Wireless Pers Commun (2017) 92:33–49
DOI 10.1007/s11277-016-3837-0

Liberalising Deployment of Internet of Things Devices and Services in Large Scale Environments

Andrej Mihailovic[1,2]

Published online: 4 November 2016

Abstract There is an ongoing enormous expansion of Internet of Things devices and services in everyday life, notably in novel large scale urban environments called Smart Cities. There, availability and uses of Internet of Things by end users and businesses is mainly palpable subject to prior knowledge of the relevant providers and use of dedicated applications that are associated with them. This current reality can be largely ascribed to the property of "verticality" of autonomous Internet of Things eco-systems in Smart Cities, where Internet of Things devices (e.g. sensor nodes) are connected over a communication infrastructure to service-cloud platforms that deliver and process data that is then presented at the applications level. This paper explains possibilities for revolutionary changes needed towards liberalising deployment and visibility of IoT services and data associated with them. It advocates a conceptual approach termed "horizontal networking for Internet of Things" facilitating a more open and generic presence of Internet of Things through the proposed Internet of Things identification meta-data. The vision is built on needed novel practical features in the current communication setups. The features comprise combinations of the opportunistic and near-match search and discovery model, Internet of Things identification meta-data also reflecting the physical and network-based dimensions of devices' locations, novel routing and data flow models emerging via Information-Centric Networking and changes required in the elements of the current telecommunication infrastructure and the Internet.

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

✉ Andrej Mihailovic
andrej.mihailovic@kcl.ac.uk

[1] Centre for Telecommunications Research, King's College London, Strand, London WC2R 2LS, England, UK

[2] Research Centre for ICT, Faculty of Electrical Engineering, University of Montenegro, Bulevar Dzordza Vasingtona bb, 81000 Podgorica, Montenegro

1 Introduction

The emerging IoT (Internet of Things) systems and their compositions are wide ranging. IoT systems span from independent or small-scale installations of communicating IP-capable device(s), to large scale deployments of autonomous cloud-enabled IoT eco-systems in urban environments (i.e. Smart Cities). Properties of IoT devices (i.e. "things") also vary, from simple autonomous sensor nodes or actuators (or clusters of them), to unconstrained machines capable of smart operations and PC-like processing [1]. At this moment, an underling consensus of the global IoT initiatives and visions sees IP reachability and connectivity as the defining property of IoT communications. It is projected that there will be as much as 26 million devices with IP reachability by 2020 [2] by unleashing the IPv6 extended volume of addresses. Deployment trends show [3, 4] that IoT are nowadays associated with diverse application areas: from small scale eHealth solutions, smart homes, to automation of production processes, then, agriculture applications, smart cities, transport applications etc.

As the full impact of the worldwide endorsement of IPv6 addressing lingers, many current autonomous IoT systems are effectively hybrids of configurations of Wireless Sensor and Actuator Networks that emanate their data to the Internet level of visibility via dedicated transitional features [5–8]. Hence, IPv6 addresses and reachability for each "thing" in the Internet is far from being fully realized and, in fact, for a large number of small devices and associated services it is neither realistically achievable nor required. Examples can include minute sensors with minimum processing and communicating capabilities. On the other hand, many such IoT installations can use a gateway-cluster type of configurations where the gateways handle the IP addressing and connectivity to the Internet. They can then compress the IP protocol inside the cluster of "things" using 6LoWPAN protocol [9] and launch internal routing inside the clusters, e.g. using RPL [10]. To accompany this, application level protocols that facilitate functioning of "things" as web servers are also available: CoAP [11], MQTT [12], CoAP/HTTP proxying [13] etc. Therefore, either as standalone or via a gateway, "things" can be connected "directly" to the Internet as IP hosts and act as web servers.

Diversity of IoT scenarios creates another set of technical requirements that generate a different model of connecting "things" to the Internet. Due to scenarios of large scale implementations in urban, Smart City cases [14] and formations of European open platforms[1] and dedicated standards[2] [15], IP reachability of stand-alone devices and gateways is often not a dominant requirement. Rather, data from devices is being presented onto the web level of the Internet after processing at dedicated, often commercially and administratively closed data processing installations (e.g. a platform/cloud run by a Smart City company). Such emerging IoT systems can be defined as enclosed architectures of data delivery and presentation that are assembled as autonomous platform/cloud-based service compositions. They typically run over the existing communication infrastructures, thereby constituting Smart City IoT eco-systems. These IoT eco-systems have a common underlying practical composition that characterizes their architecture and technical requirements: there are dedicated functionalities that connect and collect data from "things", before these are presented in applications. In simplified terms, "things" are inactively connected to the Internet via their stemming data after it has been processed, linked or often simply gathered

[1] https://www.fiware.org/2015/03/25/fiware-a-standard-open-platform-for-smart-cities/.

[2] http://www.itu.int/net/pressoffice/press_releases/2015/22.aspx#.VtQYyVJcAnJ.

within a dedicated IoT eco-system architecture. Hence, IoT environments often grow without the IP connectivity of standalone devices or gateways as the prerequisite meaning that data is not directly fetched from them by users.

The content of the paper is founded on the current picture of the expansion of IoT eco-systems sketched in the previous paragraphs specifically in the dense and commercially-driven environments such as Smart Cities. Novel conceptual directions of integration are formulated that can open ways for solutions that would liberalize IoT proliferation, deployments and services. By this notion it is meant that IoT devices are to be freely deployed in the future and integrated in the global Internet populations with the main property that their discovery and use will not be tied to a vertically composed IoT eco-system presented above the service levels. They would be more flexibly integrated and visible elements of the available units of technology in everyday life and environments.

The underpinning argument of the paper is that IoT devices' and services' search and discovery can be revolutionised if IoT identification is widely accepted and promoted to reflect the nature of IoT connectivity and data provisioning. In practical terms, this means that the search and discovery would go beyond the knowledge of the service and application levels (e.g. a web address of a service provider). As IoT future is tied to IPv6 addressing its deployment can be galvanized if IoT devices are integrated in the Internet and cellular networks as its "special" IP hosts. The challenge arises due to the "things", to a large extent, distorting the standard Internet communication that relies on a reactive communication model of regular IP hosts. IoT communication model is largely proactive, i.e. "things" automatically communicate data by emitting small chunks of data values or statuses (sensor data is usually from 10 to 100 bytes in size) that are collected and presented at application level points.

Content of the paper is organised as follows: Sect. 2 discusses concepts of IoT communications and current principles of the Internet, analysing the related work on the subject and thereby giving the case for the specific angle of the vision supported in the paper. Section 3 outlines functionalities that would facilitate the shift towards liberalized IoT deployment and data distribution by presenting envisaged scenarios, needed functional enablers and implementation issues. Section 4 concludes the paper.

2 Formulations of the Concepts for Novel IoT Communication Models

Verticality of IoT (eco)-systems, is often applied to note the property of how systems are composed from actual devices/"things" to presentation of data at the service and applications layers.[3] This is a generalization and many IoT deployments can in fact be interpreted as not entirely abiding to this generic system form. However, verticality is here applied as a general property in a light manner in order to highlight the flow directions of control/data and setup of architecture elements that justify the purpose of IoT deployment (e.g. for data collections). The left side of Fig. 1 sketches a simplified layout of an IoT eco-system's architecture blocks. The chosen IoT eco-system setup shows a large scale deployment of IoT in Smart City environments, consisting of installations of "things" at the physical (ground) level, their communications via access infrastructure (e.g. cellular

[3] 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." There are numerous projects that started recently addressing the challenge.

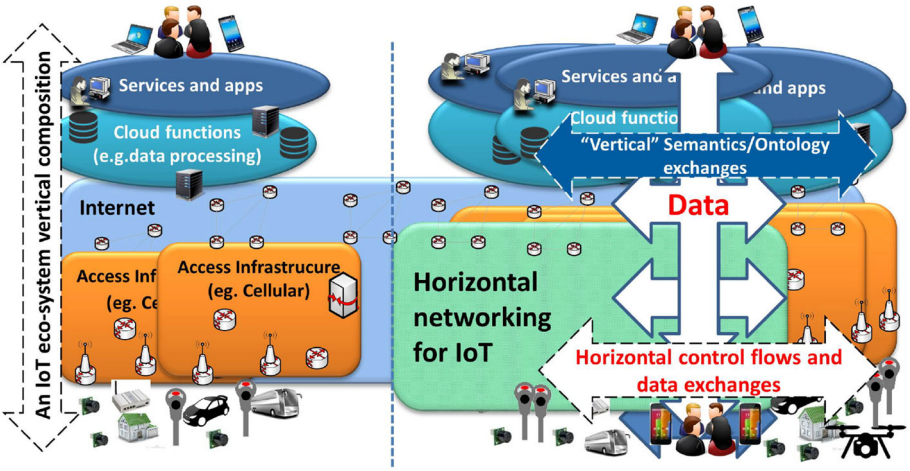

Fig. 1 IoT eco-system(s) verticality and placement of horizontal networking area

networks, WiFi hot-spots etc.), then, via Internet communications to the installations of an 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 offerings to users. Such a setup constitutes the *vertical composition of an IoT eco-system.*

Right side of Fig. 1 draws out a combination of topics that form the basis for the postulates discussed in the paper by showing coexistence of a large population of IoT eco-systems belonging to different service/application providers (e.g. such scenarios are now existent in many Smart Cities). It shows a contemporary challenge for interoperability and convergence of IoT eco-systems in the forms of collaborations and exchanges of data at the data processing and/or cloud level (e.g. using standardized semantics or ontological data structures as depicted in Fig. 1 [16–19]). The need for such a convergence of IoT eco-systems has been recognised from the early advent of the impact of IoT diversity in many environments including the foreseen growth in Smart Cities [18]. There are significant solutions and platforms available for interoperability at the eco-system level [18], e.g. provided by EU collaborative initiatives such as FI-WIRE, IoT-A architectures etc. Although such global solutions would greatly increase the deployment efficiency of a city-wide IoT system and improve the visibility and availability of data, aligning complex data structures such as semantics or ontology between different eco-systems is a complex global task both in terms of the (subjective) logic applied to link the data and lack of incentives for complete interoperability. Reality sees the drivers of IoT services in Smart Cities often dictated by independent Smart City companies and there is also a significant share of the IoT population to emerge via stand-alone IoT devices and clusters that can independently connect to the Internet as web servers (as mentioned in the previous section).

In addition, even if the interoperability and convergence is greatly improved at the cloud/middleware level and complementarities between the data models are working, some properties of verticality and eco-system separations would still apply (visibility of processed data at the level of applications). As shown in Sect. 3 some of the features proposed in the paper are agnostic to data languages/model (e.g. ontology) as a near-match search and discovery principle is proposed and based on the novel revolutionary approach of networking facilitated by concepts of Information-Centric Networking (ICN). To facilitate

that, a simplification of IoT descriptions is the essential requirement to facilitate the discovery of IoT data and services in liberalised scenarios. The need for liberalisation of IoT discoveries, hence deployments, is recognised through expecting very high density of IoT devices and providers to be present in Smart Cities. Solutions that provide quick discovery and access to IoT data might be facilitated by novel networking methods and are more fitting with the reality than expecting alignments at system levels as existent today. However, it is noted that while direct IoT data fetching might be sufficient in many scenarios, some IoT services are only possible after data has been further processed and linked, in which case, interoperability and convergence at the system level are necessary. This intersection defines the specific contribution of the paper towards the property of horizontality of IoT data and service distributions.

Figure 1 also shows the explanatory concept termed *horizontal networking for IoT*, distributed in the Internet, arbitrary access infrastructure and IoT devices on the physical level. It primarily explains communications and control/data flows from IoT in almost direct manner surpassing the need to obey the vertical compositions in some instances of communications.

2.1 Conceptualisations of a Case for Liberalising IoT Deployment

The main concepts are discussed below using some key observations of the properties of IoT communications:

2.1.1 Proactive Nature of Data Flows in IoT Communication

Application-level visibility of IoT data is the effective outcome of many IoT services, whether the needed IoT data is directly emanated by devices/"things" or whether it is firstly processed or linked (i.e. data/cloud processing towards applications). An example can be a parking space occupancy solution in a city street supported by parking slot sensors and delivered via Smart City company's applications. A user as a service beneficiary could be located in the proximity of IoT device(s) that generate such data. Data harvesting is typically a proactive action. The IoT data can be either pulled or pushed (something subscribed to) "into" the system upon a change or obtained periodically. The user receives data from the system, de facto from an intermediary location, i.e. as a web level data presentation. It often does not directly contact the sensor. A disparity can be noticed with the way the traditional Internet data exchanges occur, that are mostly reactive: there, a user establishes an end-to-end communication after discovering the IP address of the end-host of its communication request, e.g. using DNS. Hence, the conventional way is that the communication is setup between the actual IP hosts: data source and data seeker; in IoT setups, as described, data undergoes collections, and sometimes processing, via service platforms.

2.1.2 Different Fundamentals of Search and Discovery of IoT Devices, Services and Data

As explained in the previous sub-section, in IoT, data flows happen proactively, while the typical Internet communication it is reactive.[4] Then, IoT is not about the end-points as in

[4] Due to expanding types of IoT/Internet devices and services, exceptions or hybrids are likely between proactive and reactive communications.

the typical Internet communications. End-points in IoT are generally active in data delivery, not in session establishment with whoever seeks the information as in the conventional Internet. As the Internet's engines are DNS lookup and web-level searches (e.g. Google) a similar notion would apply for IoT discovery. However, IoT bring a physical, spatial, timely, use-related and connectivity factors in the equation when thinking about the search and discovery. As shown in [16], some of these factors have been recognised as key descriptions of sensors from the early advent of the technology and have in fact been the triggers for development of Semantic Sensor Web (SSW) using ontology languages such as OWL/RDF that are being perfected by international initiatives and working groups [17, 19]. Much of the SSW ideas have gone into complex environmental descriptions and application-level search and processes. In the following, some of these are revisited as rudimentary dimensions of space, time, connectivity and ownership and are extracted as items that would facilitate the simplified *search and discovery* fundamentals for liberalised IoT deployments:

- *Physical location*: e.g. when in a city area such as a street, a search can include the actual physical location as the main search criteria. The physical location can also include geographical coordinates/tags, regions, streets, building etc. Currently, users know the service in advance by knowing the web address/apps of the IoT provider in an area. Running a search with a city's region such as a street using the traditional Internet search engine would be futile or require a skilful or lengthy searching to discover the location-related IoT service(s) of the actual IoT provider.
- *Timely dimension*: what is being searched for often has a real meaning if time is known or recorded.
- *Ownerships*: knowing the responsible company, public body or individual (sometime even devices' manufacturer) that own the IoT devices or services and certify the data, would make the search and data fetching more meaningful. Quite importantly, 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 also applies to addresses (e.g. IP address or subnet[5]) as connectivity identifiers.
- *Data Name, Attribute, Status and Query Logic*: running a generic search such as "temperature" or "traffic congestion", a URI name or path/query name segment (more on naming is given in Sect. 3), or applying a simple query logic (e.g. seek only air pollution values from a public provider in a city location) would render a targeted and relevant resolving of the information. In addition, an open search could return some of the previous items such as the physical location, time, ownership, cell ID etc. In other words, it can facilitate the actual discovery of IoT devices and their data relative to a user's location.

While the above list is neither exhaustive nor mandatory for all items listed, it serves to elucidate the shift from the traditional Internet regarding the information needed to facilitate the IoT search and discovery. Currently, much of the IoT data formulations are concerned with data names and attributes. In order to link data with a more complex relevance and interrelations sophisticated semantical and ontological solution [17–19] are proposed. However, they are yet to be universally endorsed, aligned, federated and globally understood. Most importantly, IoT eco-system providers such as Smart City

[5] It is difficult to imagine a scalable DNS system for IoT devices if there would be billions of them in the future and identical to the DNS use for standard IP hosts.

companies are likely to use their own closed models. The solutions discussed in the paper are of less descriptive complexity and relate to meta-data that would facilitate the direct search and discovery principles of IoT communications. These would be relevant in scenarios of diverse large scale deployments of many IoT devices belonging to different owners and providers and densely scattered in cities. As such they would enable more liberalised integration and visibility of such devices in the fabric of Internet.

Another argument here is that the more complex data semantics/ontology are items of information that are relevant after data has been fetched by a user on the ground or are already inside the eco-system. The search and discovery explained "happens before" referring to user-centric search for IoT devices that can happen in real situations in cities. IoT communications could be significantly augmented if there are available information that define the presence of IoT devices in the physical, communication, timely and ownership dimensions, as reasonably simple data fields.

2.1.3 Emerging Novel Networking and Routing Models

The traditional host centric and packet forwarding models of the Internet routing fabric are working well but are also evolving. In a nutshell, Internet routing is currently based on processing IP addresses in routers using simple forwarding rules. For an envisaged future grand population of billions of IPv6 IoT devices there are few immediate concerns (practical problems of IoT Networking and traditional TCP/IP suite are given in [21]):

1. *topological relevance of stand-alone IP-enabled IoT devices/gateways* could become a big future puzzle when put in practice. It gets further complicated if permanent/temporary address allocations are shuffled and a significant percentage of IoT devices is mobile.
2. *the proactive nature of IoT communications*, as discussed previously and due to the verticality of IoT eco-systems, leads to a consideration that the appropriate routing model for IoT is not the end-to-end host-centric reactive model applied in the Internet. Rather, in large scale dense IoT environments, the new models should be a means to discover and fetch data from IoT devices with relevance to locations and to facilitate such a makeshift horizontal networking flow of control and data harvesting (e.g. between users and local IoT devices).

Two novel trends in networking can be extracted that support the case of IoT paradigm shift:

- *On-demand and flexible routing installations*: This is being enabled by Software Defined Networking (SDN) solutions [22] via abstracted separations of control and data planes in network infrastructures. A control entity (control plane) can install routing commands in programmable routers (data plane) upon a flow/session communication request. A communication request in IoT can be search and discovery step (as an "IP-less" layer2/3 message), hence, network's control can point to data location[6] or install routing pointers/deliver the actual data. In addition, data flows in IoT are often localised, sporadic, bursty and small. SDN solutions can surpass the conventional routing rules of today's networks and allow for (localised) networking framework that accommodates for the specific nature of IoT communications.

[6] Instead of the conventional request that uses the destination IP address as the pointer of the routing solution.

- *Routing based on the context of the search*: The pivotal new thinking is embodied in the Named-Data Networking (NDN) [23] proposal that follows an ongoing line of research under Information Centric Networking [24] for traditional Internet type communications. To summarize, data that is sought is specified as the Interest search packet by the receiver/seeker (e.g. data is identified similar to URLs) and such Interest travels "upwards" towards the data source or intermediate storing routers as a search-and-path-establishment packet. When the data content is found at an intermediate router, it follows back the search path. The concept has initially been recognised as very fitting to IoT environments [25] and has already been proposed and trialled as a solution for IoT search and collections at scoped campus-type environments [26, 27], automation scenarios in buildings [32], direct intercommunications between vehicles [20] etc. In these cases the search Interest packet specifying the assigned data name is a preset data structure that specifies the data type (e.g. temperature, humidity, noise, voltage, on/off indications for environmental conditions or actuation states…) and the named location (e.g. a room in building [27]). Recently, a summary of NDN potentials and solutions for IoT was surveyed and grouped as ranges of issues and challenges [28]. In parallel, there is a notable novel proposal for ICN/NDN-based IoT solution [29] using a slightly different search and routing model than the mentioned NDN for IoT solutions but following the same conceptual foundations. Rather than performing a name-based search from the very initial search step, in [29] the search first locates the root CoAP-based Resource Directory (RD) as specified in [30] using IP address/URL of the RD (i.e. via DNS or pre-configuration with RD's IP address). From then on, the search can continue to other RDs located at nearby network elements (i.e. gateways, access points, routers) using NDN principles. Interestingly, the solution in [29] does not directly use a specific NDN-type names for IoT (e.g.*/ndn/kcl.edu/strand_building/1st_floor/room_17/temperature*) for each IoT resource but uses a more scalable and manageable generic and opportunistic search process using attributes of IoT data (e.g. "traffic") and following the format of IoT data annotations used by CoAP [11] and specified as CORE Link Formats [31]. If an immediate match is not found, the RD distributes the attribute-based search to all network elements acting as RDs before match(es) are found. While these solutions are already on the path of offering realization of some of the concepts proposed in this paper, in a liberalised IoT scenario, search and discovery would be much broader and liberalised in terms of the information that describes the search (as explained in bullet point 2) of this section and in Sect. 3) and would be done on a larger and open scale by being facilitated by the whole communication setup as in city environments. Hence, the *horizontal networking* concept is highlighted to indicate the shift towards "horizontal" control and data flow directions.

There has also been a significant thinking into opportunistic routing for IoT-based environments, with a related routing concept based on geographical locations of sought data sources, being a special case of the novel routing concepts applicable to IoTs. In these cases, routing is not determined by the data (neither name nor attribute) as the search (i.e. Interest) parameter, but the location of the source of the data [33] surpassing DNS as the address resolving mechanism in scoped networks. *These schemes further demonstrate that IoT communication is not always about what is being sought for, but about where an IoT device is, or, can reflect further search and discovery options subject to situations.* Clearly, in order to facilitate such flexibility and broadness of the search and discovery, knowing where and how to execute it would lead to liberalisation of IoT deployments.

3 Towards Enablers for Liberalised IoT Deployment

3.1 Envisaging Scenarios

Laying out the needed technicalities for a liberalised IoT deployment is presented in this section as a collection of hints at the future enablers and novel models of IoT communications. A generic scenario that can help in imagining the picture of the changes in IoT deployment would include a population of IoT devices scattered randomly in a city where data emanating from them or being sent to them can be harvested/transmitted by arbitrary users (e.g. located in the vicinity of the devices). Such data harvesting is done via intermediate and opportunistic collection actions. This generic scenario surpasses the rigid vertical communication models requiring web-level visibility and knowledge of the specific providers. It also opens up novel models for IoT service provisioning, e.g. via independent or operator-level providers of IoT plug&play/ready-to-deploy devices and opportunistic service compositions. Importantly, it neither excludes nor surpasses the current vertical compositions and IoT service providers. These can also conform and evolve towards the models presented, e.g. by controlled opening of their collected data to search and discovery steps. A specific scenario is described in the following reflecting on the enablers described in the next sub-section.

Scenario of liberalised IoT deployment: a driver in a car is searching for a free parking space in a city street, there is a public and a private parking nearby, one run by a public–private partnership of a Smart City company, the other by a local private parking owner. The former is connected over a different network operator than used by the user and stores data on a public database, the latter uses the same operator as the user, it is connected as stand-alone IoT network to the Internet and stores discovery meta-data in its operator's Access Point (AP) acting as a local IoT directory. User triggers a search via its smart phone and sends "parking & Geotag" using the following three methods: (1) generic API (application level): it hits the public database(s) via Internet, resolves the Geotag into local street(s) and returns nearby free parking slots information from the real-time map that belongs to the Smart City company; (2) layer-agnostic, SDN-like/ICN-type search packet sent to the AP of the operator, the AP returns the IP address/URL of the parking meter gateway of the private company found in its directory and under its coverage, user then contacts the IoT gateway of the parking meters to determine the free slot, and furthermore, receives the URL/Name of the actuator that opens the gate of the private parking (two-way search, see next sub-section) (3) layer2/3 type packet is broadcast using ad-hoc WiFi mode, the packet is received by a passing car that has stored information from the parking meters in the nearby streets and returns it to the user as list of Names and URLs of parking slots/gateways that it has collected. User builds the whole picture of the availability of parking, and check the integrity of the three search outcomes using the certificates of the messages received.

3.2 Drafting Enablers

Enablers presented in the following text open many possibilities for gradual and large-scale initiatives and trials towards liberalized IoT deployment. In is noted that some of the fragments of solutions are already partly existent in many IoT proposals mentioned. The main areas are hereby grouped where the holistic enabling of new technologies would render immediate and foundational degrees of changes in IoT proliferations:

3.2.1 Identifying IoTs

Search-based provisioning of IoT data or services means that the typical Internet DNS model of resolving domain names to IP addresses might not scale when applied to billions of IoT devices, i.e. URL/URI model of RESTful web services. IoT communications are in large not concerned with traditional session establishment, rather, with sufficiently accurate fetching of data (statuses in case of actuations). While the DNS analogy for IoT would still work it would require massive storage of real time entries per device/cluster and deal with topology, mobility and temporary address assignments of IP addresses allocated to IoT devices-URL/URI. As discussed in Sect. 2, IoT search and discovery are concerned with different dimensions of how connectivity is described, not only a web-level search or IP-address-to-name resolving. Hence, the IoT identification ought to contain a multitude of identification fields that would enable the shift in the search and discovery paradigm. This forms a new meta-data that describes the place of an IoT device in real and communication environments. As noted previously, there are neither restrictions nor requirements on data models/languages that can be used for the IoT identification meta-data. A logical recommendation is that these should be simple fields that facilitate resolving of the opportunistic and near-match search and discovery discussed under 2) below. The fields of the identification meta-data can include:

1. *Name, attribute, status, simple logic:*[7] Reasoning can be as follows: Name can refer to a full, standardised and/or conventional naming, e.g. using URL/URI/URN annotations, NDN-names, data-trees etc., where names are structured identities that are used in examples of today. *Attribute(*s) can be additional descriptive simple common-sense semantics, extracted from names, or just referring to IoT device characteristics (e.g. "temperature", "traffic congestions", "parking slot", "humidity" etc.). The term *attribute* is used to fit with the current use for IoT resource identifications as in [30, 31] and can be logically associated with: "rt" (resource type) or "if" (interface) fields but can use broader context as "title" that is used in web-based semantics, path/query segments of URI or simple human conventions. The term *status* adds the actuation dynamic to the identity. *Simple logic* can include combinations of identification meta-data (e.g. street_name & traffic)
2. *network locations:* e.g. IPv6 addresses, network operators, cell/access point ID…
3. *physical locations*: geographical location (e.g. street, building) or GPS coordinates…
4. *ownership, certificates*…

This would form the IoT meta-data fields that should describe any piece of information related to IoT devices. In conceptual terms, the tradition Internet already contains analogous meta-data structure using simple fields, this being contained in all the packet header fields and payload that constitute the comprehensive identification of an Internet communication/session. Internet cyberspace is defined by the topological relevance of IP addresses and dimensions of layers; IoT communications add the cyber-physical dimension with physical/network locations and use specifics. As explained in Sect. 2), the whole reference model for IoT communication includes the physical and other specifics of the IoT devices' connection situations. This provokes thinking beyond the traditional OSI layering in the Internet communications as the information that facilitate control and data flows are transcending many layers and include the physical and deployment dimensions.

[7] A more general set of descriptions is used here for what is often generically termed as: resources.

The whole range of information constituting the IoT identification meta-data opens up different search logics. E.g. a user can often be concerned with running a search on discovering available IoT devices in an area (e.g. cell, geographical region) or owners/providers (e.g. public "trusted" data), then, choosing data to be fetched. As depicted in Fig. 2, user can "sense" the environment around him/her before launching a search for values of data or statuses. This *two way search* makes the solutions broader than some of the existing ones, NDN solution than need specific names to launch the search [20, 26–28, 32] and provide application-level semantics for location based parts of the name (e.g. building or room names), location-based IoT routing [33] or the resource discovery-based solutions (e.g. a client's application level command GET "/.well-known/core" that retrieves resources from a CoAP RD such as a gateway [11]) that need URL or IP address (i.e. DNS) to contact the RD [29]. Such schemes can still be launched after the initial search and discovery step using the IoT identification meta-data.

3.2.2 IoT Data Distribution

The question of how to distribute meta-data that identify IoT devices and enable the search and discovery steps opens a large collection of implementation issues. Again, these practicalities challenge the traditional ways of layering and information flows in the Internet. Some of the issues are:

- *The search and discovery process ought to be opportunistic and near-match*: Not all IoT devices need to be identified with a whole range of possible identification fields. Hence, a search would be resolved with a near-match. E.g. a search for parking meter occupancy in a specific street using "the street" as the search item would return the data matching the search. There might be parking meters that don't have "the street" in their identification fields. Similarly running a search on a network cell as the search field might only return the values for IoT devices that have the "the network cell" in the identification field (and are connected to the cell's operator). Such optional relaxation of the identification fields would make the whole system grow in opportunistic but liberalized manner that can be coherently organized or standardized in its mature implementation stages. It would surpass the scalability concerns of some NDN for IoT solutions that are based on exact name searches when generally distributed in networks (name scaling can happen only within scoped regions, e.g. buildings) and matches the "attribute" based opportunistic search as in [29].
- *Locations and ownership of databases holding IoT identification:* Envisaging the locations of databases breaks the traditional layering notions. Also, data can be localized and not repeated in all databases, the search location can determine the scope and depth of the response. IoT identification data primarily ought to be timely and give the closest to real time readings of the values on the ground, or in other words, the latest. Such a requirement projects differently depending on the type of IoT devices and period of their reporting of data. Location-wise, the databases storing dynamic and timely IoT identification data can span from commercial databases in an IoT eco-system (i.e. a smart city company) to public databases storing utility data, transport, environmental data, citizen's IoT devices etc. Similar to NDN concepts, IoT meta-data can be stored in the networking infrastructure as caches, i.e. a concept of a *storing (access) router* [23]. E.g. a router or access point would usually be part of a network operator or wireless access provider [29]. For cellular and traditional networks, the data storage capability in some of the transit components of the infrastructure would require

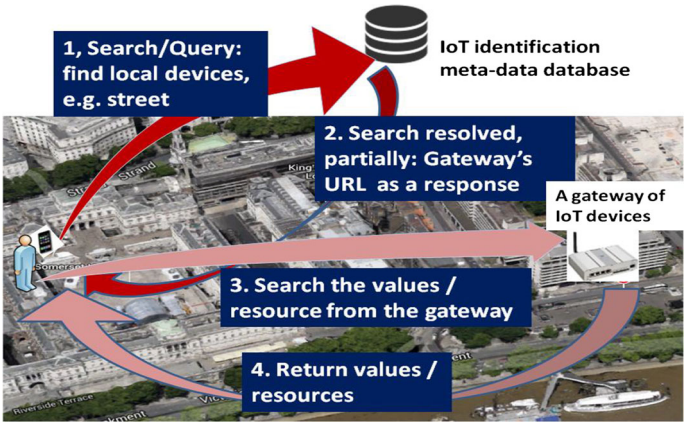

Fig. 2 A two way search example steps

similar changes as proposed in NDN, even if the storage is minimal and reduced to meta-data from the local IoT devices. One example of a wireless access provider is the access and routing infrastructure used for smart grid solution by Cisco, were storage extensions can be provided by proprietary components in the network (e.g. based on Cisco's CGR routers). Finally, the straightforward location for localized data directories keeping IoT identifications is gateways. This is already provisioned for CoAP implementation of resource directories as mentioned previously [30] regarding the action of resource discovery. Some examples of data locations are depicted in Fig. 3. Solutions in this paper propose more comprehensive search-related data such as physical locations, network access identifications etc. In fact, these can be a pre-step to discovery of gateways. This goes back to what is mentioned above that a near-match search returns a response that is subject to the search, a search for data might return an

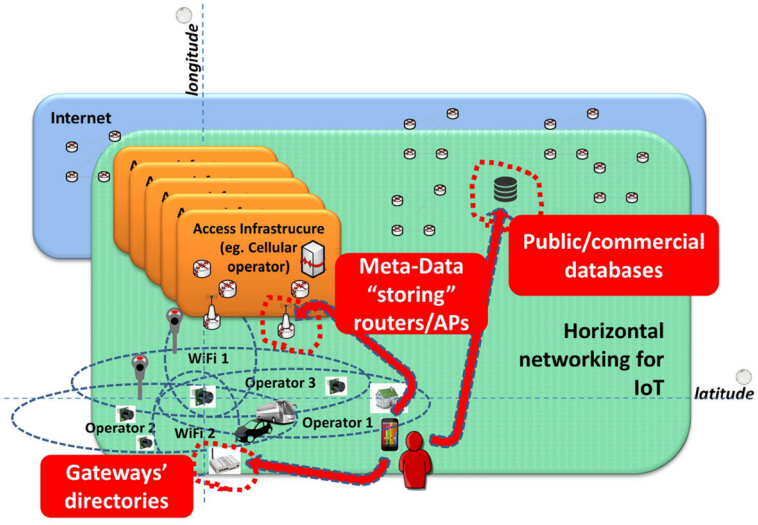

Fig. 3 Examples of locations of IoT data

address of a gateway, from where the CoAP research discovery can be applied (as shown in Fig. 2) for discovering the actual resources.

3.2.3 Facilitating Data Search and Discovery

As the overall scheme surpasses the thinking in the traditional layering sense, the actions of search and discovery are layer unbounded. They can consist of a layer-less search queries similar to NDN solutions or SDN models, public or commercial databases or a straightforward web-level API search processes, e.g. using a city area map as the search web platform. One of the main research and implementation issues would be how to direct the search to an appropriate location, as the data distributions are opportunistic, near-match and distributed. Some resolving or anycast mechanisms can be enforced to locate and direct the queries to appropriate search methods and locations as shown in Fig. 3.

3.2.4 Infrastructure Support

Traditional functionalities of infrastructure elements should be reconsidered for requirements of horizontal networking for IoT. Similarly to NDN and [29], router or access elements (e.g. base stations) can be extended with storing capabilities (e.g. Store option in routers as in NDN) and enhanced to include IoT identification options and search resolving. In addition, public/private databases would be available and discoverable at global or scoped locations in networks.

3.2.5 IoT Communication Protocols

The question remains how to distribute data with IoT identification fields to suitable database locations where search and discovery can be executed, i.e. the registration step. Most of the current IoT devices either send data to dedicated databases in raw or specific formats (e.g. JSON, XML) or are dormant until a data request arrives pulling the content from the device. In fact, many IoT devices do not have capabilities to packetize or obtain all required (or some of them) fields that would complete the IoT identification meta-data. Hence, a solution could be that the intermediate points, such as gateways or routing infrastructure, add the missing fields or some fields that such entities are capable of adding. The fields can include Geotags, physical locations, network level locations, IP addresses of gateways, ownership etc. Likewise, the fields can be appropriately added by databases, e.g. a database holding data for a building can add the building identifiers as the data tree for all data available inside it [27, 32].

3.2.6 Novel Routing and Communications

Continuing the previous two items, communication protocols would include search-based requests as the inherent features of the horizontal networking. Principles can be matched to NDN data searches, or some generic API scheme, however, in liberalized IoT deployments a search packet might not include the data being searched for but a general discovery of data sources as discussed previously. In addition, sending of the search packets would depend on the scenario as it might be sent “upstream” the networks or targeted to data location, or, directly to gateways or IoT devices [20].

3.2.7 Overall Security Considerations

Liberalisation of IoT deployments induces great challenges for opening data distributions. Besides the vast security, privacy and trust challenges encountered in IoT communications [34], a related paradigm shift is already noted in NDN [24, 25, 28] and explained as a specific novel set of security considerations. These specific challenges arise due to the departure from the traditional end-to-end security model as applied in the traditional Internet. In the case of liberalized IoT deployment: data and control, i.e. responses and searches, then, field additions by intermediate entities or databases, then, data locations and many other technicalities all add novel and diverse security challenges. Such a collection of issues calls for another extensive study outside the reach of this paper. In order to present the challenges, the following analogy can be explanatory: In the conventional Internet, searching data is based on the following generalisation—launching the search in an unrestricted manner, trusting the search engine, using judgment and reputation to trust the name of the content and the actual content. In some cases, content is restricted and requires authorization to access it. For IoT communications, the current vertical setup of IoT eco-systems puts the issue of data authenticity in the hands of the providers of IoT data (e.g. a Smart City company). In another scenario, a smart home user is the only authorized person to obtain the readings from the specific IoT devices. In the mentioned NDN for IoT solutions managed keys are used for piggybacking signatures or encrypting the data, sometimes even the names. This is a guiding scenario from NDN, however, does not cover all dimensions of broader, liberalized scenarios in large scale environments. There, a certifying/key entity might not be easy to establish on a large opportunistic scale, then addition of fields needs to be trusted and data integrity needs to be preserved. Information distributed can be public and private, so do the databases/data locations. Just these issues demonstrate the enormity of the challenge in liberalizing IoT deployment and distribution of data. As the system is already described as opportunistic and near-match, it is reasonably projected that there would be a process of trusted private or public databases or networks (providers) that would gradually provide the storage and availability of data in controlled and trusted manner along with the certificates/keys. Ultimately, there could be distributed collections of confidential and open data that resemble the data acquisition model of the traditional Internet.

3.3 Implementation Issues

Laying out a *roadmap* for the enablers presented in the previous subsection is unrealistic due to scope and diversity of issues that are involved. It is possible to facilitate some of the search and discovery mechanisms presented in the paper using a web-level platform such as a city area map where IoT devices are registered and pinging their presence and identifications. A private/public database can facilitate such a platform with a generic API [18] that would have the potential to grow and store IoT entries for open and authenticated access. Much of this is already existent in various forms and can be adapted to the identification meta-data and search and discovery principles. Similarly, access providers such as cellular operators can provide similar storage capabilities, i.e. as databases, or some more dynamic and smaller data locations such as the storing router/access points or other elements of the infrastructure.

The IoT identification meta-data can be parts of the existing databases of commercial or public providers. As explained in Sect. 2.1 this can be a storage step preceding more

complex processing using semantic or ontology tools. In fact such structured data would ease the processing complexity of much of the data manipulation entities in systems. Interestingly, IoT identification meta-data can serve as entries to Big Data databases as natural input of information from the "ground". Some of the early projections at the challenges existent in Big Data for IoT and Smart Cities [35] recommend feeding of structured data to real-time data systems, e.g. data that are tagged with geo-locations or similar structuring that helps in their sorting and classification. These would assist in faster real-time processing and data batching.

Finally, there are multitude of questions that need to be resolved in implementations of the solutions: *federation/convention/standardisation of meta-data describing the cyber-physical reality of IoT, scalability concerns, registration of meta-data, protocol adaptations, mobility of sensors, coupling with existing and more complex data models, integration with existing IoT eco-systems/platforms, coexistence with existing identification meta-data, embracing new models of IoT devices and their identities (e.g.* via *QR codes, NFC tags* etc.*), use of compression algorithms for IoT identification meta-data* etc. This clarifies that the solutions analyzed in the paper are not all-encompassing but tackle a particular portion of the space of IoT deployment in Smart Cities. As such they could open liberalized engagement and visibility of independent, small scale IoT devices and providers. As mentioned, the solutions are not in conflict with the expansion of the autonomous, vertical IoT eco-systems, in fact, they could allow for more open and wider data flows and provisioning. They also provide an opening for involvement of the stakeholders such as network operators in IoT data distributions and control of devices and services.

4 Conclusions

This paper outlines a holistic approach to IoT communications in large scale environments such as emerging urban IoT deployments called Smart Cities. These IoT environments are characterized by large density and diversity of IoT devices, uses and applications. More importantly, the Smart Cities scene finds new stakeholders, from smart city companies as market players, to public companies or bodies that aim to utilize the technologies for improvement of civil services in cities. In parallel, the existing stakeholders such as telecom operators are harnessing the opportunities by moving towards standardization of IoT-friendly wireless access technologies. The concept of vertically is widely recognized as a model of how IoT systems are composed, how IoT data flows and is processed before delivery to applications. It has caused a tremendous surge in services and visibility of IoT technology. However, the setup is fragmented in many system aspects and triggers research towards interoperability. This paper addresses some conceptual and technical issues that have caused the unravelling of the existing features of IoT systems. It aims to assist in interpreting the specifics of IoT communications mainly caused by the conflicting paradigms of the traditional Internet communication model with the IoT communication requirements. The analysis offers a different perspective on how the IoT communication can grow and become more inherently integrated in today's networks. The vision is long term, speculative and conceptual, however some functionalities such as (existing or new) public/private databases that facilitate the IoT-tailored search and discovery mechanisms could be aligned or installed quite soon as embryos of the shift towards the liberalised IoT deployments.

Acknowledgments 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. Core ideas had been contributed to a European Union Horizon 2020 proposal in 2015. The author expresses gratitude to the proposal team involved.

References

1. Giusto, D., Iera, A., Morabito, G., & Atzori, L. (Eds.). (2010). *The internet of things*. Berlin: Springer.
2. Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020. Gartner, 12 December 2013. Retrieved January 2, 2014, http://www.gartner.com/newsroom/id/2636073.
3. Atzori, L., Iera, A., & Morabito, G. (2011). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787–2805.
4. Palattella, M. R., Accettura, N., Vilajosana, X., Watteyne, T., Grieco, L. A., Boggia, G., et al. (2013). Standardized protocol stack for the internet of (important) things. *Communications Surveys & Tutorials, IEEE, 15*(3), 1389–1406.
5. Christin, D., Reinhardt, A., Mogre, P. S., & Steinmetz, R. Wireless sensor networks and the internet of things: Selected challenges. In *8th GI/ITG KuVSFachgespräch Drahtlose Sensornetze*, Germany, '09.
6. Roman, R., & Lopez, J. (2009). Integrating wireless sensor networks and the internet: A security analysis. *Internet Research, 19*(2), 246–259.
7. Mainetti, L., Patrono, L., & Vilei, A. (2011). Evolution of wireless sensor networks towards the Internet of Things: A survey. In *IEEE 19th international conference on software, telecommunications and computer networks (SoftCOM)*, Croatia.
8. Mihailovic, A., Simeunovic, M., Lekic, N., & Pejanovic-Djurisic, M. (2014). A strategy for deploying diverse sensor-based networks as an evolution towards integrated Internet of Things and Future Internet. In *Telecommunications Forum Telfor (TELFOR)*, 2014 22nd, Belgrade.
9. Mulligan, G. (2007) The 6LoWPAN architecture. In *Proceedings of EmNets '07, The 4th workshop on Embedded networked sensors*. ACM, Cork, Ireland.
10. Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., et al. (2012). RPL: IPv6 routing protocol for low-power and lossy networks. In *RFC 6550, Internet Engineering Task Force (IETF) RFC 6550.*
11. Bormann, C., Castellani, A. P., & Shelby, Z. (2012). CoAP: An application protocol for billions of tiny internet nodes. *IEEE Internet Computing, 16*(2), 62–67.
12. Stanford-Clark, A. S., & Truong, H. L. (2013). MQTT for sensor networks (MQTT-S) protocol specification. In *International business machines (IBM) Corporation version 1.2*, November 14, 2013.
13. Castellani, A., Loreto, S., Rahman, A., Fossati, T., & Dijk, E. (2015). Guidelines for HTTP-CoAP mapping implementations. In *Internet Engineering Task Force (IETF)* Interent-draft, draft-ietf-core-http-mapping-04.
14. Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things Journal*, *1*(1), 22–32.
15. IEEE Smart Cities. (2015). In *IEEE*. Web. 06 Sept 2015. smartcities.ieee.org.
16. Sheth, A., Henson, C., & Sahoo, S. S. (2008). Semantic sensor web. *IEEE Internet Computing, 12*(4), 78–83.
17. Compton, M., et al. (2012). The SSN ontology of the W3C semantic sensor network incubator group. *Web Semantics: Science, Services and Agents on the World Wide Web, 17*, 25–32.
18. Vermesan, O., & Friess, P. (Eds.). (2013). *Internet of Things: Converging technologies for smart environments and integrated ecosystems*. San Francisco: River Publishers.
19. Barnaghi, P., Presser, M., & Moessner, K. (2010). Publishing linked sensor data. In *3rd international workshop on semantic sensor networks (SSN), ISWC2010*, Shanghai, China.
20. Grassi, G., Pesavento, D., Pau, G., Vuyyuru, R., Wakikawa, R., & Zhang, L. (2014). VANET via named data networking. In *IEEE INFOCOM NOM Workshop*, Toronto, Canada.
21. Shang, W., Yu, Y., Droms, R., & Zhang, L. (2016). Challenges in IoT networking via TCP/IP architecture. NDN, Technical Report NDN-0038, Revision 1, February 10, 2016.
22. Granelli, F., Gebremariam, A. A., Usman, M., Cugini, F., Stamati, V., Alitska, M., et al. (2015). Software defined and virtualized wireless access in future wireless networks: Scenarios and standards. *IEEE in Communications Magazine, 53*(6), 26–34.

23. Zhang, L., Afanasyev, A., Burke, J., Jacobson, V., Claffy, K. C., Crowley, P., et al. (2014). Named data networking. In *ACM SIGCOMM Computer Communication Review (CCR)*.
24. Jacobson, V., Smetters, D., Thornton, J., Plass, M., Briggs, N., & Braynard, R. (2009). Networking named content. In *Proceedings of the 5th international conference on Emerging networking experiments and technologies (CoNEXT '09)*. ACM, New York, USA.
25. Amadeo, M., Campolo, C., Iera, A., & Molinaro, A. (2014). Named data networking for IoT: An architectural perspective. In *Networks and Communications (EuCNC), 2014 European Conference on, Bologna* (pp. 1–5).
26. Baccelli, E., Mehlis, C., Hahm, O., Schmidt, T. C., & Wählisch, M. (2014). Information centric networking in the IoT: Experiments with NDN in the wild. In: *1st international conference on Information-centric networking (ICN '14)* (pp. 77–86). ACM, New York, USA.
27. Shang, W., Ding, Q., Marianantoni, A., Burke, J., & Zhang, L. (2014). Securing building management systems using named data networking. *IEEE Network, 28*(3), 50–56.
28. Shang, W., Bannis, A., Liang, T., Wang, Z., Yu, Y., Afanasyev, A., et al. (2016). Named data networking of things. In *1st IEEE international conference on internet-of-things design and implementation*, April 4–8, Berlin, Germany.
29. Dong, L., Ravindran, R., & Wang, G. (2016). ICN based distributed IoT resource discovery and routing. In *23rd international conference on telecommunications (ICT '16)*, May 16–18, Thessaloniki, Greece.
30. Shelby, Z., Koster, M., Bormann, C., & van der Stok, P. (2016). CoRE resource directory. In *IETF internet draft*, draft-ietf-core-resource-directory-07.
31. Shelby, Z. (2012). Constrained RESTful environments (CoRE) link format. In *IETF RFC 6690*.
32. Burke, J., Gasti, P., Nathan, N., & Tsudik, G. (2013). Securing instrumented environments over content-centric networking: The case of lighting control. In *IEEE INFOCOMM 2013, NOMEN Workshop*, Turin, Italy.
33. Amoretti, M., Alphand, O., Ferrari, G., Rousseau, F. A., & Duda, A. (2014). DINAS: A distributed naming service for all-IP wireless sensor networks. In *IEEE wireless communications and networking conference (WCNC)* (pp. 2781–2786), 6–9 April 2014.
34. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Elsevier Computer Networks, 76*(15), 146–164.
35. Strohbach, M., Ziekow, H., Gazis, V., & Akiva, N. (2015). Towards a big data analytics framework for IoT and smart city applications. In F. Xhafa, L. Barolli, A. Barolli & P. Papajorgji (Eds.), *Modeling and processing for next-generation big-data technologies* (pp. 257–282). Switzerland: Springer.

Andrej Mihailovic received his B.Eng., MSc. and Ph.D. degrees all from King's College London, in 96, 97 and 2004 respectively. His main experience at King's in collaborative and individual projects: BRITISH TELECOM project on IP mobility (1998–2000); FP5 EU projects: BRAIN (2000–2001) and MIND (2001–2002) on IP access networks; individual project with SIEMENS, Germany (2002–2004) on IP moving networks; FP6 EU projects: E2R I (2004–2006) as the leader of sWP1.2 Architecture Models and Reconfigurability Management, and then in E2R II (2006–2008) as the main liaison in the WWI Cross Issues on System Interfaces/Architecture between the leading EU Integrated Projects; then, EU FP7 project Self-NET (2008–2011) as the leader of WP1: System Architecture for Cognitive Network Management. His also participated in standardizations Groups: IEEE P1900.4 on "Reconfiguration of multi-radio systems" (in 2007) and ESTI's "Autonomic network engineering for the self-managing future internet—AFI" (2011–2013). Andrej also worked as an expert for University of Montenegro under EU REGPOT Project Fore-MONT (2013–2016) on IoT solutions. He is also an EU Expert/Project Evaluator. Research areas include: Future Internet, IP routing/mobility, IoT and self-managed and cognitive systems.