EXPANDING THE CELLULAR-IOT UMBRELLA: AN ARCHITECTURAL APPROACH

AHMED IYANDA SULYMAN, SHARIEF M. A. OTEAFY, AND HOSSAM S. HASSANEIN

ABSTRACT

The proliferation of the Internet of Things hinges on the successful internetworking of billions of devices. While many approaches advocate for building on a thus-far versatile Internet infrastructure, many faltering claims for scalability will hinder IoT operation and responsiveness. At the heart of the problem, IoT is largely disparate in operational mandates, communication technologies, and access schemes. While such diversity could be empowering, the status quo lacks standardization, and these factors are hindering large-scale IoT connectivity [1]. Simply put, IoT devices are developed by different manufacturers, and hence understand different digital languages and communication procedures. A successful global IoT deployment must find ways to interconnect things, allowing data from these objects to be usable across the IoT network. We elaborate on the architectural challenges in scaling the IoT, and highlight mainstream approaches in interconnecting devices across IoT infrastructures, both physically and semantically. We propose a novel architectural approach to bridging Internet-based IoT networks with cellular-based IoT systems, and explore the ensuing development of interoperable IoT systems. We propose the inclusion of a DOI module in the cellular-network-based IoT platform that handles general IoT data access for both cellular and Internet-based IoT nodes. The DOI will implement access and identification methods transversally across the two architectures such that any IoT node could interact with this module, thereby allowing general IoT services over cellular networks. The primary contribution of this article is the introduction of the DOI in cellular networks, emphasizing how the proposed architecture can address the aforementioned challenges.

Ahmed Iyanda Sulyman is with Embry-Riddle Aeronautical University.

Sharief M. A. Oteafy and Hossam S. Hassanein are with Queen's University.

Digital Object Identifier: 10.1109/MWC.2017.1600433

CHALLENGES IN UBIQUITOUS IOT OPERATION

The unprecedented number of things that Internet of Things (IoT) networks will interconnect calls for urgent action on how these objects and devices will be jointly managed for effective global device-to-device (D2D), device-to-infrastructure (D2I), and device-to-human (D2H) interactions. Several works have thus recently explored IoT architectures that can be embraced either vertically or transversally across the industry [2–5].

There are two prominent IoT architectures being explored: cellular-network-based and Internet- or information technology (IT)-based platforms. The former is being promoted by cellular network players/standards bodies such as the Third Generation Partnership Project (3GPP) and its member companies like Ericsson, Huawei, Qualcomm, and Vodafone, while the latter is being promoted by global IT players and Internet standards bodies such as the Internet Engineering Task Force (IETF), European Telecommunications Standards Institute (ETSI), Cisco, IBM, and Telefonica [1, 2, 6]. However, IoT connectivity faces a number of challenges across both architectural umbrellas. We hereby address five major challenges that are hindering ubiquitous connectivity in the IoT.

AD HOC DEVICE IDENTIFICATION AND REGISTRATION

The core premise of IPv6-enabled identification, that is, connecting every possible IoT device to the Internet, presents significant challenges in managing concurrent connectivity (under a given gateway or access point), managing Name Address Translation (NAT) address spaces, and ensuring proper authentication for devices that no longer conform to a client-server coupling. That is, simply enabling unique identification via 2^{128} addresses over IPv6 does not imply that control, medium access control (MAC), and management planes can cater for ad hoc plug-and-play access to IoT devices. While earlier research argued for RFID-based identification [1], the scalability of this approach is capped by placement and power of RFID readers, parallel singulation approaches, challenges in coverage and capacity across RFID technologies, and sheer security/privacy challenges. Even with rapid standardization efforts, mass-scale identification using RFID remains an open challenge in IoT systems [7].

More importantly, as the IoT scales, the responsiveness of different services cannot always assume uniform packet-level routing as supported over the current Internet. In fact, significant resource management planes are needed to ensure that tactile Internet and other real-time

1536-1284/17/$25.00 © 2017 IEEE

services are able to access IoT devices with guaranteed delay and quality requirements [8]. The proposed digital object identifier (DOI) architecture provides an interface to the cellular system that can recognize the addressing and identification systems adopted in the IoT, thus allowing interaction between the systems.

Robust Authentication and Security

One of the most challenging hindrances to IoT uptake is establishing security. This lack of trust in how IoT devices are authenticated and included under an IoT paradigm is hindering the development and adoption of many services, especially when direct consumer interaction is involved [9]. This, for example, is the main reason behind the slow uptake of home automation IoT solutions, as they are often seen as security vulnerabilities.

The status quo in IoT is adopting a centralized authentication model per IoT "zone" [2]. That is, given an area where an IoT hub or backhaul access point would be deployed (e.g., in a home automation system), IoT things would authenticate their access to that access point, and thereafter carry out D2D communications. Security is then introduced on a number of layers, depending on the underlying authentication model. For example, some IoT products (e.g., Arduino Yun and Raspberry PI) are built on single board computers (SBCs) integrated with sensors. These systems have security and TCP/IP-based communication modules built in them [1].

Our security and authentication challenges are not in their specific implementations, but rather in realizing them across heterogeneous things in the IoT. That is, if IoT is built on efficient communication between devices registered (and authenticated) by heterogeneous entities, how can we establish trust and secure communication across these systems? More importantly, many challenges arise from the inherent vulnerabilities of the Internet as a connecting backbone, whereby end-to-end secure channels could be established, but identity revealing associations and potential vulnerabilities from the aggregation of IoT traffic are not trivially solvable.

Managing Heterogeneous D2X Communication

Sheer traffic over the Internet is already posing a challenge in scalability, mainly driven by video content demand and sheer connectivity of M2M and IoT devices. Simply assuming that ad hoc connectivity of IoT devices to the Internet will somehow enable their coordinated operation is unrealistic. This is a pressing challenge, especially when we account for the sheer amount of IoT traffic, projected to grow from 1 Exabyte/month in 2015 to 6.3 Exabyte/month by 2020 [10].

Our challenges in managing heterogeneous D2I/D-H (D2X) communication surpass simple association, identification, and authentication of IoT things. A scalable approach to resource discovery, access, communication, and control must take into account the growing demand on the Internet, and the possibility that we cannot depend on it as a backbone architecture for all D2X communication. As the Internet strives to scale with growth in video demand, piggybacking both control and data communication on the Internet will slow down IoT systems, and inevitably hinder their expansion in regions where access to broadband Internet is not abundant.

This challenge is further manifested in IoT applications that target emergency response, disaster mitigation, and power failures, or are simply deployed in regions without Internet access. While major strides have been achieved in improving ad hoc D2D communication without the Internet, especially in home automation, most IoT infrastructures argue for offloading control and data management to cloud services or remote servers. In a technology that promises global connectivity and remote management of devices, we are in need of newer approaches than simple cloud services offloading if IoT systems are to augment existing Internet-based communications.

Surviving the RF Smog

The sheer amount of devices competing for RF access in a given frequency band are drawing increasing challenges in MAC protocols, especially for devices operating on the industrial, scientific, and medical (ISM) bands. As we attempt to survive the ensuing RF smog [11], IoT devices are inevitably dragged by other networks, especially those operating over the IEEE 802.11/15 families.

While these challenges are currently researched under cross-technology interference (CTI) management schemes, such as CrossZig [12], we need to build on dynamic provisioning of channel assignments under fifth generation (5G) developments and other dedicated infrastructures. Spectrum allocations and operating on licensed and unlicensed bands should be further investigated to establish mission-critical and time-sensitive IoT connectivity.

Standardizing IoT Interfaces

Many IoT alliances and standardization efforts are taking place, mainly because this technology has outpaced any concrete definition or consensus on how it will operate or what it will encompass. A major challenge was identifying how IoT systems will interact, and discussions started on whether we should build toward a common backbone (being the Internet) or if specific modules should be introduced to achieve functional integration between IoT systems.

A major challenge was identifying how IoT systems will interact, and discussions started on whether we should build towards a common backbone (being the Internet) or if specific modules should be introduced to achieve functional integration between IoT systems.

Currently, there are three major IoT alliances driving the development of systems and standards: the AllSeen Alliance (building the AllJoyn framework), the Industrial Internet Consortium (IIC), and the Open Interconnect Consortium (OIC). These are augmented by the IEEE P2413 standard for an architectural framework for the IoT. In addition, there are some specific markets such as home automation, which is led by Google's Thread group.

A major challenge in most of these standardization efforts is the disparate definitions of IoT on which they are built. While some alliances aim to integrate with others (e.g., Thread, which is likely to adopt AllSeen or OIC for upper layers), others are redefining different components of the IoT system based on the industrial backing of specific technologies. As a result, it is difficult to draw an architectural common ground on which new IoT

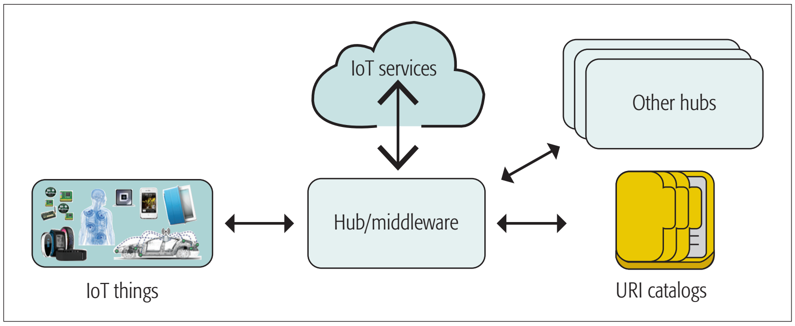

FIGURE 1. A hub architecture for Internet-based IoT (e.g., as adopted in Hypercat [4]).

systems could interact and develop ubiquitous access.

STATUS QUO IN INTERNET-BASED IOT CONNECTIVITY

The IETF-based standardization effort has also recently led to the release of the IoT architectural reference model (IoT-A) document [13]. This reference model formed the basis for some emerging Internet-based IoT testbeds/platforms such as the Hypercat project funded by the Technology Strategy Board (TSB) in the United Kingdom [4], and the Padova smart city project [3]. Figures 1 and 2 illustrate the architectures used in these two systems, respectively.

Hypercat is a hub-based middleware project that aims to demonstrate a worldwide interoperable hubs development platform, where each hub implements hyper catalogs that are accessible by end-user applications and by other hubs, allowing IoT nodes connected to these hubs to be discoverable and addressable anywhere from the Internet. In the Hypercat architectural model shown in Fig 1, services and applications connect to a data hub running middleware programs via an IP network, and the hub in turn manages access to a worldwide network of hubs containing catalogs describing the uniform resource identifiers (URIs) of connected things. Each item in a catalog refers to a single IoT resource via its URI, which may be an IoT node or another catalog containing lists of URIs [4].

The resource discovery phases in Hypercat are illustrated in Fig. 3, whereby an application attempts to find and access a resource from the hub catalog. Applications are therefore able to uniquely address connected things and use the data received from these things for their intended services.

All communication takes place over the Internet, and the middleware is responsible for providing the transcoding operations needed between IoT protocols implemented on the connected things and the Internet protocol implemented on the interconnecting IT networks.

The Padova project adopts a similar concept as the IoT applications, and services considered are also web-based. In the system architecture, a remote user connects to a server via web links and runs an application, such as smart city application on a municipality network, to capture necessary data as shown in Fig. 2. IoT nodes in the system are all based on IEEE 802.15.4 (wireless sensor networks standard) and 6LoWPAN, which is a constrained version of the Internet (IPv6) protocol for low-capacity IoT devices. Nodes collectively deliver their data to a sink node, which connects to a gateway. Three distinct functional layers have been identified as abridged versions of the current Internet protocol stack that can be implemented on low-capacity IoT nodes to enable them to be reachable/uniquely addressable from the Internet via an IoT middleware system. These are the data encoding, transport, and network layers [3]. On the Internet, protocols available in these three layers are HTML/XML, HTTP/TCP/UDP, and IPv4/IPv6, respectively. On the IoT networks, efficient XML interchange (EXI), constrained application protocol (CoAP), and 6LoWPAN are implemented as constrained versions of the respective Internet protocols in these three layers.

The IoT gateway has the role of interfacing the constrained IoT protocol with the Internet protocol and performing the transcoding needed between them. Note that IoT nodes are also free to implement any of the unconstrained Internet protocols such as UDP and IPv6 if they have resources in the IoT device to do so. Gateway transcoding operations are simply skipped when all nodes in the IoT network implement the unconstrained protocols.

The Hypercat and Padova projects are essential for Internet-based IoT because they complement one another. One focuses on the semantic interoperability of machine readable IoT node discovery systems, while the other focuses on the interconnection of IoT devices with the Internet. When these two projects are harmonized, a foundation for an interoperable Internet-based IoT system could be realized.

THE DRIVE OF CELLULAR IOT

The 3GPP members initiated the standardization of narrowband IoT (NB-IoT) in LTE for cellular systems in its Release 13 specifications document of September 2015, which was finalized in June 2016 [6]. Support for bandwidth-intensive IoT applications, however, is expected later in future cellular IoT standardization efforts in the context of the fifth generation (5G) cellular standard. 5G cellular is expected to drive large numbers of IoT connections given the enhanced data rate/capacity expected in the 5G system, and the improved outdoor RF coverage achievable when using large

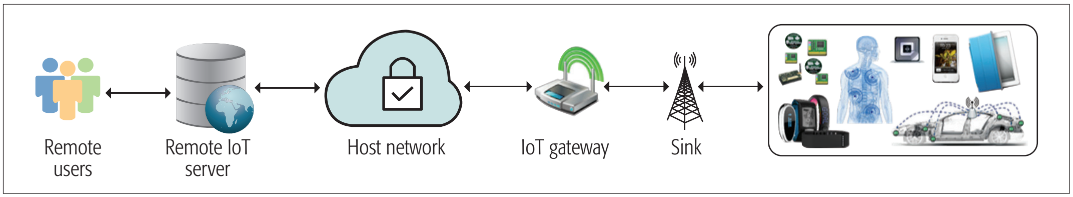

FIGURE 2. The discovery process of IoT resources via URIs in a hub catalog.

numbers of base stations (BSs) prompted by the limited millimeter-wave (mmWave) reach [14]. It was shown in [14] that 5G base station spacing could be as small as 100 m apart, which is similar to present-day streetlight spacing. Such BS density will suitably serve city-wide IoT coverage for smart city and other applications. For this reason, many recent research works have developed 5G channel models suitable for both cellular and IoT connections [15].

According to the current cellular IoT specification, the NB-IoT system can be deployed in three scenarios: "in-band," utilizing radio resource blocks within a normal LTE carrier; in the unused radio resource blocks within an LTE carrier's guard-band; or as a "standalone" deployment in a dedicated spectrum. The standard allows IoT connectivity based on orthogonal frequency-division multiple access (OFDMA) signaling in LTE using 180 kHz RF bandwidth for both uplink and downlink [6]. This is enough to support IoT applications that have low throughput and low delay sensitivity requirements, such as smart meter reading, environmental data sensing, and basic retail data displays/services. It may also support some intelligent transport system (ITS) and healthcare applications that do not require video signals. We discuss below a use case for a class of IoT applications and services that can be realized using the current cellular IoT standard.

In a cellular-network-based IoT architecture, IoT devices (mobiles, RFID, etc.) owned by active subscribers to cellular networks connect to the IoT infrastructure of the cellular network and are able to connect to the Internet via the middleware implemented by the operator. What is missing in such an architecture are methods by which IoT devices based on other IoT visions, such as the IETF's protocol stack, could be identified and allowed access to the IoT networks via the operator's middleware, especially without compromising the security of the cellular system.

Not only will cellular-IoT enable high-speed data access and wider coverage, but it can drive many advancements in ubiquitous services, especially time-critical ones such as health services. For such services, It is infeasible to build such services on multi-homing devices (ones that connect to multiple networks, e.g., cellular and WiFi, in an ad hoc manner) under the stringent connectivity and mobility demands. In fact, the support for high mobility and always-on connectivity in 4G-LTE/5G networks could expedite the uptake of cellular connectivity in wearable devices (by far the largest adoption in IoT technologies). Currently, cellular connectivity in wearable devices lagged at only 3 percent in 2015, and is projected to grow to a mere 7 percent in all wearable technologies by 2020 [10].

Bridging IoT Devices: the Status Quo

Both cellular and Internet IoT architectures have modules that allow data flow from an application to a middleware (or data hub), and then to the connected things (IoT nodes and modems/digital objects/mobile phones/computing devices, etc.). For the case of cellular-based IoT architecture, the middleware manages the connected things via an IP-based access network, over wireless links based on the cellular or Wi-Fi standard. In the case of the IT-based architecture, the middleware manages the connected things via any network with IP compatibility. The nature of the final connectivity to the connected things is thus unspecified, allowing both wireless and wireline links. However, the connected things are IoT nodes with full protocol stack, specified in the IoT-A standard, implemented on each node.

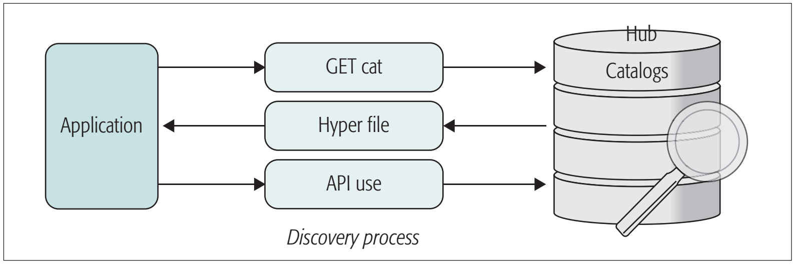

Figure 3. Internet IoT architecture based on the Padova smart city project [3].

With these protocols implemented on an IoT node, end-to-end services can be delivered over any IP-based network such as the Internet, as well as 4G-LTE/5G cellular networks via a middleware offering the transcoding service needed between the Internet and the constrained IoT protocols. However, cellular networks must first include modules in their architecture that extend wireless access to such IoT nodes to offer such services, and devise innovative "on demand" subscription procedures suitable for the same.

To this end, we propose the inclusion of a DOI interface at the bottom of the middleware in the cellular network architecture, where mapping between the addressing/identification methods used in both cellular and Internet IoT systems could be implemented. This allows interoperable cellular and Internet IoT services to be deliverable over cellular networks.

Proposed Architecture: The Cellular-IoT Bridge

Our objective is to enable modular interconnection between cellular-based IoT systems and their Internet-based counterpart. In addressing the challenges stated previously, we aim to integrate a DOI module that will enable rapid discovery, identification, authentication, access, and continuing communication with IoT devices that are connected to a cellular system. We present an architecture to interface these two systems to the cellular network architecture via a DOI module. The DOI can be updated as more standardized Internet IoT platforms emerge, and opens the door for policy management frameworks that will regulate heterogeneous access. An IoT protocol stack (e.g., based on the IoT-A standard spearheaded by IETF/ETSI) could be implemented in IoT nodes in order to connect them to the network infrastructure.

The architectural interaction between cellular and Internet-based IoT can be achieved via the introduction of a DOI module at the middleware level of the mobile network architecture, as shown in Fig 4. In the proposed modified cellular network architecture, the DOI will have the functionality to communicate with and identify IoT nodes belonging to cellular network and other IoT platforms, and decide on the types of services the network operator can offer to them. This provision has immense benefits for cellular network operators. It allows off-the-shelf IoT modems and devices to be purchased by end users and deployed for IoT access on cellular networks in a plug-and-play manner by simply purchasing SIM cards from the desired network operator, similar to the way smartphones are utilized today across different technology platforms and cellular networks. Without the proposed architecture, such plug-and-play integrated services will not be possible: IoT devices must be manufactured for particular cellular networks, making IoT technology adoption across various industries somewhat slow and expensive.

Benefits of this integrated architecture include helping to drive volumes of common IoT devices, which reduces manufacturing cost for IoT components, opening ways for new enterprise solutions such as IoT hotspot services based on availability of IoT connectivity from long-reach and robust cellular links, and increased revenue for cellular operators by billing IoT hotspot service providers per nodes connected. This provision has immense benefits for cellular network operators. It allows off-the-shelf IoT modems and devices to be purchased by users and used for IoT access on cellular networks by simply purchasing modems or SIM cards, similar to the way smartphones are utilized today across different technology platforms.

Digital object data and access type	DOI input	DOI output
RFID via IoT access	Tag ID	Tag ID mapped to URI
IoT data collected by smartphone and received via IoT access	GS1/QR codes	Codes mapped to URI
Sensing node via IoT access	Unique node ID	ID mapped to URI
Generic IoT devices	IPv6 address	Device IP mapped to URI

TABLE 1. Sample input/output mappings at the DOI; the URIs are ubiquitously discoverable from the Internet.

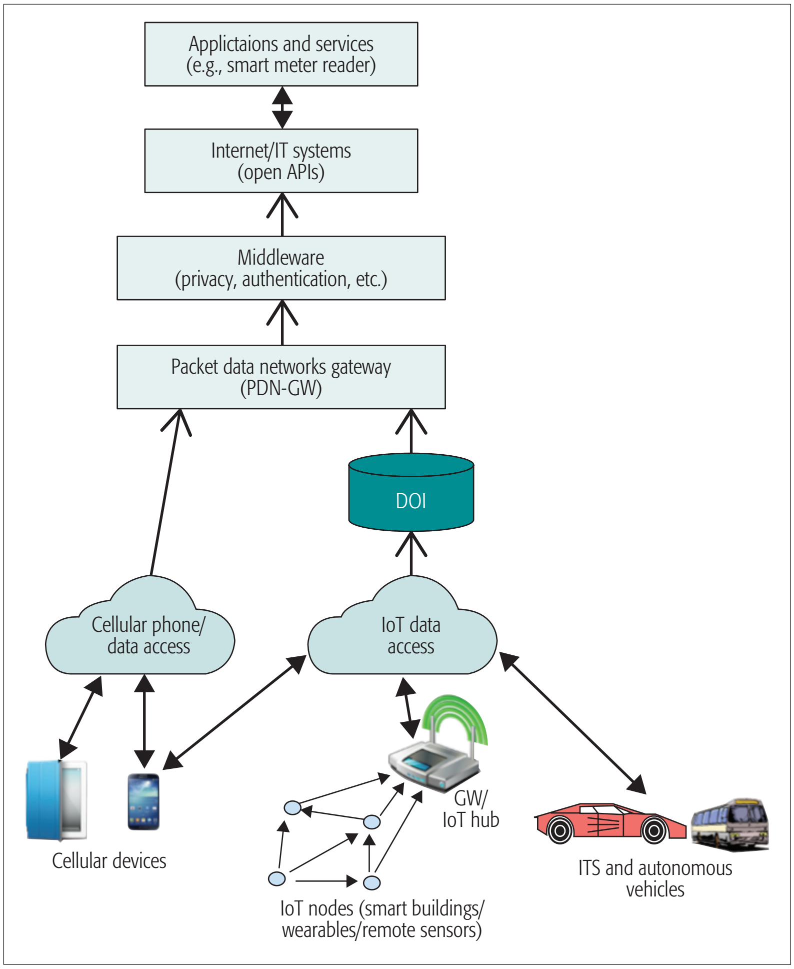
Applictaions and services
(e.g., smart meter reader)
Internet/IT systems
(open APIs)
Middleware
(privacy, authentication, etc.)
Packet data networks gateway
(PDN-GW)
DOI
Cellular phone/
data access
IoT data
access
GW/
IoT hub
Cellular devices
IoT nodes (smart buildings/
wearables/remote sensors)
ITS and autonomous
vehicles

FIGURE 4. Proposed cellular-network-based IoT architecture with DOI module.

IMPACT OF CELLULAR IOT WITH DOI: SAMPLE SCENARIOS

Many IoT services are projected to encompass highly mobile devices (e.g., in vehicles or wearable devices for transiting passengers), and we are in need of an architecture that inherently manages handovers, high-speed data access, and user/device mobility. The proposed architecture will prove particularly useful in discovering IoT resources in dynamic settings, soliciting sensing tasks over vehicles on the road, delivering low-latency access to sensor readings for traffic management and emergency response systems, and leveraging ubiquitous access managed on reliable cellular infrastructures.

In another scenario, where autonomous vehicles require rapid access to contextual data from nearby IoT resources, it would be crucial to connect to a cellular IoT system with DOI support to leverage nearby resources in near time, and offload significant overhead in managing communication and discovery messages to the cellular infrastructure, especially as service coordination on top of such resources will dictate low latency and rapid authentication hardly realizable by any Internet-based IoT architecture, whether proprietary or hub-based.

While many IoT architectures are advocating for localizing D2D and D2I communication to zones of interest, such as within a home/office/vehicle setting, it is important to cater for ubiquitous access beyond these zones. That is, the cellular IoT umbrella can realize a synergy between existing zone-based IoT systems, whether via physical (e.g,, Amazon Echo) or virtual hubs and large-scale IoT systems. This can be achieved by direct translation schemes that adopt one-to-one mappings between the DOIs' input and the URIs, as shown in Table I. This, for example, can extend the umbrella of remote patient monitoring, which can enable contextual information (e.g., location, room temperature, ambient activity) in pairing up with wearable technologies and otherwise disparate systems to deliver a fine-tuned overview of patient status to health care professionals.

As we advocate for scalable IoT access over cellular and Internet-based IoT systems, we empower services that can aggregate a multitude of infrastructures and orchestrate high-level services on those provided exclusively by each paradigm. These services can thereby integrate authentication and access advantages from cellular IoT, with service management and orchestration that is empowered by hub-based or semantic service matching over Internet-based IoT systems.

References

[1] A. Al-Fuqaha *et al.*, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surveys & Tutorials*, vol. 17, no. 4, 4th qtr. 2015, pp. 2347–76.

[2] J. Gubbi *et al.*, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems*, vol. 29, Feb. 2013, pp. 1645–60.

[3] A. Zanella *et al.*, "Internet of Things for Smart Cities," *IEEE Internet of Things J.*, vol. 1, no. 1, Feb. 2014, pp. 22–32.

[4] M. Blackstock and R. Lea, "IoT Interoperability: A Hub-Based Approach," *Proc. Int'l. Conf. Internet of Things*, Oct. 2014, pp. 79–84.

[5] S. Oteafy and H. Hassanein, "Resilient IoT Architectures over Dynamic Sensor Networks with Adaptive Components," *IEEE Internet of Things J.*, 2016

[6] 3GPP Rel. 13 doc., "Narrowband IoT (NB-IoT)," RAN mtg. #69, RP-151621, Sept. 2015; http://www.3gpp.org/news-events/3gpp-news/1733-niot.

[7] L. Yang *et al.*, "Shelving Interference and Joint Identification in Large-Scale RFID Systems," *IEEE Trans. Parallel Distrib. Systems*, vol. 26, no. 11, Nov. 1 2015, pp. 3149–59.

[8] G. P. Fettweis, "The Tactile Internet: Applications and Challenges," *IEEE Vehic. Tech. Mag.*, vol. 9, no. 1, Mar. 2014, pp. 64–70.

[9] S. Sicari *et al.*, "Security, Privacy and Trust in Internet of Things: The Road Ahead," *Computer Networks*, vol. 76, Jan. 2015, pp. 146–64.

[10] Cisco, "Cisco Visual Networking Index: Forecast and Methodology, 2015–2020," Feb. 2016

[11] S. Gollakota *et al.*, "Clearing the RF Smog: Making 802.11n Robust to Cross-Technology Interference," *ACM SIGCOMM Computer Commun. Review*, vol. 41, no. 4, Aug. 2011, pp. 170–81.

[12] A. Hithnawi *et al.*, "CrossZig: Combating Cross-Technology Interference in Low-Power Wireless Networks," *ACM/IEEE Int'l. Conf. Info. Processing in Sensor Networks*, Apr. 2016, pp. 1–12.

[13] IoT-A architectural reference model, doc. 257521; http://www.iot-a.eu/public, accessed July 2016

[14] A. I. Sulyman *et al.*, "Radio Propagation Path Loss Models for 5G Cellular Networks in the 28 and 38 GHz Millimeter-Wave Bands," *IEEE Commun. Mag.*, Sept. 2014, pp. 78–86.

[15] A. I. Sulyman *et al.*, "Directional Radio Propagation Path Loss Models for Millimeter-Wave Wireless Networks in the 28, 60, and 73 GHz Bands," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, 2016, pp. 6939–47.

Biographies

Ahmed Iyanda Sulyman [SM'09] obtained his Ph.D. degree from the Department of Electrical and Computer Engineering, Queen's University, Canada, in 2006. He was a teaching fellow at Queen's University, 2004–2006, a postdoctoral fellow at the Royal Military College of Canada, 2007–2009, and an assistant/associate professor at King Saud University, Saudi Arabia, 2009–2016. He joined the Department of Electrical Engineering at Embry-Riddle Aeronautical University, Prescott, Arizona, in February 2017, where he is currently an associate professor. He has published over 70 journal/conference articles on wireless communications and networks, with most recent contributions in the areas of millimeter-wave 5G cellular systems and IoT. He has been a Session Chair and Technical Program Committee member for many top-tier IEEE conferences, including IEEE ICC 2016.

Sharief Oteafy [S'08, M'13] is an adjunct assistant professor at the School of Computing, Queen's University. He received his Ph.D. in 2013 from Queen's University, focusing on adaptive resource management in next generation sensing networks, introducing the notion of organic senor networks that adapt to their environment and scale in functionality with resource augmentation. His current research focuses on dynamic architectures for enabling large-scale synergy in the Internet of Things, encompassing dynamic resource management across IoT platforms, in addition to managing the proliferation of big sensed data. He is actively engaged in the IEEE Communications Society, and an ACM member since 2008. He is an active member of the IEEE ComSoc Standards Association and is currently the Ad Hoc and Sensor Networks Standards Liaison and a voting member in the ComSoc Tactile Internet Standard WG. He co-authored a book, *Dynamic Wireless Sensor Networks* (Wiley), and presented over 40 peer-reviewed publications in sensing systems and the IoT. He has co-chaired a number of IEEE workshops, in conjunction with IEEE ICC and IEEE LCN, and served on the TPC of numerous IEEE and ACM symposia. He has delivered tutorials on big sensed data management at IEEE ICC, IEEE CAMAD, and IEEE GLOBECOM, and serves as an Associate Editor for *IEEE Access*.

Hossam Hassanein [S'86, M'90, SM'06, F'17] received his Ph.D. degree in computing science from the University of Alberta, Canada, in 1990. He is a leading authority in the areas of broadband, wireless, and mobile networks architecture, protocols, control, and performance evaluation. His record spans more than 500 publications in journals, conferences, and book chapters, in addition to numerous keynotes and plenary talks at flagship venues. He is also the founder and director of the Telecommunications Research Lab, School of Computing, Queen's University, with extensive international academic and industrial collaborations. He is an IEEE Communications Society Distinguished Speaker and a past Chair of the IEEE Communication Society Technical Committee on AHSN. He has received several recognitions and best paper awards.