Microlocation for Internet-of-Things-Equipped Smart Buildings

Faheem Zafari, *Graduate Student Member, IEEE*, Ioannis Papapanagiotou, *Member, IEEE*, and Konstantinos Christidis, *Member, IEEE*

***Abstract*—Microlocation is the process of locating any entity with a very high accuracy (possibly in centimeters), whereas geofencing is the process of creating a virtual fence around a point of interest (PoI). In this paper, we present an insight into various microlocation enabling technologies, techniques, and services. We also discuss how they can accelerate the incorporation of Internet of Things (IoT) in smart buildings. We argue that microlocation-based location aware solutions can play a significant role in facilitating the tenants of an IoT-equipped smart building. Also, such advanced technologies will enable the smart building control system through minimal actions performed by the tenants. We also highlight the existing and envisioned services to be provided by using microlocation enabling technologies. We describe the challenges and propose some potential solutions, such that microlocation enabling technologies and services are thoroughly integrated with IoT-equipped smart building.**

***Index Terms*—Beacons, geofencing, Internet of Things (IoT), microlocation, systems of interaction.**

I. Introduction

THE developments in the field of information and communication technologies (ICT) have resulted in the widespread use of reliable and affordable communication services such as the Internet. Internet of Things (IoT) is defined as the ability of various things to be connected to each other through the Internet [1]. The number of Internet-equipped devices overtook the human population in 2011 [2]. As of 2013, there were 9 billion interconnected devices that are poised to reach 24 billion in 2020 [3]. Groupe Speciale Mobile Association (GSMA) predicts that these devices will result in a $1.3 trillion revenue [4] for the mobile network operators through different services such as health, utilities, automotive, and consumer electronics. IoT is a diverse field and broadly covers machine to machine (M2 M) communication, smart grids, smart buildings, smart cities, and many more. The basic motive behind IoT is to provide advanced residential and enterprise solutions through the latest technologies in an energy efficient and reliable manner without jeopardizing the service and comfort level. It is poised to highly impact the every day life and behavior of the potential users. Due to the increasing interest in IoT and its supposed impact on us, the U.S. National Intelligence Council (NIC) has included IoT in the list of "six disruptive civil technologies" [5]. NIC forecasts IoT to penetrate the everyday entities by 2025 including furnitures, home appliances, and food packages. The report discusses the vast horizon of opportunities that can exist in the future. For example, integrating the popular demand with the technological advancements will drive a broad diffusion of the IoT that will contribute highly to the economic development just like Internet right now.

IoT plays a key role in the transformation of residential and enterprise buildings to being "smart." Smart buildings aim to provide solutions that are energy efficient, environment friendly, disaster manageable, and comfortable. Therefore, any solution that can potentially increase the comfort level and provides the fore-mentioned services can be incorporated into smart buildings. Indeed, it is a system that allows for the buildings to have a "brain" [6], so that they can handle the human and natural disasters properly, and maintain the energy expenditure (hence reducing the greenhouse gas emission) while providing the level of comfort that the tenant asks for. Microlocation is the process of locating an entity with a high accuracy (in centimeters). Geofencing is a related concept that creates a virtual entity around any point of interest (PoI). Microlocation can assist in locating a tenant within an IoT-equipped smart building. The position of the user can then be utilized to provide him with effective and efficient solutions. In this paper, we aim to provide a thorough survey of various microlocation enabling technologies that can assist the IoT-equipped smart buildings. We discuss various microlocation-enabled services that will improve the tenant experience. We argue that due to the huge proliferation of smart phones with multiple sensors, the tenant–building interaction can be optimized for an enhanced user experience through the utilization of microlocation enabling technologies and provision of microlocation-enabled services. We also highlight some of the challenges that microlocation is currently facing and propose effective solutions. In summary, our work presents the following concepts.

1) A thorough survey of various microlocation enabling technologies, microlocation enabling techniques.
2) Current and envisioned microlocation-enabled services that can enhance the tenant's experience.
3) Various challenges of incorporating microlocation in IoT-equipped smart buildings and possible general solutions that can address the challenges.

Manuscript received April 27, 2015; revised May 21, 2015; accepted May 29, 2015. Date of publication June 09, 2015; date of current version January 20, 2016.

F. Zafari and I. Papapanagiotou are with the Department of Computer and Information Technology, Purdue University, West Lafayette, IN 47096 USA (e-mail: faheem0@purdue.edu; ipapapan@purdue.edu).

K. Christidis is with the Department of Electrical and Computer Engineering, IBM Emerging Technology Institute, North Carolina State University, Raleigh NC 27695 USA (e-mail: kchrist@ncsu.edu).

Digital Object Identifier 10.1109/JIOT.2015.2442956

This paper is organized as follows. Section II provides the basic description of smart buildings and IoT. Section III presents a description of various microlocation enabling technologies. Section IV describes the microlocation enabling techniques. Section V presents an insight into various microlocation-enabled services that are currently provided and envisioned to be provided in future. Section VI highlights the current challenges and some of the suggested solutions, and we conclude this paper in Section VII.

II. IoT and Smart Buildings

Both IoT and smart buildings are inter-related. Indeed, smart buildings will mostly rely on IoT for serving the tenants. In this section, we provide a basic description of smart buildings and IoT. Following section discusses smart buildings.

A. Smart Buildings

The Institute for Building Efficiency [7] defines smart buildings as the buildings that can provide low-cost services such as air conditioning, heating, ventilation, illumination, security, sanitation, and various other services to the tenants without adversely affecting the environment. The basic motive behind the construction of smart buildings is to provide the highest level of comfort and efficiency. For example, once a tenant enters an enterprise, the temperature, humidity, and the lighting are adjusted according to his personalized levels of comfort; his computer and the corresponding applications are turned ON [6]. At the same time, the interconnection of the automation systems can assist with the disaster management and provide emergency services. For example, the fire sensors can alert the ventilation system to turn OFF the fans; hence, the smoke and the fire can be contained in a specific area. The damages in the attack on Pentagon in 2001 were reduced, thanks to the advanced automation system (smart building) [6]. In order to do so, there is a need for added intelligence that starts from the design phase until the building gets functional. Smart buildings utilize IT for interconnection of various subsystems (usually independently operated). Such interconnection results in the sharing of information that optimizes the performance of the building, allows the building to interact with the tenant, and even be connected with other adjacent smart buildings. At the same, as the IoT is integrated into the smart building, there is a need to store, process, and analyze the information obtained from the interacting entities (tenants, other buildings, sensors, etc.). A smart building also has some level of energy independence. It has to have its own power generation through renewable energy resources, and incorporate energy efficient technologies. For example, solar photovoltaic windows can collect energy [8]. At the same time, the smart building is connected with the smart grid; hence, the excess energy can be provided to the grid or other buildings based on the relative agreements. This may result in an extra revenue for the building. Hence, the general characteristics of a smart building are as follows:

1) various interconnected business systems;
2) equipping the tenants or people with technology;
3) connection to various other buildings;
4) connection to the smart grids.

Fig. 1 presents various IoT components that are part of the smart buildings. Section V contains detailed information about how these IoT components can benefit from microlocation and geofencing to enhance the performance of smart buildings. Significant amount of research has been done to improve the architectural design of smart buildings and incorporate more technologically advanced systems into the architecture. There are two open communication standards for building automation known as building automation and control networks (BACnet) and LonWorks (where Lon stands for local operating network). Both these systems have a different approach toward the integration of different subsystems. BACnet being a communication, only standard is mostly concerned with electrical and mechanical systems. LonWorks combines the communication part with hardware and was used in transportation and utilities industry; however, it is now used in buildings as well. These two networks are not mutually exclusive and BACnet can work with some specific hardware as well. Both the systems perform their tasks differently. While BACnet defines different priority levels for performing the tasks such as the priorities of signals in the event of a fire, LonWorks might use different channels for different signals. While these two communication standards have started to establish themselves in building automation, there is still a long way to go. Such building automation systems help in reducing the operation cost [6].

Wireless sensor networks (WSNs) are playing a key role in the smart building automation. The WSNs are mainly design for control and automation of smart buildings. Hence, the collaboration and interconnection of all these sensors is bringing the attention to the IoT. Localization has also been a fundamental area of research in WSNs. Interested readers are referred to [9] and [10] for further information about positioning in WSN. There are two different WSN architectural approaches, the IP-based and non-IP-based approaches [1]. The Internet protocol version 6 (IPv6)-based low-power wireless personal area network (6LoWPAN) is the IP-based system. IPv6 is deployed over the 6LoWPAN protocol along with constrained application protocol (CoAP). The IEEE 802.15.4 Zigbee protocol serves as the link layer and the IPv6-6LoWPAN provides the services of the network or IP layer. The application layer services are provided by the CoAP. In the non-IP-based system, the physical and link-level services are provided by IEEE 802.15.4; however, a simpler network layer protocol called Rime can be used. It is the inbuilt IP layer of Contiki [11] and provides addressing as well as multihop networking facilities such as unicasting and broadcasting [12]. Rime cannot provide transport layer services, so a combined transport and application layer service is implemented via the exchange of JavaScript Object Notation (JSON) objects for the handling of application layer messages. The IP-based system performs better in terms of latency and energy consumption; however, the non-IP-based system outperforms the IP-based architecture in terms of memory footprint [1].

B. IoT

The integration of sensing with embedded computing devices in smart buildings results in the evolution of the embedded Internet. Ashton coined the term IoT in 1999; however, it was

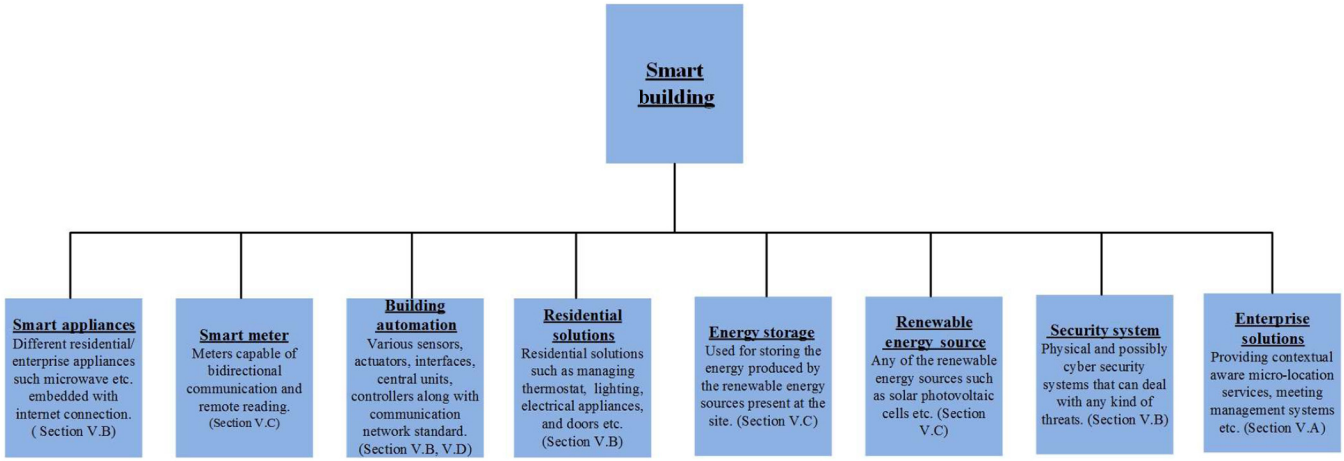

Fig. 1. IoT components of a smart building.

TABLE I
KEY WIRELESS TECHNOLOGIES USED IN IOT

Technology	Maximum range	Maximum frequency	Maximum throughput
Bluetooth IEEE 802.15.1 [16]	upto 100 m for Class A	2.4 GHz	24.0 Mbps with version 4
ZigBee IEEE 802.15.4 [17]	upto 100m with certain tradeoffs	2.4 GHz	2–250.0 Kbps
IEEE 802.11a [18], [19]	5000 m outdoor	5 GHz	54 Mbps
IEEE 802.11b	140 m outdoor	2.4 GHz	11 Mbps
IEEE 802.11g	140 m outdoor	2.4 GHz	54 Mbps
IEEE 802.11n	250 m outdoor	2.5/5 GHz	600 Mbps
IEEE 802.11ac	35 m indoor	5 GHz	1.3 Gbps with 3 antennas and 80 MHz
IEEE 802.11ad	Couple of meters	60 GHz	4.6 Gbps
WiMAX [20]	Depends on cell	2.3 GHz, 2.5 GHz and 3.5 GHz	365 Mbps downlink/376 Mbps uplink
Long term evolution [21]	Depends on cell	2600 MHz	300 Mbps downlink/75 Mbps uplink
Long term evolution-advanced [22]	Depends on cell	4.44-4.99 GHz	1 Gbps downlink/500 Mbps uplink
Ultra wide band (UWB) [23]	10–20 m	10.6 GHz	Upto 480 Mbps
Radio frequency identification (RFID) [24]	Upto 200 m	upto 10 GHz	Upto 1.67 Gbps [25]
WiFi direct [26]	Upto 200 m	2.4/5 GHz	Upto 250 Mbps

in the field of supply chain management [13]. The term over the years has incorporated various applications that can range from health care, transportation, and utilities. The fundamental idea for IoT is the interconnection of various "Things" such as sensors, smart phones, actuators, or physical items tagged/embedded with sensors such as chemical containers with temperature sensors. The cooperation among these devices forms the basic pillar upon which IoT stands and makes it possible for them to achieve the common goals [14]. The IoT is becoming extremely popular as the community looks into the possibilities from the generation of data from simple static IoT objects (e.g., a coffee machine) to the mobile devices, which come with sensing, computing, and communication capabilities. At the same time, IoT is strongly tied to the big data era due to the enormous data that the "Things" can generate. For the interconnection of these devices, different wired or wireless standards exist [15]. Some of the common wireless standards that are used for IoT are presented in Table I.

The application and services provided by the IoT can be both residential and commercial ranging from e-health [27], e-marketing [28], intelligent car parking system [29], intelligent transportation system [30]–[32], automation, and logistic services. However, new services are nowadays deployed based on the IoT, as it is foreseen that by the year 2025, IoT will encompass most of the appliances, food packaging, documentations, furniture, and many more [5], [33].

For a thorough integration of the IoT into the real world, there are several challenges that need to be addressed including the interoperability of the devices, device smartness, security, privacy, device energy consumption, device processing capability, and network addressing [27]. Fig. 2 presents an exemplar IoT infrastructure. Various systems and devices are interconnected through the Internet. It is evident from the figure that various devices used in residential, transportation, enterprise, healthcare environments, and literally everything else in the world can be connected through the Internet. Hence, current standards and technologies have to be optimized to support the multitude of wireless devices [34], [35]. Hence, the long envisioned release of 128-bit IPv6 addresses [36] is becoming a need as we move toward the IoT era. Due to the increase in the popularity of IoT, some research initiatives are in place now. The European Commission started pushing for IoT technologies-related initiatives in 2005 [37]. National Science Foundation (NSF) in the USA includes the IoT as part of their cyber–physical systems,

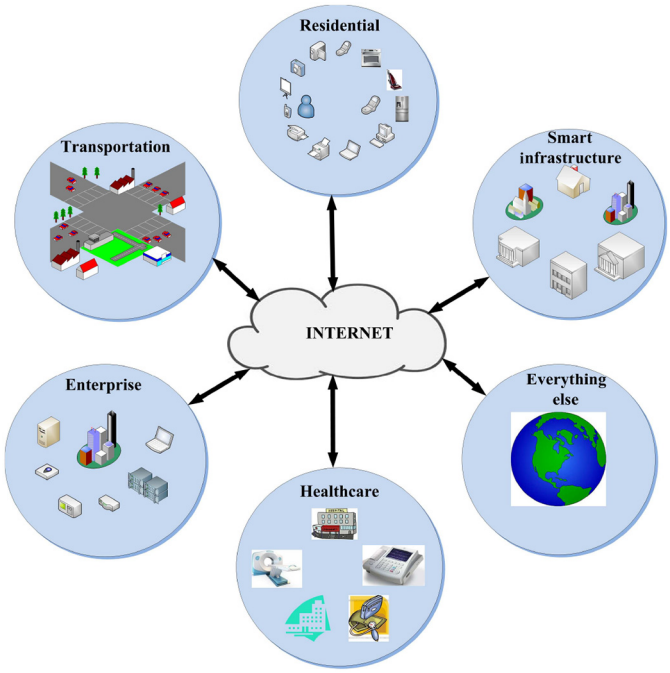

Fig. 2. IoT: connecting everything through the Internet.

where the goal is to design systems that merge physical and computational resources [38]. However, this program also covers a wide area of applications such as smart grids, intelligent transportation, smart manufacturing, and smart health care.

IoT has huge potential and a wide range of applications that it can be applied to. As of now, only a very small amount of services are provided to the consumers [27]. The future applications are envisioned to enhance the life quality of the tenants at the office, home, gym, library, hospital, etc. Particularly, smart environments such as in residential or enterprise domain have a great potential. Solutions that can improve the indoor environment experience will open up lots of revenue earning sources as well as enhance the tenant comfort level. Using IoT in smart cities/smart buildings can certainly provide reliable and efficient solutions as it will allow the user to interact with the entities.

C. Application Layer Technologies

The basic feature of any application layer technology in the IoT is the fact that these devices are resource-constrained and may function in constrained IP networks. A constrained IP network may exhibit high packet loss, small packet sizes, but needs to scale to a substantial number of devices. These devices, otherwise referred as the Things, may switch several times to sleep mode, and "wake up" for brief periods of time. A resource-constrained device has also limited RAM and processing capabilities. Constrained networks can occur as part of home and building automation, energy management, and the IoT.

To this end, there are two IETF efforts to standardize the transactions in the IoT world. The constrained restful environment (CoRE) working group defines the framework for a limited class of applications, i.e., those that deal with the manipulation of minimal resources in constrained environments. This class includes the Things, whether they are sensors (e.g., temperature sensors, light switches, and power meters) or control actuators (e.g., light switches, heating controllers, and door locks).

The second effort refers to concise binary object representation (CBOR) protocol, a data format meant as a building block for IoT protocols. CBOR messages can be serialized using compact code to fairly small message sizes. Both of these characteristics allow for faster transmission and processing on resource constrained IoT nodes. The data format is based on the JSON data model, a plus given the development community's direction toward end-to-end JavaScript for Web services. CBOR allows the encoding of binary data, and is itself encoded in binary. Finally, it is extensible through a tagging mechanism that identifies data that warrants additional information.

Moreover, using IoT in smart buildings will require using a large number of sensor nodes for the provisioning of various services. The management of such large number of sensors is an issue itself. The network must have the capability of efficiently self-diagnosing and self-healing. The integration of various standards results in the building management systems (BMSs). Open framework middleware (OFM) can be used for the management of WSN in smart buildings [39]. A rule-based fault analysis engine and structured knowledge when coupled with the OFM will help in root cause analysis and the network event correlation. Such systems can be explicitly interfaced with the BMS. Such a solution is one of its kind since the management of sensors to be used for IoT in smart buildings is an uphill task and there is hardly any general purpose WSN management middleware present in the literature. Software architectures can be used for asset management in smart buildings that can facilitate the engineers in receiving and updating the word orders and information about assets through utilization of mobile technologies and augmented reality [40]. A three-layered architecture that contains different modules consisting of data collection, work order and asset management, and event enrichment and management can help in BMS. Message queue telemetry transport protocol (MQTT) can be used for message exchange among various system components, while common alert protocol can be used to model the order of work and different alerts that can be then forwarded to the augmented reality application. The significance of such architecture is that the system functionality can be encapsulated and the interoperability of various subsystems is guaranteed. Also, various data standards can be integrated and the maintenance, upgrading, and management of the various service requests and building assets become easy.

III. Microlocation Enabling Technologies

In smart buildings due to the indoor nature, it is of primary importance to locate the user to enable the interaction with the rest of the interconnected things. Furthermore, the location of the user can be used to provide a wide range of novel services. Microlocation and geofencing fall in the broad category of the location-based services (LBS).

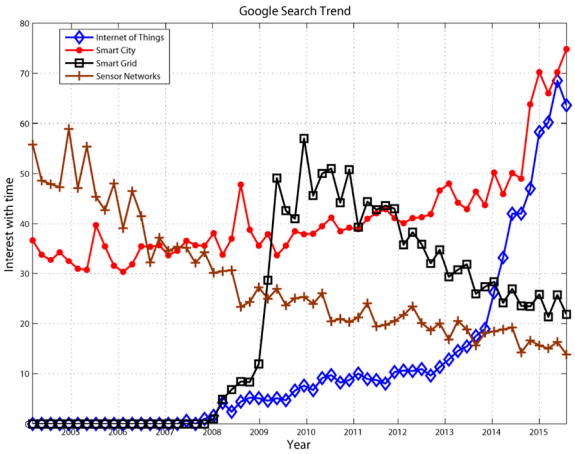

Fig. 3. Google search trend for keywords IoT, smart cities, smart grids, and sensor networks.

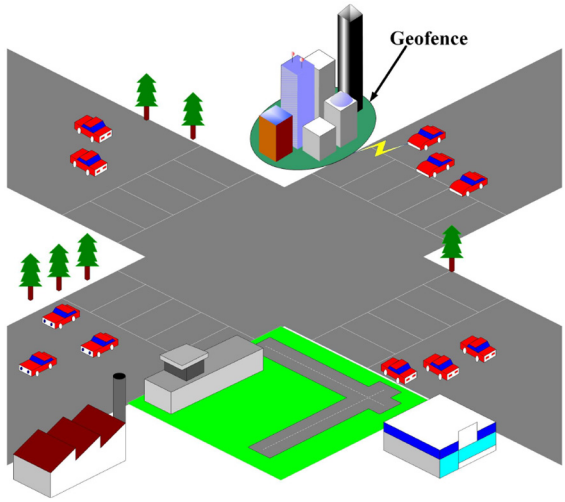

Fig. 4. Circular geofence around a smart building that advertises electric charging facility to an electric vehicle.

LBSs have been widely used in outdoor environments for navigation services in cars, airplanes, etc. For example, the widely used global position system (GPS) allows a user to identify their coordinates on a map with an accuracy of approximately 10 m [41]. This fact, combined with the system's poor performance indoors (no line of sight with the satellites) and its high toll on battery life, renders it unsuitable for use in a smart building setting [42], apart from rough geofencing. There is an increasing interest in IoT and smart cities/buildings as depicted in Fig. 3 [43] that can further increase by incorporation of microlocation and geofencing-based services in such IoT-equipped smart buildings. Realizing the significance of microlocation and geofencing-based services and technologies in IoT-equipped buildings, the number of microlocation and geofencing-enabled products is seeing a significant increase such as: for instance, in 2013, Qualcomm released the Gimbal [44] that uses the recent iBeacon protocol by Apple [45]. Similarly, Estimote [28] in 2014 released a combination of Beacons and a software development kit (SDK) that can be used to develop microlocation applications. Several other big companies are moving toward this direction like Google [46] and Cisco [47], as the IoT is considered by many the next "Big Thing" in the market and equipping smart buildings with IoT can provide much efficient solutions. In this work, we specifically focus on the use of microlocation and geofencing techniques in IoT-equipped smart buildings with emphasis on indoor area, in which IoT can be seen as a system of interaction, which is a term recently coined by IBM [48]. Effectively, a system of interactive things can enhance the performance of smart buildings and can result in efficient solutions. Therefore, from hereon, we would particularly stress on microlocation and geofencing LBS as its incorporation into IoT in smart buildings is full of potential.

Geofencing is considered a zone-based LBS [49]. It defines a virtual fence around a certain PoI. This fence can take various geometric shapes, be it rectangular, circular, or polygonal. The goal of a geofence is to provide targeted services related to a predefined area. Fig. 4 depicts a geofence example. There are numerous examples: a customer that enters a museum is notified about the proper path toward the exhibition of his interest, or an electric vehicle that is close to the geofence of a charging facility can be notified about a discount coupon. In microlocation, the goal is to have the location of a user or object pinpointed with the highest degree of accuracy possible [50]. This essentially allows the system to place the user within a geofence with certainty; it also gives rise to other capabilities, such as allowing the user to position themselves within a building and track their path. Some of the enabling technologies for geofencing and microlocation are presented below.

A. *Bluetooth Low-Energy-Based Beacons/iBeacons*

The Bluetooth Special Interest Group (SIG) proposed the Bluetooth low energy (BLE) or Bluetooth smart that is also known as version 4 of the Bluetooth technology [51]. It consists of the following layered architecture.

1) *Physical layer (PHY)*: It handles the transmission and reception of the data.
2) *Link layer (LL)*: It provides the medium access, flow control, and connection establishment related services.
3) *Logical link control and adaptation protocol (L2CAP)*: It multiplexes higher layer data and provides services such as fragmenting and reassembling the large data packets.
4) *Generic attribute protocol (GATT) and generic access profile (GAP)*: These are the top two layers of the Bluetooth stack.

A BLE device can be either a master or a slave. A master BLE device can simultaneously connect to various slave devices; however, each slave is connected to a single master. In contrast to the earlier Bluetooth versions, a BLE slave advertises on either one or all three allocated advertisement channel in order to be discovered. The master BLE device scans the channels periodically to discover the slave devices. After the master discovers the slaves, the data are transferred through periodic connection events where both the master and device sleep and wake up to exchange the frames. The devices sleep

for most of the time that enhances the energy efficiency of the devices.

The energy efficiency feature of BLE has made it an attractive technology for the miniscule devices known as iBeacons. The iBeacons were introduced by Apple [45] and the BLE-based iBeacon protocol is meant to assist any BLE-enabled device to detect its proximity to the iBeacon device. The iBeacon periodically transmits a beacon that can be picked up by the BLE-enabled device that subsequently allows them to position themselves within the building. Due to the low energy consumption of BLE, the iBeacons can be powered through any coin cell battery which can run for years based on the configuration of the beacon parameters such as transmission power and probing frequency. The iBeacons can be used for both microlocation and geofencing. They can be used for both indoor and outdoor environments with indoor environment being the dominant one.

Apple has standardized the iBeacon advertisement format [52] and the advertising packet consists of the following components.

1) *Universally unique identifier (UUID)*: It is the mandatory 16 byte string that is used for identification of the ibeacons used by a specific brand or company "A."
2) *Major value*: The major value is an optional 2 byte string that can be used to distinguish the iBeacons of a specific brand "A" that are located in different localities such as a city "B."
3) *Minor value*: Just like major value, the minor value is also an optional 2 byte string that is used to identify the beacon of any brand "A," in city "B," and department "C,"
   The iBeacons particularly perform the task of the following.
   a) *Distance measurement*: In order to measure the distance from a particular beacon, the BLE-enabled device uses the received signal strength indicator (RSSI). The value of the RSSI is an indicator of not only the proximity of the device to the iBeacon but also shows the accuracy of the obtained estimation results.
   b) *Ranging*: The distance of the BLE-enabled device and the iBeacon can be in any of the following four ranges [53].
      - *Immediate*: The device is very close to the iBeacon.
      - *Near*: The device will be in the "near" range if it is located at a distance of about 1–3 m with line of sight (LoS).
      - *Far*: A device estimated to be far indicates that the confidence about the accuracy of the estimated proximity is low.
      - *Unknown*: A device which is in the unknown range might not be close to the iBeacon or it can be due to the absence of recent initiation of ranging.

Once the BLE-enabled receiver picks up the beacon from the iBeacons, it sends the specific UUID to either a server or cloud where the particular event related to the UUID is sent back to the BLE-enabled receiver and is handled accordingly. It is also possible that due to obstructions, a device's range might be falsely detected. iBeacons is an attractive technology that can be used for microlocation purposes. Due to the expected impact of the iBeacons, it has garnered significant interest from different companies. Several companies are producing beacons and are offering beacon-based services; we list some of these in Table II. Recently, the University of Mississippi decided to start using Gimbal's beacons for facilitating its sports fans [54]. The basic idea is to use the beacons to enhance the game time experience of the fans and facilitate them with check in to the arena and provide them with relevant information and notifications. The beacon technology is poised to provide better consumer experience and increase the profits of the companies. The ability to provide accurate microlocation-based marketing and other services can assist the consumer and be a source of great income for companies. The mobile influenced retail sales are forecasted to be 689 billion U.S. dollar in the USA by the year 2016, overtaking e-commerce [55]. Therefore, these technologies have a great potential and their incorporation into smart buildings will facilitate both the consumer and the seller.

TABLE II
BEACON-BASED SERVICES

Company	Service description
Apple Inc.[45]	The iBeacons are used for micro-location purposes. They are Bluetooth Low Energy devices that enable LBS
Gimbal [44]	Gimbal's beacons provides a context-aware advertising platform. The beacon's communicate through bluetooth smart and they are as per the specifications of Apple's i-beacon
Onxy beacon [65]	Onxy Beacon also provides beacon based services that can help in better marketing and LBS. Onxy beacon also offers a beacon management system that is cloud based and helps in building micro location enabled applications for the beacons
Swirl using iBeacon [66]	Swirl uses iBeacons and provides end-to-end mobile marketing platform within a store. It is an enterprise grade platform that helps to create, manage and optimize the LBS based mobile marketing
Sonic notify [67]	Sonic Notify uses beacons to provide enterprise proximity solutions
Estimote [28]	Estimote utilizes beacons for creating new and contextually rich mobile services

B. UWB-Based Microlocation

The UWB-based radio technology has a fractional bandwidth that is greater than or equal to 20% where fractional bandwidth is the ratio of transmission bandwidth to the band center frequency [60]. UWB has an absolute bandwidth greater than 500 MHz. There are a number of advantages associated with using high bandwidth that can facilitate both communications- and radars-based applications. Using high bandwidth provides higher reliability because the probability of signals going around any obstacle increases due to the availability of wide range of signals having different frequencies. Also, the power spectral density decreases since the signal power is spread over

a large number of frequencies. There is a decrease in interference as well as interception probability. For microlocation, the UWB has two different phases [61].

1) Ranging: The process of ranging involves estimation of the distance or angles between any two nodes [61]. There are a number of techniques available for ranging such as angle of arrival (AOA), received signal strength (RSS), time of arrival (TOA), or the hybrid of any of these two. Since UWB has a good time-domain resolutions due to wide bandwidth that can provide subcentimeter resolution ability, therefore, TOA-based tecniques are used with UWB for ranging.

2) Localization: The process of ranging results in range estimates between the fixed device (known position) and the mobile device (unknown position). The fixed device for a UWB-based system is the UWB access point (AP), while the mobile device can be any smartphone, sensor, etc. The next step is localization, i.e., estimating the location of the mobile device. There are a number of various methods available for estimating the position of the mobile device such as the nonlinear least square (NLS) estimator.

UWB technology went out of favour couple of years ago due to the complexity and various other issues; however, it has recently seen a rise in interest since UWB-based microlocation can potentially provide an accuracy as high as 10 cm [57].

C. Wireless Positioning Systems

Wireless positioning systems are used for geofencing; they employ cellular towers for positioning outdoors, and Wi-Fi AP when considered in an indoor setting [62]. As is the case with UWB-based microlocation, some of the techniques based on WPS for positioning are AOA, time difference of arrival (TDOA), and enhanced observed time difference of arrival (E-OTD). Such geometric approaches are based on the transformation of the radio frequency (RF) signal measurements into estimated distances and angles, which are then used to deduce the location of the signal source using triangulation and standard geometry. WiFi infrastructure has also been used in [63] for indoor localization purposes without using any site survey. While site survey can assist the performance of WPS, the proposed system is optimized to work efficiently even in the absence of any site survey. The main concern associated with WPS is privacy. The cellular towers or Wi-Fi APs are vulnerable and can result in corruption of privacy. Attacks such as man-in-the-middle attack [64] can allow any third party to access the information by any user sent to an AP or cellular network. The user might be communicating his positioning information to the AP that the third party can have access to, hence violating the user privacy.

D. Magnetic Field Mapping

Modern day smart phones are equipped with the ability of sensing and recording the variations in the earth's magnetic field that can be used to create an indoor location map. IndoorAtlas [68] is the pioneer in providing this innovative technology for finding the location of any device hence providing us with the microlocation.

E. Radio Frequency Identification

RF identification (RFID) is a technology that assists in data storage and retrieval utilizing the electromagnetic transmission to some integrated circuit that is compatible with RF [69]. The entire RFID system consists of a number of basic components such as RFID readers, tags, and their intercommunication. The RFID reader is responsible for reading the data emitted by the tags. RFID systems use specific frequency as well as protocols that govern the transmission and reception of data. The RFID tags are categorized as follows.

1) *Active RFIDs*: They are equipped with a battery as well as radio transceivers which enhances their range.
2) *Passive RFIDs*: They operate without any battery and reflect the RF signal which is transmitted by the reader. The information is added through modulation of the reflected signal. They are meant to replace the traditional bar codes and are lighter and cheaper than their active counterparts.

Despite their limited range, they can be used for positioning purposes and can be a viable option for positioning purposes environment when used in triangulation with Wi-Fi and near-field communication (NFC) [70]. Since most of the users rely on smart phones, the problem with RFID is that most of the devices right now do not have RFID chips or tags. It can be used for microlocation purposes and can provide accuracy as high as 20–30 cm [24]. There are other technologies in the market that can provide positioning services such as infrared and ultrasound. Google [71], AlterGeo [72], Skyhook Wireless [73], Navizon [74], Infosoft [75], and Combain [76] are some of the most well-known providers of positioning services. Table III presents a summary of the discussed technologies that can provide LBS for IoT in smart buildings.

IV. Microlocation Enabling Techniques

In the previous section, we covered the major technologies used for indoor localization. This section focuses on the forms of location (i.e, physical, symbolic, absolute, and relative. The physical location is measured in two-dimensional/one-dimensional (2-D/1-D) coordinates (e.g. degree/minutes/seconds). Symbolic location is natural expression of the location in a smart building, e.g., office and elevator. The absolute location is based on a reference grid for all located objects. The relative location determines the proximity to a known object. Each of these techniques is independent of the utilized technology.

A. Triangulation

Triangulation is the technique that involves using three dimensions to estimate the location of the target. There are two different derivations of triangulation [77].

1) *Lateration:* The object's position is estimated through the measurement of the distance between the object and various reference points. It is also called range measurement technique.

TABLE III
POSITIONING TECHNOLOGIES

Technology	Accuracy	Transmission power	Cost	Battery impact	Feasibility for micro location
Beacon	0.1 m	0–10 dBm [56]	Low	Low	Yes
UWB based locationing	0.1 m [57]	–41.3 dBm/MHz [56]	High	Low	Yes
Magnetic field mapping	0.1m–2 m [58]	N/A	N/A	N/A	Yes
Hybrid of RF and IR, or RF and ultrasonic technologies	1 m [59]	N/A	N/A	N/A	Yes
WLAN,	3 m [59]	15–20 dBm [56]	High	High	No
Zigbee	3 m [59]	–25–0 dBm [56]	Low	Low	No
GPS	10 m outdoor [59]	Very high	High	High	No

2) *Angulation:* Relies on the computation of angles relative to a number of reference points for estimating the position of any entity.

Rather than measuring the distance directly through RSS, the TOA, or TDOA, the distance is obtained through either the computation of emitted signal strength attenuation or multiplication of travel time and radio signal velocity.

1) Lateration Techniques:

a) TOA: In TOA, the distance between the reference unit and target (either stationary or mobile) is proportional to the time of propagation. In order to locate any target in a 2-D environment, there is need for TOA measurements with respect to the signals that are emitted by at least three reference nodes. Fig. 5 shows how an object's position can be found out using three different reference points in a 2-D scenario. In TOA-based systems, the propagation time (one way) is determined, and is then used to obtain the distance between the measuring unit and the signal transmitter. The problem associated with TOA is the need for precise synchronization between the system transceivers [77]. Also, there is a need for a time stamp that has to be attached to the transmitted signal, so that the receiver can verify that the signal traveled directly, i.e., without being affected or reflected by any obstacle. A number of techniques such as direct sequence spread spectrum (DSSS) are used for TOA measurements. There are number of methods to determine the position of the target. A simple method is to use the geometric method for computing the intersection points of the TOA circles. An alternative method is using the least-squares algorithm [78], [79] that calculates the position of any entity through the minimization of the sum of squares of the nonlinear cost function [77]. The assumption for such technique is that the target entity located at (x_0, y_0) transmits a signal at time instant t_0, so the K-fixed stations positioned at $(x_1, y_1), (x_2, y_2), (x_3, y_3), \ldots, (x_K, y_K)$ receive that particular signal emitted by the target at time instances $t_1, t_2, t_3, \ldots, t_K$. The cost function is formulated as

$$C(x) = \sum_{j=1}^{K} {\beta_j}^2 c_j(x)^2. \tag{1}$$

The β_j depends on the signal reliability received at unit j, while $c_j(x)$ can be calculated as

$$c_j(x) = v(t_j - 1) - \sqrt{(x_j - x)^2 + (y_j - y)^2} \tag{2}$$

where v is the speed of light and $\mathbf{x} = (x, y, t)^T$. The function can be formed for any measuring unit $j = 1, 2, \ldots, K$ and

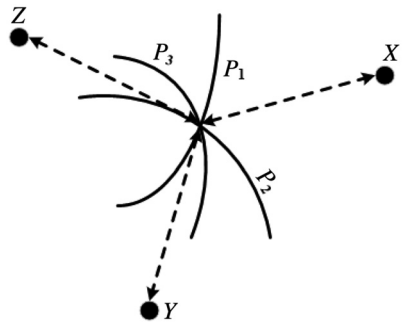

Fig. 5. TOA/RTOF-based localization of object.

$c_j(x)$ can be zero using specific values of x, y, and t. The estimated location can be obtained through the minimization of $C(x)$.

b) TDOA: The concept behind using TDOA is to determine the relative position of any mobile device through the examination of time difference at which a specific signal arrived at various measuring units. The difference between TOA and TDOA is that the latter relies on time difference rather than the absolute arrival time. For every single measurement of TDOA, the transmitter must be lying on the hyperboloid with a constant difference in range between two units of measuring. The hyperboloid equation is

$$R_{j,k} = \sqrt{(x_j - x)^2 + (y_j - y)^2 + (z_j - z)^2} - \sqrt{(x_k - x)^2 + (y_k - y)^2 + (z_k - z)^2}. \tag{3}$$

The (x_j, y_j, z_j) and (x_k, y_k, z_k) are used to represent the stationary receivers j, k and x, y, z represent the target's coordinates. An easier method to solve (3) is to use Taylor-series expansion and formulate an iterative algorithm. Nonlinear regression can also provide the exact solutions to (3). Correlation techniques can also be used for computing the TDOA estimate [77]. Fig. 6 shows how the location of target in 2-D environment is estimated through the intersection of two or more TDOA measurements. The TDOA measurement at the points (X, Y, Z) forms two different hyperbolas that can be used to locate the target W.

c) RSS-Based: Both TDOA and TOA are affected by multipath effect since both of them rely on the TOA of a signal and the arrival time of a signal is itself affected by multipath effect [77]. Therefore, the accuracy of the estimated position is not always great in an indoor environment. So, the alternative method that is used is to estimate the mobile unit distance from

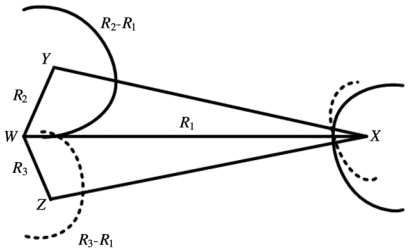

Fig. 6. TDOA-based localization of object.

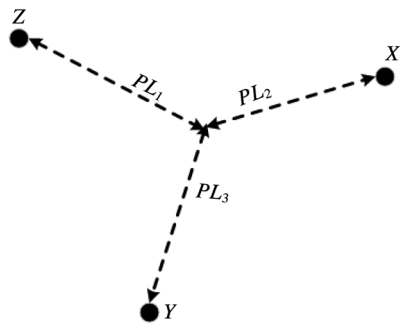

Fig. 7. RSS-based localization of object. PL_1, PL_2, and PL_3 are the path loss.

a set of measuring units utilizing the emitted signal strength attenuation. Such methods are aimed at calculating the signal path loss due to propagation. There are a number of empirical and theoretical models that can be utilized for interpreting the difference between the transmitted and RSS into the estimate of range. This is shown in Fig. 7.

The path-loss models might not hold true due to the presence of extreme shadowing and multipath fading which is the characteristic of indoor environments. The parameters of the path-loss model are site specific and the accuracy of the obtained results can be enhanced using premeasured values of the RSS contours that are centered at the receiver. An alternative method to improve the accuracy is through multiple measurements at a number of base stations. Fuzzy logic algorithm can also improve the accuracy of RSS-based location estimation [80].

d) Round Trip of Flight (RTOF): RTOF method relies on the measurement of round trip time of flight of any particular signal that is traveling from the transmitter to the measuring unit [77]. Fig. 5 shows the concept of RTOF which is also the figure for TOA. The difference between TOA and RTOF is also that the clock synchronization requirement for RTOF is not a stringent as it is for TOA. The mechanism of range measurement in both TOA and RTOF is the same. For both the systems, a common radar can be the measuring unit, while the target replies back to the radar signal. The complete round-trip time is measured at the measuring unit. Measuring unit is again affected by the problem of knowing the exact amount of delay or processing time that is caused by the target. The delay can be ignored if it is comparatively smaller than the transmission time in a long or medium-range system, but short-range systems cannot ignore it. For short-range systems, modulation reflection can be a viable concept [81]. It is worth mentioning that the positioning algorithms that are used for TOA can also be used for RTOF.

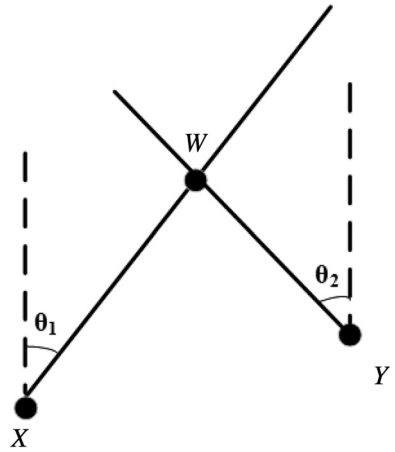

Fig. 8. AOA-based localization of an entity at point W.

2) Angulation Technique: In angulation technique such as AoA which is also known as direction finding, the object's position is determined through the intersection of a number of pairs of angle direction lines that is formed by a circular radius of a base station to the moving target [77]. Fig. 8 shows a sketch of how angulation technique can work. For estimating the location of any entity in 2-D, the method requires at least two known reference points and two angles, i.e., (X, Y) and θ_1, θ_2, respectively. The user's location can be estimated using AOA either through the use of array of antennas or directional antennas.

The advantage of AOA over other techniques is that we can use AOA to estimate the position of any entity in three-dimensional (3-D) using a minimum of three measuring units. Furthermore, AOA does not require any time synchronization among the units of measuring. The disadvantage of using AOA is that it requires complex and large hardware, and the accuracy of the estimation degrades significantly when the entity moves away from the measuring units. In order to obtain an accurate estimate of the location of the entity, the angles must be measured accurately; however, this might be impeded by the presence of multipath and shadowing in indoor environments.

B. Proximity

The proximity-based algorithms aim to provide information about the symbolic relative position [77]. Such algorithms rely on using a dense grid of antennas where the position of every antenna is known. When any antenna detects a target, the target is thought to be colocated with it. However, when more than one antennas detects the target, then it is assumed to be colocated with the antenna with the highest signal strength. Compared to other methods, the proximity-based methods are easy to implement and its implementation is possible over a range of various physical mediums. Systems that are based on RFID and IR usually rely on proximity-based methods.

V. Microlocation-Enabled Services

IoT in smart buildings utilizes microlocation-enabled services for various residential and enterprise solutions, in order to

TABLE IV
EXISTING GEOFENCING AND MICROLOCATION-BASED SERVICES

Services	Description	Technologies
Fleet management [50]	It involves managing the transportation fleets e.g. planes, cars, vans, ships, rail cars and trucks	GPS, Zigbee
Freight management [50]	It involves managing the carriers belonging to a third party for ensuring the reliable, quick and cost effective delivery of various shipments that can involve integration of a range of services	GPS (outdoor), UWB, Beacons, Magnetic Field Mapping, WLAN, Zigbee and Hybrid of RF and IR, or RF and Ultrasonic Technologies (indoor)
Mobile tourism [83]	This service can assist tourists during their tour. Various context aware, LBS based guidance and notifications can be provided	GPS, Zigbee
Area sensitive gaming enablement [84]	This service enables gaming without a specific area	UWB, WLAN, Zigbee, Beacons, Magnetic Field Mapping
Device location and route adherence [85]	It helps in locating a device and making sure the device stays within a specific location	Beacons, GPS, WLAN, Zigbee, Magnetic field mapping, Hybrid of RF and IR, or RF and Ultrasonic Technologies
E-marketing	Using geofencing and micro location, the user can be provided with location based advertisement. It is relatively new application and is considered to be the major application in the envisioned future smart buildings	Beacons,UWB, Hybrid of RF and IR, or RF and Ultrasonic technologies, and Magnetic Field Mapping

increase the tenants' comfort and satisfaction level. An inability to integrate such microlocation-enabled services reduces the overall system efficiency and impedes innovation [82]. Several current uses of geofences and microlocation are shown in Table IV. We list some developing and envisioned scenarios below.

A. Targeted E-Marketing

Geofencing and microlocation can play a great role in e-marketing. Already, there are some companies in the market that offer targeted advertising facilities that can be an added source of income. A hardware shop owner can create a specific geofence around his shop that will send coupons, offers, and deals of the day to targeted customers who enter the geofence. Since context-awareness is accompanied with the geofence and microlocation, it can help in proper advertisement and attracting the customers to the shop. Different microlocation enabling technologies can be used for the targeted e-marketing; however as of now, the BLE-enabled beacons are emerging as a viable option. The beacon-based context-aware platforms are the main pillar of the targeted e-marketing and they can certainly provide numerous efficient solutions. There are numerous examples of the services that can be provided through these beacon-based context-aware platforms [44] such as the following.

1) A customer in the geofence of any retail store is notified about the special discounts.
2) A customer notified about the availability of his prescription when he enters the geofence of a pharmacy. It is timely personalized service provided to the customer through LBS.
3) A sports fan welcomed and given information about special discounts once he enters into a sports arena.
4) Updating commuters proactively when traveling from point X to Y [86].
5) A customer provided with information about a shirt that might match the shoes he just bought.

Context awareness is one of the basic requirements of targeted e-marketing since the system must know about the preference of a particular customer. In the absence of such information, the system might be flooding advertisements to the customers that can lead to customer irritation. The customers can then unsubscribe to the service. As mentioned earlier, the BLE-based beacons' fundamental use as of now is targeted e-marketing and different companies [28], [44], [66] can provide such service. Although companies have already started some of the services, they are still in infancy and there is a lot of room for improvement. The services can be further improved and can incorporate various novel concepts as well. The use of geofencing and microlocation will also enhance the enterprise solutions (see Fig. 1) that the IoT can provide in smart buildings. Using the positioning information for meeting management systems is one such possible application.

B. Tenant Assistance

The whole idea behind IoT and smart buildings is the facilitation of the tenant and provision of comfort and assistance to the tenants. Tenant/user assistance is a general term and can cover a wide area of services. An art fan who enters a museum and is looking for his favorite art collection can be facilitated by the smart buildings, utilizing the system of interaction [48] for communicating context-aware location information obtained through microlocation and geofencing technologies. Due to the context awareness, the smart building will know that the user is looking for a specific piece of art. So, the interconnectivity of various systems will help the building find the user's favorite art collection and can then provide him/her with the directions to reach the designated area. Furthermore, the user can leave digital comments attached to the the artifact that other users in the vicinity can browse. The user will also be facilitated in "liking" or tweeting due to contextual awareness. The content can be bookmarked for later use. Such geofencing and microlocation-based services can also help enhance the museum experience

through interactive guides and contextual interpretation. It is worth mentioning here that geofencing detected the entrance of the user into the building, microlocation found out his exact location, the context awareness helped in finding out about the user's preferred art collection, while system of interaction helped in interaction of the tenant with the building by conveying obtained information and facilitating the user. All these systems working in sync with numerous other systems then facilitated the user to reach the spot. This is a classic example of how an IoT-equipped smart buildings can benefit from context-aware microlocation-enabled services.

In another scenario, geofencing and microlocation can facilitate a manager with efficient service provisions. As soon as the manager enters into the geofence of the company, his office computer and the HVAC will be turned ON and the office temperature will be adjusted as per his choice using context awareness. A patient who needs emergency medical care can be facilitated by providing him with proper treatment using context awareness as well as location information for providing him immediate medical aid. Similarly, geofencing and microlocation can be used in huge retail stores for guiding a consumer to reach a specific lane and get special discounts on his/her entity of interest. San Francisco airport is testing the beacon-based microlocation system to assist the visually impaired travelers [86]. The project is visioned to be extended to help everyone at the airport in the future, providing them with information about everything around them. In short, the range of facilities that can be provided are unlimited and it is only a matter of time until these services are provided. The use of such microlocation services for IoT in smart buildings is certainly increasing the comfort level of the tenant and providing brand new areas of services that will result in a better standard of life. Provision of better security, i.e., both cyber and physical, efficient building automation systems, and optimum utilization of smart appliances (see Fig. 1) is certainly made possible through the use of microlocation and geofencing. A geofence around a smart appliance will notify the appliance about entrance or exit of a user which can then adjust itself accordingly.

C. Energy Efficiency

One of the driving forces behind the adoption of smart buildings is the need for energy-efficient buildings. Smart buildings through the cooperation of various systems provide energy-efficient solution and minimize the waste of energy. In order to obtain energy-efficient smart buildings' solutions, the buildings and houses must be equipped with various capabilities such as demand side management, storage of energy on a microlevel, the use of renewable energy sources on a microlevel, and an electricity consumption controller that relies on price signals for providing efficient solutions [87]. Using system of interaction and IoT in smart buildings will allow the energy consuming devices to be connected to Internet that will allow the user to control and monitor various appliances through a simple smartphone or any wireless terminal [88], [89]. Using the microlocation-enabled services, a user's location can be utilized by the energy-consuming appliances that can also interact among each other and act accordingly to optimize the resources, i.e., using the least possible energy to provide the optimal level of comfort to the tenant. System of interaction facilitates the interaction of the devices and certainly will result in a paradigm shift [90].

Microlocation-enabled services can help increase the energy efficiency of the IoT-equipped smart buildings in two different ways: 1) reducing the waste of energy and 2) optimizing the performance of the appliances and energy-consuming devices. In order to provide efficient tenant assistance, the tenant must be willing to subscribe to the services. Also, the tenant's position and his preferences should be used to provide the solutions properly.

D. Disaster Management

In this text, we refer to disasters inflicted by natural phenomena (floods, tornadoes, storms), equipment failure (e.g., fire due to a short circuit), or terrorist attacks. Traditional buildings are characterized by a low or nonexistent level of preparedness for disaster management. On the other hand, smart buildings can mitigate or even completely eliminate the adverse effects of such events. For example, in the case of a fire, in addition to the fire alarm going off, the tenants will be alerted using microlocation-enabled services, and the HVAC will turn OFF in the burning area, so that the smoke cannot transfer to other parts of the building.

Crowd sourcing can provide efficient disaster management solutions when it is used in smart buildings [91]. It can certainly provide accurate data to the disaster managers, which can then be utilized for better management. Social network analysis can also be applied to interlink the objects for investigating and deepening the understanding of IoT paradigm [92]. There are a number of ways to interlink IoT that can be analyzed utilizing social network analysis. Such analysis can certainly help in disaster management and provide efficient results. The utilized smart buildings framework tend to prioritize the group safety over the safety of an individual [93]. In order to implement such systems, it is practically and ethically required that the system should account for the uncertainty revolving around the clinical condition of every individual that can be obtained using a context-aware microlocation-enabled service. All of these services require high positioning accuracy, usually finer than 1 m. As we have shown in Table II, UWB and BLE can provide accuracy as high as 10 cm [57].

VI. Challenges and Proposed Solution

The application of microlocation enabling technology and services in IoT-equipped smart buildings is supposed to make things easier for the tenants; however, there are certain challenges that can serve as a hurdle in the efficient utilization of microlocation-enabled services. In this section, we will discuss some of those challenges and propose solutions for them.

A. Accuracy

Since the main purpose of using microlocation enabling technologies and services in any IoT-equipped smart building is to

locate any user within the building to provide efficient services and solutions, the accuracy of the estimated position is of significance. Microlocation enabling technologies are supposed to have high accuracy, so that the exact location of the tenant can be found out. In past, various positioning technologies such as GPS [59], WLAN, Zigbee, RF, infrared (IR), ultrasounds, or a hybrid of these technologies [59] have been used to find out the position of the user. These technologies can use different techniques such as RSSI, TDOA, and TOA [61] to provide the position of the user. These technologies are not as accurate as required for microlocation purposes (see Table III). GPS is not suitable for indoor environment, while the other technologies despite functioning in the indoor environments cannot attain high accuracy. The accuracy range is out of the required range and there is significant room for improvement. Using various filtering techniques can enhance the accuracy of various technologies. Although UWB-based technologies have the highest accuracy as of now, beacon-based microlocation services' accuracy can be enhanced by using filters such as Kalman filter, extended Kalman filter, and particle filters. There is need for further research to identify the optimal filter for microlocation and how it can further be improved to give us the best possible accuracy.

B. Interoperability

As mentioned earlier, there are a number of microlocation enabling technologies that can be used for provision of efficient and effective solutions. These various microlocation enabling entities lack interoperability. Following sections classify the interoperability on the basis of various parameters.

1) Technologies: As of now, there are a number of microlocation enabling technologies available that were discussed in Section III. All these technologies are different and utilize different concepts to location with a high accuracy. IoT requires the interconnectivity and interoperability of all the various entities that constitute it. The end-user in an IoT-equipped smart building is not concerned about the technologies that are used, rather his position is of significant importance since that will enhance the comfort level and provide efficient services. Therefore, the interoperability of different microlocation enabling technologies is of significant importance. Currently, existing microlocation enabling technologies are not interoperable, i.e., a UWB-based microlocation system cannot be integrated with an ibeacon-based system. The two systems based on different technologies cannot function as one unit. Similarly even within the iBeacon platform, there are different vendors that provide ibeacon-based microlocation enabling services; however, they lack interoperability. Estimote [28]-based ibeacon cannot be detected by Gimbal's [44] mobile application and vice versa. This is because the vendors have their own frameworks and libraries that they use when they are developing an application. This causes lack of interoperability between the ibeacons of different vendors.

2) Software Development Kits: iBeacon vendors tend to provide their own SDKs, as a means of facilitating the development of applications. However, SDKs of different vendors are different, and cause a vendor lock-in problem, i.e., the ibeacons of some other vendor cannot be incorporated in the beacon network as they are tied to vendor-based SDK. In other words, application developers on iBeacons will have to develop different applications for their applications to function under different vendors. This also leads to issues like upgrading the iBeacons to a future generation that might involve updating the whole end-to-end system.

3) Protocols: Another challenge is that there are not standardized protocols for microlocation enabling services. Considering again the case of iBeacons, we have observed two main protocols that are available both utilizing the BLE interface. For example, Apple[45] owns the ibeacon closed-source protocol that specifies the packet and communication structure of the ibeacons and is only available to the ibeacons manufacturers. Similarly, there are other vendors that provide BLE-enabled beacons; however, they are not compatible with the Apple's standard. In such a scenario, the ibeacon will not work with the beacons that are not as per the Apple's standard. Clearly, there is a need for protocols and standardization that can assist in the interoperability of technology-wise different but task-wise similar systems. All these devices have to work in sync to attain the required common goal, i.e., to provide microlocation-enabled services. Making these different technologies will also increase the overall system efficiency.

C. Privacy

One of the main concerns with the use of microlocation enabling technologies and services is privacy. Although they are supposed to provide efficient services to the tenants of any IoT-equipped building, revealing user's location is a privacy issue. As of now, the microlocation enabling technologies and services require the approval of the tenants and it is only after the tenant approves, such technologies then start operating. Most of the tenants might find it a breach of their privacy to let their location be traced through their smart phone or any other Bluetooth-enabled device; therefore, they might be reluctant to use such technologies and services. This is a major challenge as without tenant's consent, the microlocation enabling technologies can not reach its ultimate potential and market penetration might not be as expected.

Furthermore, once the user's position is obtained, the data might be stored and used for future use. This can help in analyzing the user interest and be used for contextual-aware marketing, etc. However, storing the user data requires the data collection that needs to be properly handled [27]. Different subsystems of the IoT and microlocation enabling technologies will interact with the human beings and obtain data that need to be properly stored and taken care of. However, it is important to make sure that the data should not be used for malicious purposes. Policy broker [94] can be used to guarantee that the data are used specifically by the authorized agency for an authorized task [27]. Policy broker uses proxy that interacts with user at one end and the services at the other. This guarantees that the user does not provide more information than required. Virtual private networks (VPNs) can also be used to secure the data within an organization [95]; however, this is not feasible for IoT as it requires interconnectivity around the world.

The integrity and confidentiality of the IoT can also be improved using a transport layer security (TLS). However, every single object naming service (ONS) would require a new TLS connection that affects the information searching as new layers are added. DNS security extensions (DNSSEC), onion routing, and private information retrieval (PIR) discussed in [95] can also facilitate privacy protection. The location privacy solutions used in Vehicular Networks can also be modified to be used for privacy issues in IoT and microlocation. The protocol proposed in [96] relies on the creation of cryptographic mix-zones that can be used in various points within a building. This will mitigate the threat of eaves droppers that are computationally constrained. Their proposed protocol can be utilized efficiently for the privacy protection of the tenants of smart buildings.The pseudonym-based approach proposed in [97] can be used for energy affluent IoT devices in smart buildings; however, it is not feasible for energy constrained devices due to the complexity involved. The use of anonymous public keys presented in [98] for vehicular ad hoc networks (VANETs) can also be used for IoT; however, it cannot be used in its current form with microlocation, particularly with beacon-based microlocation. The use of anonymous public keys can benefit IoT, particularly, in disaster management scenarios as the message will be mostly safety messages that will not have any of the private user information. In order to facilitate the growth of microlocation enabling technologies and services, the service providers must provide the tenant with a guarantee that the location information will be only used to enhance the comfort level of the tenant and will not be used for any other purpose. There is also a need for strict laws and penalties if any service provider is found violating the user privacy by using the location information for any other purpose other than the agreement with the tenant. Winning the tenant trust is an important factor in the growth of such technologies and services. Such services can only attract tenants once the tenant is assured of their privacy protection. The service providers can also attract the tenant's attention by utilizing different marketing strategies that will encourage the tenants to adopt the microlocation enabling technologies and services.

D. Energy Consumption

Enhancing the energy efficient of the microlocation enabling technologies and services is of significant importance as such technologies and services can be energy consuming. The energy consumption for microlocation can be divided into two broad categories.

1) Microlocation Enabling Devices: The devices used for microlocation such as the ibeacons, the UWB transceivers, the magnetic field mappers, and the wireless positioning system must be energy efficient. The energy consumption of such technologies can serve as a hurdle in its wide scale adoption. With the ibeacons particularly, its transmission power and transmission time period can be adjusted to save energy at the cost of performance. For energy consumption purposes, a device with lower transmission power and higher interval between the transmission of beacons is favorable.

2) User Devices: The user device is one of the main component of microlocation system. No matter what specific microlocation enabling technology is used, the user device is the end device that can assist in providing the position of the user. Since the battery technology has not kept up with the pace at which the other technologies have improved, optimizing the energy consumption of the device is an important issue. The energy consumption of the devices differ based on the microlocation enabling technology used.

a) BLE-Enabled Devices: The BLE-enabled devices due to the presence of the BLE are less energy consuming. These devices can communicate with the ibeacons and be used for microlocation purposes. When the ibeacon used transmits with a high time period, then that will also enhance the energy efficiency of the user devices since it will have the ability to sleep for longer periods.

b) UWB: UWB compared to the Wi-Fi technologies provide higher bandwidth, lower power consumption but shorter range. They are also low cost [23]. However, they still consume a significant amount of energy from battery-limited devices, like smart phones; hence, microlocation services need to take this into account.

c) RFID: Although the passive RFIDs do not use any battery, their range is shorter. Active RFIDs due to better range need battery power. The reliance of range on battery (due to transmission power) certainly affects the performance of the RFID. Although the smart phones as of now do not have RFID chips/tags [24], other user devices might be affected adversely due to the energy consumption of the RFID system. To the author's knowledge, the effect of the energy consumption in microlocation services has not been studied. This is an important and open problem as these services are widely deployed and contest for minimal energy resources. Simplifying the microlocation technologies without affecting their accuracy is an interesting research problem that has to be addressed.

E. Security

Although the motive behind the use of microlocation enabling technologies and services in the IoT-equipped smart buildings is to facilitate that tenant with efficient and reliable solutions, there are significant security challenges that threaten both microlocation and IoT. The devices used for the purpose of microlocation are supposed to be cost-efficient and simple to minimize the power utilization, which makes them vulnerable to various attacks. All these devices can act as a point of entry for any attacker into the network; therefore, their security is an important issue. The two major security related problems that IoT faces are data integrity and authentication [27]. While most of the prominent authentication mechanisms rely on the extensive exchange of messages, they are not feasible for IoT and microlocation. A number of solutions are present in literature for sensor networks [99]; however, they are not feasible in their current form for IoT. IoT also relies on the communication among "things" so a fundamental challenge that it faces in terms of security is the man-in-the-middle attack [27]. Data integrity requires that the sent or received data should not be modified in any form by any third party. The data should reach

TABLE V
SUMMARY OF CHALLENGES AND PROPOSED SOLUTIONS

Challenge	Description	Proposed solution
Interoperability	Different micro-location enabling technologies are not inter-operable such as UWB micro-location system cannot work in sync with an iBeacon based micro-location system	There is a need for proper standardization and protocols that can help in making different technologies inter-operable
Privacy	The tenant's location information is sensitive and if used for any purpose other than its specific use, can result in corruption of user privacy	Provision of guarantee to the user that his location will be only used for designated purposes as well as implementing strict laws that can punish the violators
Energy consumption	The tenants might be reluctant to use the micro-location enabling technologies and services due to the associated energy consumption	Develop micro-location enabling technologies and services that are highly energy efficient. Also, there is need for improving the battery technology in order to provide long lasting performance
Accuracy	Micro-location requires high positioning accuracy to provide better services however as of now there are some accuracy issues with micro-location enabling technologies	In order to improve accuracy, there is a need for cutting edge research. Different filtering algorithms can be used to obtain better accuracy
Security	Security of the micro-location technologies and services in IoT equipped smart building can be under threat. Since some of the these technologies can use cloud, so the traditional security threats affiliated with the cloud can affect micro-location enabling technologies	Checking the viability of distributed and centralized security mechanisms
Artificial intelligence enabled devices	The smartness of the devices should be enhanced further to achieve the tasks required by micro-location enabling technologies and services in IoT equipped smart buildings	Use of Artificial Intelligence based techniques improving the devices and enhancing their smartness

its destination without any manipulation. The problem of data integrity in sensor networks has been studied extensively and further information can be found in [100]; however, the devices in the IoT are mostly unattended, which adds more into the challenge. Adversaries can modify the data either at the node or when it traverses in the network [27]. Memory protection in various tag technologies and solutions is used as the precautionary step to save the data from being tampered at the node, while keyed-hash message authentication code (HMAC) solution can be used to protect the data, while it is traversing across the network. Further information on security related issues of IoT with suggested solutions can be found in [2], [95], [101].

Authentication mechanisms can also facilitate the security of IoT and microlocation. Current authentication mechanisms rely on the binding of an identity to a pre-shared secret (e.g., a password or generated random value), an RSA key pair, and its associated X.509 certificate or one-time token passwords [102]. Such credentials may be prohibitive as they may be unmanned or the devices have such a small footprint, lacking in memory required to host the X.509 certificate and/or lacking in the CPU power to execute the cryptographic operations to validate the X.509 certificates (or any type of public key operation).

More advanced security challenges exist: as a plethora of indoor sensor, actuators, and embedded systems are deployed in smart buildings, they need to adhere to a single common standard to facilitate zero-tough configuration and provisioning. The scalability of microlocation-enabled services in an IoT-equipped smart building brings new challenges as deployments must now serve millions huge number of endpoints. Similarly for IoT, serving a rich multiservice edge along with all the required policies to serve the different millions endpoints forces larger and more distributed scale deployments than the classical IT.

Such a reality teaches us that a perfect secure solution is unlikely to be achieved at any level. A real-time intelligent security and risk management capability provides a complementary solution to address the security gaps and threats. Hence, a flexible security framework is required. Any microlocation enabling technology or service deployment must encompass the following components: 1) authentication; 2) authorization and access control; and 3) network enforced policy.

For the sake of context-aware services, user's information is saved on the cloud and is meant to be used for marketing purposes; however, it can used for nonrelevant purposes in any way that can be hazardous to the overall system. Also, due to various network attacks, precious data can be manipulated and exposed that can not only affect the seller but also the user. With the advent of beacon-based LBS, a new window of marketing has opened up; however, its security has to be tightened and the privacy concerns of the users should be handled as well.

The traditional security protocols and methods cannot guarantee the security of microlocation enabling technologies and services in IoT-equipped smart buildings and there is need for cutting edge research to properly secure the network. While securing the network, it should also be made sure that the proposed solution is practically implementable on energy-constrained devices. The security mechanism should be reliable as well as quick. Furthermore, those microlocation enabling technologies and services that use the cloud for data storage and other tasks face the challenges that any typical cloud-based application will, so the traditional security solutions applied for security of the cloud can be applied here as well.

F. Artificial Intelligence-Enabled Devices

Microlocation-enabled services in an IoT-equipped smart building are meant to enhance the tenant satisfaction and increase the overall efficiency. Due to the expected increase in future use and the overall demand of the users for intelligent and autonomous systems that will facilitate the user, there is need for enhancing the device smartness. A smart device will use user's positioning in an effective way to fulfill the tasks. In the absence of device smartness, a user might be alerted about a particular grocery to buy based on his position which might not be the best possible option in terms of price; however, with the added intelligence in device, the device can find the optimum option for the user taking a number of parameters into account. This is one of the envisioned microlocation-enabled services. Similarly, the user's past location can be of use in predicting his future location that can be then used to provide contextual-aware information with better reliability. Such services that are to be provided in an IoT-equipped smart building are challenging and require the devices to exhibit higher level of smartness than the current level in order to accomplish their envisioned tasks in the future smart buildings. The use of artificial intelligence (AI) algorithms can certainly help in enhancing the smartness of the devices. Formulating AI algorithms that are less complex while simultaneously enhances the smartness is a challenging task. Such algorithms will equip the devices to properly accomplish their tasks in the current and envisioned microlocation-enabled services in IoT-equipped smart buildings. Table V provides a summary of the challenges and the proposed solutions.

VII. Conclusion

In this paper, we focused on microlocation enabling technologies and services for an IoT-equipped smart building. We described various microlocation enabling technologies that are used right now. We argued that using such microlocation enabling technologies in an IoT-equipped smart buildings, we can provide the tenant with a wide range of services that will enhance the comfort level as well as increase efficiency of the overall system. We presented some of the microlocation-enabled services and described some example use cases. Using the microlocation-enabled services can open the door to various novel services that are only possibly due to the integration of the IoT within a smart building. Recently, there have been advancements in the field of microlocation and various new technologies and techniques have been proposed. However, these advancements come with several challenges. For example, security and privacy, as well as accuracy and energy consumption of the devices, provide avenues for interesting research problems. To conclude, we believe that microlocation enabling technologies and services in IoT-equipped smart buildings have a huge potential.

References

[1] O. Evangelatos, K. Samarasinghe, and J. Rolim, "Evaluating design approaches for smart building systems," in *Proc. IEEE 9th Int. Conf. Mobile Ad hoc Sensor Syst. (MASS'12)*, 2012, pp. 1–7.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[3] K. Figueredo. (2012). "Connected living: Realising the market potential," [Online]. Available: http://www.gsma.com/connectedliving/wp-content/uploads/2012/05/1-Ken-Figueredo-Introduction.pdf, accessed on Nov. 23, 2014.

[4] Telecoms. (2013). "MNOs are already making the IoT connection!," [Online]. Available: http://www.telecoms.com/166122/mnos-are-already-making-the-iot-connection/, accessed on Dec. 9, 2014.

[5] D. C. T. National Intelligence Council. "Six technologies with potential impacts on US interests out to 2025," Conf. Rep. CR 2008–07, 2008 [Online]. Available: http://www.dni.gov/nic/NIC_home.html

[6] D. Snoonian, "Smart buildings," *IEEE Spectr.*, vol. 40, no. 8, pp. 18–23, 2003.

[7] Institute for Building Efficiency. "What is a smart building?," 2008 [Online]. Available: http://www.institutebe.com/smart-grid-smart-building/What-is-a-Smart-Building.aspx, accessed on Sep. 2, 2014.

[8] R. Yin, P. Xu, and P. Shen, "Case study: Energy savings from solar window film in two commercial buildings in Shanghai," *Energy Build.*, vol. 45, pp. 132–140, 2012.

[9] Y. He, Y. Liu, X. Shen, L. Mo, and G. Dai, "Noninteractive localization of wireless camera sensors with mobile beacon," *IEEE Trans. Mobile Comput.*, vol. 12, no. 2, pp. 333–345, Feb. 2013.

[10] Z. Yang, L. Jian, C. Wu, and Y. Liu, "Beyond triangle inequality: Sifting noisy and outlier distance measurements for localization," *ACM Trans. Sens. Netw. (TOSN)*, vol. 9, no. 2, p. 26, 2013.

[11] Contiki, "The opensource OS for the Internet of Things," [Online]. Available: http://www.contiki-os.org/, accessed on Sep. 19, 2014.

[12] A. Dunkels, "Rime—A lightweight layered communication stack for sensor networks," in *Proc. Eur. Conf. Wireless Sensor Networks (EWSN)*, Poster/Demo session, Delft, The Netherlands, 2007.

[13] K. Ashton, "That 'Internet of Things' thing," *RFiD J.*, vol. 22, pp. 97–114, 2009.

[14] D. Giusto, A. Lera, G. Morabito, and L. Atzori, *The Internet of Things*. New York, NY, USA: Springer, 2010.

[15] O. Vermesan and P. Friess, *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*. River Publishers, 2013 [Online]. Available: http://www.riverpublishers.com/

[16] S. C. Ergen, *Zigbee/IEEE 802.15. 4 Summary*. Berkeley, CA, USA: UC Berkeley, 2004, vol. 10, p. 17.

[17] J. A. Gutierrez, M. Naeve, E. Callaway, M. Bourgeois, V. Mitter, and B. Heile, "IEEE 802.15. 4: A developing standard for low-power low-cost wireless personal area networks," *IEEE Netw.*, vol. 15, no. 5, pp. 12–19, Sept./Oct. 2001.

[18] Intel, "Wireless LAN standards study," [Online]. Available: http://www.intel.com/content/dam/www/public/us/en/documents/case-studies/802-11-wireless-lan-standards-study.pdf, accessed on Sep. 3, 2014.

[19] I. Papapanagiotou, G. S. Paschos, S. A. Kotsopoulos, and M. Devetsikiotis, "Extension and comparison of QoS-enabled Wi-Fi models in the presence of errors," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM'07)*, Nov. 2007, pp. 2530–2535.

[20] I. Papapanagiotou, D. Toumpakaris, J. Lee, and M. Devetsikiotis, "A survey on next generation mobile WiMAX networks: Objectives, features and technical challenges," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 4, pp. 3–18, fourth quarter 2009.

[21] S. Sesia, I. Toufik, and M. Baker, *LTE: The UMTS Long Term Evolution*. Hoboken, NJ, USA: Wiley, 2009.

[22] A. Ghosh, R. Ratasuk, B. Mondal, N. Mangalvedhe, and T. Thomas, "LTE-Advanced: Next-generation wireless broadband technology [invited paper]," *IEEE Wireless Commun.*, vol. 17, no. 3, pp. 10–22, Jun. 2010.

[23] M. Shaik, "Ultra wide-band vs. Wi-Fi—A study and comparison of the two technologies," [Online]. Available: https://www.academia.edu/4810093/Ultra_Wide-Band_vs._Wi-Fi_A_Study_and_Comparison_of_the_two_technologies, accessed on Dec. 12, 2014.

[24] S. Nadler, V. Soroka, O. Fuchs, R. Korenshtein, and E. Sonsino, "Presence zones for contextual location based services," [Online]. Available: http://www.icin.co.uk/files/2008papers/Session4B-2.pdf

[25] V. Pillai, H. Heinrich, D. Dieska, P. V. Nikitin, R. Martinez, and K. S. Rao, "An ultra-low-power long range battery/passive RFID tag for UHF and microwave bands with a current consumption of 700 nA at 1.5 V," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 54, no. 7, pp. 1500–1512, Jul. 2007.

[26] W. Alliance, "How far does a Wi-Fi direct connection travel?," [Online]. Available: http://www.wi-fi.org/knowledge-center/faq/how-far-does-a-wi-fi-direct-connection-travel, accessed on Apr. 22, 2014.

[27] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, 2010.

[28] Estimote, "Estimote real world context for your apps," [Online]. Available: http://www.estimote.com, accessed on Sep. 26, 2014.

[29] F. Faheem, S. Mahmud, G. Khan, M. Rahman, and H. Zafar, "A survey of intelligent car parking system," *J. Appl. Res. Technol.*, vol. 11, no. 5, pp. 714–726, 2013.

[30] R. J. Weiland and L. B. Purser, "Intelligent transportation systems," *Transp. New Millennium*, pp. 1–3, 2000.

[31] I. Bayram and I. Papapanagiotou, "A survey on communication technologies and requirements for internet of electric vehicles," *EURASIP J. Wireless Commun. Netw.*, vol. 2014, no. 1, p. 223, 2014.

[32] I. S. Bayram, G. Michailidis, I. Papapanagiotou, and M. Devetsikiotis, "Decentralized control of electric vehicles in a network of fast charging stations," in *Proc. Global Commun. Conf. Symp. Sel. Areas Commun. (GLOBECOMSAC'13)*, 2013, pp. 2785–2790.

[33] P. I. Project. (2014). "The Internet of Things will thrive by 2025," [Online]. Available: http://www.pewinternet.org/2014/05/14/internet-of-things/, accessed on Nov. 23, 2014.

[34] I. Papapanagiotou, E. M. Nahum, and V. Pappas, "Configuring DHCP leases in the smartphone era," in *Proc. Int. Meas. Conf. (IMC'12)*, Nov. 2012, pp. 365–370.

[35] I. Papapanagiotou, E. M. Nahum, and V. Pappas, "Smartphones vs. laptops: Comparing web browsing behavior and the implications for caching," in *Proc. 12th ACM SIGMETRICS/PERFORMANCE Joint Int. Conf. Meas. Model. Comput. Syst.*, 2012, pp. 423–424 [Online]. Available: http://doi.acm.org/10.1145/2254756.2254824

[36] CISCO, "IPv6," [Online]. Available: http://www.cisco.com/web/solutions/trends/ipv6/index.html, accessed on Sep. 6, 2014.

[37] L. Yan, Y. Zhang, L. T. Yang, and H. Ning, *The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems*. Boca Raton, FL, USA: CRC Press, 2008.

[38] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Netw.*, vol. 10, no. 7, pp. 1497–1516, 2012.

[39] R. Brennan, W. Tai, D. O'sullivan, M. S. Aslam, S. Rea, and D. Pesch, "Open framework middleware for intelligent WSN topology adaption in smart buildings," in *Proc. IEEE Int. Conf. Ultra Mod. Telecommun. Workshops (ICUMT'09)*, 2009, pp. 1–7.

[40] L. R. Suzuki, K. Brown, S. Pipes, and J. Ibbotson, "Smart building management through augmented reality," in *Proc. IEEE Int. Conf. Perv. Comput. Commun. Workshops (PERCOM Workshops'14)*, 2014, pp. 105–110.

[41] A. LaMarca *et al.*, "Place Lab: Device positioning using radio beacons in the wild," in *Pervasive Computing*. New York, NY, USA: Springer, 2005, pp. 116–133.

[42] D. Namiot and M. Sneps-Sneppe, "Geofence and network proximity," in *Internet of Things, Smart Spaces, and Next Generation Networking*. New York, NY, USA: Springer, 2013, pp. 117–127.

[43] Google, "Search trend," [Online]. Available: https://www.google.com/trends/explore#q=Internet%20of%20Things%2C%20%2Fm%2F09g9zkw%2C%20Smart%20Grid%2C%20Sensor%20Networks&cmpt=q, accessed on Oct. 4, 2014.

[44] Gimbal, "Context aware platform," [Online]. Available: http://www.gimbal.com/, accessed on Sep. 15, 2014.

[45] Apple, "iBeacons for developers," [Online]. Available: https://developer.apple.com/ibeacon/, accessed on Sep. 15, 2014.

[46] G. C. Platform, "Internet of Things," [Online]. Available: https://cloud.google.com/solutions/iot/, accessed on May 19, 2015.

[47] CISCO, "Internet of Things (IoT)," [Online]. Available: http://www.cisco.com/web/solutions/trends/iot/overview.html, accessed on Dec. 30, 2014.

[48] IBM. *System of interaction* [Online]. Available: http://www-01.ibm.com/software/solutions/systems-of-interaction/, accessed on Sep. 19, 2014.

[49] U. Bareth, A. Kupper, and P. Ruppel, "Geoxmart—A marketplace for geofence-based mobile services," in *Proc. IEEE 34th Annu. Comput. Softw. Appl. Conf. (COMPSAC'10)*, 2010, pp. 101–106.

[50] F. Reclus and K. Drouard, "Geofencing for fleet & freight management," in *Proc. IEEE 9th Int. Conf. Intell. Transp. Syst. Telecommun.(ITST'09)*, 2009, pp. 353–356.

[51] M. Siekkinen, M. Hiienkari, J. K. Nurminen, and J. Nieminen, "How low energy is bluetooth low energy? Comparative measurements with ZigBee/802.15. 4," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW'12)*, 2012, pp. 232–237.

[52] PassKit, "How does iBeacon work?," [Online]. Available: https://passkit.com/how-ibeacon-works/, accessed on Nov. 11, 2014.

[53] Apple. (2014). "Getting started with iBeacon," [Online]. Available: https://developer.apple.com/ibeacon/Getting-Started-with-iBeacon.pdf, accessed on Nov. 11, 2014.

[54] M. B. Journal. (2014). "Ole Miss offering new beacon technology for sports fans," [Online]. Available: http://msbusiness.com/blog/2014/07/08/ole-miss-offering-new-system-sports-fans/, accessed on Sep. 15, 2014.

[55] D. Consulting, "The dawn of mobile influence," [Online]. Available: http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/RetailDistribution/us_retail_Mobile-Influence-Factor_062712.pdf, accessed on Sep. 15, 2014.

[56] J.-S. Lee, Y.-W. Su, and C.-C. Shen, "A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi," in *Proc. IEEE 33rd Annu. Conf. Ind. Electron. Soc. (IECON'07)*, 2007, pp. 46–51.

[57] Decawave, "Real time location: An introduction," [Online]. Available: http://www.decawave.com/sites/default/files/resources/aps003_dw1000_rtls_introduction.pdf, accessed on Dec. 1, 2014.

[58] IndoorAtlas, "Ambient magnetic field-based indoor location technology bringing the compass to the next level," White Paper, Jul. 2012.

[59] Y. Wang, "Performance analysis of smart space with indoor localization capabilities," M.S. thesis, Dept. Electr. Comput. Eng. North Carolina State Univ., Raleigh, NC, USA, 2014 .

[60] S. Gezici *et al.*, "Localization via ultra-wideband radios: A look at positioning aspects for future sensor networks," *IEEE Signal Process. Mag.*, vol. 22, no. 4, pp. 70–84, Jul. 2005.

[61] C.-C. Chong, I. Guvenc, F. Watanabe, and H. Inamura, "Ranging and localization by UWB radio for indoor LBS," *NTT DOCOMO Tech. J.* (English version), vol. 11, no. 1, pp. 41–48, 2009.

[62] T. Manodham, L. Loyola, and T. Miki, "A novel wireless positioning system for seamless internet connectivity based on the WLAN infrastructure," *Wireless Pers. Commun.*, vol. 44, no. 3, pp. 295–309, 2008.

[63] C. Wu, Z. Yang, Y. Liu, and W. Xi, "WILL: Wireless indoor localization without site survey," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 4, pp. 839–848, Apr. 2013.

[64] Y. Desmedt, "Man-in-the-middle attack," in *Encyclopedia of Cryptography and Security*. New York, NY, USA: Springer, 2011, pp. 759–759.

[65] OnxyBeacon, "OnxyBeacon helps you develop context aware mobile apps," [Online]. Available: http://www.onyxbeacon.com/, accessed on Sep. 15, 2014.

[66] Swirl, "Secure cast beacons," [Online]. Available: http://www.swirl.com/platform.html, accessed on Sep. 15, 2014.

[67] S. Notify, "Join the companies that have been leveraging our enterprise proximity solution for the past two years," [Online]. Available: https://sonicnotify.com/l, accessed on Sep. 15, 2014.

[68] IndoorAtlas, "Game changing indoor location," [Online]. Available: https://www.indooratlas.com/, accessed on Sep. 15, 2014.

[69] L. M. Ni, Y. Liu, Y. C. Lau, and A. P. Patil, "LANDMARC: Indoor location sensing using active RFID," *Wireless Netw.*, vol. 10, no. 6, pp. 701–710, 2004.

[70] B. Rekha, "Location is personal," *Geospatial World*, vol. 6, pp. 31–38, 2011.

[71] Google, "Google wireless positioning system," [Online]. Available: www.google.com, accessed on Sep. 14, 2014.

[72] AlterGeo, "AlterGeo positioning solutions," [Online]. Available: http://platform.altergeo.ru/index.php?mode=products, accessed on Sep. 14, 2014.

[73] Skyhook [Online]. Available: http://www.skyhookwireless.com/apps-enterprise/, accessed on Sep. 14, 2014.

[74] Navizon, "Navizon indoors for navigation," [Online]. Available: http://www.navizon.com/product-navizon-indoors-navigation, accessed on Sep. 14, 2014.

[75] Infsoft, "Infsoft wireless positioning solutions," [Online]. Available: http://www.infsoft.com/, accessed on Sep. 14, 2014.

[76] Combain, "Combain positioning solutions," [Online]. Available: http://www.combain.com/, accessed on Sep. 14, 2014.

[77] H. Liu, H. Darabi, P. Banerjee, and J. Liu, "Survey of wireless indoor positioning techniques and systems," *IEEE Trans. Syst. Man Cybern. C, Appl. Rev.*, vol. 37, no. 6, pp. 1067–1080, Nov. 2007.

[78] B. T. Fang, "Simple solutions for hyperbolic and related position fixes," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 26, no. 5, pp. 748–753, Sep. 1990.

[79] M. Kanaan and K. Pahlavan, "A comparison of wireless geolocation algorithms in the indoor environment," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2004, vol. 1, pp. 177–182.

[80] A. Teuber, B. Eissfeller, and T. Pany, "A two-stage fuzzy logic approach for wireless LAN indoor positioning," in *Proc. IEEE/ION Position Location Navigat. Symp.*, 2006, vol. 4, pp. 730–738.
[81] A. Günther and C. Hoene, "Measuring round trip times to determine the distance between WLAN nodes," in *NETWORKING 2005. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems*. New York, NY, USA: Springer, 2005, pp. 768–779.
[82] IBM. (2013). "Delivering system of interaction," [online]. available: http://www.slideshare.net/ibmsverige/systems-of-interaction, accessed on Sep. 19, 2014.
[83] D. Martin, A. Alzua, and C. Lamsfus, "A contextual geofencing mobile tourism service," in *Proc. ENTER*, 2011, pp. 191–202.
[84] F. Beckley and M. Ward, "Device and network enabled geo-fencing for area sensitive gaming enablement," U.S. Patent App. 11 323 265, Dec. 30, 2005.
[85] L. S. Humphries and H.-J. Ngo, "Method and system for tracked device location and route adherence via geofencing," U.S. Patent 7 164 986, Jan. 16, 2007.
[86] T. Verge. (2014). "San Francisco Airport testing Beacon system for blind travelers," [Online]. Available: http://www.theverge.com/2014/7/31/5956265/san-francisco-airport-testing-beacon-system-for-blind-travelers, accessed on Sep. 29, 2014.
[87] B. Morvaj, L. Lugaric, and S. Krajcar, "Demonstrating smart buildings and smart grid features in a smart energy city," in *Proc. IEEE 3rd Int. Youth Conf. Energ. (IYCE)*, 2011, pp. 1–8.
[88] S.-J. Jeon, S.-Y. Ko, J.-H. Park, and M.-K. Youn, "Remotely controlling appliances using a wireless terminal," U.S. Patent App. 10/856,862, 2004.
[89] H. Y. Amro, J. P. Dodson, G. Kraft IV, and K. R. Taylor, "Method and system for remotely controlling an appliance using a personal digital assistant," U.S. Patent 6 507 762, Jan. 14, 2003.
[90] S. Haller, S. Karnouskos, and C. Schroth, *The Internet of Things in an Enterprise Context*. New York, NY, USA: Springer, 2009.
[91] E. Asimakopoulou and N. Bessis, "Buildings and crowds: Forming smart cities for more effective disaster management," in *Proc. IEEE 5th Int. Conf. Innov. Mobile Internet Serv. Ubiq. Comput. (IMIS'11)*, 2011, pp. 229–234.
[92] A. Zelenkauskaite, N. Bessis, S. Sotiriadis, and E. Asimakopoulou, "Interconnectedness of complex systems of Internet of Things through social network analysis for disaster management," in *Proc. IEEE 4th Int. Conf. Intell. Netw. Collab. Syst. (INCoS)*, 2012, pp. 503–508.
[93] H. Borrion, T. Mitchener-Nissen, J. Taylor, and K.-M. Lai, "Countering bioterrorism: Why smart buildings should have a code of ethics," in *Proc. IEEE Eur. Intell. Secur. Informat. Conf. (EISIC'12)*, 2012, pp. 68–75.
[94] G. V. Lioudakis *et al.*, "A proxy for privacy: The discreet box," in *Proc. IEEE Int. Conf. Comput. Tool (EUROCON'07)*, 2007, pp. 966–973.
[95] R. H. Weber, "Internet of Things—New security and privacy challenges," *Comput. Law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, 2010.
[96] J. Freudiger *et al.*, "Mix-zones for location privacy in vehicular networks," in *Proc. 1st Int. Workshop Wireless Netw. Intell. Transp. Syst. (Win-ITS)*, 2007 [Online]. Available: http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A429057&dswid=3758
[97] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for secure and private vehicular communications," in *Proc. IEEE 7th Int. Conf. ITS Telecommun. (ITST'07)*, 2007, pp. 1–6.
[98] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, 2007.
[99] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. 9th ACM Conf. Comput. Commun. Secur.*, 2002, pp. 41–47.
[100] R. Acharya and K. Asha, "Data integrity and intrusion detection in wireless sensor networks," in *Proc. IEEE 16th Int. Conf. Netw. (ICON'08)*, 2008, pp. 1–5.
[101] C. M. Medaglia and A. Serbanati, "An overview of privacy and security issues in the Internet of Things," in *The Internet of Things*. New York, NY, USA: Springer, 2010, pp. 389–395.
[102] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X. 509 internet public key infrastructure online certificate status protocol-ocsp," Internet Eng. Task Force, Tech. Rep. RFC 2560, 1999.

Faheem Zafari (GSM'14) received the B.S. degree in electrical engineering from the University of Engineering and Technology, Peshawar, Pakistan, in 2013, and is currently working toward the M.S. degree in computer and information technology at Purdue University, West Lafayette, IN, USA.

He also attended University of Idaho, Moscow, ID, USA, as an Exchange Student, funded by the U.S. Department of the State, in Fall 2011. His research interests include Internet of Things, positioning technologies, and scheduling in wireless communication systems.

Ioannis Papapanagiotou (S'04–GSM'06–M'12) received the Dipl.Ing. degree in electrical and computer engineering from the University of Patras, Patras, Greece, in 2006, and the M.Sc. degree and dual Ph.D. degrees in computer engineering and operations research from North Carolina State University, Raleigh, NC, USA, in 2009 and 2012, respectively.

He is currently an Assistant Professor with the Department of Computer and Information Technology, Purdue University, West Lafayette, IN, USA, and an Adjunct Assistant Professor with the Department of Electrical and Computer Engineering, North Carolina State University. He is also a Faculty Member with the Center for Education and Research in Information Assurance and Security (CERIAS) and Purdue Energy Center, Purdue University. He is also the Co-PI of the NVIDIA CUDA Research Center, Purdue University. Previously, he was a Software Engineer involved in the areas of mobile and cloud computing with IBM's Emerging Technology Institute, an in-house incubator team directly reporting to the CTO. His research interests include the domains of cloud computing (specifically on cloud storage and microservices), Internet of Things (focusing on proximity/geofencing and security), and network systems.

Dr. Papapanagiotou was the recipient of the Best Paper Award of the IEEE GLOBECOM 2007 and the IEEE CAMAD 2010. As a Graduate Student, he was the recipient of the IBM Ph.D. Fellowship and the Academy of Athens Ph.D. Fellowship, and as a Faculty Member, the NetApp Faculty Fellowship. He was also the recipient of an IBM Ph.D. Fellowship.

Konstantinos Christidis (GSM'11) received the Dipl.Ing. degree in electrical and computer engineering from the Aristotle University of Thessaloniki, Thessaloniki, Greece, in 2011, the M.Sc. degree in computer engineering from North Carolina State University, Raleigh, NC, USA, in 2013, and is currently working toward Ph.D. degree at North Carolina State University.

He is currently a Software Developer with the IBM Emerging Technology Institute, North Carolina State University. His research interests include energy storage systems for smart grid (particularly resource allocation and scheduling policies), as well as Internet of Things applications for smart buildings.