Measurement 58 (2014) 468–475

Contents lists available at ScienceDirect

Measurement

journal homepage: www.elsevier.com/locate/measurement

RF fingerprint measurements for the identification of devices in wireless communication networks based on feature reduction and subspace transformation

J.L. Padilla [b], P. Padilla [a,*], J.F. Valenzuela-Valdés [c], J. Ramírez [a], J.M. Górriz [a]

[a] Department of Signal Theory, Telematics and Communications – CITIC, University of Granada, 18071 Granada, Spain
[b] Department of Electronics and Computer Technology – CITIC, University of Granada, 18071 Granada, Spain
[c] Department of Computer and Telematic Systems Engineering, University of Extremadura, 06800 Merida, Spain

ARTICLE INFO

Article history:
Received 9 October 2013
Received in revised form 23 April 2014
Accepted 5 September 2014
Available online 16 September 2014

Keywords:
RF Fingerprint
Subspace transformation
Wireless communications
Network identification

ABSTRACT

This document proposes a radiofrequency (RF) fingerprinting strategy for the proper identification of wireless devices in mobile and wireless networks. The proposed identification methods are based on the extraction of the preamble RF fingerprint of a device and its comparison with a set of already known device RF fingerprints. The identification method combines techniques for feature reduction such as Principal Component Analysis (PCA) and Partial Least Squares regression (PLS), both based on subspace transformation, along with a similarity-based analysis. In this work, a complete procedure for RF fingerprint data extraction and analysis is provided. In addition, some experimentation with commercial Wi-Fi devices is carried out for the methods validation.

1. Introduction

The technological advances in last years have enhanced the development of a variety of systems and services, based on wireless communications. Compared to wired networks and systems, the propagation channel in wireless networks is prone to suffer from interferences or security threats such as signal interception, spoofing or jamming, among others [1,2]. As a consequence, the secure identification of the forming devices of a wireless network is an issue of great concern regarding the network security. One of the most common and harmful security threats is related to jamming attack strategies [1]. Despite the considered jamming modality, affecting either the link layer or the physical one, the key fact to avoid such attacks is to properly identify the jammer. This jamming agent, acting either as a network user or as an external one must not only be identified but also blacklisted. Thus, subsequent attacks coming from this blacklisted jammer can be quickly identified and its jamming effects controlled, neglected or mitigated [2,3].

This paper provides a method for the proper identification of network devices in a network to detect jamming agents. The method is based on the analysis of the radiofrequency (RF) fingerprint of the devices of a wireless network. The premise in RF fingerprinting is that the signals transmitted by a wireless device are repeatedly extractable and unique. As a consequence, they may be used to identify the device when transmitting in the network. Recent works demonstrate that this uniqueness exists, being attributable to various factors: manufacturing, aging, environmental, etc. [4–6].

The manuscript is organized as follows: in Section 2, the basics of RF fingerprinting are provided. Section 3 is devoted to the identification methods based on feature reduction and similarity analysis. In section 4, the experimental setup is presented, along with the test procedure. In section 5, the

* Corresponding author. Tel.: +34 958248899.
E-mail address: pablopadilla@ugr.es (P. Padilla).

http://dx.doi.org/10.1016/j.measurement.2014.09.009
0263-2241/

evaluation and results of the proposed methods are provided. Eventually, in Section 6, conclusions are drawn.

2. RF fingerprinting

The process of identifying wireless transmitters by examining the signal RF characteristics at the beginning of transmission is commonly referred as RF fingerprinting. The analysis and extraction of relevant parameters of the RF signal let define the RF identification data of a wireless device [4]. RF fingerprinting is focused on the registration and storage of the RF features of the signal transmitted by any device in the network. This group of RF features is the fingerprint of the wireless device [4,5].

The procedure for the extraction of the RF fingerprint of a wireless device implies the capture and analysis of the initial preamble of the RF signal [5,6]. In the literature, it can be found a list of parameters to be extracted: the transient waveform, the instantaneous phase or amplitude of the signal, their evolution in time, the signal tendency (first or second order derivative), the transient ramp profiles in a temporal range, etc. [4]. Fig. 1 shows an example of the RF preamble for two different wireless network devices at 2.4 GHz (Wi-Fi). Other issues regarding RF fingerprinting may be found in [7–11].

3. Identification method based on feature extraction and similarity analysis

Once the RF fingerprint of the wireless device is available, it is possible to define a procedure for its analysis and further identification. Some procedures have been proposed in the literature, based on four steps: channel monitoring, signal transient detection (preamble starting location), feature extraction (fingerprint) and classification/identification [6,8]. In this way, the approach proposed in this work combines a reduction in the feature space dimensionality given by each fingerprint with the comparison of each resulting fingerprint sample with a set of already labeled samples.

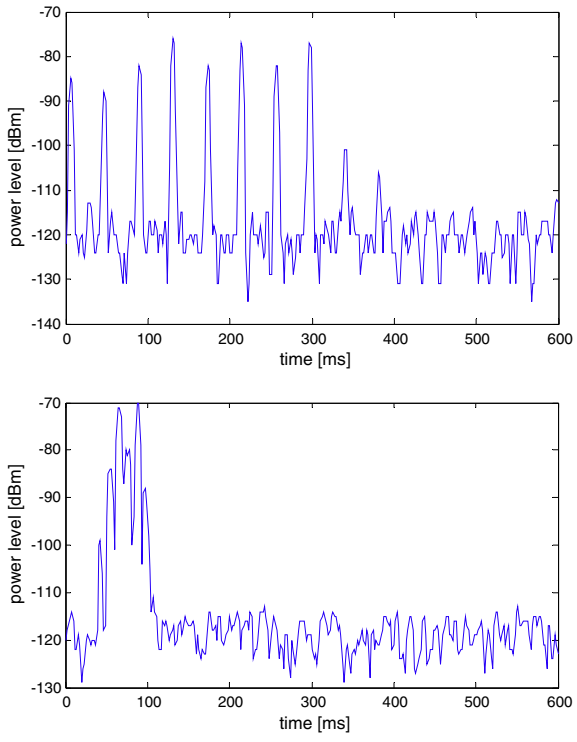

Fig. 1. Example of RF fingerprints of two different Wi-Fi devices.

3.1. Feature extraction and reduction based on PCA and PLS

In most of the cases, not all the available variables in the samples of a dataset contain relevant information. In order to extract the highest amount of information from these samples, feature reduction strategies are followed. The most common reduction methods are those based on latent structures for dimensionality reduction. Standard projection models are Principal Component Analysis (PCA) [12] and Partial Least Squares (PLS) [13]. Both of them are widely applied in data mining and data modeling.

PCA is applied to find the space of maximum variance in the M-dimensional feature space of a $(N \times M)$ zero-mean matrix $\mathbf{X}$, formed by N samples of M variables each one. The space transformation is linear, obtained using a calibration. PCA lets transform the original set of samples into a lower number K of uncorrelated features, called principal components (PCs), according to the expression:

$$\mathbf{X} = \mathbf{T} \cdot \mathbf{P}^{\mathbf{T}} + \mathbf{R} \tag{1}$$

where $\mathbf{T}$ is the $N \times K$ score matrix containing the projection of the original set in the K-subspace, $\mathbf{P}$ is the $M \times K$ matrix containing the K eigenvectors of $\mathbf{X}^T \cdot \mathbf{X}$, and $\mathbf{R}$ is residual of the transformation.

Another useful dimensionality reduction strategy consists on the least squares regression approach, PLS. The linear regression in PLS includes additional information to the original set of data (i.e. labels of the samples in the dataset). PLS is a linear algorithm for modeling the relation between two data sets $\mathbf{X}$ and $\mathbf{Y}$. The aim of the PLS regression is to estimate $\mathbf{Y}$ from a subspace of $\mathbf{X}$ which maximizes its covariance with $\mathbf{Y}$. This subspace of $\mathbf{X}$ is formed by the latent variables (LVs) in $\mathbf{X}$, in a similar way to PCA and its PCs. PLS decomposes the matrix of zero-mean variables $\mathbf{X}$ and the matrix of zero-mean variables $\mathbf{Y}$ into the form:

$$\mathbf{X} = \mathbf{T} \cdot \mathbf{P}^{\mathbf{T}} + \mathbf{E} \tag{2}$$

$$\mathbf{Y} = \mathbf{U} \cdot \mathbf{Q}^{\mathbf{T}} + \mathbf{F} \tag{3}$$

where $\mathbf{T}$ and $\mathbf{U}$ are the score matrices which contain the projections of $\mathbf{X}$ and $\mathbf{Y}$ to the latent subspace, $\mathbf{P}$ and $\mathbf{Q}$ are the regression matrices, and $\mathbf{E}$ and $\mathbf{F}$ are the matrices of residuals of $\mathbf{X}$ and $\mathbf{Y}$, respectively.

Then, the PLS regression is performed according to the expression:

$$\mathbf{Y} = \mathbf{X} \cdot \mathbf{S} \cdot \mathbf{Q}^{\mathbf{T}} + \mathbf{F} \tag{4}$$

$$\mathbf{S} = \mathbf{W} \cdot (\mathbf{P}^{\mathbf{T}} \cdot \mathbf{W})^{-1} \tag{5}$$

where $\mathbf{W}$ is a matrix of weights to be computed in the regression. As already mentioned, in most of the cases,