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*

Right click to open a feedback form in a new tab to let us know how this document benefits you.

Follow this and additional works at: https://uknowledge.uky.edu/slis_facpub

Part of the Computer Sciences Commons, and the Library and Information Science Commons

Repository Citation

https://uknowledge.uky.edu/slis_facpub/36

This Article is brought to you for free and open access by the Information Science at UKnowledge. It has been accepted for inclusion in Information Science Faculty Publications by an authorized administrator of UKnowledge. For more information, please contact UKnowledge@lsv.uky.edu.
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.

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...
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\(^5\):

- **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>
<thead>
<tr>
<th>Features</th>
<th>Wireless Sensor Networks</th>
<th>Ubiquitous Sensor Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Computational Capabilities</strong></td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Communication Infrastructure</strong></td>
<td>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.</td>
<td>Devices may have multiple network interfaces, with infrastructure-based networks (e.g. ISPs, cellular networks) and end-to-end TCP/IP communication.</td>
</tr>
<tr>
<td><strong>Communication Security</strong></td>
<td>Cross-layer design for security is needed due to low power and limited computational capabilities.</td>
<td>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).</td>
</tr>
<tr>
<td><strong>Network Management</strong></td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Network Maintenance</strong></td>
<td>Performed by the entity that owns the WSN. Network can be costly to deploy and maintain.</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Scalability</strong></td>
<td>Potentially thousands of devices in a single system.</td>
<td>Potentially billions of devices in a single system.</td>
</tr>
</tbody>
</table>
Table 1. A comparison of features of Wireless Sensor Networks (WSNs) and Ubiquitous Sensor Networks (USNs).

### Architectural Models and Applications of Ubiquitous Sensor Networks

As USNs consist of the following components:

- **Sensor Infrastructure**: The major functionality of these components of the architecture is to collect data. Sensor software and protocols such as Transport Layer Security (TLS) to establish end-to-end secure communication channels between 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.

#### Data Integrity

In USNs, users may have control over several sensors and data collecting devices. Their direct access to these components could be utilized to launch spoofing attacks by submitting false, incorrect, or fake data. 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. 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.

#### 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:

---

Perez, Zeadally, Jabeur / Procedia Computer Science 00 (2015) 000–000
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 kriging, 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\textsuperscript{41,43}, as well as approaches that
detect an abnormal increase in the power consumption at runtime\textsuperscript{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\textsuperscript{47}); (2) dynamic analysis (i.e., analysis of programs during their execution to detect and document program errors and vulnerabilities\textsuperscript{48}); (3) formal methods (i.e., use of mathematical logic and specifications to prove program correctness\textsuperscript{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\textsuperscript{51}.

- **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\textsuperscript{3} and cloud-based solutions\textsuperscript{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\textsuperscript{62}.

- **User Participation:** Salim et al.\textsuperscript{51} identified that the successful, large-scale user participation in USNs consists

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

<table>
<thead>
<tr>
<th>Security Issues</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Integrity</strong></td>
<td>Spooﬁng</td>
</tr>
<tr>
<td></td>
<td>Estimation and Filtering</td>
</tr>
<tr>
<td></td>
<td>Kridging</td>
</tr>
<tr>
<td></td>
<td>Clustering</td>
</tr>
<tr>
<td></td>
<td>Gaussian Mixture Models Clustering</td>
</tr>
<tr>
<td></td>
<td>Anomaly Detection Support Vector Machines</td>
</tr>
<tr>
<td></td>
<td>Neural Networks</td>
</tr>
<tr>
<td></td>
<td>Bayesian Networks</td>
</tr>
<tr>
<td></td>
<td>Statistical methods</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>User authentication</td>
</tr>
<tr>
<td></td>
<td>Biometric methods</td>
</tr>
<tr>
<td></td>
<td>Smart cards authentication</td>
</tr>
<tr>
<td></td>
<td>Two-factor authentication</td>
</tr>
<tr>
<td><strong>Sensor Authentication</strong></td>
<td>Secure brokering hardware</td>
</tr>
<tr>
<td></td>
<td>Trusted Execution Environments</td>
</tr>
<tr>
<td><strong>System Availability</strong></td>
<td>Interference attacks on communication between sensors and first-level</td>
</tr>
<tr>
<td></td>
<td>integrators</td>
</tr>
<tr>
<td></td>
<td>Frequency hopping</td>
</tr>
<tr>
<td></td>
<td>Sensor repositioning</td>
</tr>
<tr>
<td></td>
<td>Protocol modiﬁcation</td>
</tr>
<tr>
<td></td>
<td>Physical layer jamming avoidance (directional antennas, spread spectrum,</td>
</tr>
<tr>
<td></td>
<td>channel diversity)</td>
</tr>
<tr>
<td></td>
<td>Battery exhaustion attacks</td>
</tr>
<tr>
<td></td>
<td>Power-aware Operating Systems</td>
</tr>
<tr>
<td></td>
<td>Assessing Power consumption of task before installed</td>
</tr>
<tr>
<td></td>
<td>Anomaly detection for power consumption at runtime</td>
</tr>
<tr>
<td>**Availability at second-level</td>
<td>Elastici ty</td>
</tr>
<tr>
<td>integrators**</td>
<td>Hybrids between client-server and P2P architectures Cloud-based solutions</td>
</tr>
<tr>
<td></td>
<td>Denial of Service</td>
</tr>
<tr>
<td></td>
<td>DoS countermeasures for cloud services and traditional network environments</td>
</tr>
<tr>
<td></td>
<td>Attacks on user participation</td>
</tr>
<tr>
<td></td>
<td>Incentives</td>
</tr>
<tr>
<td></td>
<td>Micropayments</td>
</tr>
<tr>
<td></td>
<td>Altruistic incentives</td>
</tr>
<tr>
<td></td>
<td>Social incentives</td>
</tr>
</tbody>
</table>

Perez, Zeadally, Jabeur / Procedia Computer Science 00 (2015) 000–000
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 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 for user-generated content. In the context of USNs, micropayments were first evaluated by Lee et al. 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, the Personal Environmental Impact Report (PEIR), and NoiseSPY.

- **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, fitness application such as Runtastic and game such as Pokemon GO.

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, or the task may create physical harm to the user (e.g., theft, kidnapping, accidents).

- **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, 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

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.
64. T. Pultarova, "Webcam hack shows vulnerability of connected devices", Engineering & Technology vol. 11 no. 11, 2016, pp.10-10.