Identification of Wireless Devices From Their Physical Layer Radio-Frequency Fingerprints

Gianmarco Baldini
European Commission – Joint Research Centre, Italy

Gary Steri
European Commission – Joint Research Centre, Italy

Raimondo Giuliani
European Commission – Joint Research Centre, Italy

INTRODUCTION

Extensive research has been performed in recent years for the identification of wireless devices from their radio frequency (RF) emissions both intentional or unintentional. The term "intentional" is used to identify the RF emissions generated by a wireless device to implement a specific wireless standard. For example, the RF emission of the uplink transmission of a mobile phone, which implements a specific wireless communication standard. The term "unintentional" instead, identifies the RF emissions not directly related to the services offered by the wireless device or the wireless standard, but which are generated due to the operation of the device. For example, the RF emission generated by the electronic components of the device. It is well known in literature that electronic devices can release RF emissions containing information on the operation of the device, thus disclosing sensitive information and generating a security threat. This was one of the primary drivers for the definition of the TEMPEST (Telecommunication and Electronic Material Protected from Emanating Spurious Transmission) standard. TEMPEST refers to the possibility of spying on information systems through leaking emanations, including unintentional radio or electrical signals, sounds, and vibrations (see Rohatgi, P., (2009) for a description of the TEMPEST standard). This issue is also known as emission security (EMSEC), which is a subset of communications security (COMSEC). Since there is already a well-defined standard (i.e., TEMPEST) and a considerable amount of work in EMSEC and COMSEC for "unintentional" emissions, this chapter focuses only on the collection of fingerprints from "intentional" emissions, which are generated by the wireless device while performing its communication function or other services.

The main idea of identifying a wireless device through its RF emissions is that the electronic circuits and the RF components have specific characteristics determined by the production and manufacturing processes. These characteristics, which result in unique differences, can be used to distinguish a wireless device from another. The RF components can include filters, amplifiers, oscillators and other electronics, which are used to compose and transmit the RF signal. The differences on the electronic components are randomly generated, and are mainly due to imperfections in the material or the component itself. For example, the material can have impurities due to the presence of different substances or tiny differences in the soldering or casing of the amplifier, which have an impact in the generation of the RF emissions. These imperfections

DOI: 10.4018/978-1-5225-2255-3.ch533

appear as a subtle modification of the RF signal in space even if the wireless device generates a signal conformant to the standard. For example, a GSM mobile phone can transmit a RF signal with the modulation and range of frequencies defined in the GSM standard, but the physical imperfections will produce minor changes in the amplitude or phase of the signal, which can be collected and processed by a receiver. Note that these minor changes will be substantially the same from statistical point of view in every transmission of the signal and they can be used as a fingerprint of the wireless component (and, consequently, of the GSM mobile phone). As it will be described in the following sections of this article, machine learning or signal processing techniques can be applied to the collected RF signal to extract the imperfections and the related fingerprints.

RF fingerprints can have many applications if the level of identification accuracy is high (e.g., 80-90% or more). The possibility of identifying wireless devices from their RF fingerprints can be used for multi-factor authentication, where a wireless device can be authenticated not only on the basis of conventional cryptographic methods but also by processing the RF fingerprints. Another potential application is to fight against the distribution of counterfeit products. Counterfeit wireless devices (e.g., mobile phones) have electronic components of worst quality in comparison to the genuine ones (Tehranipoor et al., 2015). For example, if a counterfeit phone has been built with low grade RF amplifiers in the uplink transmission chain, it will generate different RF fingerprints compared to an original one.

The structure of this article is the following: the *Background* section provides the main definitions and a literature review on this topic. The section *RF fingerprinting methodology* describes the main workflow for the collection and processing of the RF signals to generate the fingerprints. It also highlights the main outstanding challenges. The section *Solutions and recommendations* identifies and describes the potential approach and techniques that can be used to address the outstanding challenges described in the previous section. In case gaps are identified, the section *Future research directions* describes future possible research developments. Finally, the *Conclusions* section concludes the chapter.

BACKGROUND

The possibility to identify wireless devices from the intrinsic characteristic of their components has grown in importance in the last 10-15 years, due to the improvement in the radio frequency sensors and receivers' capabilities for A/D processing, which have also led to a decrease in price. In fact, the possibility to extract valuable RF fingerprints is possible only when the collected RF signals (i.e., the observables) are digitized with a high degree of clock precision. Many papers describe the use of high-end spectrum analyzers or oscilloscopes to collect and process the RF signal. For example, in Reising et al., (2010), the authors have used a high grade spectrum analyzer to capture and process the signals from a GSM mobile phone. Then the signals were down-converted, digitized and stored as complex in-phase and quadrature (I-Q) components. From the IQ samples, the authors have extracted statistical features, which are representative of the imperfections in the communication path and are used to generate the needed fingerprints. A filter was used to remove bias and unwanted interference, since the latter could degrade or remove the fingerprints. In other words, the collection and processing algorithm would not be able to identify and distinguish the fingerprints in the signal, if the wireless interference had overpowered the fingerprints in the signal. Another important aspect is the need to remove the content related information from the signal, otherwise the fingerprints would be biased by information content. Using this approach only the non-content sections of the GSM bursts are useful for device identification. Figure 1 provides