Analysis of Deployment Options to Enhance Horizontal Information Sharing and Networking in Internet of Things

Andrej Mihailovic
King's College London
43 PUBLICATIONS **333** CITATIONS

Marko Simeunović
University of Donja Gorica
36 PUBLICATIONS **112** CITATIONS

M. Pejanovic-Djurisic
University of Montenegro
129 PUBLICATIONS **179** CITATIONS

Analysis of Deployment Options to Enhance Horizontal Information Sharing and Networking in Internet of Things

Andrej Mihailovic[1,2], Marko Simeunovic[2], Milica Pejanovic-Djurisic[2]
[1]King's College London, London, UK
[2]Research Centre of ICT, University of Montenegro, Podgorica, Montenegro
andrej.mihailovic@kcl.ac.uk, marko.simeunovic@ac.me, milica@ac.me

Abstract—**Proliferations and uses of Internet of Things (IoT) services are greatly underlined by purpose-based and autonomous compositions of IoT eco-systems. This trend is commonly encountered in large scale IoT environments such as Smart Cities. Consequently, expansion of IoT services affirms a specific property of their compositions, that is, verticality. This means shielded information flows for control, management and data and results in web-level visibility of IoT data. Following the recent initiatives towards horizontality-enabling solutions for IoT, our work revisits some basic assumptions encountered when an IoT system is built from scratch. These are relevant when considering various deployment possibilities, applications, use of equipment, data provisioning/sharing and facilitation of networking tools for specifics of IoT communications. We give an analysis of two possible deployment paths for enhancing the horizontal information sharing and networking. One is based on the default view of the integration of stand-alone devices and small scale IoT networks into the IP networking suite with scalable adaptations of discovery options such as DNS and APIs. The other one takes a radically different approach based on novel concepts of Information Centric Networking/Named-Data Networking and adapts them to IoT specifics. It applies it as a long term research direction for horizontal data distributions and IoT search-and-discovery models in future large scale deployment environments such as Smart Cities.**

Keywords—Internet of Things, Future Internet, Smart Cities, Information Centric Networking, Named-Data Networking

I. Introduction

Proliferation of Internet of Things (IoT) devices, services and technologies has undoubtedly been one of the most impacting novelty and expansion areas of telecommunications and accompanying technology. The term IoT has been applied as a universal meaning to a plethora of technicalities, devices and systems with wide ranging compositions and uses. In terms of the compositions, IoT refer both to stand-alone or small-scale installations of communicating device(s) as well as large scale installations of many system components in grand deployment environments such as Smart Cities. IoT eco-systems in Smart Cities effectively become operational as IoT services based on the operational integration of: devices, cloud-like databases, tools for data processing, control, management and final delivery at the application/web-level. Observing the properties and technicalities of the actual devices draws attention to their varying characteristics and uses, i.e. IoT devices refer to simple low-processing sensor nodes or actuators (or clusters), to vehicles, then, unconstrained machines capable of smart operations and PC-like processing [1] etc. IoT deployment trends also show [2][3] great diversity of application areas: from small scale eHealth, smart homes, to automation of production processes, then, agriculture applications, smart cities, transport applications etc.

Many of the explanations of this paper are influenced by the diversity of issues related to IoT. Progress in the areas of IoT shows many, both novel and ongoing, initiatives for more organised and standardised approaches to many dimensions of IoT deployment: from PHY/MAC to application layer [3], integration into new standards for cellular technologies (i.e. 5G [4]), to achieving coherence of data representation tools between databases/clouds of different IoT eco-system providers [7][8]. It can be postulated that there is an ongoing global effort towards aligning and consolidating the understanding of diversity of IoT and their impact on the existing systems. In this paper, we focus on two angles: i) the particular technical space of networking and data provisioning tools; ii) large scale coexisting implementations of independent IoT devices or groups of IoT eco-systems. These are relevant to both the support for IoT in the Internet, eco-system architecture compositions and take their particular significance in dense large scale urban deployment areas called Smart Cities [9][10].

To accompany our study we observe a chronological and consequential process of forming many relevant IoT implementations. Many IoT-termed implementations of today have occurred as a transformation of Wireless Sensor (and actuator) Networks (WSNs) [1][2][5] forming IoT eco-systems typically bounded by functional and commercial structures (e.g. a Smart City company installations). A technical formulation can be stated from an engineering stance as a crosscheck and reflecting on the current IoT implementations: IoT was idealistically introduced to signify IP-reachability of various devices as "tiny" IP hosts being facilitated by large volume of IPv6 addresses. This approach has its discrepancy when reflected against the current IoT eco-systems structures where achieving independent IP network (and data) visibility for every IoT device is not the practical requirement. Rather, the IoT eco-systems provide visibility in an integrated and processed form at the application level.

II. Formulation of IoT Specifics and Challenges

A. Issues with Vertical Composition of IoT eco-systems

An IoT system is described as vertical to denote the property of system components organisation from devices/"things" on the ground to presentation of data at the service/application level [29]. Verticality is applied in a generic sense highlighting the flow directions of control/data and setup of architecture elements that support the deployment of IoT (e.g. for data collection purposes)[1]. Figure 1 sketches a simplified layout of IoT eco-system architecture components. The chosen IoT eco-system setup shows a large scale deployment of IoTs in Smart City environments, consisting of installations of "things" at the physical (ground) level, their communications via access infrastructure (e.g. cellular networks, WiFi hot-spots etc.), then, via Internet communications to the installations of a vertical IoT service provider with data processing facilities (e.g. a cloud infrastructure) and final delivery of digested data in the forms of services and applications towards the users. This setup assumes digestion of situations on the physical/ground levels, exposed via data collections, by processing data and presentation at the application level. This summarises the vertical composition of an IoT eco-system.

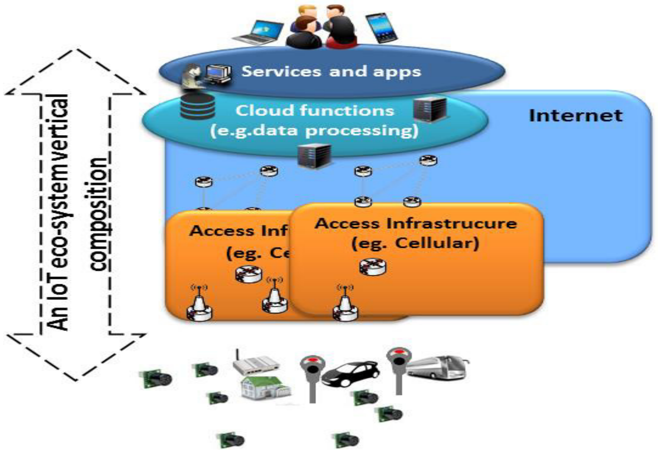

Figure 1. An example generic setup of a vertical IoT eco-system

Existence of many separate IoT eco-systems in Smart Cities of today induces a challenge of enabling their interoperability in exchanges and correlations of data at the data processing and/or cloud level (e.g. using standardized semantics or ontological data structures [7][8][11]). Aligning complex data structures between different eco-systems is a burdensome task at the system-level both in terms of the logic applied to link the data and lack of openness for complete interoperability. In addition, some properties of verticality would still apply (visibility of processed data at the application level) even if ideal aligning between the data models is achieved.

B. Challenges for Horizontal Information Sharing and Networking

We apply the concept of IoT horizontality as existences of deployment situations and supporting functionality that allow processes of IoT discovery and service provisioning in manners not bound to vertical installations of IoT eco-systems. Hence, the IoT service is not to be discovered and utilised only using specific web-level presentation of IoT data but as inherent and integrated features of the future networks. We note that this might already be a work-in-progress whereas we discuss some open and needed changes in the Internet functionalities and use of novel networking paradigms. Some specific challenges and observations are listed below, highlighting the need for IoT horizontality (more is given in [29]):

- An underling consensus of the global IoT initiatives and visions confirms IP reachability and connectivity as the defining property of IoT communications, i.e. facilitated by IPv6 addresses. It is projected that there will be billions of IoT devices by the end of this decade [6] by unleashing the IPv6's addresses. Many of the deployed devices would be independent installations that are not bound to commercial and functional compositions of an IoT eco-system provider. As IETF provides the tools for hosting IP protocol on IoT "tiny" devices [12][13][14], the challenge is how to accommodate large population of IP hosts regarding the Internet functions such as DNS, APIs, topological configuration of IP address, Service Provider logic etc.
- Many of the challenges surface when IoT are considered from the commercial deployment perspective specifically in deployment areas such as Smart Cities[2]. Communication paradigm for IoT differs from the conventional Internet, which is built on "human-to-human" or "human-to-server" communication model [13][23]. IoT communications are combinations of "device-to-device/human/database/ automation…" models and vice versa.
- IoT deployment is marked by the specific action of device configuration. This is a process of software and hardware setup that ensures operation and communication of IoT devices. This action requires dedicated engineer skills and has greatly been the reason for the nature and properties of current IoT systems (i.e. verticality and evolution of early sensor network installations). It is a significant constraint to global and liberalised deployment of IoT devices as many users often do not possess sufficient skills to configure and setup IoT devices. Hence, horizontal enablers are needed to ease the deployment process. Commercial forecasts accordingly highlight the device management as the risk associated with deployment of IoT devices at large scale[3].
- Another facilitator of horizontality can be looked for in the vision of Named-Data Networking (NDN) [15][16][17] for IoT that stems from the novel ideas and proposals of

[1] European Commission project call ICT 30 in 2015 "*The biggest challenge will be to overcome the fragmentation of vertically-oriented closed systems, architectures and application areas and move towards open systems and platforms that support multiple applications.*"

[2] http://www.iottechnews.com/news/2016/apr/11/why-network-cornerstone-smart-cities/

[3] http://www.iottechnews.com/news/2016/apr/07/why-device-management-presents-risk-iot-adoption-scale/

Information Centric Networking [18][19]. The vision is founded on the principle that IoT communications are typically concerned with data provisioning of small chunks of data (several bytes) that are named as the types of sensory or actuation purposes of IoT devices (e.g. temperature, pollution, meter readings, then, light/equipment on/off statuses). NDN is based on address-less routing, where the search packet specifies the Interest and upon Interest/data discovery in its upstream path, returns the content to the seeker host. Such a paradigm accordingly fits with the IoT communications and is currently applied to cases searching data in buildings, vehicles [20][21][22] etc. We extend the vision with a proposal for more comprehensive search and discovery data items that would not only identify the value of the sensory or actuation equipment, but provide the geographical, network-based, ownership-based search and discovery of IoT devices and services in large scale deployment areas such as Smart Cities.

The following sections discuss two development paths for horizontal deployment of IoT devices. The first one discusses support of the standard Internet suite for accommodating large scale IoT populations. The second one summarises a long term vision [29] of extending NDN concepts to comprehensive discovery of IoT devices and services in large scale urban deployments.

III. Fitting IoT Device Populations In The Internet

A. *Example IoT Architecture Composition*

Independent IoT devices are yet to be seamlessly integrated in the Internet protocol suite. Barriers are in the accommodation of large scale populations of IoT devices in the Internet as well as in the availability of practical skills for setting up of hardware and software. Our university setup strategy for IoT deployments and accompanying functionality is depicted in Figure 2 [23][24]. The development is carried as a test-bed platform termed as a multipurpose and generic IoT system. Its multipurpose is ascribed to the property that it can be deployed for various application scenarios from pure networking research to applications such as Smart Cities and Smart Agriculture. In addition, generic properties are associated with functionalities of devices that have functionality that can be adapted, usually with network administrator interventions, to many different purposes and configurations.

The protocol composition of the IoT network is given in Figure 3 [24]. In essence, the architecture consist of two types of IoT devices (*processing* and *gathering* devices with either sensory and actuation components) and two types of IoT Gateways (with standard and localised processing capabilities). Choices behind the features are explained in [24]. The network is setup to function using a model of data provisioning in two ways:

1. Data provisioning using a centralised data storage and application delivery: Data is gathered in a centralised platform and delivered in a manner suitable to application requirements. Ranges of applications are diverse subject to data processing and extractions from the centralised platform. Such a model follows the vertical setups of IoT eco-systems.

2. Deployment of IoT Devices as independent "tiny" IP hosts: Provided by the features of CoAP [14] and CoAP/HTTP proxying [25], data collections from IoT devices are possible "directly" via standard Internet communications. The process can involve direct communications using an IP address of an IoT device (in case it is stand-alone) or via an IoT Gateway that connects its local cluster of IoT devices to the Internet.

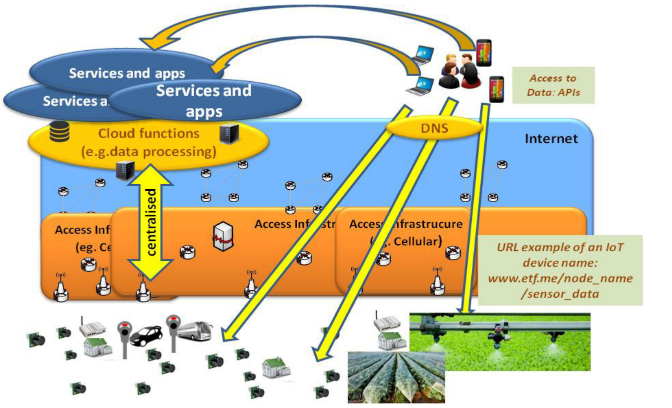
Services and apps
Services a
Services and apps
Cloud functions (e.g.data processing)
centralised
DNS
Internet
Access to Data: APIs
Access Inf (eg. Ce
Access Infr
Access Infrastrucure (.. Cellular)
URL example of an IoT device name: www.etf.me/node_name /sensor_data

Figure 2: Basic configuration of a multipurpose and generic IoT device deployment strategy

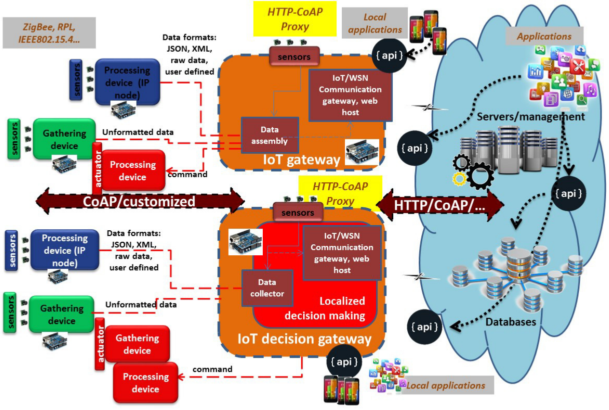

Figure 3: Composition of protocols for multipurpose and generic IoT networks [24]

B. *Discussion on the Deployment Requirements*

The architecture provides some options that are driven by considerations of uses, applications and commercialisation. These options can be discussed as general considerations for IoT deployments in the Internet:

- *(Horizontal) IoT Service Provider*: We note a necessity for formulating IoT Service Provider that allows its customers a generic and multipurpose service of IoT deployments, both using a centralised data platform and using independent IoT device/cluster deployment. The former is common nowadays, while the latter (i.e. Horizontal) is deemed needed due to skills required to setup and connect IoT devices as IP hosts, often not possible by customers themselves (this option is the focus below). This step largely differs from setting up of a conventional IP host in an office or home. In addition, such a (Horizontal) IoT Service Provider might not able to associate the connectivity of its IoT devices with the physical connectivity to its network (i.e. IoT Service Provider need not own an access network). This differs from the configuration of existing ISP providers for regular Internet hosts/customers. Rather, IoT devices by nature of the deployments are often scattered and connected over various access networks and physical location (e.g. in diverse locations in cities)[4].

- *IPv(6) Addressing*: It is realistic to assume that locations of IoT devices are not to be bound to deterministic network locations (subject to customers preferences) and that such configuration might not be static, i.e. IoT can be mobile (e.g. vehicular, re-deployments etc). Following this, sole assignment of IPv6 addresses might not suffice to enable the connectivity of large populations of IoT devices to the Internet. It is often the case in the current networks that IP hosts receive a temporary IP address (or private IP address due to Network Address Translation). A question might be how to bind an IP address of an independent IoT device into DNS. In other words, assuming a standard API such as REST is applied to pinpoint data unto an IoT device, i.e. DNS needs to resolve the IoT device's URL/URI to the exact network location/address.
- *IoT DNS Extensions*: Limitations of DNS for IoT Networking via Internet (i.e. TCP/IP architecture) are already noted in [26] considering DNS-based service discovery (DNS-SD) [27] and CoAP based Resource Discovery [28]. However, these discoveries are relevant when IP address of an IoT Gateway or device is known and where a resource can then be appropriately queried. In the model we advocate, it is assumed that customers usually know the resources they want to fetch or control, hence, the priority is in establishing a simplified means of reaching the device. In the horizontal deployment discussed in this paper, we focus on resolving large scale URL/URI-to-IP address mappings to locate the IoT device(s). We foresee some options for modifications of the standard DNS mechanisms and extension of APIs (e.g. REST API) to accommodate for the specifics of IoT deployments:

  a) *Extensions to DNS's name-to-address resolving steps*: Devices' names and query can be contained in the URL/URI description of the IoT. This step supplements and/or precedes the mentioned CoAP Resource Discovery and its Link Formats and assumes that users/customers will ping their devices with pre-set names and known resources. Such an assumption is based on the existence of the IoT Service Provider. An example URL/URI structure can include an IoT Service Provider's domain name (e.g. http/coap://etf.me) followed by URI/URN fields such as path and query that can contain the device's name and preset syntax describing its resource or a more complex query logic.

  b) *Scaling DNS by localised Registries*: Following the described model for (Horizontal) IoT Service Providers and the global projections for billions of IoT connected devices it is reasonable to expect that DNS needs to be scalable to accommodate for the explosion of "tiny" IP hosts. We foresee a two-way DNS URL/URI resolving where the first address resolving can point to a localised IoT DNS/Registry that keeps bindings of current IP addresses of IoT Devices/Gateways and redirects the application layer request (e.g. using HTTP/CoAP redirection) to provide the current address of the IoT device (analogous to dynamic DNS or mobility management agents). It is assumed that this step will contain the necessary authentication and protection against malicious attacks (e.g. by naming or authentication steps) before returning the address locations of IoT devices.

IV. Vision of Extended Named-Data Networking for IoT

NDN paradigm fits with the nature and requirements of IoT communications. As much of the IoT communication is proactive and concerned with data delivery of small chunks of data, using a search driven NDN routing can accordingly fit with distribution of data from IoT devices. There are already numerous positioning papers and trial solutions that couple NDN concepts [18][19] and IoT deployment [15][16][19][20] [21][22]. As NDN is about using "data interest" as the search and routing pointer, the IP discovery methods such as the conventional DNS are obsolete. Examples of IoT NDN implementations include setting up of data repositories in buildings where sensory/actuation data is obtained using the data search, then, vehicular network etc. The search usually reflects the nature of sensory/actuation hardware (i.e. the name of the data) and it is fairly simple (e.g. room temperature in a building etc).

We extend the thinking behind the NDN application for IoT with a vision of a broader inclusion of search items, that is, data names that describe IoT devices. This leads to the meta-data that would present the comprehensive description of IoT devices and include some of the following items for its discovery (more is given in [29]):

- **Physical location**: a search can include the actual physical location as the main search criteria, e.g. a city region such as a square, geographical coordinates/tags, streets, buildings etc. Currently, users refer to prior knowledge of the web address/apps of the IoT provider in the relevant area. Running a web-level search using a city's region as the IoT-search-item would be rather inefficient in finding the local devices and services.
- **Timely dimension**: values, statues and device populations are highly dynamic.
- **Ownerships**: knowing the responsible company, public body or individuals that own the IoT devices or services and certify the data, would make the search and data fetching more meaningful. It would define the trust and data integrity framework.
- **Connectivity**: a defining item of the search can include network or access location, such a seeking specific (cellular) network operators or wireless access points. This option can also apply addresses (e.g. IP address or subnet).
- **Data Type, Name, Status and Query Logic**: running a generic search such as "weather conditions", a URI path/query segment, or applying a simple query logic (e.g. seek only weather values from a public provider/owner in a city area)

[4] Emerging Low Power Wide Areas IoT networks aim to offer direct access to IoT provider networks

would render a targeted and relevant resolving of the information and is already contained in NDN solutions for IoT. **The search for IoT devices and their data and services would be an opportunistic and near-match action**. The vision is targeted as a future research direction for large scale implementation of IoT devices such as in Smart Cities. As shown in Figure 4, locations of data repositories can be distributed at various locations in networks, from gateways, to elements in the access infrastructure to public/private databases with web-level maps in cities.

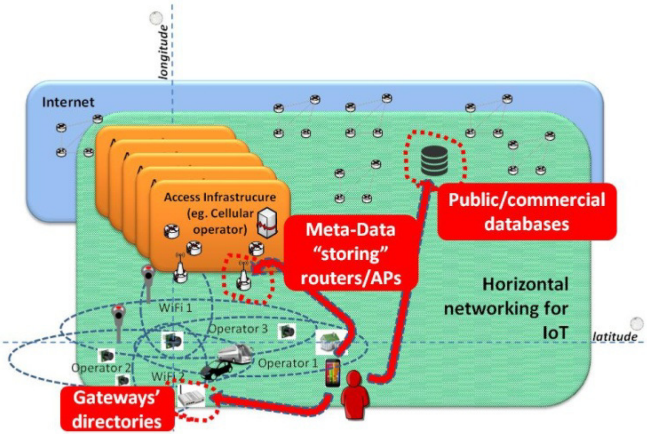
longitude
Internet
Access Infrastructure (eg. Cellular operator)
Meta-Data "storing" routers/APs
Public/commercial databases
Horizontal networking for IoT
latitude
WiFi 1
Operator 3
Operator 2
Operator 1
WiFi 2
Gateways' directories

Figure 4: Examples of locations of IoT data for NDN-driven horizontal networking for IoT communications (from [29])

V. CONCLUSIONS

This paper contains an analysis of deployment options for IoT termed as horizontal and discusses topics that diverge from the current typical configurations of IoT eco-system. The current eco-system generally fit into a structure that is considered as vertical, referring to the composition of the elements of the eco-system, from IoT devices to web-level applications. Such configurations are relevant to deployments of IoT in large scale urban environments, i.e. Smart Cities. We give two alternatives driven by the expectation that IoT will be deployed in a liberalised manner not bounded by provider services of today. The first alternative observes adaptations needed in the conventional Internet setups for supporting a large population of IoT devices. The other one considers extensions to NDN novel routing paradigms that can fit with the nature of IoT communications.

Acknowledgment

Work is funded by European Union project Fore-Mont as a part of Seventh Framework Programme (Grant Agreement No. 315970 FP7-REGPOT-CT-2013) http://www.foremont.ac.me.

References

[1] D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.), The Internet of Things, Springer, 2010.

[2] L. Atzori, A. Iera, G. Morabito, "The Internet of Things: A survey", Computer Networks, Vol. 54, Is. 15, pp. 2787-2805, October 2011.

[3] M.R. Palattella, et all, "Standardized Protocol Stack for the Internet of (Important) Things," Communications Surveys & Tutorials, IEEE , vol.15, no.3, pp.1389,1406, 3rd Quarter 2013.

[4] M.R. Palattella, et al, "Internet of Things in the 5G Era: Enablers, Architecture and Business Models", IEEE Journal on Selected Areas In Communications, 2016

[5] L. Mainetti, L. Patrono, A. Vilei, "Evolution of wireless sensor networks towards the Internet of Things: A survey", IEEE 19th SoftCOM conference, Croatia, Sep. 2011

[6] "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020". Gartner, 2013-12-12, http://www.gartner.com/newsroom/id/2636073, Retrieved 2014-01-02.

[7] M. Compton, et al., "The SSN ontology of the W3C semantic sensor network incubator group", Web Semantics: Science, Services and Agents on the World Wide Web, Volume 17, December 2012, pp. 25-32

[8] P. Barnaghi, M. Presser, K. Moessner. "Publishing linked sensor data", 3rd International Workshop on Semantic Sensor Networks (SSN), ISWC2010, Shanghai, China, Nov. 2010.

[9] A. Zanella et all, "Internet of Things for Smart Cities", IEEE Internet of Things Journal, Vol.1 No.1, Feb. 2014.

[10] "IEEE Smart Cities" IEEE, Web. 06 Sept 2015 smartcities.ieee.org

[11] A. Sheth, C. Henson and S. S. Sahoo, "Semantic Sensor Web," in IEEE Internet Computing, vol. 12, no. 4, pp. 78-83, July-Aug. 2008.

[12] G. Mulligan, "The 6LoWPAN architecture", 4th Workshop on Embedded networked sensors, EmNets, ACM, Jun. 2007, Cork, Ireland.

[13] T. Winter et al, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, IETF RFC 6550, Mar. 2012.

[14] C. Bormann, A. P. Castellani, and Z. Shelby, "CoAP: An Application Protocol for Billions of Tiny Internet Nodes," IEEE Internet Computing, vol. 16, no. 2, pp. 62–67, 2012.

[15] W. Shang et al., "Named Data Networking of Things", 1st IEEE International Conference on Internet-of-Things Design and Implementation, Apr. 4-8, Berlin, Germany 2016.

[16] M. Amadeo, C. Campolo, A. Iera and A. Molinaro, "Named data networking for IoT: An architectural perspective," European Conference on Networks and Communications (EuCNC), Bologna, 2014, pp. 1-5.

[17] E. Baccelli, C. Mehlis, O. Hahm, T. C. Schmidt, and M. Wählisch, "Information centric networking in the IoT: experiments with NDN in the wild". 1st international conference on Information-centric networking (ICN '14) ACM, 2014 New York, USA, pp. 77-86

[18] L. Zhang et al, "Named Data Networking", ACM SIGCOMM (CCR), Jul. 2014.

[19] V. Jacobson, D. Smetters, J. Thornton, M. Plass, N. Briggs, R Braynard, "Networking named content", In Proceedings of the 5th international conference on Emerging networking experiments and technologies (CoNEXT '09), ACM, New York, USA, 2009.

[20] W. Shang, Q. Ding, A. Marianantoni, J. Burke, L. Zhang, "Securing Building Management Systems Using Named Data Networking", IEEE Network, vol. 28, no. 3, pp. 50-56, May/June 2014.

[21] J. Burke, P. Gasti, N. Nathan, G. Tsudik, "Securing Instrumented Environments over Content-Centric Networking: the Case of Lighting Control", IEEE INFOCOMM 2013, NOMEN Workshop, Turin, Italy, Apr. 2013.

[22] G. Grassi et al, VANET via Named Data Networking", IEEE INFOCOM NOM Workshop, Toronto, Canada, April-May 2014.

[23] A. Mihailovic, M. Simeunović, N. Lekic, M. Pejanović-Djurišić, "A strategy for deploying diverse sensor-based networks as an evolution towards integrated Internet of Things and Future Internet," 22nd TELFOR, Nov. 2014, Belgrade, Serbia

[24] M. Simeunović, A. Mihailović, and M. Pejanović-Djurišić, "Setting up a multi-purpose internet of things system," 23rd TELFOR Nov. 2015, Belgrade, Serbia

[25] A. Castellani, S. Loreto, A. Rahman, T. Fossati, E. Dijk, " Guidelines for HTTP-CoAP Mapping Implementations", Internet Engineering Task Force (IETF) Interent-draft, draft-ietf-core-http-mapping-04, Jan. 2015.

[26] W. Shang, Y. Yu, R. Droms, L. Zhang, "Challenges in IoT Networking via TCP/IP Architecture", NDN Technical Report NDN-0038, Feb. 2016

[27] S. Cheshire and M. Krochmal, "DNS-Based Service Discovery", RFC 6763 (Proposed Standard), Feb. 2013.

[28] Z. Shelby, M. Koster, C. Bormann, and P. van der Stok, "CoRE Resource Directory", draft-ietf-core-resource-directory-05, Oct. 2015.

[29] A. Mihailovic, "Liberalising Deployment of Internet of Things Devices and Services in Large Scale Environments". Springer Journal Wireless Personal Communications, Nov. 2016.