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

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.