Anomaly Detection Using RFID-Based Information Management in an IoT Context

Raúl Parada, Dipartimento di Ingegneria dell’Informazione, Università degli Studi di Padova, Padova, Italy
Joan Melià-Seguí, Estudis d’Informàtica, Multimèdia i Telecomunicació, Internet Interdisciplinary Institute (IN3), Universitat Oberta de Catalunya (UOC), Barcelona, Spain
Rafael Pous, Departament de Tecnologies de la Informació i les Comunicacions, Universitat Pompeu Fabra, Barcelona, Spain

ABSTRACT

IoT-based environments may infer anomalies based on the data processed from their heterogeneous sensors. Within the technologies evolving the IoT concept, nowadays the Radio Frequency Identification (RFID) technology is a de facto standard in areas like retail or logistics. For instance, most retailers attach RFID-labels to their items to avoid stock-out in the inventory or speed up cash processes. Besides identification, RFID provides further RF data which can be used for information management like anomaly detection (i.e. a shoplifting in a RFID loss prevention system). This manuscript presents two IoT scenarios to detect anomalies using multivariate outlier detection methods, uniquely using RFID data. This research empirically evaluates the authors’ proposed methods by reproducing a RFID-enabled store, and the two proposed scenarios. The evaluation achieved a False Positive Rate around 0.1% and a True Positive Rate around 87%.

KEYWORDS

Loss Prevention Systems, Machine Learning, Multivariate, Outlier, Radio Frequency Identification

INTRODUCTION

Nowadays, the rapid advancement in miniaturizing technologies allows an easier adaptation of heterogeneous data generators to our daily lives such as sensors and actuators. The communication between these heterogeneous elements brings up the paradigm of the Internet of Things (IoT) technology. The ubiquity of heterogeneous technologies opens new ways of solving current issues in the context of IoT-based environments. For instance, thanks to data collected by IoT sensors, a wide range of events may be detected such as traffic patterns, citizen preferences, or energy consumption. Moreover, IoT-based scenarios may also infer anomalies based on the information managed by their heterogeneous sensors.

The detection of anomalies in IoT spaces can go from network security breaches to machinery performance, including human activity recognition. Within the technologies evolving the IoT concept, nowadays the Radio Frequency Identification (RFID) technology is well known. The RFID technology allows the identification to item-level through wireless communication. The Ultra High Frequency (UHF) RFID, is defined in the Electronic Product Class 1 Gen2 (EPC Gen2) (EPCglobal, 2013), is the de facto standard in retail. Retailers attach RFID-labels to their items to avoid stock-out in the inventory or speed up cash processes. Besides its own identification, RFID tags generate useful data based on Radio Frequency (RF) indicators such as Received Signal Strength Indicator (RSSI) or tag

DOI: 10.4018/JOEUC.2018070101

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
reading rate. These data may provide useful insights on context-aware information like classifying user-interest. RFID may be also used for anomaly detection, based on managing outlier information.

An IoT-based environment where the management of RFID-based outliers information can be applied to anomaly detection is retail stores. Loss prevention systems are installed in most retails in order to avoid shoplifting or at least to dissuade from doing it. Throughout the years, different technologies to detect theft acts were implemented in loss prevention systems or within the store such as Electronic Article Surveillance (EAS), Closed-circuit television (CCTV), Dye Ampule, and nowadays in RFID. Even with the implementation of disruptive technologies such as RFID, there are still some security issues out of scope from off-the-shelf RFID equipment. Loss prevention systems together with RFID allows the detection and identification of heterogeneous objects within its read range, even those near the gate. That fact can cause an infinite acoustic alarm indicating the loss prevention system is detecting a product within the read range. One solution could be the deactivation of RFID from those particular products. Although the alarm from the loss prevention system would stop, these products would be more vulnerable to thieves for being stolen.

This paper evaluates the implementation of different methods for detecting secured products leaving the loss prevention system zone. By analyzing the RFID system, these stolen heterogeneous objects can be identified as outliers in the data, that is, detecting an anomaly. By definition, outliers are difficult to detect due to their scarcity. Literature provides definitions about outliers. Hawkins (Hawkins, 1980) defines it as “an observation which deviates so much from other observations as to arouse suspicions that it was generated by a different mechanism”. In most of the applications, outliers appear along with a sequence of normal samples where those possible anomalies can be detected by comparing them with previous and posterior data after post-processing the dataset. Nevertheless, that is not suitable in situations where a fast outlier detection is needed.

We envision a retail store equipped with an RFID loss prevention system where even shopliftings occurred near the gate can be detected and the product(s) identified and displayed on a screen. Figure 1 represents a shoplifting event where the user is leaving the retail store without paying a garment located near the gate, and the system detects it. A screen displays the detected product for a faster identification by employees or the security guard.

The overall goal of this work is to improve the state-of-the-art of anomaly detection in IoT spaces based on RFID outliers identification. We provide the following contributions:

- A study of the behavior of RFID tags in movement within the read range of an anti-theft system using RFID technology.
- A comparison of several outlier detection techniques with multivariate RFID data.
- An empirical comparison of two realistic methods to detect anomalies in IoT spaces, in the context of Smart Cities.

The remainder of this paper is organized as follows: Section Motivation & Related Work details the problem motivation and the related state of the art. Outlier detection methods are introduced in Section Anomaly Detection Methodology, Section Outlier detection in an RFID-based scenario presents the IoT scenarios and the features to feed the described methods. We empirically compare the described methods in Section Experiments & Results. Finally, the paper is concluded in Section Conclusion & Future Work, also pointing out future work directions.

MOTIVATION AND RELATED WORK

In the context of Smart Cities, more and more retailers invest in technologies within their stores for providing a smarter environment. While some applications’ goal is to increase sales (i.e. recommender systems) others try to reduce expenses such as loss prevention systems. Retailers secure
Exploring the Measurement of End User Computing Success
[www.igi-global.com/article/exploring-measurement-end-user-computing/55762?camid=4v1a](www.igi-global.com/article/exploring-measurement-end-user-computing/55762?camid=4v1a)

DSOA: A Service Oriented Architecture for Ubiquitous Applications
[www.igi-global.com/chapter/dsoa-service-oriented-architecture-ubiquitous/73218?camid=4v1a](www.igi-global.com/chapter/dsoa-service-oriented-architecture-ubiquitous/73218?camid=4v1a)