Internet of Things (IoT): Research, Simulators, and Testbeds

M. Chernyshev, Z. Baig, O. Bello, S. Zeadally

***Abstract*—The Internet of Things (IoT) vision is increasingly being realized to facilitate convenient and efficient human living. To conduct effective IoT research using the most appropriate tools and techniques, we discuss recent research trends in the IoT area along with current challenges faced by the IoT research community. Several existing and emerging IoT research areas such as lightweight energy-efficient protocol development, object cognition and intelligence, as well as the critical need for robust security and privacy mechanisms will continue to be significant fields of research for IoT. IoT research can be a challenging process spanning both virtual and physical domains through the use of simulators and testbeds to develop and validate the initial proof-of-concepts and subsequent prototypes. To support researchers in planning IoT research activities, we present a comparative analysis of existing simulation tools categorized based on the scope of coverage of the IoT architecture layers. We compare existing large-scale IoT testbeds that have been adopted by researchers for examining the physical IoT prototypes. Finally, we discuss several open challenges of current IoT simulators and testbeds that need to be addressed by the IoT research community to conduct large-scale, robust and effective IoT simulation, and prototype evaluations.**

***Index Terms*—Internet of Things, Simulator, Testbed, Tool**

I. Introduction

The vision of the Internet of Things (IoT) is to build a smart environment by utilizing smart things/objects/devices that have sensory and communication capability to autonomously generate data and transmit it via the Internet for decision making. Such decisions are used to address issues related to human living such as energy management, climate change, transportation, healthcare, business logistics, building automation and others [1]. The IoT vision encompasses several building blocks that integrate and engage multi-disciplinary and inter-disciplinary activities from both business and technical domains [2]. This implies that there must be a symbiotic interaction among various entities of the IoT ecosystem to facilitate its growth and success. Within the ecosystem, information will be shared among diverse sub-systems to make timely decisions that impact human living. Therefore, the long-term success of IoT will depend on the evolution and development of sub-systems of the IoT ecosystem.

Since the inception of IoT, several research works have been undertaken in many areas. These efforts can be classified into business-related or technical-related research. In this paper, we focus on some of the most recent technical research activities reported for IoT. First, we classify these technical research works based on the main components of the IoT ecosystem. Thus, the classification is based on research works that have actually focused on the following IoT aspects: IoT devices, communication and connectivity i.e., networks, smart services and data.

Technical research in the IoT area is challenging because of the rapid pace of technological advances, the inter-disciplinary collaboration required in some areas and the ever-increasing demands of society [1]. To achieve an effective IoT ecosystem, a right balance must be created among research activities involving the technical components or systems and subsystems of the IoT because an unbalanced proportion of the research activities may affect the overall growth of the IoT in the near future.

Research in the IoT area should give attention to and include all components and elements that make up the IoT ecosystem. In this work, we review some of the trends in IoT research activities, and particularly on the technical sub-systems of IoT over the past five years. We consider recent publication trends of three main databases of publishers of Information and Communication Technology (ICT) research namely, Springer Link, Association for Computing Machinery (ACM), Elsevier and the Institute of Electronics and Electrical Engineers (IEEE) Xplore. As with any research and development, we realize that IoT research works should produce tangible results that can be utilized, leveraged and exploited by IoT product manufacturers, industries and service providers directly or indirectly to accelerate the creation of a smart environment for the benefit of society [1], while promoting standardized best practices in design, implementation and manufacturing of IoT products and services. For each classification of the IoT technical component, we discuss various areas that have been receiving the most attention from the research community and we present the goal and achievements of these IoT research efforts. Finally, we review some of the simulators that can be used for IoT research and we also present a number of existing open IoT testbeds that have been recently deployed by various research groups globally for conducting large-scale IoT research.

The aim of this paper is to provide guidance for planning the IoT research activities – specifically, to outline the significant IoT research trends, and provide an overview of existing IoT research tools that support the proof-of-concept and prototyping phases of the research lifecycle. We summarize the main contributions of this paper as follows:

1. We present IoT technical research trends for the past 5 years.
2. We highlight prioritized research areas and goals of the IoT research community and their basis.
3. We present a comparative analysis of simulation tools and open testbeds that are currently being used by IoT researchers.

Manuscript received September 15, 2017; revised December 3, 2017; accepted December 12, 2017.

M. Chernyshev and Z. Baig are with Edith Cowan University, Australia.
O. Bello is with Johns Hopkins University, USA.
S. Zeadally is with the University of Kentucky, USA.

4. We discuss a few open research challenges associated with simulators and testbeds used for IoT research.

II. Internet of Things Research Areas

A. Recent Trends in IoT Research

Research publications have consistently provided the means to access information that can advance technical innovation and the evolution of developing concepts or technologies. They also create a platform for knowledge dissemination of research activities being carried out in any subject area of a professional discipline. As with any research and development, several factors influence the research activities in IoT. These include funding, level and amount of research expertise, industry direction and interest, consumer demands and needs. These factors have a huge impact in the trend and direction taken by researchers in carrying out their respective research works. To better understand the trend of IoT research activities, we present the number of publications on "Internet of Things" over the last five years from four of the leading publishers of research works on ICT.

Usually, conference, journal and book publishers require researchers to provide relevant keywords that are used for indexing and categorizing publications. These keywords assist readers to find publications related to these keywords from the search engines. Thus, the keyword: "Internet of Things" was used to obtain the data given in table 1 and figure 1.

Table I lists the number of publications on IoT that have been published by ACM, Springer Link, IEEE Xplore and Elsevier for different publication types (conference proceedings, journals/articles and books, and so on). Figure 1 shows the trend in the number of publications over the last five years. The total number of publications presented comprise research works that cover four main technical areas of IoT such as IoT devices, communication and connectivity, smart services and data. Since these are the building blocks for the IoT ecosystem and with the 2017 top trending IoT areas [3], IoT research works can be classified under these technical areas. As shown in figure 1, the data obtained from Springer Link and Elsevier reflects a consistent increase in the number of IoT publications from 2012 to 2017, However, IEEE Xplore and ACM had a slight decline in their conference publications, and the total number of publications during 2016-17; albeit with an increase in the number of journal and Early Access publications during the same period.

IoT publications that focus on data explore how the capturing of real world physical data, knowledge and information can be achieved in a reliable and secure manner. IoT research efforts have been undertaken in the areas of data sensing and generation, data collection, data storage (cloud and fog technologies), data mining and management, data analytics, automation and machine learning. IoT research activities on big data received the most research attention for the data category [4].

Networks and connectivity refers to the components of the IoT ecosystem that enable seamless and continuous communication among IoT devices. The IoT publications in this area investigate the design of scalable wired networks, wireless long-range and wireless short-range networks infrastructure for the IoT, how to achieve efficient and reliable data transmission, routing, security and Quality of Service (QoS) within the IoT. Other hot topics are the design of energy efficient resource allocation and optimization schemes for communication networks in the IoT. In addition, some IoT research efforts have investigated how smart objects can autonomously operate and communicate with other IoT objects to achieve distributed decision making without the support of a centralized infrastructure. In this context, device discovery and cognitive protocols for context-awareness in general, and content-aware communications between devices are some of the areas that have been investigated. Moreover, significant research literature has also been published on wireless sensor and actuator networks [4] and network virtualization, most probably because these are the primary research domains driving the technological advances of IoT.

In the devices category, research efforts extend over sensors, Radio Frequency IDentification (RFID) devices, contactless devices, wearable devices, smart consumer appliances, driverless vehicles, embedded systems, and energy harvesting for these devices. Others areas of investigation include; enabling security and privacy, addressing and identification of devices, design and modeling of miniaturized smart objects. Areas that are increasingly attracting research interest include

TABLE I
TOTAL NUMBER OF PUBLICATIONS ON IOT BY EACH PUBLISHER BETWEEN 2012 AND 2017.

IEEE Xplore							
Year / Type	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**Total**
Conferences	675	1123	1678	2892	4061	2848	**13277**
Journals	30	104	251	438	754	1035	**2612**
Early Access Article	0	13	18	62	10	371	**474**
Books/e-books	27	0	0	5	20	83	**135**
Courses	2	0	0	1	6	5	**14**
Standards	0	0	0	0	0	3	**3**
Total	**734**	**1240**	**1947**	**3398**	**4851**	**4345**	**16515**
ACM							
Year / Type	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**Total**
Conference proceedings	17474	17190	18716	18748	21090	18744	**111962**
Journals	1238	1553	1541	1700	1802	1937	**9771**
Books	1	2	0	0	0	0	**3**
Technical reports	0	0	1	1	5	1	**8**
Videos	0	0	0	0	0	3	**3**
Newsletters	956	731	787	852	769	733	**4828**
Magazines	596	557	578	570	571	464	**3336**
Total	**20265**	**20033**	**21623**	**21871**	**24237**	**21882**	**129911**
Springer Link							
Year / Type	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**Total**
Book Chapters & Conference papers	7232	8431	9168	9697	11165	10920	**56613**
Articles	1993	2309	2443	2731	3532	4968	**17976**
Reference work Entry	78	140	300	377	355	391	**1641**
Book	3	6	5	3	12	16	**45**
Protocol	15	4	6	7	8	6	**46**
Conference Proceeding	0	2	2	6	6	4	**20**
Total	**9321**	**10892**	**11924**	**12821**	**15078**	**16305**	**76341**
Elsevier							
Year / Type	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**Total**
Review Articles	113	109	144	156	224	362	**1108**
Original Research	1871	2091	2498	3073	3362	4595	**17490**
Encyclopedia	67	35	33	185	45	57	**422**
Book Chapters	848	802	845	880	977	1063	**5415**
Others	221	267	268	325	398	409	**1888**
Total	**3120**	**3304**	**3788**	**4619**	**5006**	**6486**	**26323**

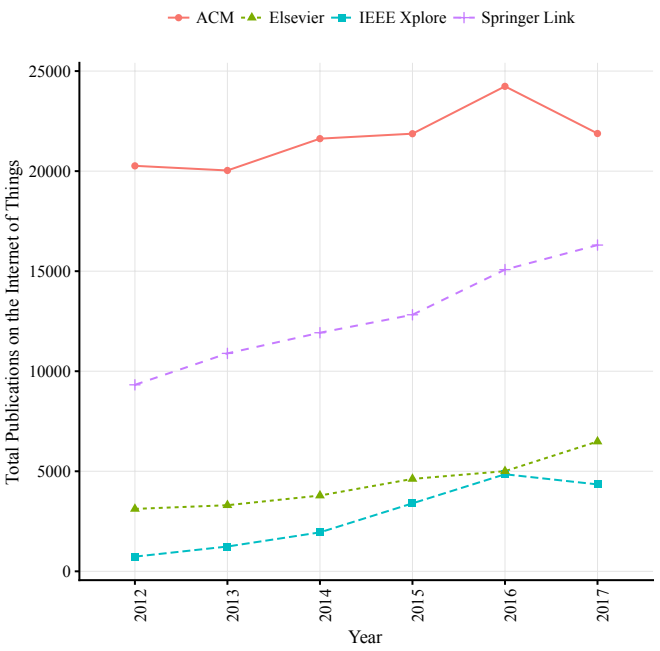

FIGURE 1: TOTAL NUMBER OF PUBLICATIONS ON THE INTERNET OF THINGS PER YEAR BY EACH PUBLISHER.

the development of protocols that enable cognition and intelligence in devices for the creation of activity-aware, policy-aware and process-aware devices, objects or things [5]. Research works on activity, policy and process-aware devices, objects or things generally include enabling of devices to: capture and interpret human-user actions, perceive and instruct their respective environments (e.g., setting off an alarm for a detected anomaly/perceived abnormal action), analyze device observations and to communicate these results to other objects through the Internet.

Moreover, since the smart services and applications provided by the IoT are sustained through decision making processes, these smart services are supported by leveraging concepts in other research domains such as application, algorithm and software development, mobile computing, automation through artificial intelligence and machine learning, and location-based services. Smart services and applications include smart city, smart grid, smart transportation, smart health (health monitoring, assisted living), home and building automation and home area networks. Other IoT research activities that overlap with these research domains are; research on energy efficiency, artificial intelligence, augmented reality, IoT architectures, standards and the inter-operations of legacy Internet systems with state-of-the art IoT components. These areas are playing a fundamental role in the development of the IoT environment [1].

B. IoT Research Goals for the Future

An inherent feature of the IoT ecosystem is the integration of the physical world with the Internet, which is achieved through devices that exhibit self-X capabilities, where X refers to functionalities such as configuring, optimizing, management, healing, and adaptive (ability to autonomously react to changing environmental conditions) [1]. These devices form networks wherein data is generated, transmitted, analyzed and applied to make decisions with minimal or no human intervention [6]. In addition, many of the devices are resource-constrained in terms of memory, processing power and battery life.

Based on the above features, we highlight some IoT research goals that will enable the successful realization of the IoT now and in the future.

1) ***Achieving lightweight protocols without compromising efficiency and reliability:*** Communication between devices in the IoT environment involves miniature sensors and wearables that are deployed in places that are out of reach for humans. Due to their miniature characteristic, these devices do not have the capability to operate with the heavyweight protocols designed for legacy Internet devices. Therefore, a major research goal is to design efficient and reliable lightweight protocols that are not resource-intensive. IoT protocols designed for these purposes (routing, QoS, resource allocation, security, interoperability) must be lightweight and at the same time achieve the efficiency, scalability and reliability of legacy Internet protocols used for the same purpose.

2) ***Enabling longer battery life through the design of energy efficient mechanisms for devices:*** The battery life of IoT devices raises a lot of concern for device manufacturers and the research community. Many rigorous research efforts have been devoted to this area [6]. Since most devices are deployed in harsh and remote environments out of reach for humans; frequent battery charging and re-charging may not be possible. Thus, devising energy efficient protocols continues to be of immense interest to the research community. Other vital related research areas include the development of mechanisms that enable devices to self-generate, harvest, re-cycle and store energy [7]. These efforts include adjusting the protocol stack of networking technologies to support energy efficiency [6][8] because power consumption is generally high in legacy protocol stacks such as the traditional IEEE 802.11 family of network protocols, Bluetooth and DECT [9].

3) ***Facilitating cognition and intelligence to enable the smartness of IoT objects/things/devices:*** IoT envisions to control human living and environment by autonomously monitoring, sensing and even directly interacting with the physical world, human life activities, collecting information from these activities and transmitting or communicating the data obtained so that appropriate decisions can be made. In most scenarios, this process may not involve humans, therefore high-level cognition close to human intelligence is required. In the IoT ecosystem, cognition occurs when an object/thing/device is programmed with the ability to mimic the human brain and thought processes. Such cognitive ability facilitates smartness [10]. As such, IoT devices will not be merely intelligent devices, but will incorporate cognition to learn from related data sources (including the environment) just like humans do. Cognition is achieved with the use of cognitive computing, artificial intelligence and machine learning solutions. Thus, another major challenge for researchers is to investigate innovative techniques to enable precise cognition to be achieved in the IoT environment so that the smartness of relevant IoT devices can be achieved. For example, cognitive intelligence has already been applied to applications for cooperative spectrum sensing in the Internet of Vehicles (IoV)

to improve primary channel availability [11]. Smartness can also be realized by combining IoT with a Cognitive Dynamic System (CDS) to further enhance current smart home applications using almost identical sensors and actuators [12]. Conceptually, efforts in the area form the sub-field of the Cognitive Internet of Things (CIoT), with several unresolved future research challenges [13].

4) ***Device/objects/things identification, addressing and discovery:*** Scalable addressing and identification mechanisms are required for IoT because of the continuous increase in the number of connected devices. Moreover, the design of such scalable mechanisms is being challenged by the heterogeneity of devices, which are configured with the Internet Protocol (IP) as well as a non-IP addressing format. Therefore, the primary goal of research efforts in this area is to address the challenges of device identification and addressing by designing lightweight protocols and schemes that support flexible address allocation, address collision or duplicate address detection (for security), address recycling, address translation and auto-configuration of addresses by devices. Such addressing protocols are necessary for scalable and seamless ubiquitous connectivity in the IoT ecosystem.

5) ***Achieving robust security and privacy within the ecosystem:*** The IoT is an open ecosystem in which all devices are interconnected making these devices vulnerable to malicious attacks. Due to this risk, several research efforts have focused on mechanisms to achieve reliable, at the same time, lightweight IoT security and privacy.

6) ***Addressing the challenges introduced by big data and data fusion***: These challenges include capturing, storage, analysis and presentation (visualization) for accurate decision making [14]. Huge amounts of data will be generated by heterogeneous IoT sources. Such data may have non-uniform schemas and structures and in many cases these diverse data formats have to be intelligently integrated for accurate analysis. Numerous research efforts are investigating solutions to solve challenges related to big data in IoT. Furthermore, efficient utilization of large volumes of highly heterogeneous data can be realized using data fusion [15]. For example, data provided by sensors that use low accuracy in the interest of power conservation can be fused with other data collected to produce more accurate information. Data fusion is expected to be highly beneficial for autonomous vehicles, deep learning and smart city applications.

7) ***Enabling end-to-end seamless connectivity and mobility***: Realizing ubiquitous, continuous and seamless end-to-end connectivity for every IoT device, whether stationary or mobile, is crucial for the IoT ecosystem, thus making it one of the goals for IoT researchers. Mechanisms supporting seamless communication and handover to ensure that devices remain connected to each other or a network infrastructure irrespective of their movement status, continue to be explored.

8) ***Miniaturization of devices*****:** As IoT becomes pervasive, the design of miniature devices becomes easier and cheaper per Moore's Law. Thus, research activities in this area focus on the development of practical technologies that can enable the design of low-cost miniature devices.

C. IoT Research Results

It is worth pointing out that some of the goals discussed above are yet to be accomplished and new goals are emerging due to changes in user demands and expectations with the emergence of new smart applications. Table II presents a few of the common, prominent IoT research goals and some of their associated results to date. These results have yielded solutions that have addressed some of the challenges that would have otherwise stalled the successful operation and advancement of the IoT paradigm now and in the future. Research results listed in Table II are currently being adopted across many industries to help deploy the Internet of Things ecosystem into their respective operational environments.

TABLE II
IOT RESEARCH GOALS AND RESULTS.

Research Goals	Research Results
Lightweight protocols	6LoWPAN, uIP, RPL, NanoIP, TSMP.
***Energy efficiency**	Device protocol stack focused solutions: EnOcean [16] [17], LoRa [18], SigFox, Ingenu, Weightless, DECT ULE [19], BLE [20], IEEE 802.11ah (WiFi HaLow), IEEE 802.11af (White-WiFi), IEEE 802.11ba (WUR) [21].
Cognition	Bio-inspired algorithms, Artificial Intelligence, Machine learning [10].
Security	Light weight cryptographic algorithms such as CLEFIA, PRESENT, ENOCORO, TRIVIUM [22]
Identification, addressing and discovery	EPC, uCode, IPv6, URIs, mDNS, UPnP, Hypercat.
Data	Concepts include big data analytics, cloud computing, fog computing. Protocols include MQTT, CoAP, AMQP, DDS, URI.
Connectivity	D2D networks such as IEEE 802.11 family, Bluetooth, ZigBee, Z-wave, NB-IoT, Sigfox [23]. Others include LTE-advanced, D2D in LTE, ICN, SDN, NFV, CCN.
Miniaturized devices	SoC, Smart dust, Nanotechnology, NoC

**We have listed device protocol stack solutions because solutions which have focused on protocols are also classified under lightweight protocols.*

III. IOT SIMULATORS AND TESTBEDS

The design, development and evaluation of new IoT products and protocols prior to their deployment in the target environment requires appropriate testing and evaluation using a wide variety of tools. For example, prototyping on a large scale using a large number of hardware nodes may not be practical during the initial exploratory design and evaluation phase due to economical and operational constraints, especially when the reliability and utility of the protocol under consideration are yet to be proven. Additionally, setting up reliable and reproducible experiments involving real hardware can be challenging and often requires specific expertise and domain knowledge [24].

Thus, a typical IoT research process cycle [25], which starts with the formulation of an idea and culminates with real-world deployment, comprises both *virtual* and *real* elements. A proof-of-concept is typically realized in the virtual domain using simulation, and the subsequent real prototype is devised via experimentation on a testbed. In this section, we examine some of the prominent simulators and large scale open testbeds that

are currently available and in use for IoT research and discuss their characteristics with reference to the three-layer (perceptual, network, and application) IoT architecture [26].

A. Simulators

Generally, an IoT simulator needs to offer high fidelity for scenarios comprising heterogeneous elements, support scalability, provide energy or computation efficiency, and be extensible to be able to support custom requirements such as new protocol evaluation [27]. There are three categories of simulators that can be used for IoT research, based on scope and, subsequently, the level of architectural layer coverage.

The first category comprises the full stack simulators that have been developed in response to the emergence of the IoT paradigm. These simulators aim to provide end-to-end support of all IoT elements. The second category includes simulators that focus on the big data processing aspects of IoT applications. The third category comprises network simulators. It is worth pointing out that some of these simulators were not originally created to support the IoT paradigm, but later evolved to include the implementations of the necessary IoT-specific components. Table III presents a summary of selected IoT simulators. The justification for the selected comparison criteria is provided as follows:

- **Scope** – defines the level of coverage of IoT architectural layers with "IoT" meaning full coverage.
- **Last update** – a representation of the level of maintenance activity.
- **Citation count** – a measure of simulator popularity based on published research literature.
- **Type** – type of simulation paradigm reflects the underlying assumptions about the entities and relationships being modeled.
- **Language** – reflects the degree of portability of simulated primitives for reuse in subsequent hardware prototyping (usually only available when using C).
- **Evaluated scale** – the scale at which documented simulator evaluations have been performed.
- **Built-in IoT standards** – represents protocol coverage to achieve a wide range of research goals (as shown in Table II).
- **Mobility** – indicates the support for one of the critical features of IoT deployments.
- **Cyberattack simulation** – research support related to one of the key challenges of IoT in the presence of existential adversarial threat.
- **Target domain** – indicates the degree of specialization.
- **Overall practicality** – a qualitative measure of utility for simulating an end-to-end IoT service across all architectural layers.

1) Full Stack Simulators

Specialized IoT simulators in this category include DPWSim [28], and iFogSim [29]. DPWSim has a specific focus on applications based on the Devices Profile for Web Services (DPWS) standard supported by the Organization for the Advancement of Structured Information Standards (OASIS). Using a combination of spaces, devices, operations and events, researchers can represent the desired IoT application, and model the necessary DPWS interactions. Being standard-based, this simulator is highly specialised. Although it does provide a complete DPWS simulation stack, it has no support for other enabling protocols and technologies.

In contrast, the iFogSim simulator provides a full stack environment that also supports fog computing and it achieves this by extending the CloudSim toolkit [30]. The simulator supports sensors, actuators and application processing elements allowing one to construct realistic network topologies and application service representations. The simulator can be used for conducting performance evaluations (control loop latency, network bandwidth and energy utilization) of various service deployment approaches, such as cloud-only versus fog computing.

2) Big Data Processing Simulators

Simulators in this category focus on cloud performance and big data processing and they include IOTSim [31] and SimIoT [32]. The IOTSim simulator focuses on the application layer and provides an environment for evaluating big data processing capabilities of IoT applications using cloud computing based on the MapReduce programming model. This simulator reproduces data center mechanics (such as virtual machine configurations, computational requirements and cost) rather than sensor network interactions and is also based on the CloudSim toolkit [30].

Similarly, SimIoT can be used to evaluate job processing times in a specific cloud-based data processing system configuration, based on data submitted by the sensors or users of the IoT service. In its current state (at the time of writing), this simulator has its primary focus on data center performance evaluation, with future plans to include support for sensor heterogeneity and topology management.

3) Network Simulators

This category contains the majority of available simulators. Network protocol research pre-dates the IoT paradigm and many of the previously available tools used for Wireless Sensor Network (WSN) or basic networking research have been adapted to incorporate additional IoT-specific elements. The survey conducted in [33] includes more than 30 WSN simulators that can potentially be used as part of IoT research. Some of these simulators include CupCarbon [34], Cooja [35], OMNeT++ [36], NS-3 [37], and QualNet [38].

CupCarbon was originally designed as a simulator with a strong emphasis on supporting geographic node mobility based on real-world environments. Despite its initial lack of maturity [39], it has gradually evolved into an established IoT simulation platform for smart city environments with support for mobile agents that can represent Unmanned Aerial Vehicles (UAVs) and detailed street-level topology based on real world maps. Unfortunately, despite being IoT-specific, CupCarbon does not support application-level IoT communication protocols.

Cooja is a companion simulator available as part of the Contiki Operating System (OS), which is one the most popular OSs that is used to program the IoT sensors [40]. Cooja is very popular in the WSN research community with over one hundred publications available on IEEE Xplore mentioning this simulator in their title. Simulated WSN motes in Cooja theoretically have access to the majority of standards and protocols implemented by Contiki and, thus, researchers have the ability to reproduce realistic scenarios that incorporate

TABLE III
COMPARISON OF SELECTED IOT SIMULATORS
YES: SUPPORTED, NO: NOT SUPPORTED

Simulator	Scope	Last update	Citation count	Type	Language	Evaluated scale	IoT architecture layers	Built-in IoT standards	Mobility	Cyber attack simulation	Target domain	Overall practicality
DPWSim [28]	IoT	2014	IEEE: 5 ACM: 0 SL: 1 E: 0	Not known	Java	Small scale	Application	Devices Profile for Web Services (DPWS)	No	No	Generic	Medium
iFogSim [29]	IoT	2016	IEEE: 2 ACM: 0 SL: 4 E: 0	Discrete-event	Java	Not known	Perceptual Network Application	No	No	No	Generic	Medium
IOTSim [31]	Data analysis	2016	IEEE: 0 ACM: 0 SL: 0 E: 3	MapReduce model	Java	Large scale	Application	No	No	No	Generic	Medium
SimIoT [32]	Data analysis	2014	IEEE: 1 ACM: 0 SL: 3 E: 2	Discrete-event	Java	Small scale	Application	No	No	No	Generic	Medium
CupCarbon [34]	Network	2017	IEEE: 4 ACM: 7 SL: 4 E: 0	Agent-based and discrete-event	Java / Custom scripting	Small scale	Perceptual Network	802.15.4 LoRaWAN	Yes	No	Smart city	High
Cooja [35]	Network	2017	IEEE: 121 ACM: 26 SL: 167 E: 0	Discrete-event	C/Java	Small scale	Perceptual Network	All protocols supported by Contiki OS	Yes	Using custom extensions	Generic with focus on low power sensors	High
OMNeT++ [36]	Network	2017	IEEE: 703 ACM: 140 SL: 1,464 E: 4	Discrete-event	C++	Large scale	Perceptual Network	Manual extension	Yes	Using custom extensions	Generic	Medium
NS-3 [37]	Network	2016	IEEE: 786 ACM: 47,822 SL: 9,516 E: 2,010	Discrete-event	C++	Large scale	Perceptual Network	802.15.4 LoRaWAN	Yes	No	Generic	High
QualNet [38]	Network	2017	IEEE: 418 ACM: 51 SL: 512 E: 2	Discrete-event	C/C++	Large scale	Perceptual Network	802.15.4 (Zigbee only)	Yes	Yes	Generic	Medium

popular application-layer protocols such as Message Queue Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP) implemented over 802.15.4 and IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN). The simulation firmware running on virtual nodes can subsequently be deployed to real physical hardware with minor modifications bridging the gap between the proof-of-concept and prototyping phases. Strictly speaking, Cooja is not a simulator, rather, it is an emulator capable of instruction-level emulation of node firmware execution in a simulated wireless communications environment. It should be noted that some researchers question the validity of previous simulations based on Cooja due timing inaccuracies between virtual and real implementations [41] that have been discovered in the past.

The OMNeT++ simulator is another popular network simulation framework that is extensively used in WSN research. This framework is well-established and it is extensible. It can be used to incorporate external elements for specialized needs such as urban mobility provisioning using the Simulation of Urban MObility (SUMO) tool [42]. These bidirectional integration capabilities of OMNeT++ have been leveraged to create a specialized vehicular network simulator called Veins, which has been used for evaluating the smart transportation scenarios [43]. Unfortunately, OMNeT++ appears to lack built-in support for IoT-specific radio models and application-level protocols. As such, the incorporation of missing elements remains a manual process [44].

The NS-3 simulator, the successor to NS-2, can also be used to create realistic simulations of WSNs for replicating the perceptual layer of IoT. Similar to OMNeT++ and despite having native support for 6LoWPAN over 802.15.4, NS-3 also lacks support for application-level protocols.

In addition to open-source tools, commercial products can also be used in IoT research. One example is the QualNet simulator by Scalable Networks [38]. This simulator can support high fidelity simulations comprising heterogeneous network components. IoT-specific simulations can be achieved by using the additional Sensor Networks Library extension for QualNet, which adds support for 802.15.4 networks (specifically, the Zigbee derivative).

Discussion

With the large number of simulators to choose from, researchers face a challenging selection process, possibly complicated by conflicting simulator selection

recommendations [33, 45]. Furthermore, to the best of our knowledge, at present there is no generally available all-in-one simulator that can be used to create a detailed representation of an end-to-end IoT service comprising:

1. A WSN simulation that fully supports IoT-specific infrastructure and application protocols including support for multiple WSNs and bidirectional edge communications.
2. An IoT application layer simulation that integrates with the WSNs to provide the necessary big data storage and processing features using cloud or fog computing as an integrated element of the WSN simulation.

Consequently, in order to simulate a complete IoT architecture we need to use multiple simulators (such as the use of a network simulator for packet tracing and data generation and a big data processing simulator for data processing) with increased complexity. One approach to address this problem could be based in multi-level simulation architectures as proposed in [46]. During multi-level simulation, modeling takes place at varying levels of detail and possibly entirely within different simulation domains (such as networking and urban mobility) and the resulting state information is synchronized and exchanged using inter-model interactions at runtime. At level zero, a high-level simulator, also acting as the simulation controller or coordinator, triggers lower-level simulations with finer granularity as required based on the specifications of the simulated scenario. This approach can also theoretically incorporate various specialized simulators to achieve improved accuracy at lower levels.

Finally, as Table III shows, the various simulators have varying degree of support for popular IoT standards and essential IoT service features such as mobility and security. While we expect that the full stack and specialized big data processing evaluation simulators may not support these features, the lack of built-in support for popular IoT standards by some of the more established network simulators currently limits their practical applicability for IoT research. Although mobility is generally supported, there is lack of built-in support for cyberattack simulations. Manual integration of additional attack frameworks such as NETA [47] for OMNeT++ and RPL Attacks Framework [48] for Cooja can be done to address some of these shortcomings.

B. Open Testbeds

While simulators can be useful for proof-of-concept development, a growing number of researchers are relying on experimentation-based prototyping in their research efforts. According to [25], concepts validated by simulations were verified using experimental testbeds in the majority (more than two thirds) of the 596 analyzed studies. Previously, a testbed would need to be implemented as part of a research project introducing the need for additional resources and skills and resulting in extra overheads. However, with the emergence of a number of open testbeds, researchers have access to readily available and deployed hardware and networks for experimentation. The key advantage of using open testbeds is akin to that of a simulator – *reproducibility* across multiple instances of the same scenario by researchers who have not created the testbed themselves. Next, we provide an overview of the some of the current large-scale open IoT testbeds and describe their characteristics.

1) FIT IoT-LAB

The FIT IoT-LAB [49] is a large scale multi-site and multi-user concurrent open access testbed located in France across 6 different sites. Cumulatively, the testbed provides access to 2728 heterogeneous wireless sensor nodes communicating over IEEE 802.15.4. In addition to providing a set of standard nodes, users can also incorporate custom hardware into their experiments. Mobility is provided via the use of programmable robots that can follow a circuit-like mobility model while other models such as random waypoint and user-controlled mobility are currently be developed. Today, this facility is considered to be the largest open IoT experimental testbed available to researchers.

2) SmartSantander

SmartSantander [50] is a city-scale experimental facility that provides an environment for evaluating IoT services targeted at the smart city domain. Originally, it was deployed in the city of Santander in Spain and it was subsequently extended to include additional federated locations across Serbia, Germany, and the United Kingdom. The original Santander deployment includes a highly heterogeneous set of sensors comprising 802.15.4 sensor nodes, parking sensors, Radio-Frequency IDentification (RFID) and Quick Response (QR) codes. The set of sensors features both fixed and mobile nodes fitted into vehicles such as buses and taxis. The variety of sensors allows for experimentation with a wide range of smart city services such as smart parking, smart irrigation and environmental monitoring, as well as support augmented reality. City inhabitants can also engage in participatory sensing using their mobile devices. A key feature of this testbed is its support for Over-The-Air Programming (OTAP) that allows researchers to deploy new firmware to supported nodes remotely. Using dual radio interfaces, core service provisioning remains decoupled from the experiments.

In addition to the primary deployment in Santander comprising around 12,000 IoT devices, the testbed includes approximately 8,000 more nodes spread across Guildford United Kingdom), Lübeck (Germany) and Belgrade (Serbia). These sites represent a smart campus (Guidlford), a small-scale indoor and outdoor node cluster (Lübeck) and a smart public transport system environment (Belgrade). In the latter case, researchers are not able to access the sensors for experimentation purposes, but can utilize historical observations collected by the service as part of their scenarios.

3) Japan-wide Orchestrated Smart / Sensor Environment (JOSE)

The JOSE [51] testbed is located in Japan and is based on the Infrastructure as a Service (IaaS) model for IoT service evaluation. The testbed provides support for the concurrent execution of multiple IoT services each having its own physical sensor network and virtual cloud infrastructure at the application layer. The testbed application layer infrastructure is spread across five data centers in Japan. The testbed provides extensive capabilities around the management and customization of the service-specific virtual infrastructure and networking using Software-defined Networking (SDN) thereby enabling flexible experimentation at the application layer of the architecture as well. At the perceptual layer, the testbed

TABLE IV
COMPARISON OF SELECTED OPEN IOT TESTBEDS

Testbed	Scale	Environment type	Heterogeneity		Mobility	Concurrency	Federation	Primary use case
			Node type	Protocol				
FIT IoT-LAB [49]	Medium (> 2,700 sensors)	Laboratory-like environment	Yes	Yes	Yes (robot-driven)	Multi-user	Yes (Fed4Fire)	Protocol and algorithm performance analysis
Smart Santander [50]	Large (~20,000 sensors)	Real city	Yes	Yes	Yes (vehicle-based)	Service provisioning and experimentation	Yes (Fed4Fire)	Smart city IoT service development
JOSE [51]	Large (sensor count not known)	Outdoor environment	Yes	Yes (non-IoT specific)	Not known	Multi-service	-	Environment and structural monitoring

provides an unspecified number of IEEE 1888-compliant sensors that collect and transmit environmental data using standard protocols such as IEEE 802.11, 3G and LTE. At present, the testbed supports 27 experimental IoT services [52].

Table IV shows a summary of the open testbeds discussed above. The justification for the selected comparison criteria is provided as follows:

- **Scale** – defines the maximum size of the prototype supported by the testbed as a measure of additional realism expected in multi-service deployments.
- **Environment type** –defines practical applicability (such as smart city prototypes ideally need to be evaluated in a realistic city-like environment as opposed to a laboratory).
- **Node and communication protocol heterogeneity** – the ability to support a wide range of hardware sensors and protocols so that extensive prototype evaluations can be conducted.
- **Mobility** – indicates support for one of the critical features of IoT deployments.
- **Concurrency** – the ability to support multiple distinct parallel evaluations at once.
- **Federation** – the ability to offer streamlined access to a broad heterogeneous set of experimental capabilities via a standardized toolchain and platform.
- **Primary use case** – indicates the level of specialization.

The testbeds are implemented in a variety of different environments and aim to support different use cases. The limitations of testbed specialization can be mitigated via federation – linking different scope testbeds using standard interfaces to be able to leverage the combined set of capabilities centrally [53]. In addition to federation support, testbed evaluation can be done in terms of the level of provided support for mobility, scalability, heterogeneity, repeatability, concurrency and user involvement for impact evaluation [54].

In addition to the large-scale open testbeds, other smaller scale testbeds such as Kansei, TWIST and WISEBED are also available [55]. Researchers can also access data from a number of highly heterogeneous additional experimental services. For example, the Federated Interoperable Semantic IoT Testbeds and Applications (FIESTA-IoT) European Union project includes 10 testbeds that can facilitate evaluation of semantic interoperability of IoT service data, applications and experiments across different participating testbeds [56]. The emergence of open testbeds, driven by growing demand for reproducible experiments and facilitated by easily accessible and standards-based tools have also triggered the emergence of the IoT Testbed-as-a-Service (TaaS) [57] and Experiment-as-a-Service (EaaS) [58].

IV. OPEN CHALLENGES

The successful execution of the IoT research process will rely upon the next generation of IoT research tools, and more specifically simulators for proof-of-concept design and evaluation and experimental testbeds for real prototyping. Having access to and being able to select the most appropriate research toolkit will be paramount to the success of future IoT research projects. Next, we highlight and discuss some of the key challenges associated with existing IoT simulators and testbeds that need to be addressed in the future.

A. Lack support for common IoT infrastructure standards

Simulators have varying degrees of support for popular IoT communication protocols. For instance, widely popular network simulators such as OMNeT++ still do not provide a built-in implementation of the IEEE 802.15.4 standard, which is prominent in WSNs that fall under the IoT perceptual layer. Other simulators, while being able to model the IoT protocols at the physical and Media Access Control (MAC) layer, do not offer support for the necessary application-level protocols such as CoAP and MQTT out of the box. Although these missing elements can be added through custom extensions, doing so represents additional overheads and will likely be undesirable. As simulation is only part of the overarching research process, expending additional resources during this phase may be detrimental to other phases. Subsequently, simulators striving to establish their place in an IoT research toolbox should provide built-in support for scenarios involving common IoT infrastructure standards.

B. Lack of support for end-to-end service simulation

Simulators such as DPWSim and iFogSim aim to model the interactions across all layers of the IoT architecture. However, they are either highly specialized (e.g., DPWSim focuses on the

DPWS standard) or use abstractions for representing the elements of the perceptual layer (iFogSim). As we have discussed previously, to the best of our knowledge, there is no simulator that can support end-to-end IoT service scenario modelling with detailed representation of entities and their interactions across all layers of the IoT architecture. For example, WSN simulators such as Cooja can be used to create detailed scenarios for the perceptual layer and to an extent, the network layer using a simulated gateway. However, it is not possible to model the application layer and end-user IoT services as part of the same simulator, in an integrated fashion. It may be possible to combine virtualization to realize the application layer externally to the WSN simulator, but being a decoupled component, this approach would need to address synchronization challenges and take into consideration timing issues. Thus, future work is required to provide ways that can support end-to-end IoT service simulation possibly by extending existing tools or introducing intelligent bridges or proxies that can combine simulators representing different architectural layers into a single platform.

C. Complexity of emerging IoT implementations

From an end-to-end IoT service perspective, a holistic model needs to include a range of highly diverse elements, such as sensor nodes with or without fog computing capabilities, edge and cloud data center representations, as well as data storage and processing activities such as data mining and data programming models with support for elastic storage and computing. Cumulatively, this set of dynamic interwoven elements represents a complex IoT Data Analytics Platform (IoTDAP) [59], which is challenging to model and subsequently simulate. Answering the questions pertaining to holistic modelling of highly heterogeneous IoTDAPs in a scalable and extensible fashion with realistic parameters will require a highly interdisciplinary approach.

D. Threat to Validity

Given the high heterogeneity of simulation tools and the underlying modeling paradigms, it is not surprising to see significant variations between simulated results and real-life evaluations, as reported in [18]. Simulators need to achieve trustworthiness by facilitating verifiable valid results. This is especially relevant because simulators are used to develop the initial proof-of-concept of the research lifecycle. The long-standing foundational challenges of model verification and validation originally discussed in [60] also apply to IoT simulation.

V. Conclusion and Future Directions

This work demonstrates that the IoT paradigm has been the subject of intense research focus over the last five years. Based on the continued growth in the number of studies published through major venues, we foresee that this trend will continue. IoT research trends reported in this work reveal that researchers are increasingly working towards improving existing IoT protocols to enable cognition and intelligence in devices, and the development of activity, process and policy-aware IoT ecosystems of the future.

Many concepts such as software development, mobile computing, Artificial Intelligence, and others from related disciplines are increasingly being leveraged by the IoT research community. Our analysis provides tangible results that can be utilized, leveraged and exploited by IoT product manufacturers, industries and service providers directly or indirectly to accelerate the creation of a smart environment for the benefit of society.

However, given the fact that the IoT paradigm itself is the result of convergence of multiple pre-existing technological paradigms namely, wireless sensor networks, the Internet, and cloud computing, the path to conducting full-cycle IoT research is not always clear. Research in this area is especially challenging due to the need to examine both virtual and physical realms as well as highly distinct technological constructs and their interactions.

A virtual proof-of-concept can be realized using simulators. However, existing simulators are generally specialized in the sense that they focus on a particular architectural layer (such as the network layer or the perceptual layer) whilst exhibiting limited capabilities for being able to holistically represent an end-to-end IoT service with high fidelity. One solution to overcome this could be to combine multiple specialized simulators at various levels of granularity in a hierarchical fashion [46].

Furthermore, despite there being a set of core communication protocols in use by the IoT services (such as 802.15.4 and CoAP HTTP translation via proxying), existing simulators provide varying levels of support for these core protocols and some do not implement the protocols beyond the Media Access Control layer. Finally, support for fundamental features such as mobility and cybersecurity attacks by many IoT services is also limited. When new specialized simulators are being introduced to address specific research needs, more effort should be directed toward enabling end-to-end simulations where packet-level cross layer communications and cascading failures and cyberattack effects can be traced from the sensor all the way up into the cloud service and downstream into consumer services and vice versa.

From a physical prototyping perspective, there are a few large scale open testbeds that can be leveraged to validate simulation-aided proof-of-concepts. Due to the diverse nature and the capabilities of these testbeds, interoperability remains an important consideration and some efforts such as FIESTA-IoT are focusing on addressing these challenges. Given the identified trends, such as the emergence of the IoT Testbed-as-a-Service (TaaS) [57] and Experiment-as-a-Service (EaaS) [58] concepts, testbeds could become commoditized making it possible to realize accessible physical prototypes easily.

Coupled with the increasing complexity of emerging IoT implementations, challenges such as the lack of support for IoT infrastructure standards, robust IoT service simulators and large-scale interoperable testbeds must still be addressed in the future.

Appendix

List of acronyms for table 2

6LoWPAN: IP version 6 over Low power Wireless Personal Area Networks
uIP: Micro IP
RPL: IPv6 Routing for Low Power/lossy networks
TSMP: Time Synchronized Mesh Protocol
LoRa: Low range
DECT ULE: Digital Enhanced Cordless Telecommunication Ultra Low Energy
BLE: Bluetooth Low Energy
WiFi: Wireless Fidelity **WUR**: Wake-Up-Radio
EPC: Electronic Product Code
uCode: Unique Code
URI: Universal Resource Identifier
mDNS: multicast Domain Name System
UPnP: Universal Plug and Play
MQTT: Message Queuing Telemetry Transport **CoAP**: Constrained Application Protocol
AMQP: Advanced Message Queuing Protocol
DDS: Data-Distribution Service for Real-Time Systems
NB-IoT: Narrow-Band IoT
D2D: Device-to-Device
ICN: Information Centric Networking
SDN: Software Defined Networking
NFV: Network Function Virtualization
CCN: Content-Centric Networking
SoC: System on Chip
NoC: Network on Chip

ACKNOWLEDGMENTS

We thank the anonymous reviewers for their valuable suggestions and comments which helped us to improve the content and presentation of this work.

REFERENCES

[1] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I. S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer, P. Doody, "Internet of Things Strategic Research Roadmap," Available: http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2011.pdf.

[2] L. Veronesi, "IoT Today: Be A Disruptor or Be Disrupted – Look At Your Business In A Whole New Way", 21-Sep-2017. Available: http://www.digitalistmag.com

[3] N. Jones "Top 10 IoT Technologies for Digital Business in 2018 and 2019", Report ID: G00328777, 12 September 2017.

[4] C. Rudinschi, "Top 20 Internet of Things Research Frontiers of the Leaders", http://iiot-world.com/digital-disruption/top-20-internet-of-things-research-frontiers-of-the-leaders/

[5] G. Kortuem, F. Kawsar, V. Sundramoorthy, and D. Fitton, "Smart objects as building blocks for the internet of things," IEEE Internet Computing pp. 30–37, January/February 2010.

[6] C. Gomez, M. Kovatsch, H. Tian, Z. Cao, "Energy-Efficient Features of Internet of Things Protocols", May, 2017.

[7] F. Shaikh and S. Zeadally, "Energy Harvesting in Wireless Sensor Networks: A Comprehensive Review", Renewable & Sustainable Energy Reviews, Vol. 55, March 2016.

[8] S. Zeadally, S. Khan, N. Chilamkurti, "Energy-efficient Networking: past, present, and future", Journal of Supercomputing, Vol. 62, No. 3, December 2012.

[9] L. Frenzel "Long-Range IoT on the Road to Success", May 2017. Available: http://www.electronicdesign.com/embedded-revolution/long-range-iot-road-success.

[10] Frost & Sullivan, "The Top 17 Trends for 2017, Report ID: 4084984, pp. 44, Feb. 2017.

[11] A. Paul, A. Daniel, A. Ahmad, and S. Rho, "Cooperative cognitive intelligence for internet of vehicles," IEEE Systems Journal, vol. 11, no. 3, pp. 1249-1258, 2017.

[12] S. Feng, P. Setoodeh, and S. Haykin, "Smart Home: Cognitive Interactive People-Centric Internet of Things," IEEE Communications Magazine, vol. 55, no. 2, pp. 34-39, 2017.

[13] Q. Wu et al., "Cognitive internet of things: a new paradigm beyond connection," IEEE Internet of Things Journal, vol. 1, no. 2, pp. 129-143, 2014.

[14] I. Anagnostopoulos, S. Zeadally, E. Exposito, "Handling Big Data: Research Challenges and Future Directions", Journal of Supercomputing, Vol. 72, No. 4, 2016.

[15] F. Alam, R. Mehmood, I. Katib, N. N. Albogami, and A. Albeshri, "Data Fusion and IoT for Smart Ubiquitous Environments: A Survey," IEEE Access, vol. 5, pp. 9533-9554, 2017.

[16] ISO/IEC 14543-3-10:2012, "Information technology -- Home electronic system (HES) architecture -- Part 3-10: Frequency modulated wireless short-packet (FMWSP) protocol optimized for energy harvesting -- Architecture and lower layer protocols". 2012.

[17] ISO/IEC 14543-3-11:2016, "Information technology -- Home electronic system (HES) architecture -- Part 3-11: Frequency modulated wireless short-packet (FMWSP) protocol optimized for energy harvesting -- Architecture and lower layer protocols". 2016.

[18] B. Vogel, "Networking achieved with low power", Technical paper, Swiss Federal Office of Energy (SFOE) Version: November 2016.

[19] ETSI EN 300 175-5, "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 5: Network (NWK) layer". Version 2.6.1, July 2015. Available: https://portal.etsi.org.

[20] [Bluetooth® Low Energy, Litepoint [Online], Available: www.litepoint.com/whitepaper/Bluetooth%20Low%20Energy_WhitePaper.pdf.

[21] Standard by IEEE, "IEEE 802.11ba Battery Life Improvement, IEEE Technology Report on Wake-Up Radio: An Application, Market, and Technology Impact Analysis of Low-Power/Low-Latency 802.11 Wireless LAN Interfaces, Jan. 2017.

[22] ISO/IEC 29192-1:2012, Information technology — Security techniques — Lightweight cryptography — Part 1: General, "ISO, Geneva, Switzerland, 2012.

[23] Pallavi Sethi and Smruti R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," Journal of Electrical and Computer Engineering, vol. 2017, Article ID 9324035, 25 pages, 2017. doi:10.1155/2017/9324035.

[24] G. Z. Papadopoulos, J. Beaudaux, A. Gallais, T. Noël, and G. Schreiner, "Adding value to WSN simulation using the IoT-LAB experimental platform," in 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2013, pp. 485-490.

[25] G. Z. Papadopoulos, A. Gallais, G. Schreiner, E. Jou, and T. Noel, "Thorough IoT testbed characterization: From proof-of-concept to repeatable experimentations," Computer Networks, vol. 119, pp. 86-101, 2017/06/04/ 2017.

[26] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, 2015.

[27] M. Sharif and A. Sadeghi-Niaraki, "Ubiquitous sensor network simulation and emulation environments: A survey," Journal of Network and Computer Applications, vol. 93, pp. 150-181, 2017.

[28] S. N. Han et al., "DPWSim: A simulation toolkit for IoT applications using devices profile for web services," in Internet of Things (WF-IoT), 2014 IEEE World Forum on, 2014, pp. 544-547.

[29] H. Gupta, A. Vahid Dastjerdi, S. K. Ghosh, and R. Buyya, "iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments," Software: Practice and Experience, vol. 47, no. 9, pp. 1275-1296, 2017.

[30] R. Buyya, R. Ranjan, and R. N. Calheiros, "Modeling and simulation of scalable Cloud computing environments and the CloudSim toolkit: Challenges and opportunities," in 2009 International Conference on High Performance Computing & Simulation, 2009, pp. 1-11.

[31] X. Zeng, S. K. Garg, P. Strazdins, P. P. Jayaraman, D. Georgakopoulos, and R. Ranjan, "IOTSim: A simulator for analysing IoT applications," Journal of Systems Architecture, vol. 72, pp. 93-107, 2017.

[32] S. Sotiriadis, N. Bessis, E. Asimakopoulou, and N. Mustafee, "Towards Simulating the Internet of Things," in 2014 28th International Conference on Advanced Information Networking and Applications Workshops, 2014, pp. 444-448.

[33] A. Nayyar and R. Singh, "A comprehensive review of simulation tools for wireless sensor networks (WSNs)," Journal of Wireless Networking and Communications, vol. 5, no. 1, pp. 19-47, 2015.

[34] K. Mehdi, M. Lounis, A. Bounceur, and T. Kechadi, "Cupcarbon: A multi-agent and discrete event wireless sensor network design and simulation tool," in Proceedings of the 7th International ICST Conference on Simulation Tools and Techniques, 2014, pp. 126-131: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[35] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross-level sensor network simulation with Cooja," in 31st IEEE conference on local computer networks, 2006, pp. 641-648: IEEE.

[36] [A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," in Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops, 2008, p. 60.

[37] T. R. Henderson, M. Lacage, G. F. Riley, C. Dowell, and J. Kopena, "Network simulations with the ns-3 simulator," SIGCOMM demonstration, vol. 14, no. 14, p. 527, 2008.

[38] Scalable Network Technologies. (2017, September 5). QualNet Network Simulator Software. Available: http://web.scalable-networks.com/qualnet-network-simulator-software
[39] V. Garcia-Font, C. Garrigues, and H. Rifà-Pous, "A Comparative Study of Anomaly Detection Techniques for Smart City Wireless Sensor Networks," Sensors, vol. 16, no. 6, p. 868, 2016.
[40] A. Dunkels, B. Gronvall, and T. Voigt, "Contiki - a lightweight and flexible operating system for tiny networked sensors," in 29th Annual IEEE International Conference on Local Computer Networks, 2004, pp. 455-462.
[41] K. e. Roussel, Y.-Q. Song, and O. Zendra, "Using Cooja for WSN Simulations: Some New Uses and Limits," presented at the Proceedings of the 2016 International Conference on Embedded Wireless Systems and Networks, Graz, Austria, 2016.
[42] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "SUMO–simulation of urban mobility: an overview," in Proceedings of SIMUL 2011, The Third International Conference on Advances in System Simulation, 2011: ThinkMind.
[43] C. Sommer, R. German, and F. Dressler, "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis," IEEE Transactions on Mobile Computing, vol. 10, no. 1, pp. 3-15, 2011.
[44] M. Kirsche and M. Schnurbusch, "A New IEEE 802.15. 4 Simulation Model for OMNeT++/INET," arXiv preprint arXiv: 1409.1177, 2014.
[45] I. Minakov, R. Passerone, A. Rizzardi, and S. Sicari, "A Comparative Study of Recent Wireless Sensor Network Simulators," ACM Trans. Sen. Netw., vol. 12, no. 3, pp. 1-39, 2016.
[46] G. D. Angelo, S. Ferretti, and V. Ghini, "Simulation of the Internet of Things," in 2016 International Conference on High Performance Computing & Simulation (HPCS), 2016, pp. 1-8.
[47] L. Sánchez-Casado, R. A. Rodríguez-Gómez, R. Magán-Carrión, and G. Maciá-Fernández, "NETA: evaluating the effects of NETwork attacks. MANETs as a case study," in Advances in Security of Information and Communication Networks: Springer, 2013, pp. 1-10.
[48] A. D'Hondt, H. Bahmad, and J. r. m. Vanhee, "RPL Attacks Framework," Université catholique de Louvain2016.
[49] C. B. des Roziers et al., "Using senslab as a first-class scientific tool for large scale wireless sensor network experiments," in International Conference on Research in Networking, 2011, pp. 147-159: Springer.
[50] L. Sanchez et al., "SmartSantander: IoT experimentation over a smart city testbed," Computer Networks, vol. 61, pp. 217-238, 2014.
[51] National Institute of Information and Communications Technology. (2017). Large-scale open test-bed JOSE. Available: https://www.nict.go.jp/en/nrh/nwgn/jose.html
[52] Y. Teranishi, Y. Saito, S. Murono, and N. Nishinaga, "JOSE: An Open Testbed for Field Trials of Large-scale IoT Services," NICT Journal, vol. 6, no. 2, pp. 151-159, 2016.
[53] A. Sanchez et al., "Testbed federation: An approach for experimentation-driven research in cognitive radios and cognitive networking," in 2011 Future Network & Mobile Summit, 2011, pp. 1-9.
[54] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo, "A survey on facilities for experimental internet of things research," IEEE Communications Magazine, vol. 49, no. 11, 2011.
[55] A.-S. Tonneau, N. Mitton, and J. Vandaele, "How to choose an experimentation platform for wireless sensor networks? A survey on static and mobile wireless sensor network experimentation facilities," Ad Hoc Networks, vol. 30, pp. 115-127, 2015/07/01/ 2015.
[56] A. Gyrard, P. Patel, S. K. Datta, and M. I. Ali, "Semantic Web Meets Internet of Things and Web of Things," presented at the Proceedings of the 26th International Conference on World Wide Web Companion, Perth, Australia, 2017.
[57] M. Hossain, S. Noor, Y. Karim, and R. Hasan, "IoTbed: A Generic Architecture for Testbed as a Service for Internet of Things-based Systems," in *2nd IEEE International Congress on Internet of Things (ICIoT)*, 2017.
[58] T. W. Edgar and T. R. Rice, "Experiment as a service," in *2017 IEEE International Symposium on Technologies for Homeland Security (HST)*, 2017, pp. 1-6.
[59] G. Kecskemeti, G. Casale, D. N. Jha, J. Lyon, and R. Ranjan, "Modelling and Simulation Challenges in Internet of Things," IEEE Cloud Computing, vol. 4, no. 1, pp. 62-69, 2017.
[60] R. G. Sargent, "Verification and validation of simulation models," in Proceedings of the 37th conference on Winter simulation, 2005, pp. 130-143: winter simulation conference.

Maxim Chernyshev received a Master's degree in software engineering from Edith Cowan University Perth, WA, Australia in 2008. He is a researcher with the Edith Cowan University Security Research Institute (ECUSRI), Perth, WA, Australia where he is also currently pursuing his PhD. His research interests include wireless network security, IoT security and digital forensics.

Zubair Baig is a senior lecturer in the School of Science at Edith Cowan University. His research interests include cybersecurity, machine learning, and digital forensics. He received a PhD in computer science from Monash University, Australia in 2008.

Oladayo Bello received the Ph.D. degree in electrical engineering from the University of Cape Town, Cape Town, South Africa. She is currently a Senior Lecturer with the School of Information Technology, Monash University, South Africa Campus, Johannesburg, South Africa. She is the author of several peer-reviewed international journals, conference papers, and newsletter articles. Her research interests include communication in the Internet of Things, interworking multi-hop wireless networks, and resource allocation in wireless networks. She served in several voluntary leadership positions within the IEEE and she has also served as the Chair of the IEEE Women In Engineering, South Africa Section.

Sherali Zeadally received his bachelor's degree from the University of Cambridge, Cambridge, England, in 1991 and his doctoral degree from the University of Buckingham, Buckingham, England, in 1996, both in computer science. He is an Associate Professor with the College of Communication and Information, University of Kentucky, Lexington, KY, USA. He is a Fellow of the British Computer Society and the Institution of Engineering Technology, England.