and to meet demands of applications.

• *Forwarding.* The majority of IoT applications is foreseen to use wireless access technologies. To increase the coverage, also multi-hop communications can be performed. However, signal propagation on the wireless medium may be adversely affected by channel impairments like path loss, multipath fading, shadowing and interference from devices operating in the same band. It is also worth noticing that IoT Data may travel different heterogeneous segments before reaching a destination (e.g., a Zigbee network, a Wi-Fi network, a wired segment). NDN-IoT systems should develop robust forwarding mechanisms able to perform smart collision and broadcast storm avoidance schemes, likely based on overhearing, in the wireless segment, similarly to what deployed in mobile ad hoc networks [4], while different policies may be adopted in wired segments to cope with link failures and congestion.

• *Transport.* Congestion, channel-induced losses together with the potential sleep operations of nodes could cause Interest/Data losses. Transport mechanisms should be highly related to the service model, the underlying access technology, so to trade-off between efficiency, in network/device resources usage, and robustness. In case of pull communications, if the service must be reliable (e.g., an action triggering), Interest packets are retransmitted in case the Data is not received in a reasonable time interval. Instead, Data retransmissions may be issued at the provider side, in case of unsolicited event-triggered packets. Per-hop confirmations or acks from the end consumers can be taken into account in case of long-lived Interests, whose handling is strictly related to the management of PIT entries.

C. A preliminary use case

To figure out how the overhauled and newly conceived NDN modules for IoT will work in practice, let us refer to a *demand/response (DR) application* as a concrete use case. To enforce a wise energy usage, utility companies periodically monitor load information from the smart meters located at the customers' premises. *Long lived Interests* are issued by the utility to this purpose. When high demands situation occur, in response to power grid needs, the utility sends an *authenticated Interest to notify* nodes participating to the DR program about the need to reduce the use of electricity. After verifying the packet, the smart meter issues a set of *authenticated Interests* to its controlled home appliances in order to turn off lighting, air conditioning, pumps, and other non-essential equipment. The controlled devices acknowledge the execution of the task with a Data packet sent back to the smart meter. The application namespace, identity and security rules of controlled appliances are provided by the conceived *configuration* functionalities.

V. Conclusions

Like any new concept deviating from conventional practice, the architectural perspective discussed in this paper is expected to raise a number of interesting questions. In addition to discussed technical challenges, deployment options need to be debated to let the proposed architecture to work in practice when considering global connectivity via NDN. At the beginning, the conceived NDN architecture could be easily and successfully deployed as a clean-slate solution in any stand-alone WSAN. Proxy functionalities could be introduced in gateways between the local and wide-area domains to ensure backward compatibility. Then, it could be incrementally deployed between different NDN islands and as an overlay over the TCP/IP layers in the core network interconnecting them. The identified NDN benefits and the still IoT open problems suggest that there are wide opportunities to contribute to this topic, e.g., by further specifying the mechanisms abstracted in the conceived architecture. Future work will be also devoted to understand the mutual relationships between the *revolutionary* NDN concept and *evolutionary* IETF approaches to figure out possible interworking to target performance improvement.

References

[1] Z. Sheng *et al.*, "A survey on the IETF protocol suite for the Internet of Things: standards, challenges, and opportunities," *Wireless Communications, IEEE*, vol. 20, no. 6, pp. 91–98, 2013.

[2] B. Ahlgren *et al.*, "A survey of Information-Centric Networking," *Communications Magazine, IEEE*, vol. 50, no. 7, pp. 26–36, 2012.

[3] L. Zhang *et al.*, "Named Data Networking (NDN) Project," PARC, Tech. Rep. NDN-0001, October 2010.

[4] M. Amadeo, *et al.*, "E-CHANET: Routing, Forwarding and Transport in Information-Centric Multihop Wireless Networks," *Comp. Comm.*, vol. 36, no. 7, April 2013.

[5] V. Jacobson, D. K. Smetters, J. D. Thornton, M. Plass, N. Briggs, and R. L. Braynard, "Networking Named Content," in *ACM CoNEXT*, 2009.

[6] Z. Ren *et al.*, "CCN-WSN a lightweight, flexible Content-Centric Networking Protocol for Wireless Sensor Networks," in IEEE ISSNIP'13.

[7] R. Ravindran *et al.*, "Information-Centric Networking based Homenet," in *IFIP/IEEE ManFI Workshop*, 2013.

[8] W. Shang *et al.*, "Securing building management systems using Named Data Networking," Tech. Rep., 2013.

[9] J. Burke *et al.*, "Securing Instrumented Environments over Content-Centric Networking: the Case of Lighting Control and NDN," in *IEEE Infocom NOMEN Workshop*, 2013.

[10] Y. Zhang *et al.*, "ICN based Architecture for IoT," in *Internet-Draft*, Dec. 2013.

[11] A. Carzaniga *et al.*, "Content-Based Publish/Subscribe Networking and Information-Centric Networking," in *ACM ICN*, 2011.

[12] V. Perez M. T. Garip, S. Lam, and L. Zhang, "Security evaluation of a control system using Named Data Networking," in *IEEE ICNP*, 2013.