J Inf Process Syst, Vol.14, No.2, pp.286~308, April 2018
https://doi.org/10.3745/JIPS.03.0094

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Security and Privacy in Ubiquitous Sensor Networks

Alfredo J. Perez*, Sherali Zeadally**, and Nafaa Jabeur***

Abstract

The availability of powerful and sensor-enabled mobile and Internet-connected devices have enabled the advent of the ubiquitous sensor network (USN) paradigm. USN provides various types of solutions to the general public in multiple sectors, including environmental monitoring, entertainment, transportation, security, and healthcare. Here, we explore and compare the features of wireless sensor networks and USN. Based on our extensive study, we classify the security- and privacy-related challenges of USNs. We identify and discuss solutions available to address these challenges. Finally, we briefly discuss open challenges for designing more secure and privacy-preserving approaches in next-generation USNs.

Keywords

Human-Centric Sensing, Internet of Things, Opportunistic Sensing, Participatory Sensing, Privacy, Security, Ubiquitous Sensing

1. Introduction

Ubiquitous sensor networks (USNs) have become an important paradigm in sensor network systems. The International Telecommunication Union (ITU) defines a USN as a conceptual network built over existing physical networks that makes use of sensed data and provides knowledge services to anyone—anywhere and at any time—and generating that information via context awareness [1]. The increasing availability and pervasiveness of mobile devices and Internet of Things (IoT)-enabled devices (expected to reach 30 billion by 2020 [2]) are opening revolutionary opportunities toward next-generation services, systems, and applications in various areas, including environmental monitoring, transportation, entertainment, security, and healthcare.

The wide adoption of USN presents significant security and privacy challenges and risks. The limited data acquisition, storage, processing, and communication capabilities of the related sensing infrastructures, as well as their proprietary technologies, are making USN devices vulnerable to a wide range of attacks. Although intensive efforts have been undertaken to improve USNs' security and privacy (e.g., [3–11]), additional efforts are necessary to maintain data integrity and system availability. USN devices still cannot guarantee users' data privacy. Concerns related to re-identification and context privacy still challenge USNs' effective implementation. Thus, in this paper, we present an overview of these issues

Manuscript received November 26, 2017; first revision December 18, 2017; accepted December 29, 2017.
Corresponding Author: Alfredo J. Perez (perez_alfredo@columbusstate.edu)
* TSYS School of Computer Science, Columbus State University, Columbus, GA, USA (perez_alfredo@columbusstate.edu)
** College of Communication and Information, University of Kentucky, Lexington, KY, USA (szeadally@uky.edu)
*** Dept. of Computer Science, German University of Technology in Oman (GUtech), Muscat, Oman (nafaa.jabeur@ gutech.edu.om)

along with potential solutions.

The rest of this paper is organized as follows. Section 2 presents architectural aspects of USNs, and compares USN with wireless sensor networks (WSNs) while highlighting USN applications. In Section 3, we discuss security and privacy issues for USNs. Section 4 presents solutions that secure and protect privacy in USNs. Section 5 considers open challenges. Section 6 offers concluding remarks.

2. Architecture and Applications of Ubiquitous Sensor Networks

USNs make use of Internet-connected devices to collect data of interest [12]. These devices are either owned by the government, private-sector companies, or common citizens. USNs differ from WSNs in multiple ways; Table 1 highlights some of the main differences. These differences are based on the architecture of both types of sensor networks, the communication and capabilities of the devices involved in data collection, and how the sensor networks are deployed. This includes the device's power and energy management (USN devices are either connected to a reliable power source or easily recharged), communication capability between devices in USNs (depending on the infrastructure-based networks available to access the Internet), and user involvement (typically, USNs rely on user contributions to collect the data of interest). The typical hardware architecture of USNs (shown in Fig. 1) consists of the following tiers [12]: sensors, first-level integrators, data transport, and second-level integrators.

- *Sensors.* The major function of sensors is to collect data on objects and events of interest. To this end, they act individually or within clusters to acquire the right data, at the right time, from the right area, while optimizing the use of the available resources. Sensors connect to first-level integrator devices using wired or wireless connections via personal area networks such as Bluetooth, near-field communication (NFC), IEEE 802.15.4 (Zigbee), or some other wireless local area network (LAN) technology.
- *First-level integrators.* The first-level integrators tier performs initial sensor data verification, aggregation, and analysis (e.g., feature extraction). Any device (e.g., smartphones and Internet-connected devices) that supports IP-based communication can serve as a first-level integrator.
- *Data transport.* In USNs, data transport is provided by any IP-based communication network (e.g., Internet service providers [ISPs]) that enables the end-to-end transfer of data from first-level integrators to second-level integrators. Data transport mechanisms should adapt to the USN's changing spatial distribution. They should also optimize the use of available resources.
- *Second-level integrators.* The second-level integrators tier collects and stores data sent by any component from the first-level integrators tier. It also provides analytics services (e.g., data analysis and machine learning that cannot be performed at first-level integrators) and feedback to the first-level integrator devices as well as to external entities who did not participate in collecting data. Second-level integrators are implemented on servers and/or as cloud-based services.

USNs are currently deployed in various application domains such as environmental monitoring, entertainment, transportation, security, and healthcare. These applications can be grouped into four major categories [12]:

- *Location-based systems (LBS).* Available since the late 1990s, LBS make use of location sensors to receive/collect geotagged data [13,14]. Applications of LBS include asset management, tracking systems, and geofencing.

Table 1. Comparison of features for wireless sensor networks (WSNs) and ubiquitous sensor networks (USNs)

Features	WSNs	USNs
Computational capabilities	Devices, which are battery-powered, are designed for low power consumption. They are limited in computational power, memory, and communication. They often operate unattended for a long period of time. They could be commercial off-the-shelf (COTS) products or custom-made.	Devices equipped with several gigahertz multicore processors as well as several gigabytes of memory are typically used. Devices have rechargeable batteries or they are connected to a reliable power source. The USN may make use of COTS devices, sensors, and operating systems.
Communication infrastructure	Devices must collaborate to perform ad hoc network routing and maintenance. A single network interface with low-power protocols (e.g., IEEE 802.15.4) is used.	Devices may have multiple network interfaces, with infrastructure-based networks (e.g., Internet service providers [ISPs] or cellular networks) to support end-to-end TCP/IP communication between integrator devices.
Communication security	Cross-layer design for security is needed because of low power and limited computational capabilities.	USNs use standard protocols such as Transport Layer Security (TLS) and common cryptographic algorithms/protocols (e.g., Advanced Encryption Standard [AES], RC4, and elliptic curve) to provide end-to-end security. USNs assume reliable communication by ISPs.
Network management	Devices are designed and deployed for a single purpose. Devices participate in one WSN at a time, and network management is performed by one organization (e.g., a government agency).	Multiple organizations participate in managing the USN. For instance, one organization (e.g., a company or government agency) collects the data. Also, each entity could have multiple roles. For instance, data collection tasks may be issued by more than one organization. In addition, devices can be used to support various network management functions (e.g., sensor data collection, data analysis, and aggregation). Devices may participate in more than one USN simultaneously.
Network maintenance	This is performed by the entity owning the WSN. The network can be costly to deploy and maintain.	Maintenance is performed by the custodians of data collection devices and organizations collecting the data. USNs' maintenance can be cheap or affordable. However, the process to collect data may depend on users' participation to achieve the USN's goals.
Scalability	There are potentially thousands of devices in a single system.	Potentially billions of devices can be in a single system.

- *Community-based sensing systems (CBS).* CBS (also known as crowdsensing) track variables of interest for communities (e.g., neighborhoods, cities, citizen associations, leisure/gaming associations, and government). Such variables may include pollution, noise, and street congestions [15–18]. CBS can be classified as participatory or opportunistic [19].
- *Human-centric sensing systems (HCS).* HCS track human-related variables such as physiological variables with the goal of improving individuals' wellbeing. Some examples of HCS include security and safety systems (e.g., home security, human-fall detection), mobile health (m-Health), and personal health systems (e.g., fitness tracking) [20,21].
- *Hybrid systems.* Hybrid systems incorporate characteristics from LBS, CBS, and HCS. Common examples of hybrid systems include augmented reality games (e.g., Pokemon GO [22]) and scavenger hunt applications.

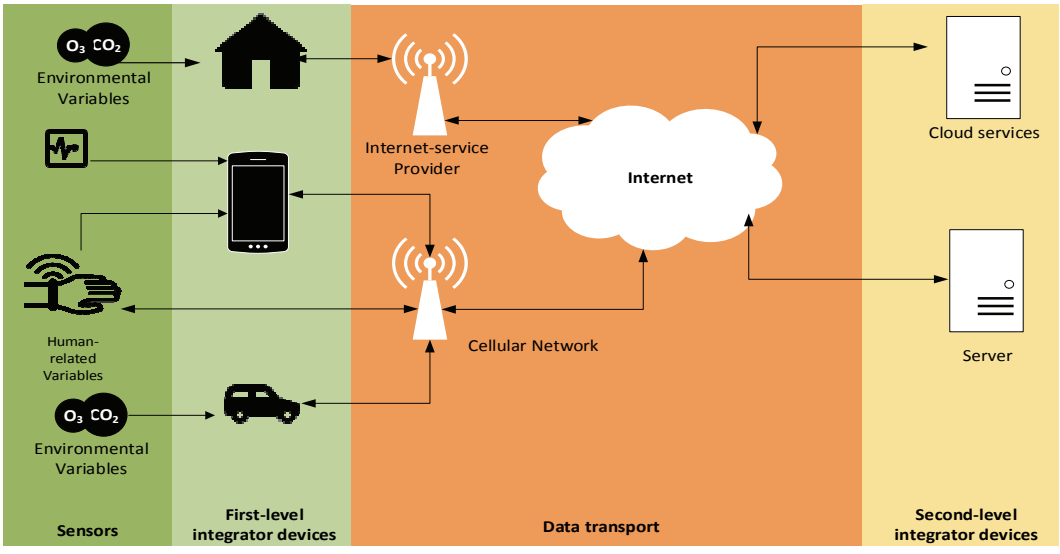

Fig. 1. Typical hardware architecture of ubiquitous sensor networks.

3. Security and Privacy Issues in Ubiquitous Sensor Networks

3.1 Security Issues

WSNs often operate unattended for long periods of time in extreme conditions, so frequently the devices are powered by batteries instead of a reliable power source. These constraints make the design of WSN devices limited in their communication and processing capabilities. To save battery power, WSN devices use energy-efficient routing protocols that were initially designed for infrastructureless, ad hoc network protocols to route data from sensors to base stations. In a WSN only the devices that are within the wireless communication range of the base station can broadcast data without having to route it through other devices.

Establishing secure communication channels in WSNs is a major priority, to protect the data's integrity as it is routed through the network, while also minimizing the power used. Therefore, much

WSN security-related research (from the communication perspective) focuses on developing power-aware cryptographic methods and key distribution protocols over wireless ad hoc routing protocols [23–25]. However, key distribution and power-efficient cryptography are not an issue for USNs, because first-level integrator devices are connected to the Internet and long-term power consumption is not a concern (devices easily can be recharged or connected to a reliable power source).

USN integrator devices make use of infrastructure-based networks and well-known security protocols for the TCP/IP network stack such as Transport Layer Security (TLS), Secure Sockets Layer (SSL), and Virtual Private Networks (VPNs) to communicate data between integrator devices. Consequently, given the features of USNs presented in Table 1, and assuming secure communication channels to avoid man-in-the middle attacks between integrator devices by using the aforementioned protocols, the security issues in USNs are related to the integrity of data collected from non-trusted user devices, and mechanisms to avoid availability attacks (e.g., denial-of-service attacks at integrator devices). Thus, in the following, we classify the security issues for USNs into two major categories [26]: data integrity and system availability.

3.1.1 Data integrity

In contrast to traditional WSNs, in which devices are trusted because they are deployed and maintained by a single organization, the maintenance of first-level integrator devices that collect data is performed by USN's users; this brings unique challenges. The direct access to these components by users could be utilized to launch spoofing attacks by submitting false, incorrect, or fake data [27,28]. Another type of spoofing attack could be performed by tampering and modifying the physical environment (i.e., for a temperature sensor, this type of attack intentionally increases the room temperature). In this case, although the sensor's readings are correct, the sensed data are generated from fake or tampered environments [29].

In USNs it is difficult for systems to identify who is injecting false data and block these users, because many USNs make use of anonymization techniques to protect the privacy of users contributing sensor data (especially for CBS). This aspect brings a tradeoff between authentication and privacy that has an impact on data integrity: how to authenticate users while at the same time protecting their privacy? In addition, for HCS systems, including m-Health and fitness tracking systems, data integrity is critical. M-Health applications collect health-related data and provide feedback that could include intrusive actions on a patient's body automatically (e.g., delivering medication). In such cases, the violation of data integrity can have serious, life-threatening consequences [26,30]. Thus, data, user, and sensor authentication are major security concerns for human-centric USNs [3,4].

3.1.2 System availability

Because data transport between integrator devices in USNs is provided by TCP/IP communication over the Internet, USNs make use of reliable networks (provided by ISPs) and secure communication protocols such as TLS, SSL and VPNs to send data securely between integrators. Therefore, we argue that there are three ways attackers can launch attacks on system availability in USNs:

- *Availability at the first-level integrators tier*. In this type of attack, the adversary's goal is to deny data collection at first-level integrators by interfering with the hardware, software, or

communication infrastructure between sensors and first-level integrators. If the adversary is successful in these types of attacks, the USN will not collect data. We identify these attacks as follows: (1) attacking the communication infrastructure between sensors and the first-level integrator devices by interfering with the communication media [5–7]; (2) attacking and/or depleting the power supply with battery exhaustion attacks [8,9]; or (3) making the operating system unresponsive by exploiting security vulnerabilities of the host operating system [10,11,31].

- *Availability at the second-level integrators tier.* In this type of attack, the adversary's goal is to deny data collection at second-level integrators by interfering with the services that collect and analyze the data forwarded by first-level integrators. If successful, the adversary will disable the USN's ability to collect and analyze the data. Two major issues arise when managing availability for second-level integrator devices: elasticity and denial of service (DoS). Even though the result of not managing both issues correctly is the same (no availability), they differ in terms of lack of availability. On one hand, elasticity deals with the ability of the system or service to satisfy and adapt to workload changes [32]. On the other hand, DoS represents deliberate attacks to the system or service by malicious parties [33].
- *User participation.* USNs require participation and collaboration from users and custodians to collect data and enable the system to provide a certain level of quality of information (QoI) [27,34] to be useful. This is because unless users contribute to data collection with their devices, the USN will not accomplish the goals for which it was designed. With no data collected (due to users' unwillingness to contribute or participate), the result is similar to an availability attack on the USN, because the system does not have the data available to process and provide feedback. Attacks on user participation may include availability attacks at first-level integrators and users' resulting hesitancy to contribute and collect data (e.g., lack of motivation to participate, low opinions of the USN system, and concerns about privacy and participation).

3.2 Privacy Issues

USNs may expose users to significant privacy risks, because they make use of devices that can potentially register and forward data and metadata continually about users' actions through the data collection cycle shown in Fig. 2 [35–37]. This collection cycle is composed of the following processes:

- *Task distribution.* The goal of task distribution is to release the sensing task to user participants. This is accomplished in two ways: participants either makes use of the sensing task from a server (second-level integrators), or the task is pushed to the users' devices (first-level integrators) from second-level integrators.
- *Data collection.* Once tasks are configured at the participants' devices, the tasks perform sensing and initial analysis that may include extracting features from sensor data, smoothing and filtering of outliers in the data, and data analytics that can be performed locally without the need of second-level integrators.
- *Data submission.* Tasks that execute at first-level integrators forward the collected data to second-level integrator devices. Depending on the USN's goals, data submission can be performed continuously or based on events (identified in the data collection process), and data can be submitted in real time or later (e.g., at the end of the day).

- *Data analysis and sharing.* In this process, second-level integrator devices use the collected data from first-level integrators to perform analytics services (e.g., data analysis and machine learning) and provide feedback to first-level integrator devices. The feedback may include the release of new sensing tasks to user participants, resulting in a new data collection cycle. In addition, data may be released to external parties outside the USN system through this process.

Attacks on user privacy can be performed at any stage during the data collection cycle and they may lead to different privacy risks based on the goals of the USN. Next, we classify these risks into three major categories: re-identification; context privacy; and external data sharing. These categories enable us to study privacy issues that arise when a participant contributes data to the system.

3.2.1 Reidentification

The first concern when collecting data in a USN (from users' point of view) is how their identities can be discovered or protected. Thus, given the data (or metadata) submitted by users in the USN, reidentification attacks attempt to discover any user's identity who uses or participates in the system. These attacks are successful when an entity (internal or external to the system) discovers, without permission or consent, the user's identity. Reidentification issues can be grouped into two categories:

- *Reidentification from network identifiers.* The attackers infer the user's identity by associating the network addresses (e.g., IP addresses, MAC addresses, cookies) needed to send and receive data between integrator devices on the Internet [36–39].
- *Reidentification from task management*. The attackers infer the user's identity from any of the processes required to manage the data collection cycle for a sensing task (Fig. 2). This issue is particularly important in CBS and HCS systems, where downloading an application or authenticating users in a system could reveal their identities [36,37].

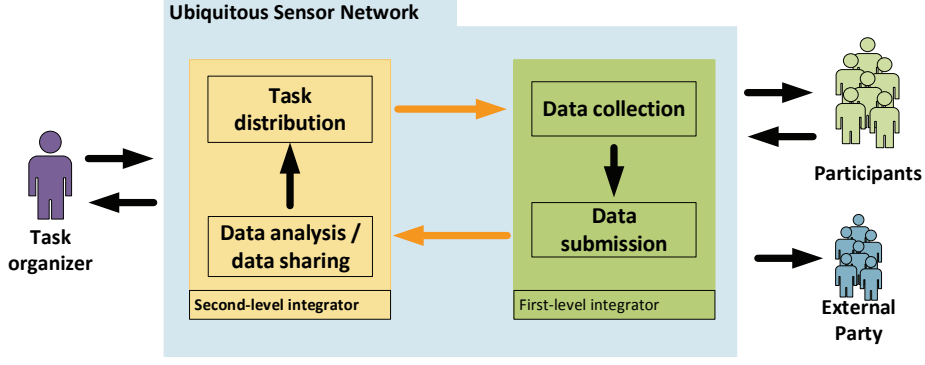

Fig. 2. Data collection processes for USNs.

3.2.2 Context privacy

Given the data (or metadata) submitted to the system by participants, attacks on context privacy attempt to discover and associate aspects considered private by users/participants with their identities. Some examples in this category include inferring users' locations, activities, behaviors, and/or health state based on the collected data [36,37]. We classify attacks on context privacy into two groups:

- *Location privacy*. Location data by itself can reveal a lot of contextual information about a user (e.g., user's interests, social/business activities, and profile). Location privacy issues can be categorized further into two groups: privacy in location-based queries (including location data submission) [40–49], and path privacy [50–55]. In location-based queries, the goal is to avoid the release of location data that may be used to infer users' sensitive contexts. For example, collecting location data at a particular type of hospital may reveal that the user has some type of terminal illness, and the user may not want to reveal that he/she is suffering from that illness. In path privacy, the goal is to protect user participants explicitly from releasing a set of locations (a path) that may compromise the user's privacy or disclose what the user is doing.
- *Sensor data and metadata privacy*. Sensor data and metadata privacy corresponds to the issues that arise when an attacker infers information about the user's context or actions (e.g., if a user is sick) from the sensor data or metadata submitted to the system (e.g., the hardware or software used, or the time when a particular application was used). An example of how metadata can be used to infer context is when an attacker knows the amount of time that a user spends on a device, and from that the attacker discerns the type of activity that the user is performing, even without collecting sensor data.

3.2.3 External data sharing

In USNs, data are usually forwarded to a service in the cloud that aggregates, analyzes, and provides feedback to users. The collected data may include several objects and/or events of interest, such as environmental data (in case of LBS or CBS) or health-related data. Sharing this data with external entities outside the USN occurs either by creating infographics on which the data is summarized and visualized (i.e., through maps and visualizations) or by sharing the raw data with organizations external to the USN system [36]. This sharing represents one of the biggest threats to privacy, especially when data are not protected or curated before their release. In this case, an attacker could infer information about contributors and perform malicious actions accordingly [56].

External data sharing in USNs depends on the type of USN. For example, in the US, unless the USN is part of a comprehensive (medical) healthcare system (i.e., m-Health), the organization that develops and deploys the USN system does not have to follow the guidelines in the law when sharing data externally. Some of these guidelines providing a legal framework in the US to share data to external organizations are specified in the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) [57]. Similar laws exist in other countries [57,58]. As such, the protection of users' data depends on the stipulation of privacy policies.

4. Solutions to Security and Privacy Issues for Ubiquitous Sensor Networks

In this section, we discuss some of the security and privacy issues for USNs.

4.1 Securing Ubiquitous Sensor Networks

Next, we discuss security solutions that mitigate the attacks discussed in Section 3.1.

4.1.1 Data integrity

We can prevent eavesdropping and data integrity attacks by protecting communication channels through encryption from sensors to first-level integrators, as well as from first-level integrators to second-level integrators. However, faulty sensor readings and users' actions such as tampering with sensors (or the environment) are examples where encryption alone fails to maintain data integrity in USNs. In this section, we present solutions that can protect data integrity.

- *Estimation and filtering.* For certain types of USNs, including community-based systems, the management of errors in the data (e.g., wrong measurements, outliers, or faulty sensor readings) assumes that there are enough participants to handle errors in the data at a macro level [59–61]. By this, we mean that there is enough redundancy (of first-level integrators) along with statistical models to keep the system's estimation capabilities from being impaired. Some examples of techniques for estimation and filtering of data used in USNs include interpolation techniques (such as kriging), Markov random fields, Principal Component Analysis [59], clustering, Gaussian mixture models [60], and anomaly detection algorithms (such as unsupervised/ supervised machine learning methods—including support vector machines, neural networks, Bayesian networks—and parametric/non-parametric methods adapted for anomaly detection [61]).
- *User and sensor authentication*. Solutions to handle authentication in USNs include biometrics [62,63], smart card authentication [64,65], two-factor authentication [66,67], and secured brokering hardware [68,69]. Using mobile phone-based biometric authentication methods (e.g., fingerprint sensors or face recognition) combined with other wearable and/or implantable sensors may provide novel approaches to achieve user authentication [70]. The use of hardware-based, trusted execution environments (TEEs) [71] can provide solutions for device authentication, especially because TEEs are currently used in mobile phones as a standard feature for network device authentication (e.g., International Mobile Equipment Identity) [72].

4.1.2 System availability

We discuss below availability issues related to integrators and user participation.

- *Availability at first-level integrators.* Mitigating DoS attacks on communication channels between sensors and first-level integrator devices can be achieved by using several mechanisms, including frequency hopping, repositioning of sensors, modification of protocols, and physical layer jamming avoidance techniques (e.g., directional antennas, spread spectrum, channel diversity) [5]. In the case of battery exhaustion attacks, potential methods include developing power-aware operating systems and frameworks [73,74]. They may also include techniques for assessing an app's power consumption or employing a sensing task before downloading and installing it at a first-level integrator device [75–77], as well as approaches that detect an abnormal increase in power consumption at runtime [78–80]. In the case of detecting operating system vulnerabilities, the following techniques could be used: static analysis (i.e., analysis of source/compiled code

before execution by using tools such as Metal [81]; dynamic analysis (i.e., analysis of programs during their execution to detect and document program errors and vulnerabilities [82]; and formal methods (i.e., the use of mathematical logic and specifications to prove program correctness [83,84]). The detection of vulnerabilities is always a race against the clock, as they must be corrected before they are exploited by attackers. It is possible for a vulnerability or bug to go undetected and be exploited for long periods of time (even years) [31] before it is fixed.

- *Availability at second-level integrators.* To deal with the availability at second-level integrators, USN systems should focus on addressing the problems of elasticity and DoS (see Section 3). Given the possibility of billions of Internet-connected devices performing data collection for USNs, not being able to manage or cope with different types of workloads will render the system useless. To deal with elasticity in USNs, various approaches have been considered, such as hybrid architectures of client-server and peer-to-peer architecture designs [12] and cloud-based solutions [85,86]. In the case of DoS, the issue is similar to any other service being provided on the Internet. Therefore, countermeasures for traditional network infrastructure and cloud-based environments can be used [87].
- *User participation.* Salim and Haque [88] identified that the successful, large-scale user participation in USNs consists of five steps. First, identify the needs and dilemmas (dilemmas in this context represent the users' decision to participate in the USN given the possible associated risks and costs such as privacy risks, monetary costs, user reputation, or physical security). Second, identify stakeholders. Third, identify incentives. Fourth, gather evidence and experience. And fifth, provide tools and affordance (affordance in this context means the provisions, tools, and interfaces for the user to interact with the USN in a usable manner—not only to collect data, but also to understand the information from the collected data). User participation relates to security in USNs, because if users do not participate in collecting data, the USN will have an availability issue (no data will be available for processing). Thus, USN systems must be mindful of an individual or community and assure that any data collection preserves their wellbeing, to assure adequate participation and even increase it. The following are means of monetary or non-monetary incentives [89] to help:
  - *Micropayments.* These are monetary incentives that pay small fractions of a dollar to users who contribute data to the USN. Micropayments were developed in the 1990s during the Web's explosion, as an incentive to sell online content [90] for user-generated content. In the context of USNs, micropayments were first evaluated by Lee and Hoh [91], using dedicated algorithms based on game theory;
  - *Altruistic incentives.* Users participate because of the benefits to the community that a USN can provide. Common examples include P-Sense [15], the Personal Environmental Impact Report (PEIR) [16], and NoiseSPY [17];
  - *Social incentives.* In this category, the incentives are social or human-centric rewards, such as a better reputation, improved health, or interacting with other users to achieve mutual goals. Common examples in this group include e-bird [18], fitness applications (such as Runtastic [21]), and games (such as Pokemon GO [22]).

Table 2 presents a summary of the issues, along with their solutions discussed in Section 4.

Table 2. Security issues and solutions for USNs

Security issues	Solutions
Data integrity	
Spoofing	Estimation and filtering (e.g., methods such as kriging and Gaussian mixture models) Anomaly detection (e.g., methods such as support vector machines, neural networks, Bayesian networks)
Authentication	
User authentication	Biometric methods Smart card authentication Two-factor authentication
Sensor authentication	Secure brokering hardware Trusted execution environments
System availability	
Availability at first-level integrators	
Interference attacks on communication between sensors and first-level integrators	Frequency hopping Sensor repositioning Protocol modification Physical layer jamming avoidance (e.g., directional antennas, spread spectrum, and channel diversity)
Battery exhaustion attacks	Power-aware operating systems Assessing power consumption of tasks before installation Anomaly detection for power consumption at runtime
Operating system vulnerabilities	Static analysis Dynamic analysis Formal methods
Availability at second-level integrators	
Elasticity	Hybrids between client-server and peer-to-peer (P2P) architectures Cloud-based solutions
Denial of service (DoS)	DoS countermeasures for cloud services and traditional network environments
User participation	Incentives (e.g., micropayments, altruistic incentives and social incentives)

4.2 Solutions to Privacy Issues in Ubiquitous Sensor Networks

In this section, we present privacy solutions to address the privacy issues discussed in Section 3.2.

4.2.1 Reidentification

Encryption alone is not enough to protect users' privacy from third parties eavesdropping on communication channels. Indeed, users' identities could be revealed from network identifiers as well as from the incorrect management of processes related to the sensing tasks in USNs. Next, we explore available solutions to avoid reidentification at first- and second-level integrators.

- *Reidentification from network identifiers.* Solutions that avoid reidentification from network identifiers aim to hide users' network addresses (such as IP addresses). They include the use of peer-to-peer (P2P) anonymization networks [36–38], disposable network identifiers [39], and

double encryption via brokers [92,93].

- *Reidentification from task management.* Solutions that prevent reidentification from task management seek to hide the users' identity at different stages during the data collection stage for sensing tasks. As such, different solutions for user authentication, task distribution, and data submission have been proposed to decrease the risk of reidentification. In the case of authentication for USNs, solutions include using pre-shared keys in the sensing software [37], group authentication [92], and pseudonyms [94–97]. For task distribution solutions, options include using beacons that distribute tasks through broadcast signals from the beacons or access points (such as Wi-Fi access points) [92]. Downloading tasks at crowded spaces to diminish the risk of reidentification [92], and using anonymization networks that hide a user's identity [37,38] are also options used to protect privacy in task distribution.

During data submission, several methods have been proposed to protect data privacy. These methods include using anonymization networks and double encryption, using anonymization methods in databases (e.g., k-anonymity, ℓ-diversity, and obfuscation) [92], group-based signatures, micro-aggregation (calculating averages on sensed data values from k users in a particular area [98]), data aggregation (calculating statistics based on groups of users) [99,100], and using representative samples from data collected in a region [101,102].

Vergara-Laurens [103] discussed the tradeoffs between information loss, computational complexity, communication overhead, and power consumption for different privacy-protection schemes for data submission. Vergara-Laurens suggested using different anonymization schemes based on geographical cells with various sizes. For smaller cell sizes where users can be identified more easily, the scheme uses encryption to protect users' privacy and increase the quality of information. For bigger cells where it is more important to protect users' privacy, the scheme makes use of anonymization and data obfuscation techniques at of the cost of decreasing the quality of information (the submitted data are perturbed in this latter technique) [103].

4.2.2 Context privacy

The goal of solutions for context privacy is to diminish or eliminate the risks of discovering and associating aspects or contexts considered private by users and contributors from the data (or metadata) submitted to the system. Here, we explore solutions that can protect context privacy.

For location data privacy protection, methods can be classified into those that aim to protect privacy in location-based queries (including the location of data submission) [40–49], and others that aim to protect path privacy [50–55]. For location-based queries, methods to protect privacy include adaptations of k-anonymity [40–44,95,96] and location obfuscation methods [45–50]. In the case of solutions that use k-anonymity, the idea is that the original location data from a particular user cannot be distinguished from $k - 1$ other locations within a particular area, and within a particular timeframe. In the second group (obfuscation methods), the goal is to modify/perturb the submitted location by selecting or calculating a new location for the submitted location data. Some examples of the last approach add random noise [47–49], make use of known landmarks [50,51], or select a point from a redefined area where the user's true location is identified [46]. Methods for path privacy protection include the use of location query protection algorithms, schemes based on geographical contexts (such as virtual fences [53]), and obfuscation schemes (that mix true and fake locations along a path [54] and

use cloaking regions to blur paths [55]).

Mechanisms for sensor data privacy protection include allowing or denying data collection in specific contexts. The ultimate goal is to create rules for the device to collect data only when the user wishes to do so. Good examples of allowing data collection only in particular contexts include bubble sensing [97]. In this case, contexts are identified based on sensor data readings—as well as on the concept of privacy bubbles [98] on which users define contexts—to manage content for submission to second-level integrators in mobile environments. Mechanisms to deny data collection in specific locations are explored in Kapadia et al. [99]. The authors proposed the virtual walls approach, where users explicitly restrict the contexts of where data collection should not happen.

4.2.3 External data sharing

Technical solutions for external data sharing for USNs focus on anonymization techniques in databases [100]. These solutions fall into two major categories: anonymization for the release of microdata (un-aggregated data) [104–106]; and anonymization for the release of aggregated data [100,107]. In the first category, the goal is to guarantee that if a record is released (in the microdata), an attacker cannot associate confidential attributes of a record in the microdata with an identifier from the record (e.g., a name, Social Security number, or face). Some examples of methods for anonymizing microdata include k-anonymity (where each record in a microdata release is indistinguishable from at least $k - 1$ other records with respect to certain identifying attributes) [104], ℓ-diversity (the microdata table contains at least ℓ well-represented values with respect to a sensitive or confidential attribute) [105], and t-closeness (the distance between the distribution of a sensitive attribute in an anonymized group should not be different from the global distribution by more than a threshold value t) [106]. In the second category (aggregated data), the goal is to guarantee whether the release of a statistical value (e.g., an average) from the database can reveal information about a particular record in that database or reveal an identifier that was used to create the statistical value. Differential privacy has been proposed as an approach to handle privacy in the release of aggregated data [107]. Table 3 presents a summary of these privacy issues and solutions.

5. Future Security and Privacy Challenges for Ubiquitous Sensor Networks

In this section, we discuss some of the security and privacy issues for USNs.

5.1. Security Challenges for Ubiquitous Sensor Networks

As USNs make strong use of consumer devices to collect data of interest, these devices still will be exposed to human intervention in the future. In addition, trust in devices (as they are developed for the consumers with less emphasis on built-in security), trust in the sensing tasks (as they can be maliciously engineered and implemented to cause harm), and trust in the organizations that delegate the sensing tasks (as they could have goals that may affect users' privacy and security) are key aspects in the successful deployment of future USNs. In this context, we identify current challenges that should be

addressed to build more robust and secure USNs. These challenges include trustworthy tasking and data integrity for human-centric USNs.

Table 3. Privacy issues and solutions for USNs

Privacy issues	Solutions
Reidentification	
Reidentification from network identifiers	Disposable network identifiers P2P anonymization Double encryption (trusted broker)
Reidentification from task management	
Authentication	Group authentication Use of pseudonyms
Task distribution	Beacon-based distribution Task downloading at crowded spaces Anonymization network schemes
Data submission	Anonymization network schemes Use of double encryption via brokers Group-based signatures *k*-anonymity *ℓ*-diversity Obfuscation Use of pseudonyms Micro-aggregation Data aggregation Use of representative samples
Context privacy	
Location privacy	
Location-based queries	k-anonymity Random noise in location submission Use of known landmarks for location submission
Path privacy	Adaptations of location-based queries mechanisms Virtual fences Fake locations Cloaking regions
Sensor and metadata privacy	Allowing sensor data collection on task contexts only Denying sensor data collection in contexts considered private
External data sharing	
Microdata release	*k*-anonymity *ℓ*-diversity *t*-closeness
Statistical (summarized) data release	Differential privacy

5.1.1 Trustworthy tasking

USNs have been developed under the principle that the sensing task and the organizations that collect data are trusted. As such, most of the research in securing USNs assumes that threats are coming from custodians of first-level integrator devices (e.g., by submitting fake data) or from an external organization or third party with the goal of disrupting the USN (e.g., by executing a DoS attack on the USN). However, more research is needed on assessing the trust that we may have in the organizations that perform data collection, the sensing task, and the security of the device collecting data—especially given the usage of COTS devices as integrators and sensors. As an example of this issue, consider a recent incident about a U.S. federal court case involving the Federal Trade Commission and Vizio about "deceptive and unfair" data collection practices. Vizio tracked what people saw on their TV sets without actually getting user consent (the approach used by Vizio to provide notice to users was deceptive). Similar incidents involving IoT companies [108] underscore the need for research about organizations' and companies' trustworthiness, along with their practices on collecting and managing data from users.

Moreover, USN devices could be reprogrammed through a sensing task to steal data or create physical harm to the user (e.g., theft, kidnapping, or accidents) [109], because many USN devices not only collect data but also perform some type of physical action (e.g., opening doors, increasing building temperatures, driving cars without human intervention, or delivering medication automatically to user's body). Finally, USN devices could be used as zombies by botnets to attack external parties, as demonstrated by the DDoS at Domain Name Servers (DNS) attack that disrupted the Web in 2016, which involved consumer Internet connected cameras as zombies [110].

5.1.2 Data integrity for human-centric USNs

In a human-centric USN, a user usually has one type of sensor of each kind. For instance, a user has one heart rate sensor, one ECG sensor, and one breath depth sensor if using a wearable such as the Zephyr BioHarness [111]. There may also be multiple sensors of one type (e.g., a heart rate sensor on a chest strap, and another on a smartwatch) [112]. Estimation and filtering of variables of interest in addition to redundancy of sensors or multiple first-level integrators, as proposed for community-based USNs, cannot be used. This is because data in human-centric systems from a particular user is usually isolated from others due to privacy concerns. New techniques are needed to authenticate data in these scenarios. In addition, because feedback in human-centric systems could involve intrusive actions automatically (e.g., deliver medication without user intervention), novel methods are needed to continuously authenticate the user to ensure these actions' effectiveness (i.e., some of these actions can generate life-threatening consequences). These authentication methods must have the following characteristics:

- *Non-repudiation.* These methods must guarantee user identity with high assurance.
- *Unobtrusiveness.* These methods must authenticate users without explicit user intervention. Continuous authentication methods that request users to authenticate regularly are unrealistic (i.e., not usable from the human-computer interaction perspective).
- *Power-aware.* Many first-level integrators in human-centric USNs are battery-powered, thus continuous authentication methods that generate high power overhead for a first-level integrator device are not useful.

5.2. Privacy Challenges for Ubiquitous Sensor Networks

The ubiquity and use of mobile and Internet-connected devices as first-level integrators present a tradeoff: on one hand, we need to collect data as accurately as possible, but on the other hand, it is imperative that we collect or share data in a way that would preserve the privacy of users [101]. Next, we identify some of the current challenges that should be addressed to build privacy-preserving USNs. These challenges include access control and privacy of bystanders.

- *Access control.* Using privacy policies to protect users' privacy in USNs may not inform how and when the data collected is shared by second-level integrator devices. A report by the US Federal Trade Commission [102] stated that due to the length of policies, the lack of uniformity in the language, and the difficulty in understanding these policies, privacy policies are not successful in informing users about data practices. In addition, research has shown that 50% of adults in the United States cannot understand literature written at an eight grade level [113],so they will not understand privacy policies which are typically written at a level above eighth grade [114]. Mechanisms for fine-grained access control (i.e., electronic consents for data-sensor data readings) are needed for users to better handle their privacy. Fine-grained access control for sensor data using privacy-preserving contracts based on blockchains [103] may present an alternative for users to manage the sharing of sensor data with third-parties more efficiently.
- *Privacy of bystanders.* Privacy on USNs has focused on the protection of the privacy of users. However, USNs may collect identifiable data about third parties (bystanders) who may have not given consent to be part of the collection. Even though some solutions to protect the privacy of bystanders' privacy have been proposed [115], these solutions exist only as research prototypes that have not been widely adopted or implemented in consumer products. Bystanders' privacy is becoming increasingly important because the growth and availability of IoT devices are making computation transparent, in the sense that consumers are generally not aware of these devices' availability and what they do in their surroundings: with the current technological trends, computing devices are being manufactured as small as needed. The fact that an IoT company in the U.S. recently collected location data about users at brick-and-mortar shopping stores without customers' knowledge and without providing options for the consumers demonstrates the seriousness of this issue [108]. More research urgently is needed to implement and fiercely protect bystanders' privacy in USNs.

6. Conclusion and Future Work

After reviewing threats and solutions in security and privacy for ubiquitous sensor networks, we classified security issues into two major categories: data integrity and system availability. We also classified privacy issues into three major categories: reidentification, context privacy, and external data sharing privacy. Although we discussed potential solutions for improving security and protecting privacy in USNs, additional research is needed to handle several security issues (for example, ensuring trustworthy tasking and data integrity for human-centric USNs), as well as privacy issues (such as access control and bystanders' privacy). Given the current rate of adoption of mobile and IoT devices and their utilization in USNs, security and privacy will continue to play a significant role in the future.

Acknowledgement

This is an extended version of the paper "Investigating Security for Ubiquitous Sensor Networks" previously published in the *Proceedings of the 8th International Conference on Ambient Systems, Networks and Technologies (ANT-2017)*. We thank the anonymous reviewers for their valuable comments, which helped improve the paper's content, quality, and organization. Alfredo J. Perez was supported by the US National Science Foundation and the US Department of Defense's ASSURE program under award 1560214. Sherali Zeadally was partially supported by a University Research Professorship Award from the University of Kentucky.

References

[1] *Requirements for Support of Ubiquitous Sensor Network (USN) Applications and Services in the NGN Environment*, International Telecommunication Union, ITU-T Y.2221, 2010.

[2] A. Nordrum, "The Internet of fewer things," *IEEE Spectrum*, vol. 53, no. 10, pp. 12-13, 2016.

[3] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *Journal of Biomedical Informatics*, vol. 55, pp. 272-289, 2015.

[4] M. Zhang, A. Raghunathan, and N. K Jha, "Towards trustworthy medical devices and body area networks," in *Proceedings of the 50th Annual Design Automation Conference*, Austin, TX, 2013.

[5] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: the case of jammers," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 2, pp. 245-257, 2011.

[6] J. Dunning, "Taming the blue beast: a survey of Bluetooth based threats," *IEEE Security & Privacy*, vol. 8, no. 2, pp. 20-27, 2010.

[7] G. Madlmayr, J. Langer, C. Kantner, and J. Scharinger, "NFC devices: security and privacy," in *Proceedings of the 2008 Availability, Reliability and Security*, Barcelona, Spain, 2008, pp. 642-647.

[8] F. Stajano, and R. Anderson, "The resurrecting duckling: security issues for ubiquitous computing," *IEEE Computer*, vol. 35, no. 4, pp. 22-26, 2002.

[9] T. Martin, M. Hsiao, D. Ha, and J. Krishnaswami, "Denial-of-service attacks on battery-powered mobile computers," in *Proceedings of the 2004 IEEE Conference in Pervasive Computing and Communications*, Orlando, FL, 2004, pp. 309-318.

[10] A. Armando, M. Migliardi, and L. Verderame, "Would you mind forking this process? A denial of service attack on Android (and some countermeasures)," in *IFIP International Information Security Conference*. Heidelberg: Springer, 2012, pp. 13-24.

[11] H. Huang, S. Zhu, K. Chen, and P. Liu "From system services freezing to system server shutdown in android: all you need is a loop in an app," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, Denver, CO, 2015, pp. 1236-1247.

[12] A. J. Perez, M. A. Labrador, and S. J. Barbeau, "G-sense: a scalable architecture for global sensing and monitoring," *IEEE Network*, vol. 24, no. 4, pp. 57-64, 2010.

[13] M. A. Labrador, A. J. Perez, and P. M. Wightman, *Location-based Information Systems: Developing Real-Time Tracking Applications*. Boca Raton, FL: CRC Press, 2010.

[14] S. Barbeau, R. Perez, M. A. Labrador, A. J. Perez, P. Winters, and N. Georggi, "A location-aware framework for intelligent real-time mobile applications," *IEEE Pervasive Computing*, vol. 10, no. 3, pp. 58-67, 2011.

[15] D. Mendez, A. J. Perez, M. A. Labrador, and J. J. Marron, "P-sense: a participatory sensing system for air pollution monitoring and control," in *Proceedings of the 2011 IEEE Conference in Pervasive Computing and Communications*, Seattle, WA, 2011, pp. 344-347.

[16] M. Mun, S. Reddy, K. Shilton, N. Yau, J. Burke, D. Estrin, M. Hansen, E. Howard, R. West, and P. Boda, "PEIR, the personal environmental impact report, as a platform for participatory sensing systems research," in *Proceedings of the 7th international conference on Mobile Systems, Applications, and Services*, Krakow, Poland, 2009, pp. 556-68.

[17] E. Kanjo, "NoiseSPY: areal-time mobile phone platform for urban noise monitoring and mapping," *Mobile Networks and Applications*, vol. 15, no. 4, pp. 562-574, 2010.

[18] A. Wiggins, "eBirding: technology adoption and the transformation of leisure into science," in *Proceedings of the 2011 iConference*, Seattle, WA, 2011, pp. 798-799.

[19] N. D. Lane, S. B. Eisenman, M. Musolesi, E. Miluzzo, and A.T . Campbell, "Urban sensing systems: opportunistic or participatory?" in *Proceedings of the 9th Workshop on Mobile Computing Systems and Applications*, Napa Valley, CA, 2008, pp. 11-16.

[20] O. D. Lara, A. J. Perez, M. A. Labrador, and J. D. Posada, "Centinela: a human activity recognition system based on acceleration and vital sign data," *Pervasive and Mobile Computing*, vol. 8 no. 5, pp. 717-729, 2012.

[21] Runtastic Inc. [Online]. Available: https://www.runtastic.com.

[22] Niantic Inc. [Online]. Available: http://www.pokemongo.com.

[23] S. A. Camtepe and B. Yener, "Key distribution mechanisms for wireless sensor networks: a survey," Rensselaer Polytechnic Institute, Troy, NY*, Technical Report*, 2005.

[24] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in *Proceedings of IEEE 2005 Pervasive Computing and Communications Conference*, Kauai Island, HI, 2005, pp. 324-328.

[25] X. Zhang, H. M. Heys, and C. Li, "Energy efficiency of symmetric key cryptographic algorithms in wireless sensor networks," in *Proceedings of the 2010 25th IEEE Biennial Symposium on Communications*, Kingston, Canada, 2010, pp. 168-172.

[26] A. J. Perez, S. Zeadally, and N. Jabeur, "Investigating security for ubiquitous sensor networks," *Procedia Computer Science*, vol. 109, pp. 737-744, 2017.

[27] A. Kapadia, D. Kotz, and N. Triandopoulos, "Opportunistic sensing: security challenges for the new paradigm," in *Proceedings of the 1st International Communication Systems and Networks and Workshops*, Bangalore, India, 2009, pp. 1-10.

[28] P. Gilbert, L. P. Cox, J. Jung, and D. Wetherall, "Toward trustworthy mobile sensing," in *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*, Annapolis, MD, 2009, pp. 31-36.

[29] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "PyCRA: physical challenge-response authentication for active sensors under spoofing attacks," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, Denver, CO, 2015, pp. 1004-1015.

[30] A. J. Perez, K. Arroyo-Rivera, M. A. Labrador, and I. J. Vergara-Laurens, "HR-Auth: Heart Rate Data Authentication using Consumer Wearables", in *Proceedings of the 5th IEEE/ACM International Conference on Mobile Software Engineering and Systems (MOBILESoft),* Gothenburg, Sweden, 2018, pp. 1-2.

[31] A. Sharabani and Y. Amit, "Mobile vulnerabilities from data breach to complete shutdown," 2015 [Online]. Available: https://www.rsaconference.com/writable/presentations/file_upload/mbs-t09--mobile-vulnerabilities-from-data-breach-to-complete-shutdown.pdf.

[32] Y. Ma, Y. Guo, D. Silva, O. Tsinalis, and C. Wu, "Elastic information management for air pollution monitoring in large-scale M2M sensor networks," *International Journal of Distributed Sensor Networks*, vol. 9, no. 12, article no. 251374, 2013.

[33] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1-11, 2011.

[34] J. S. Lee and B. Hoh, "Sell your experiences: a market mechanism based incentive for participatory sensing," in *Proceedings of the 2010 IEEE Conference in Pervasive Computing and Communications*, Mannheim, Germany, 2010, pp. 60-68.

[35] J. Aikio, V. Pentikinen, J. Haikio, J. Hakkila, and A. Colley, *On the Road to Digital Paradise: The Naked Approach.* Rovaniemi, Finland: University of Lapland, 2016.

[36] D. Christin, "Privacy in mobile participatory sensing: Current trends and future challenges," *Journal of Systems and Software*, vol. 116, pp. 57-68, 2015.

[37] A. J. Perez and S. Zeadally, "PEAR: a privacy-enabled architecture for crowdsensing," in *Proceedings of the International Conference on Research in Adaptive and Convergent Systems*, Krakow, Poland, 2017, pp. 161-171.

[38] J. Al-Muhtadi, R. Campbell, A. Kapadia, M. D. Mickunas, and S. Yi, "Routing through the mist: privacy preserving communication in ubiquitous computing environments," in *Proceedings of the 22nd International Conference on Distributed Computing Systems*, Vienna, Austria, 2002, pp. 74-83.

[39] M. Gruteser and D. Grunwald, "Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis," *Mobile Networks and Applications*, vol. 10, no. 3, pp. 315-325, 2005.

[40] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services*, San Francisco, CA, 2005, pp. 31-42.

[41] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias. "Preventing location-based identity inference in anonymous spatial queries," *IEEE Transactions on Knowledge and Data Engineering,* vol. 19 no. 12, pp. 1719-1733, 2007.

[42] C. Bettini, S. Mascetti, X. S. Wang, D. Freni, and S. Jajodia, S, "Anonymity and historical-anonymity in location-based services," in *Privacy in Location-based Applications*. Heidelberg: Springer, 2009, pp. 1–30.

[43] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: architecture and algorithms," *IEEE Transactions on Mobile Computing*, vol. 7, no. 1, pp. 1-18, 2008.

[44] A. Gkoulalas-Divanis, P. Kalnis, and V. S. Verykios. "Providing k-anonymity in location based services," *ACM SIGKDD Explorations Newsletter*, vol. 12, no. 1, pp. 3-10, 2010.

[45] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy," in *International Conference on Pervasive Computing*. Heidelberg: Springer, 2005, pp. 152-170.

[46] C. A. Ardagna, M, Cremonini, S. D. C. di Vimercati, and P. Samarati, "An obfuscation-based approach for protecting location privacy," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 1, pp. 13-27, 2009.

[47] P. Wightman, W. Coronell, D. Jabba, M. A. Jimeno, and M. Labrador, "Evaluation of location obfuscation techniques for privacy in location based information systems," in *Proceedings of the 2011 IEEE Latin-American Conference on Communications*, Belem do Para, Brazil, 2011, pp. 1-6.

[48] D. Quercia, I. Leontiadis, L. McNamara, C. Mascolo, and J. Crowcroft, "Spotme if you can: randomized responses for location obfuscation on mobile phones, in *Proceedings of the 31st International Conference on Distributed Computing Systems*, Minneapolis, MN, 2011, pp. 363-372.

[49] M. E. Andres, N. E., Bordenabe, K. Chatzikokolakis, and C, Palamidessi, "Geo-indistinguishability: differential privacy for location-based systems," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security*, Berlin, Germany, 2013, pp. 901-914.

[50] J. Krumm, "Inference attacks on location tracks," in *International Conference on Pervasive Computing*. Heidelberg: Spribger, 2007, pp. 127-143.

[51] I. J. Vergara-Laurens and M. A. Labrador, "Preserving privacy while reducing power consumption and information loss in lbs and participatory sensing applications," in *Proceedings of 2011 IEEE GLOBECOM*, Houston, TX, 2011, pp. 1247-1252.

[52] C. Y. Chow and M. F. Mokbel, "Trajectory privacy in location-based services and data publication," *ACM SIGKDD Explorations Newsletter*, vol. 13, no. 1, pp. 19-29, 2011.

[53] B. Hoh, M. Gruteser, R. Herring, J. Ban, D. Work, J. C. Herrera, A. M Bayen, M. Annavaram, and Q. Jacobson, "Virtual trip lines for distributed privacy-preserving traffic monitoring," in *Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services*, Breckenridge, CO, 2008, pp. 15-28.

[54] K. C. Lee, W. C. Lee, H. V. Leong, and B. Zheng, "Navigational path privacy protection: navigational path privacy protection," in *Proceedings of the 18th ACM Conference on Information and Knowledge Management*, Hong Kong, China, 2009, pp. 691-700.

[55] K. T. Yang, G. M. Chiu, H. J. Lyu, D. J. Huang, and W. C. Teng, "Path privacy protection in continuous location-based services over road networks," in *Proceedings of 2012 Wireless and Mobile Computing, Networking and Communications*, Barcelona, Spain, 2012, pp. 435-442.

[56] I. Anagnostopoulos, S. Zeadally, and E. Exposito, "Handling big data: research challenges and future directions," *Journal of Supercomputing,* vol. 72, no. 4, pp 1494-1516, 2016.

[57] S. Avancha, A. Baxi, and D. Kotz, "Privacy in mobile technology for personal healthcare," *ACM Computing Surveys*, vol. 45, no. 1, article no. 3, 2012.

[58] BakerHosteler, "2015 International Compendium of Data Privacy Laws," [Online]. Available: http://towerwall.com/wp-content/uploads/2016/02/International-Compendium-of-Data-Privacy-Laws.pdf.

[59] D. Mendez, M. A. Labrador, and K. Ramachandran, "Data interpolation for participatory sensing systems," *Pervasive and Mobile Computing*, vol. 9, no. 1, pp. 132-148, 2013.

[60] D. Mendez and M. A. Labrador, "On sensor data verification for participatory sensing systems," *Journal of Networks*, vol. 8, no. 3, pp. 576-587, 2013.

[61] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: a survey," *ACM Computing Surveys*, vol. 41, no. 3, pp. 1-15, 2009.

[62] C. C. Poon, Y. T. Zhang, and S. D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 73-81, 2006.

[63] N. Henry, N. Paul, and N. McFarlane, "Using bowel sounds to create a forensically-aware insulin pump system," in *Proceedings of 2013 USENIX Workshop on Health Information Technologies (HealthTech),* Washington, DC, 2013.

[64] O. Mir, T. van der Weide, and C. C. Lee, "A secure user anonymity and authentication scheme using AVISPA for telecare medical information systems," *Journal of Medical Systems*, vol. 39, no. 9, article no. 89, 2015.

[65] J. M. Sorber, M. Shin, R. Peterson, and D. Kotz, "Plug-n-trust: practical trusted sensing for mhealth," in *Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services*, Low Wood Bay, UK, 2012, pp. 309-322.

[66] L. Xu, and F. Wu, "Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care," *Journal of Medical Systems*, vol. 39, no. 2, article no. 10, 2015.

[67] F. Wu, L. Xu, S. Kumari, and X. Li, "An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks," *Multimedia Systems*, vol. 23 no. 2, pp. 195-205, 2017.

[68] V. Pournaghshband, M. Sarrafzadeh, and P. Reiher, "Securing legacy mobile medical devices," in *International Conference on Wireless Mobile Communication and Healthcare*. Heidelberg: Springer, 2012, pp. 163-172.

[69] A. Dua, N. Bulusu, W. C. Feng, and W. Hu, "Towards trustworthy participatory sensing," in *Proceedings of the 4th USENIX Conference on Hot Topics in Security*, Montreal, Canada, 2011.

[70] A. Darwish and A. E. Hassanien, "Wearable and implantable wireless sensor network solutions for healthcare monitoring," *Sensors*, vol. 11, no. 6, pp. 5561-5595, 2011.

[71] J. E. Ekberg, K. Kostiainen, and N. Asokan, "The untapped potential of trusted execution environments on mobile devices," *IEEE Security & Privacy*, vol. 12, no. 4, pp. 29-37, 2014.

[72] K. Kostiainen, E. Reshetova, J. E. Ekberg, and N. Asokan, "Old, new, borrowed, blue: a perspective on the evolution of mobile platform security architectures," in *Proceedings of the 1st ACM Conference on Data and Application Security and Privacy*, San Antonio, TX, 2011, pp. 13-24.

[73] N. Vallina-Rodriguez and J. Crowcroft, "ErdOS: achieving energy savings in mobile OS," in *Proceedings of the 6th International Workshop on MobiArch*, Bethesda, MD, 2011, pp. 37-42.

[74] A. Merlo, M. Migliardi, and L. Caviglione, "A survey on energy-aware security mechanisms," *Pervasive and Mobile Computing*, vol. 24, pp. 77-90, 2015.

[75] M. Dong and L. Zhong, "Self-constructive high-rate system energy modeling for battery-powered mobile systems," in *Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services*, Bethesda, MD, 2011, pp. 335-348.

[76] R. Mittal, A. Kansal, and R. Chandra, "Empowering developers to estimate app energy consumption," in *Proceedings of the 18th Annual International Conference on Mobile Computing and Networking*, Istanbul, Turkey, 2012, pp. 317-328.

[77] C. Min, Y. Lee, C. Yoo, S. Kang, S. Choi, P. Park, I. Hwang, Y. Ju, S. Choi, and J. Song, "Powerforecaster: predicting smartphone power impact of continuous sensing applications at pre-installation time," in *Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems*, Seoul, Korea, 2015, pp. 31-44.

[78] X. Ma, P. Huang, X. Jin, P. Wang, S. Park, D. Shen, Y. Zhou, L. K. Saul, and G. M. Voelker, "eDoctor: automatically diagnosing abnormal battery drain issues on smartphones," in *Proceedings of the 10th USENIX Symposium on Networked Systems Design and Implementation*, Lombard, IL, 2013, pp. 57-70.

[79] A. Pathak, A. Jindal, Y. C. Hu, and S. P. Midkiff, "What is keeping my phone awake? Characterizing and detecting no-sleep energy bugs in smartphone apps," in *Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services*, Low Wood Bay, UK, 2012, pp. 267-280.

[80] F. Xu, Y. Liu, Q. Li, and Y. Zhang, "V-edge: fast self-constructive power modeling of smartphones based on battery voltage dynamics," in *Proceedings of the 10th USENIX Symposium on Networked Systems Design and Implementation*, Lombard, IL, 2013, pp. 43-56.

[81] S. Hallem, B. Chelf, Y. Xie, and D. Engler, "A system and language for building system-specific, static analyses," *ACM SIGPLAN Notices*, vol. 37, no. 5, pp. 69-82, 2002.

[82] A. Fattori, R. Paleari, L. Martignoni, and M. Monga, "Dynamic and transparent analysis of commodity production systems," in *Proceedings of the IEEE/ACM International Conference on Automated Software Engineering*, Antwerp, Belgium, 2010, pp. 417-426.

[83] G. J. Holzmann, "The model checker SPIN," *IEEE Transactions on Software Engineering*, vol. 23, no. 5, pp. 279-295, 1997.

[84] S. Gritzalis, D. Spinellis, and P. Georgiadis, "Security protocols over open networks and distributed systems: Formal methods for their analysis, design, and verification," *Computer Communications*, vol. 22, no. 8, pp. 697-709, 1999.

[85] K. Lee, D. Murray, D. Hughes, and W. Joosen, "Extending sensor networks into the cloud using Amazon web services," in *Proceedings of Networked Embedded Systems for Enterprise Applications*, Suzhou, China, 2010, pp. 1-7.

[86] Y Xu and S. Helal, "Scalable cloud–sensor architecture for the Internet of Things," *IEEE Internet of Things*, vol. 3 no. 3, pp. 285-298, 2016.

[87] O. Osanaiye, K. R. Choo, and M. Dlodlo, "Distributed Denial of Service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework," *Journal of Network and Computer Applications*, vol. 67, pp. 147-165, 2016.

[88] F. Salim and U. Haque, "Urban computing in the wild: a survey on large scale participation and citizen engagement with ubiquitous computing, cyber physical systems, and Internet of Things," *International Journal of Human-Computer Studies*, vol. 81, pp. 31–48.

[89] L. G. Jaimes, I. J. Vergara-Laurens, and A. Raij, "A survey of incentive techniques for mobile crowd sensing," *IEEE Internet of Things*, vol. 2, no. 5, pp. 370-380, 2015.

[90] N. Hardy and E. D. Tribble, *The Digital Silk Road*. Los Altos, CA: Agoric Inc., 1993.

[91] J. S. Lee and B. Hoh, "Sell your experiences: a market mechanism based incentive for participatory sensing," in *Proceedings of the 2010 IEEE Conference in Pervasive Computing and Communications*, Mannheim, Germany, 2010, pp. 60-68.

[92] M. Shin, C. Cornelius, D. Peebles, A. Kapadia, D. Kotz, and N. Triandopoulos, "AnonySense: a system for anonymous opportunistic sensing," *Pervasive and Mobile Computing*, vol. 7, no. 1, pp. 16-30, 2010.

[93] I. J. Vergara-Laurens, D. Mendez, and M. A. Labrador, "Privacy, quality of information, and energy consumption in participatory sensing systems," in *Proceedings of the 2014 IEEE Conference in Pervasive Computing and Communications*, Budapest, Hungary, 2014, pp. 199-207.

[94] I. J. Vergara-Laurens "A hybrid privacy-preserving mechanism for participatory sensing systems," Ph.D. dissertation, University of South Florida, FL, 2014.

[95] E. Snekkenes, "Concepts for personal location privacy policies," in *Proceedings of the 3rd ACM conference on Electronic Commerce*, Tampa, FL, 2001, pp. 48-57.

[96] C. Hauser and M. Kabatnik, "Towards privacy support in a global location service," in *Proceedings of the IFIP Workshop on IP and ATM Traffic Management*, Paris, France, 2001.

[97] H. Lu, N. Lane, S. Eisenman, and A. Campbell, "Bubble-sensing: a new paradigm for binding a sensing task to the physical world," *Pervasive Mobile Computing*, vol. 6, no. 1, pp. 58-71, 2009.

[98] D. Christin, P. S. Lopez, A. Reinhardt, M. Hollick, and M. Kauer, "Share with strangers: privacy bubbles as user-centered privacy control for mobile content sharing applications," *Information Security Technical Report*, vol. 17, no. 3, pp. 105-116, 2012.

[99] A. Kapadia, T. Henderson, J. J. Fielding, and D. Kotz, "Virtual walls: protecting digital privacy in pervasive environments," in *International Conference on Pervasive Computing.* Heidelberg: Springer, 2007, pp. 162-179.

[100] S. De Capitani, S. Foresti, G. Livraga, and P. Samarati, "Data privacy: definitions and techniques," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems,* vol. 20, no. 6, pp. 793-817, 2012.

[101] A. J. Perez and S. Zeadally, "Privacy issues and solutions for consumer wearables," *IT Professional*, 2017. https://doi.org/10.1109/MITP.2017.265105905.

[102] US Federal Trade Commission Report, "Protecting consumer privacy in an era of rapid change," 2012.

[103] A. Kosba, A. Miller, E. Shi, Z Wen, and C. Papamanthou, "Hawk: the blockchain model of cryptography and privacy-preserving smart contracts," in *Proceedings of 2016 IEEE Symposium on Security and Privacy*, San Jose, CA, 2016, pp. 839-858.

[104] L. Sweeney, "k-anonymity: a model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 5, pp. 557-570, 2002.

[105] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "L-diversity: privacy beyond k-anonymity," *ACM Transactions on Knowledge Discovery from Data*, vol. 1, no. 1, article no. 3, 2007.
[106] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: privacy beyond k-anonymity and l-diversity," in *Proceedings of IEEE 23rd International Conference on Data Engineering*, Istanbul, Turkey, 2007, pp. 106-115.
[107] C. Dwork, "Differential privacy: a survey of results," in *Theory and Applications of Models of Computation*. Heidelberg: Springer, 2008.
[108] A J. Perez, S. Zeadally, and J. Cochran "A review and an empirical analysis of privacy policy and notices for consumer Internet of things, " *Security and Privacy,* e15, doi: https://doi.org/10.1001/spy2.15 , 2018.
[109] CBSNews, "'Pokemon Go' being used to stage robberies, police say," [Online]. Available: http://www.cbsnews.com/news/robbery-suspects-using-pokemon-go-to-target-victims-police-say/.
[110] T. Pultarova, "Webcam hack shows vulnerability of connected devices," *Engineering & Technology*, vol. 11, no. 11, pp. 10-10, 2016.
[111] Zephyr BioHarness 3 [Online]. Available: https://www.zephyranywhere.com.
[112] A. J. Perez, K. Arroyo-Rivera, M. A. Labrador, and I. J. Vergara-Laurens, "HR-Auth: Heart Rate Data Authentication using Consumer Wearables", in *Proceedings of the 5th IEEE/ACM International Conference on Mobile Software Engineering and Systems (MOBILESoft),* Gothenburg, Sweden, 2018, pp. 1-2.
[113] Literacy Project Foundation, "Staggering illiteracy statistics," 2008 [Online]. Available: http://www.literacyprojectfoundation.org/statistics-page/.
[114] S. Winkler and S. Zeadally, "Privacy policy analysis of popular web platforms," *IEEE Technology and Society Magazine*, vol. 35, no. 2, pp. 75-85, 2016.
[115] A. J. Perez, S. Zeadally, and S. Griffith, "Bystanders' privacy," *IT Professional*, vol. 19, no. 3, pp. 61-65, 2017.

Alfredo J. Perez https://orcid.org/0000-0002-2852-2041

He received the B.Sc. (2006) in Systems Engineering from Universidad del Norte (Barranquilla, Colombia), and M.Sc. and Ph.D. degrees in Computer Science and Engineering from the University of South Florida in 2009 and 2011, respectively. He is an Assistant Professor with the TSYS School of Computer Science at the Columbus State University (Columbus, GA, USA).

Sherali Zeadally https://orcid.org/0000-0002-5982-8190

He received his bachelor degree (1991) in Computer Science from the University of Cambridge (England) and his doctoral degree (1996) in Computer Science from the University of Buckingham (England). He is currently an Associate Professor with the College of Communication and Information at the University of Kentucky (Lexington, KY, USA).

Nafaa Jabeur https://orcid.org/0000-0001-8238-6813

He received the B.Eng. degree (1998) in Computer Science from the High National School of Informatics and System Analysis, ENSIAS (Rabat, Morocco), and the M.Sc. (2001) and Ph.D. (2006) degrees Computer Science from Laval University (Canada). He is currently Chair and Associate Professor with the Department of Computer Science at the German University of Technology in Oman (Muscat, Oman).