6-12-2017

Investigating Security for Ubiquitous Sensor Networks

Alfredo J. Perez
Columbus State University, perez_alfredo@columbusstate.edu

Sherali Zeadally
University of Kentucky, szeadally@uky.edu

Nafaa Jabeur
German University of Technology, Oman

Digital Object Identifier (DOI)
https://doi.org/10.1016/j.procs.2017.05.432

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 109C (2017) 737–744

Procedia Computer Science

www.elsevier.com/locate/procedia

The 8th International Conference on Ambient Systems, Networks and Technologies (ANT 2017)

Investigating Security for Ubiquitous Sensor Networks

Alfredo J. Perez[a]*, Sherali Zeadally[b], Nafaa Jabeur[c]

[a] *Columbus State University, Columbus GA, 31909, USA*
[b] *University of Kentucky, Lexington, Kentucky 40506, USA*
[c] *German University of Technology, Oman*

Abstract

The availability of powerful and sensor-enabled mobile and Internet-connected devices have enabled the advent of the ubiquitous sensor network paradigm which is providing various types of solutions to the community and the individual user in various sectors including environmental monitoring, entertainment, transportation, security, and healthcare. We explore and compare the features of wireless sensor networks and ubiquitous sensor networks and based on the differences between these two types of systems, we classify the security-related challenges of ubiquitous sensor networks. We identify and discuss solutions available to address these challenges. Finally, we briefly discuss open challenges that need to be addressed to design more secure ubiquitous sensor networks in the future.

Peer-review under responsibility of the Conference Program Chairs.

Keywords: Human-centric Sensing; Internet of Things; Opportunistic Sensing; Participatory Sensing; Security; Ubiquitous Sensing.

1. Introduction

Ubiquitous Sensor Networks (USNs) have become one of the important paradigms in sensor network systems. The availability and pervasiveness of mobile devices (estimated to be around 7.5 billion in 2016[1]) and Internet of Things-enabled devices (expected to reach 30 billion by 2020[2]) have opened up new opportunities that have the potential to address a wide range of issues that affect the individual and its community in several areas including environmental monitoring, transportation, entertainment, security, and healthcare. The unrestricted adoption of this

* Corresponding author. Tel.: +1- 706-507-8194; fax: +1-706-565-3529
E-mail address: perez_alfredo@columbusstate.edu

1877-0509 © 2017 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of the Conference Program Chairs.
10.1016/j.procs.2017.05.432

sensing paradigm presents significant security challenges and risks. In this paper, we present an overview of these issues as well as solutions that can be considered to address them. The rest of this paper is organized as follows. Section 2 presents architectural models and applications for USNs. In section 3 we discuss security issues for Ubiquitous Sensor Networks (USNs). Section 4 presents solutions to secure USNs. In section 5 we present open challenges. Section 6 presents some concluding remarks.

2. Architectures and Applications of Ubiquitous Sensor Networks

Ubiquitous Sensor Networks (USNs) are sensor networks that make use of Internet-connected devices to serve as a sensing platform to collect data of interest[3]. Usually these devices are owned (or are in custody) by common citizens; however USNs can be deployed by using devices owned by the government as well as private-sector companies. USNs differ in various aspects with respect to Wireless Sensor Networks (WSNs) (table 1). The most important differences among these two classes of networks are that devices in USNs are more powerful than their counterparts in WSNs, the communication between devices in USNs depends on infrastructure-based networks and the Internet, and typically there is human involvement in the collection of data. The typical hardware architecture of USNs consists of the following components[3]:

• *Sensors*: The major functionality of these components of the architecture is to collect data. Sensor software and middleware technologies collect data from the hardware sensors and transfer it to the first-level integrators. Sensors are wired to the first-level integrator devices, or they may be connected via personal area networks such as

Table 1. A comparison of features of Wireless Sensor Networks (WSNs) and Ubiquitous Sensor Networks (USNs).

Features	Wireless Sensor Networks	Ubiquitous Sensor Networks
Computational Capabilities	Devices are battery-powered and designed for low-power consumption. Devices are limited in computational power, memory and communication. WSNs are left unattended for a long period of time. Make use of custom-made devices.	Devices with GHz multi-core processors and memory in the GB range are typical. Devices have rechargeable batteries or they are connected to a reliable power source. Make use of Commercial Off-The-Shelf (COTS) devices, sensors and operating systems.
Communication Infrastructure	Devices must collaborate to perform ad-hoc network routing and maintenance. Single network interface with low-power protocols (e.g., 802.15.4) is used.	Devices may have multiple network interfaces, with infrastructure-based networks (e.g. ISPs, cellular networks) and end-to-end TCP/IP communication.
Communication Security	Cross-layer design for security is needed due to low power and limited computational capabilities.	Use of standard protocols such as Transport Layer Security (TLS) and common cryptographic algorithms/protocols (e.g., AES, RC4, elliptic curve) provide end-to-end security. Assumes reliable communication by Internet Service Providers (ISPs).
Network Management	Single entity manages and controls the WSN. Devices are designed and deployed for a single purpose. Devices participate in a single WSN at a time.	Multiple entities participate in the management of the USN with multiple roles. Data collection tasks may be issued by more than one entity and devices can be used to address many purposes. Devices may participate in more than one USN simultaneously.
Network Maintenance	Performed by the entity that owns the WSN. Network can be costly to deploy and maintain.	Performed by the custodians of data collection devices and entities collecting data. Can be potentially cheap to maintain. May depend on participation by users/custodians to accomplish the goals of the USN.
Scalability	Potentially thousands of devices in a single system.	Potentially billions of devices in a single system.

Bluetooth, Near Field Communication (NFC), 802.15.4 (Zigbee) or some other wireless Local Area Network (LAN) technology.

• *First-level integrators*: The roles of first-level integrators are to perform initial data verification, aggregation and basic analysis (e.g., feature extraction) on the data collected by sensors. Any device that supports IP-based communication can serve as a first-level integrator. Examples include smartphones and Internet-connected devices.

• *Data transport:* In USNs, data transport is provided by any IP-based communication network that enables the end-to-end transfer of data from the first-level integrators to the second-level integrators. The data transport role is performed by Internet Service Providers (ISPs).

• *Second-level integrators:* These components collect and store data sent from first-level integrators. They also provide analytics services and feedback to first-level integrator devices and to external entities. Second-level integrators are implemented by servers and/or cloud-based services.

USNs are currently deployed in several application fields, including environmental monitoring, entertainment, transportation, security, and healthcare. These applications can be grouped into four major categories: (1) Location-based systems (LBS); (2) Community-based sensing systems (CBS); (3) Human-centric sensing systems (HCS); (4) hybrid systems. Available since the late 1990's, LBS systems make use of location sensors to receive/collect geotagged data[4,5]. CBS systems (also known as crowdsensing) track variables of interest for communities (e.g., neighborhoods, cities, citizen associations, leisure/gaming associations, government). Such variables may include pollution, noise, state and congestion of streets, among others[6,55-57]. CBS can be classified as participatory or opportunistic[7]. HCS systems track human-related variables such as physiological variables with the goal of improving the wellbeing of individuals. Some examples of HCS are security and safety systems (e.g., home security, human-fall detection), Mobile health (M-Health) and personal health systems (e.g., fitness tracking) [8,58]. Finally, hybrid systems incorporate characteristics of these three previous groups. Examples in this last group include games such as Pokemon GO [59].

3. Security Issues in Ubiquitous Sensor Networks

Since USN devices are more powerful than their WSN counterparts and USN integrator devices make use of protocols such as Transport Layer Security (TLS) to establish end-to-end secure communication channels between integrators over the Internet, many of the WSN security issues related to the establishment of secure channels (e.g., key distribution, implementation of cryptographic protocols in resource-constrained devices) and network maintenance (e.g., ad-hoc routing) are non-existent in USNs. Consequently, given the features of USNs presented in table 1, we classify the security issues for USNs into two major categories: (1) data integrity; (2) system availability.

3.1. Data Integrity

In USNs, users may have control over several sensors and data collecting devices[9]. Their direct access to these components could be utilized to launch spoofing attacks by submitting false, incorrect, or fake data[10]. Similarly, a second type of spoofing attack on the sensors could be performed by tampering and modifying the physical environment (i.e., for a temperature sensor, this type of attack would increase the room temperature on purpose). In this case, although the sensor's readings are correct, the sensed data are generated from fake or tampered environments [11]. In human-centric sensing 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 the operation of intrusive actions at a patient's body automatically (e.g., deliver medication). In such cases, the violation of data integrity can have serious, life-threatening consequences. This aspect in human-centric USNs raises another major security concern which is the authentication of sensors and users when performing data collection [12,13].

3.2. System Availability

Since data transport in USNs is provided by ISPs, it is assumed that ISPs provide reliable networks to support the communication between integrators. Therefore, there are three ways one can launch attacks on system availability in USNs as follows:

• *Availability at First-level Integrators*: In USNs, 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 [14,16]; (2) attacking and/or depleting the power supply with battery exhaustion attacks [17,18]; or (3) making the operating system unresponsive by exploiting security vulnerabilities of the host operating system[19,21].

• *Availability at Second-level Integrators:* Two major issues arise when managing availability for second-level integrator devices: (1) elasticity; (2) Denial of Service (DoS). Even though the result of not managing both issues correctly is the same (no availability), they differ in terms of availability. Elasticity deals with the ability of the system or the service to satisfy and adapt to workload changes [23], whereas DoS are deliberate attacks to the system or the service itself by malicious parties [24].

• *Attacks on User Participation:* USNs require the participation and collaboration from users and custodians to collect data and enable the system to provide a certain level of Quality of Information (QoI)[9,22] to be useful. Attacks on user participation may include availability attacks at first-level integrators and human aspects that may refrain users from contributing and collecting data (e.g., lack of motivation to participate, reputation of the USN system). If users are not willing to participate, the system will not collect data to provide the feedback at the level required by its stakeholders, resulting on a similar situation as an availability attack on the USN.

4. Securing Ubiquitous Sensor Networks

This section discusses the security solutions that can mitigate the attacks discussed in section 3. The issues along with their solutions are summarized in table 2.

4.1. Data Integrity

We can prevent eavesdropping and data integrity attacks by protecting communication channels through encryption from sensors to first-level integrators, and 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 does not help to maintain data integrity in USNs. In this section, we provide methods available to deal with data integrity.

• *Estimation and Filtering*: For certain types of USNs such as community-based systems, the management of errors in the data (e.g., wrong measurements, outliers, faulty sensor readings) assumes that there are enough participants such that the redundancy (of first-level integrators) along with statistical models can handle errors in the data at a macro level[25,27] without affecting the estimation performed by the system. Examples of techniques for estimation and filtering of data used in USNs include interpolation techniques such as kridging, Markov Random Fields, Principal Component Analysis[25], clustering, Gaussian Mixture Models[26], as well as anomaly detection algorithms such as unsupervised/supervised machine learning methods (e.g., support vector machines, neural networks, Bayesian networks) and parametric/non-parametric methods adapted for anomaly detection [27].

• *User and Sensor Authentication:* Solutions to handle authentication in USNs include the utilization of biometric methods[28,29], smart cards authentication[30,31], two-factor authentication methods[32,33], and secured brokering hardware [34,36]. The utilization of mobile phone-based biometric authentication methods (e.g., fingerprint sensors, face recognition) combined with other wearable and/or implantable sensors may provide interesting approaches to handle user authentication[35]. The utilization of hardware-based, Trusted Execution Environments (TEEs)[37] can provide solutions for device authentication, especially since TEEs are currently used in mobile phones as a standard feature for network device authentication (e.g., International Mobile Equipment Identity, IMEI)[38].

4.2. System Availability

• *Availability at First-level Integrators:* Avoiding DoS in communication channels between sensors and first-level integrator devices can be achieved using mechanisms such as frequency hopping, repositioning of sensors, modification of protocols, and physical layer jamming avoidance techniques (e.g., directional antennas, spread spectrum, channel diversity)[14]. In the case of battery exhaustion attacks, methods may include the development of power-aware operating systems and frameworks [39,40], techniques for assessing power consumption of an application or a sensing task before downloaded and installed at a first-level integrator device [41,43], as well as approaches that detect an abnormal increase in the power consumption at runtime[44,46]. In the case of detecting operating system vulnerabilities, the following techniques could be used: (1) static analysis (i.e., analysis of source/compiled code before execution by using tools such as Metal[47]); (2) dynamic analysis (i.e., analysis of programs during their execution to detect and document program errors and vulnerabilities[48]); (3) formal methods (i.e., use of mathematical logic and specifications to prove program correctness [49,50]). 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/bug to be undetected for many years [21].

• *Availability at Second-level Integrators:* To deal with availability at second-level integrators, USN systems should focus on addressing the problems of elasticity and denial of service, as mentioned in 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, approaches such as hybrids between client-server and peer-to-peer architectures[3] and cloud-based solutions [60,61] have been proposed. In the case of DoS, the issue is similar to any other service provided on the Internet, therefore countermeasures for traditional network infrastructure and cloud-based environments can be used[62].

• *User Participation:* Salim et al.[51] identified that the successful, large-scale user participation in USNs consists

Table 2. Security issues and solutions for Ubiquitous Sensor Networks (USNs).

Security Issues			**Solutions**	
Data Integrity	Spoofing		Estimation and Filtering	Kridging Clustering Gaussian Mixture Models Clustering
			Anomaly Detection	Support Vector Machines Neural Networks Bayesian Networks Statistical methods
	Authentication	User authentication	Biometric methods Smart cards 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 (directional antennas, spread spectrum, channel diversity)	
		Battery exhaustion attacks	Power-aware Operating Systems Assessing Power consumption of task before installed Anomaly detection for power consumption at runtime	
		Operating System (OS)vulnerabilities	Static analysis Dynamic analysis Formal methods	
	Availability at second-level integrators	Elasticity	Hybrids between client-server and P2P architectures Cloud-based solutions	
		Denial of Service	DoS countermeasures for cloud services and traditional network environments	
	Attacks on user participation		Incentives	Micropayments Altruistic incentives Social incentives

of five steps, namely (1) identify needs and dilemmas; (2) identify stakeholders; (3) identify incentives; (4) gather evidence and experience; (5) provide tools and affordance. USN systems must provide benefits to the well-being of an individual or a community by means of monetary or non-monetary incentives[52] as follows:

- *Micropayments:* these are monetary incentives that pay small fractions of a dollar to users that contribute data to the USN. Micropayments were developed in the 1990's during the explosion of the Web as an incentive to sell online content[53] for user-generated content. In the context of USNs, micropayments were first evaluated by Lee et al.[54] by using algorithms for micropayments 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[6], the Personal Environmental Impact Report (PEIR)[55], and NoiseSPY[56].
- *Social incentives:* In this category the incentives are social or human-centric rewards such as increase of reputation, improved health, or exposure from the interaction with other users with common objectives. Common examples in this group include e-bird[57], fitness application such as Runtastic[58] and game such as Pokemon GO[59].

5. Security Challenges for Ubiquitous Sensor Networks

Human intervention, and trust in the devices, tasks, and task issuers are key aspects in the successful deployment of future USNs. In this context, we identify some of the current challenges that should be addressed to build more robust and secure USNs. These challenges include: (1) trustworthy tasking; (2) data integrity for human-centric USNs; (3) privacy.

• *Trustworthy Tasking:* USNs have been developed under the principle that the sensing task and whoever collects data are trusted. As such, most of the research in securing USNs assumes that threats are coming from the custodians of first-level integrator devices (e.g., by submitting fake data), or an external 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 how to trust the data collection entity, the sensing task, and the security of the device itself, especially given the utilization of COTS devices as integrators and sensors. USN devices could be reprogrammed through a sensing task to steal data or could be used as zombies by botnets to attack external parties[63], or the task may create physical harm to the user (e.g., theft, kidnapping, accidents) [64].

• *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 [65], or there might be multiple sensors of one type (e.g., a heart rate sensor on a chest strap, and another on a smartwatch). Estimation and filtering of variables of interest in addition to redundancy of sensors/multiple first-level integrators as proposed for community-based USNs cannot be utilized because data in human-centric systems from a particular user are 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 the effectiveness of these actions (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.
- Unobtrusive: 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.

• *Privacy:* The ubiquity and use of mobile and Internet-connected devices as first-level integrators present a tradeoff: on one hand it is desired 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. Aspects such as context privacy (i.e., inference about the actions that could be obtained about users from the sensor data), bystander's privacy (i.e., external people's privacy that can be affected when collecting data in the USN), data sharing privacy (i.e., controlling to whom a second-level integrator releases sensor data with), as well as ownership of sensor data remain open, emerging research issues that need further investigation.

6. Conclusion and Future Work

We have reviewed some of the threats and solutions in security for ubiquitous sensor networks. Security issues were grouped into two major categories, namely data integrity and system availability. Although we have discussed some solutions that can be applied to secure USNs, more research is needed to handle several security issues such as trustworthy tasking, data integrity for human-centric USNs, as well as privacy. Given the current rate of adoption of mobile and IoT devices and their utilization in USNs, security will continue to play an important role in the future.

Acknowledgements
Alfredo J. Perez was supported by the US National Science Foundation under award 1560214. Sherali Zeadally was partially supported by a University Research Professorship Award from the University of Kentucky.

References

1. ITU, *ICT Facts and Figures 2016*, available: http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx
2. A. Nordrum, "The internet of fewer things“, *IEEE Spectrum*, vol.53, no.10, 2016, pp. 12-13.
3. A.J. Perez et al., “G-sense: a scalable architecture for global sensing and monitoring” *IEEE Network*, vol. 24, no. 4, 2010, 57-64.
4. M.A. Labrador et al., *“Location-based information systems: developing real-time tracking applications”*, CRC Press, 2010.
5. S.J. Barbeau et al., "A location-aware framework for intelligent real-time mobile applications", *IEEE Pervasive Computing,* vol 10, no 3, 2011, pp. 58-67.
6. D. Mendez et al, “P-sense: A participatory sensing system for air pollution monitoring and control”, *Proc. 2011 IEEE Pervasive Computing and Communications*, 2011, pp.344-347.
7. N. D. Lane et al.,“Urban Sensing Systems: Opportunistic or Participatory?” *Proc. ACM 9th Workshop Mobile Computing Systems*, 2008, pp. 11-16.
8. O.D. Lara et al., “Centinela: A human activity recognition system based on acceleration and vital sign data”, *Pervasive and Mobile Computing*, vol. 8, no. 5, 2012, pp. 717-729.
9. A. Kapadia et al, “Opportunistic sensing: Security challenges for the new paradigm”, *Proc 2009 IEEE Intl. Conf. on Communication Systems and Networks*, 2009, pp. 1-10.
10. P. Gilbert et al., “Toward trustworthy mobile sensing”, *Proc. ACM 11th Workshop Mobile Computing Systems*, 2010, pp. 31-36.
11. Y. Shoukry et al.,“PyCRA: physical challenge-response authentication for active sensors under spoofing attacks”. *Proc. 22nd ACM Conference on Computer and Communications Security (CCS '15)*, 2015, pp. 1004-1015.
12. C. Camara, et al., “Security and privacy issues in implantable medical devices: A comprehensive survey”, *Journal of Biomedical Informatics,* no. 55, 2015, pp. 272-289.
13. M Zhang, et al., “Towards trustworthy medical devices and body area networks”, *Proc. 50th ACM Design Automation Conf.,*, 2013, pp.1 -6.
14. K Pelechrinis et al., “Denial of service attacks in wireless networks: the case of jammers”, *IEEE Communications Surveys & Tutorials*, vol. 13, no. 2, 2011, pp. 245-257.
15. JP Dunning, et al., “Taming the blue beast: a survey of bluetooth-based threats”, *IEEE Security & Privacy*, vol. 8, no. 2, 2010, pp. 20-27.
16. G Madlmayr et al.., “NFC devices: Security and privacy”, *Proc. 3rd IEEE Intl. Conf. Availability, Reliability and Security*, 2008, pp. 642-647.
17. F. Stajano et al., “The resurrecting duckling: security issues for ubiquitous computing”, *IEEE Computer*, vol. 3, no. 4, 2002, 22-26.
18. T. Martin et al. “Denial-of-service attacks on battery-powered mobile computers”, *Proc. 2004 IEEE Pervasive Computing and Communications*, 2004, pp. 309-318.
19. A. Armando et al., “Would You Mind Forking This Process? A Denial of Service Attack on Android (and Some Countermeasures)”, *Proc. IFIP SEC 2012 27th Intl. Conf. Information Security and Privacy*, 2012, pp. 13-24.
20. H. Huang et al., “From system services freezing to system server shutdown in Android: All you need is a loop in an app”. *Proc. 22nd ACM Conference on Computer and Communications Security (CCS '15)*, 2015, pp. 1236-1247.
21. A. Sharabani et al. “Mobile vulnerabilities from data breach to complete shutdown”, *RSAConference* 2015.
22. J.S. Lee, et al “Sell your experiences: a market mechanism based incentive for participatory sensing”, *Proc. 2010 IEEE Pervasive Computing and Communications,* 2010, pp. 60-68.
23. Y. Ma et al., “Elastic Information Management for Air Pollution Monitoring in Large-Scale M2M Sensor Networks”, *Intl. Journal of Distributed Sensor Networks*, vol. 2013, pp. 1-14, 2013.
24. S. Subashini et al., “A survey on security issues in service delivery models of cloud computing”, *Journal of Network and Computer Applications*, vol. 34, no. 1, 2011, pp. 1-11.
25. D. Mendez, et al., “Data interpolation for participatory sensing systems”, *Pervasive and Mobile Computing*, vol. 9, no. 1, 2013, pp. 132-148
26. D. Mendez, et al., “On sensor data verification for participatory sensing systems”, *Journal of Networks, vol. 8 no. 3, 2013, pp. 576-587.*
27. V. Chandola, et al., “Anomaly detection: A survey”, *ACM Computer Surveys*, vol. 41, no. 3, 2009, pp. 1-15.
28. C.Y. Poon, et al. "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health", *IEEE Communications Magazine*, vol. 44, no. 4, 2006, pp. 73-81.

29. N .Henry Jr, et al., “Using bowel sounds to create a forensically-aware insulin pump system”, Proc. 4th USENIX Workshop on Health Information Technology. 2013.
30. O. Mir et al., “A secure user anonymity and authentication scheme using AVISPA for telecare medical information systems”, *Journal of Medical Systems*, vol. 39, no. 9, 2015, pp. 1-16.
31. J.Sorber, “Plug-n-trust: practical trusted sensing for mhealth”, *Proc. 10th ACM Int. Conf. Mobile Systems,Applications and Services*, 2012, pp. 309-322.
32. L. Xu et al. “Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care”, *Journal of medical systems*, vol. 39, no. 2, 2015, pp. 1-9.
33. F. Wu et al., “An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks”, *Multimedia Systems*, vol. 1 no. 11, 2015, pp. 1 - 11.
34. V. Pournaghshband et al., “Securing legacy mobile medical devices, *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. 2007, pp. 163-172.
35. A. Darwish, et al., “Wearable and implantable wireless sensor network solutions for healthcare monitoring”, *Sensors*,vol. 11,no. 6,2011,pp. 5561-5595.
36. A. Dua, et al., “Towards trustworthy participatory sensing*”, Proc. 4th USENIX conference on Hot topics in Security,* 2009, pp .1-8.
37. J.E. Ekberg et al., “The untapped potential of trusted execution environments on mobile devices”, *IEEE Security & Privacy*, vol. 12, no. 4, 2014, pp. 29-37.
38. K. Kostiainen et al., “Old, new, borrowed, blue – a perspective on the evolution of mobile platform security architectures”, *Proc. 1st ACM Conference on Data and Application Security and Privacy (CODASPY)*, 2011.
39. N. Vallina-Rodriguez et al., “ ErdOS: achieving energy savings in mobile OS”. *Proc. 6th ACM Intl. Workshop on Mobile Architecture*. 2011, pp. 37 - 42.
40. A. Merlo et al., “A survey on energy-aware security mechanisms”. *Pervasive and Mobile Computing*. vol. 24, 2015, pp. 77 - 90.
41. M. Dong, et al., “Self-constructive high-rate system energy modeling for battery-powered mobile systems”, *Proc. 9th Intl. Conf. Mobile systems, applications, and services (MobiSys)*, 2011, pp. 335-348.
42. R. Mittal et al., “Empowering developers to estimate app energy consumption”, *Proc. 18th Intl. Conf. on Mobile computing and networking (MobiCom)*, 2012, pp. 317-328.
43. C. Min et al., “PowerForecaster: Predicting Smartphone Power Impact of Continuous Sensing Applications at Pre-installation Time*”, Proc. 13th ACM Conf. Embedded Networked Sensor Systems (SenSys*), 2015, pp. 31 - 44.
44. X. Ma et al., “eDoctor: Automatically Diagnosing Abnormal Battery Drain Issues on Smartphones”, *Proc. 10th USENIX Symposium on Networked Systems Design and Implementation*, 2013, pp. 57-70.
45. A. Pathak et al., “What is keeping my phone awake? : characterizing and detecting no sleep energy bugs in smartphone apps*”, Proc. 10th ACM Intl. Conf. Mobile systems, applications, and services (MobiSys)*, 2012, pp. 267-280.
46. F. Xu, “V-edge: Fast Self-constructive Power Modeling of Smartphones Based on Battery Voltage Dynamics”, *Proc. 10th USENIX Symposium on Networked Systems Design and Implementation*, 2013, pp. 43-55.
47. S.Hallem et al, "A system and language for building system-specific, static analyses", *ACM SIGPLAN Notices*, vol. 37, no. 5, 2002, pp. 69-82.
48. A. Fattori, et al., "Dynamic and transparent analysis of commodity production systems", *Proc. IEEE/ACM Intl. Conf. on Automated software engineering*, 2010, pp. 417-426.
49. G. Holzmann, "The model checker SPIN.*" IEEE Transactions on software engineering*, vol. 23 no. 5, 1997, pp- 279 - 295.
50. S. Gritzalis et al., "Security protocols over open networks and distributed systems: formal methods for their analysis, design, and verification", *Computer Communications*, vol. 22 no. 8, 1999, pp. 697-709.
51. F. Salim et al., “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, 2015, pp. 31-48.
52. L.G. Jaimes et al., “A Survey on Incentive Techniques for Mobile Crowd Sensing”, *IEEE Internet of Things*, vol. 2, no.5, 2015.
53. N. Hardy et al. “The digital silk road. Technical report”, Agorics, Inc., 1993.
54. J.S. Lee et al., “Sell your experiences: a market mechanism based incentive for participatory sensing”, *Proc. IEEE Intl. Conf. Pervasive Computing and Communications*, 2010, pp. 60-68.
55. M. Mun et al., "PEIR, the personal environmental impact report, as a platform for participatory sensing systems research", Proc. 7th Intl. Conf. Mobile Systems, Applications, and Services, 2009, pp. 55-68.
56. E. Kanjo "Noisespy: A real-time mobile phone platform for urban noise monitoring and mapping", *Mobile Networks and Applications* vol. 15 no. 4, 2010, pp. 562-574.
57. A. Wiggins “eBirding: technology adoption and the transformation of leisure into science”,*Proc. 2011 ACM iConference*, 2011, pp. 798-799.
58. Runtastic Inc. https://www.runtastic.com/
59. Niantic Inc. http://www.pokemongo.com/
60. K. Lee et al., “Extending sensor networks into the cloud using amazon web services” , Proc. 2010 IEEE Intl. Conf. on Networked Embedded Systems for Enterprise Applications (NESEA), 2010, pp. 1-7.
61. Y. Xu et al., “Scalable Cloud-Sensor Architecture for the Internet of Things”, *IEEE Internet of Things*. vol. 3, no. 3, 2016, pp. 285-298.
62. O. Osanaiye et al., “Distributed Denial of Service (DDoS) Resilience in Cloud: Review and Conceptual Cloud DDoS Mitigation Framework”, *Journal of Network and Computer Applications*, vol. 67, 2016, pp. 147–165.
63. T. Pultarova, "Webcam hack shows vulnerability of connected devices", *Engineering & Technology* vol. 11 no. 11, 2016, pp.10-10.
64. CBSNews, "Pokemon Go" being used to stage robberies, police say“, available at http://www.cbsnews.com/news/robbery-suspects-using-pokemon-go-to-target-victims-police-say/
65. Zephyr Inc. *Zephyr Bioharness 3*. https://www.zephyranywhere.com