Types and Origins of Fingerprints

Davide Zanetti, Srdjan Capkun and Boris Danev

Abstract We present a systematic review of physical-layer identification systems and provide a summary of current state-of-the-art techniques. We further review the types of fingerprints that were discussed in prior work and highlight issues that are still open and need to be addressed in future work.

1 Introduction

Devices are traditionally identified by some unique information that they hold such as a public identifier or a secret key. Besides by what they hold, devices can be identified by what they *are*, i.e., by some unique characteristics that they exhibit and that can be observed. Examples include characteristics related to device components such operating system, drivers, clocks, radio circuitry, etc. Analyzing these components for identifiable information is commonly referred to as *fingerprinting*, since the goal is to create fingerprints similar to their biometric counterparts [2].

Here, we focus on techniques that allow wireless devices to be identified by unique characteristics of their analog (radio) circuitry; this type of identification is also referred to as *physical-layer device identification*. More precisely, physical-layer device identification is the process of fingerprinting the analog circuitry of a device by analyzing the device's communication at the physical layer for the purpose of identifying a device or a class of devices. Physical-layer device identification is possible due to hardware imperfections in the analog circuitry introduced at the manufacturing process. These hardware imperfections appear in the transmitted signals which makes them measurable. While more precise manufacturing and quality con-

D. Zanetti (✉)
Institute of Information Security, ETH Zurich, Zürich, Switzerland
e-mail: zanettid@inf.ethz.ch

S. Capkun
e-mail: capkuns@inf.ethz.ch

B. Danev
e-mail: boris.danev@inf.ethz.ch

C. Wang et al. (eds.), *Digital Fingerprinting*,
DOI 10.1007/978-1-4939-6601-1_2

trol could minimize such artifacts, it is often impractical due to significantly higher production costs.[1]

The use of physical-layer device identification has been suggested for defensive and offensive purposes. It has been proposed for intrusion detection [4, 15, 45], access control [3, 48], wormhole detection [33], cloning detection [6, 23], malfunction detection [49], secure localization [44], rogue access point detection [21], etc. It has also been discussed as one of the main hurdles in achieving anonymity and location privacy [29, 30]. Wireless platforms for which physical-layer identification has been shown to be feasible include HF Radio Frequency IDentification (RFID) transponders, UHF (CC1000) sensor nodes, analog VHF transmitters, IEEE 802.11 and 802.15.4 (CC2420) transceivers.

Being able to assess, for a given wireless platform, if physical-layer identification is feasible and under which assumptions, accuracy, and cost is important for the construction of accurate attacker models and consequently for the analysis and design of security solutions in wireless networks. So far, to the best of our knowledge, physical-layer device identification has not been systematically addressed in terms of feasibility, design, implementation and evaluation. This lack of systematization often results in misunderstanding the implications of device identification on the security of wireless protocols and applications.

The goal of this work is to enable a better understanding of device identification and its implications by systematizing the existing research on the topic. We review device identification systems, their design, requirements, and properties, and provide a summary of the current state-of-the-art techniques. We finally summarize issues that are still open and need to be addressed for this topic to be fully understood.

2 Physical-Layer Device Identification

In this section we present the main components of a physical-layer device identification system and discuss the system properties and requirements.

2.1 General View

Physical-layer device identification involves three entities as shown in Fig. 1: a wireless device, a device identification system, and an application system requesting the identification.

Physical-layer device identification systems aim at identifying (or verifying the identity of) devices or their affiliation classes based on characteristics of devices that are observable from their communication at the physical layer. That is, physical-layer device identification systems acquire, process, store, and compare signals generated

[1]This work is largely based on [8].

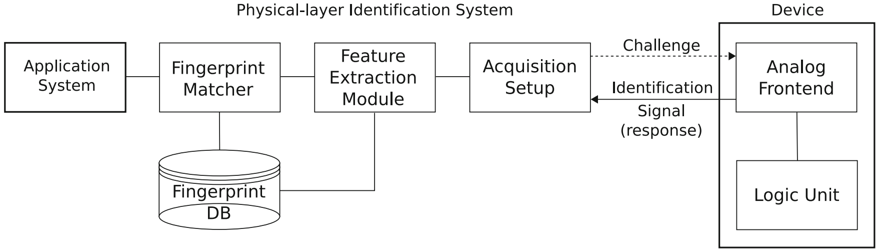

Fig. 1 Entities involved in the physical-layer identification of wireless devices and their main components

from devices during communications with the ultimate aim of identifying (or verifying) devices or their affiliation classes.

Such an identification system can be viewed as a pattern recognition system typically composed of (Fig. 1): an acquisition setup to acquire signals from devices under identification, also referred to as *identification signals*, a feature extraction module to obtain identification-relevant information from the acquired signals, also referred to as *fingerprints*, and a fingerprint matcher for comparing fingerprints and notifying the application system requesting the identification of the comparison results.

Typically, there are two modules in an identification system: one for enrollment and one for identification. During enrollment, signals are captured from either each device or each (set of) class-representative device(s) considered by the application system. Fingerprints obtained from the feature extraction module are then stored in a database (each fingerprint may be linked with some form of unique ID representing the associated device or class). During identification, fingerprints obtained from the devices under identification are compared with reference fingerprints stored during enrollment. The task of the identification module can be twofold: either recognize (identify) a device or its affiliation class from among many enrolled devices or classes (1:N comparisons), or verify that a device identity or class matches a claimed identity or class (1:1 comparison).

The typical operation of an identification module flows as follows: the acquisition setup (Sect. 2.6) acquires the signals transmitted (Sect. 2.3) from the device under identification (Sect. 2.2), which may be a response to a specific challenge sent by the acquisition setup. Then, the feature extraction module (Sect. 2.6) extracts features (Sect. 2.4) from the acquired signals and obtains device fingerprints (Sect. 2.5). Subsequently, the fingerprint matcher (Sect. 2.6) retrieves the reference fingerprints associated to the device under identification from the fingerprint database and compares them against the obtained fingerprints to determine or verify the identity (or the class) of the device under identification. The results of the fingerprint matcher can then be incorporated in the decision making process of the application system requesting the identification (e.g., to grant or not to grant access to a certain location).

The design specification of an identification system usually includes requirements for system accuracy (allowable error rates), computational speed, exception handling, and system cost [2]. We detail those aspects, as well as strategies to improve device identification performance in Sects. 2.7 and 2.8 respectively.

2.2 Device Under Identification

Physical-layer device identification is based on fingerprinting the analog circuitry of devices by observing their radio communication. Consequently, any device that uses radio communication may be subject to physical-layer identification. So far, it has been shown that a number of devices (or classes of devices) can be identified using physical-layer identification. These include analog VHF transmitters [18, 42, 43, 45–47], IEEE 802.11 transceivers [3, 14–16, 25, 40, 48], IEEE 802.15.4 transceivers [5], Bluetooth transceivers [17], UHF sensor nodes [33], HF RFID [6, 37] and UHF RFID [31, 51] transponders. All these devices are composed of antennas, analog frontends, and logic units, but have different levels of complexity, e.g., IEEE 802.11 transceivers (Fig. 2b) are complex whereas RFID transponders are relatively simple (Fig. 2a).

Although what makes a device or a class of devices to be uniquely identified among other devices or classes of devices is known to be due to imperfections introduced at the manufacturing phase of the analog circuitry, the actual device's components causing those have not been always clearly identified in all systems. For example, Toonstra and Kinsner [45, 46] based their identification system on the uniqueness of VHF transmitter's frequency synthesizers (local oscillators), while Danev et al. [6] only suggested that the proposed identification system may rely on imperfections caused by RFID device's antennas and charge pumps. Identifying the exact components may become more difficult when considering relatively-complex devices. In these cases, it is common to identify in the whole analog circuitry, or in a specific sub-circuit, the cause of imperfections. For example, Brik et al. [3] identified IEEE 802.11 transceivers considering modulation-related features; the cause of hard-

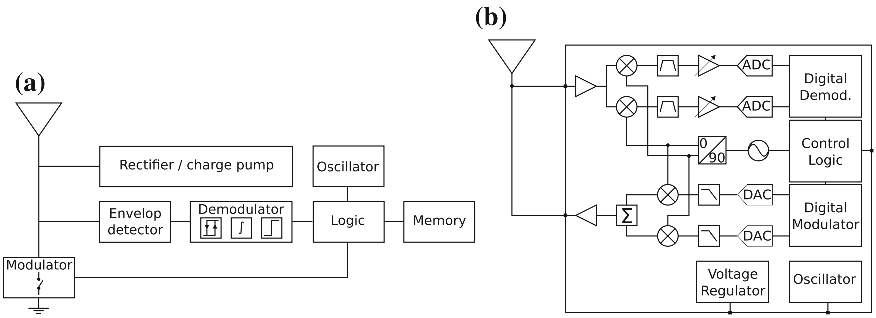

Fig. 2 Block diagrams of two classes of wireless devices. **a** RFID transponder. **b** IEEE 802.11 transceiver

ware artifacts can be then located in the modulator sub-circuit of the transceivers. Table 1 shows a non-exhaustive list of reported identification experiments together with the considered devices and (possible) causes of imperfections. Knowing the components that make devices uniquely identifiable may have relevant implications on both attacks and applications, which makes the investigation on such components an important open problem and research direction.

2.3 Identification Signals

Considering devices communicating through radio signals, i.e., sending data according to some defined specification and protocol, identification at the physical layer aims at extracting unique characteristics from the transmitted radio signals and to use those characteristics to distinguish among different devices or classes of devices. We defined *identification signals* as the signals that are collected for the purpose of identification. Signal characteristics are mainly based on observing and extracting information from the properties of the transmitted signals, like amplitude, frequency, or phase over a certain period of time. These time-windows can cover different parts of the transmitted signals. Mainly, we distinguish between data and non-data related parts. The data parts of signals directly relate to data (e.g., preamble, midamble, payload) transmission, which leads to considered data-related properties such as modulation errors [3], preamble (midamble) amplitude, frequency and phase [25, 34], spectral transformations [17, 25]. Non-data-related parts of signals are not associated with data transmission. Examples include the turn-on transients [45, 46], near-transient regions [35, 50], RF burst signals [6]. Figure 3 shows an non-exhaustive list of signal regions that have been used to identify active wireless transceivers (IEEE 802.11, 802.15.4) and passive transponders (ISO 14443 HF RFID).

2.4 Features

Features are characteristics extracted from identification signals. Those can be *predefined* or *inferred*. Table 1 shows a non-exhaustive list of reported identification experiments together with the deployed features.

Predefined features relate to well-understood signal characteristics. Those can be classified as *in-specification* and *out-specification*. Specifications are used for quality control and specify error tolerances. Examples of in-specification characteristics include modulation errors such as frequency offset, I/Q origin offset, magnitude and phase errors [3], as well as time-related parameters such as the duration of the response [32]. Examples of out-specification characteristics include clock skew [21] and the duration of the turn-on transient [33]. Figure 4a, b show a predefined, in-specification feature used to identify EPC C1G2 RFID tags [52]. The explored feature relates to the tags' transmitted data rate ($BLF = 1/T_{cycle}$). The EPC C1G2

Table 1 Non-exhaustive list of reported identification experiments together with feature-related information

Device[a]	Signal Part[b]	Feature[c]	Type[d]	Cause of Imperfections[e]	Reference
Analog VHF txmtr	Transient	Wavelets	Inferred	Frequency synthesizer	Toonstra and Kinsner [45]
Bluetooth trx	Transient	Wavelets	Inferred	–	Hall et al. [17]
IEEE 802.15.4 trx	Transient	FFT spectra	Inferred	–	Danev and Capkun [5]
IEEE 802.11 trx	Data	Modulation errors	Predefined (in-spec)	Modulator circuitry	Brik et al. [3]
ISO 14443 RFID txpndr	RF burst	FFT spectra	Inferred	Antenna, charge pump	Danev et al. [6]
IEEE 802.11 trx	Data	Clock skew	Predefined (out-spec)	Trx analog circuitry	Jana and Kasera [21]
UHF trx	Transient	Transient length	Predefined (out-spec)	–	Rasmussen and Capkun [33]
IEEE 802.11 trx	Data (preamble)	Wavelets	Inferred	–	Klein et al. [25]
EPC C1G2 RFID txpndr	Data	Timing errors	Predefined (out-spec)	Oscillator	Zanetti et al. [51]
GSM trx	Near-transient, Data	Amp., freq., phase	Predefined	–	Williams et al. [50]

[a] Device: class of considered devices.
[b] Signal Part: the signal part used to extract fingerprints.
[c] Feature: basic signal characteristic.
[d] Type: type of the considered features. *Predefined*—well-understood signal characteristics. *Inferred*—various signal transformations.
[e] Cause of Imperfections: device component likely to be the cause of exploited hardware variations.

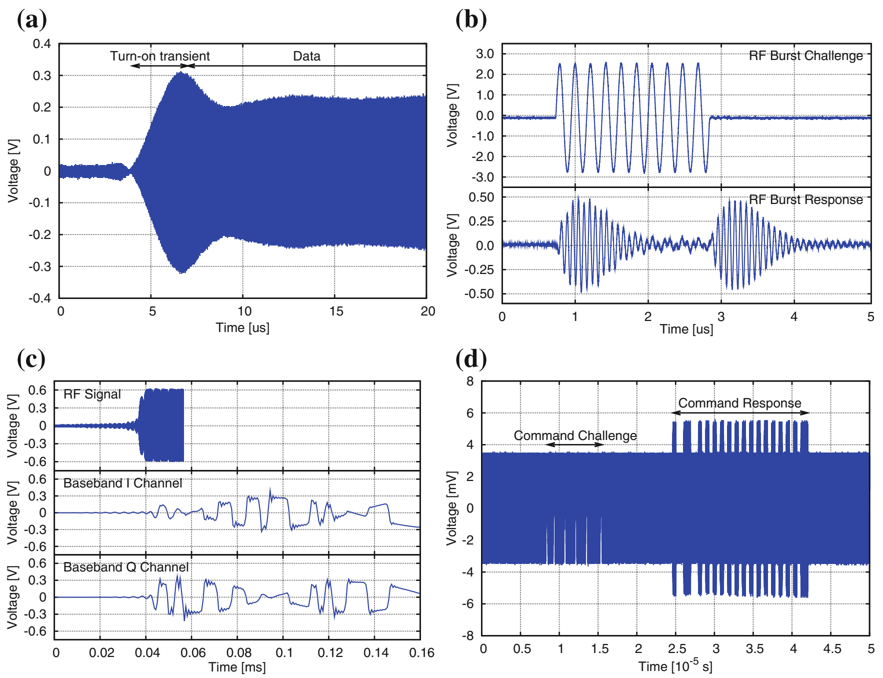

Fig. 3 Several signal parts (regions) commonly used for identification. **a** Turn-on transient of an IEEE 802.15.4 (CC2420) transceiver. **b** ISO 14443 HF RFID tag response to an out-of-specification RF burst signal. **c** Preamble and data modulated regions in IEEE 802.11 transceivers. Signal parts can be either analyzed at RF or at baseband (I/Q). **d** HF/UHF RFID tag response to in-specification commands

standard [11] allows a maximum tolerance of ±22 % around the nominal data rate: different tags transmit at different data rates.

Differently from predefined features, where the considered characteristics are known in advance prior to recording of the signals, we say that features are inferred when they are extracted from signals, e.g., by means of some spectral transformations such as Fast Fourier Transform (FFT) or Discrete Wavelet Transform (DWT), without a-priori knowledge of a specific signal characteristic. For example, wavelet transformations have been applied on signal turn-on transients [17, 18] and different data-related signal regions [25, 26]. The Fourier transformation has also been used to extract features from the turn-on transient [5] and other technology-specific device responses [6]. Figure 4c, d show an inferred feature used to identify EPC C1G2 RFID tags [51]. The explored feature relies on the spectral transformation (FFT) of the tag's data-related signal region: different tags present different signal spectra.

Both predefined and inferred features can be subject to further statistical analysis in order to improve their quality. We discuss more in detail such improvements in Sect. 2.8.

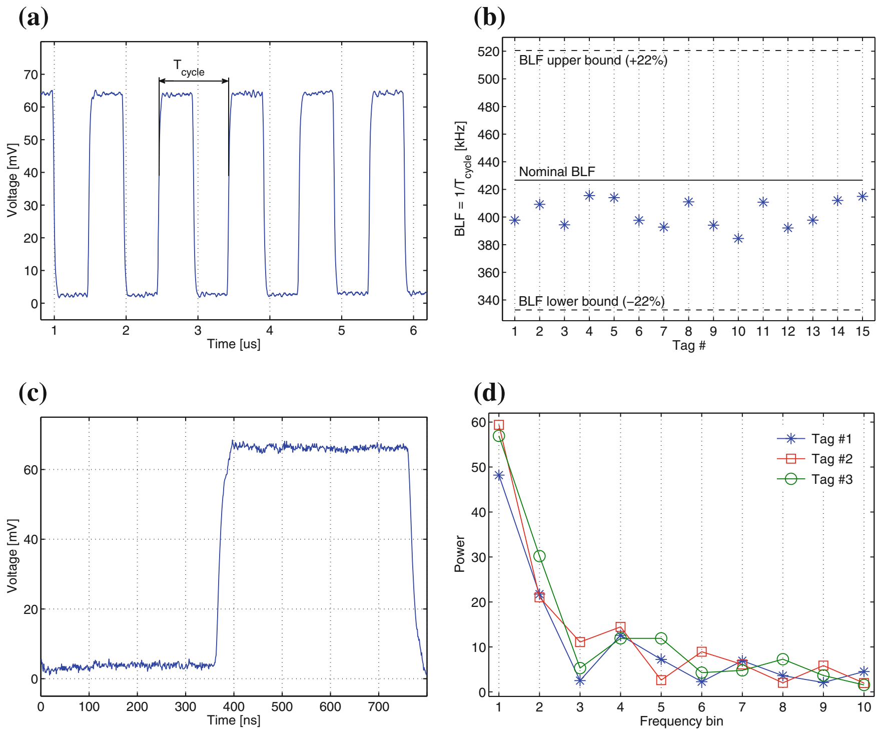

Fig. 4 Different features used for identification. Predefined feature: **a** data-modulated region of EPC C1G2 RFID tags [52] and **b** the considered predefined feature, i.e., the tags' data rate ($BLF = 1/T_{cycle}$) for different tags, as well as the given nominal data rate and tolerances according to the EPC C1G2 specifications [11]. Inferred feature: **c** data-modulated region of EPC C1G2 RFID tags [51] and **d** the considered inferred feature, i.e., the signal spectral transformation (FFT), for different tags

2.5 Device Fingerprints

Fingerprints are sets of features (or combinations of features, Sect. 2.8) that are used to identify devices. The properties that fingerprints need to present in order to achieve practical implementations (adapted from [2]) are:

- Universality: every device (in the considered device-space) should have the considered features.
- Uniqueness: no two devices should have the same fingerprints.
- Permanence: the obtained fingerprints should be invariant over time.
- Collectability: it should be possible to capture the identification signals with existing (available) equipments.

When considering physical-layer identification of wireless devices, we further consider:

- Robustness: fingerprints should not be subject, or at least, they should be evaluated with respect to (i) external environmental aspects that directly influence the signal propagation like radio interferences due to other radio signals, surrounding materials, signal reflections, absorption, etc., as well as positioning aspects like the distance and orientation between the devices under identification and the identification system, and (ii) device-related aspects like temperature, voltage level, and power level. Many types of robustness can be acceptable for a practical identification system. Generally, obtaining robust features helps in building more reliable identification systems.
- Data-dependency: fingerprints can be obtained from features extracted from a specific bit pattern (data-related part of the identification signal) transmitted by a device under identification (e.g., the claimed ID sent in a packet frame). This dependency has particularly interesting implications given that fingerprints are associated to both devices and data transmitted by those devices.

2.6 Physical-Layer Identification System

A physical-layer identification system (Fig. 1) has the tasks to acquire the identification signals (acquisition setup), extract features and obtain fingerprints from the identification signals (feature extraction module), and compare fingerprints (fingerprint matcher). The system may either passively collect identification signals or it may actively challenge devices under identification to produce the identification signals.

The acquisition setup is responsible for the acquisition and digitalization of the identification signals. We refer to a single acquired and digitalized signal as sample. Depending on the considered features to extract, before digitalizing the identification signals, those may be modified, e.g., downconverted. The acquisition process should neither influence nor degrade (e.g., by adding noise) the signals needed for the identification, but should preserve and bring into the digital domain the unique signal characteristics on which the identification relies on. Therefore, high-quality (and expensive) equipment may be necessary. Typically, high-quality measurement equipment has been used to capture and digitize signal turn-on transients [17] and baseband signals [3].

The acquisition setup may also challenge devices under identification to transmit specific identification signals. Under *passive* identification, the acquisition setup acquires the identification signals without interacting with the devices under identification, e.g., identification signals can simply relate to data packets sent by devices under identification during standard communication with other devices. Differently, under *active* identification, the acquisition setup acquires the identification signals after challenging the devices under identification to transmit them. Besides the advantages of obtaining identification signals "on demand", active identification may exploit challenges, and consequently replies that contain identification signals, that are rare, or not present at all, in standard communications. For example, RFID transponders can be challenged with out-specification signal requests as shown in [6, 51].

The feature extraction module is responsible for extracting characteristics from signals that can then be used to distinguish devices or classes of devices. To improve the accuracy of an identification system, the feature extraction module may combine several features together (Sect. 2.8). In the case of predefined features, the feature extraction module implements functions that directly relate an input sample to the features. For example, when considering features like modulation errors, the feature extraction module implements a demodulator and several other functions to quantify these errors. Differently, in the case of inferred features, feature extraction can be a form of dimensionality reduction, where an input sample of dimension (random variables) d containing both relevant and redundant (for the identification) information is reduced to a new sample of dimension $m \leq d$ containing only relevant information. For example, dimensionality reduction techniques have not only been used to reduce the dimensionality [48], but also to find more discriminant subspaces [41]. Reducing the dimensionality of a sample makes it processable and highlights relevant features that may be hidden by noisy dimensions.

The fingerprint matcher compares newly extracted device fingerprints with reference fingerprints enrolled in the fingerprint database. Depending on the application system, it can provide a yes/no answer if a device fingerprint matches a chosen reference fingerprint (identity verification) or a list of devices that the device fingerprint most likely originated from (identification). The matcher is commonly implemented by some distance measure (e.g., Euclidean and Mahalanobis distances) or a more complex pattern recognition classifier such as Probabilistic Neural Networks (PNN) and Support Vector Machines (SVM) [1]. The choice of the matching technique highly depends on the extracted device fingerprints and the requirements of the application system (Sect. 3).

2.7 System Performance and Design Issues

The performance evaluation of a physical-layer device identification system is an important requirement for the system specification. Performance should be investigated in terms of identification accuracy, computational speed, exception handling, cost, and security [2].

The system accuracy is usually expressed in error rates that cannot be theoretically established, but only statistically estimated using test databases of device fingerprints. As physical-layer device identification systems are inherently similar to biometric identification systems, they can be evaluated using already established accuracy metrics [2]. More precisely, the error rates should include the probability of accepting an imposter device (False Accept Rate or FAR) and the probability of rejecting a genuine device (False Reject Rate or FRR). These error rates are usually expressed in the Receiver Operating Characteristic (ROC) that shows the FRRs at different FAR levels. The operating point in ROC, where FAR and FRR are equal, is referred to as the Equal Error Rate (EER). The EER is a commonly used accuracy metric because it is a single value metric and also tells that one recognition system is better than another for the range of FAR/FRR operating points encompassing the EER. For the accuracy at other operating points, one has to consider the ROC. We note that it is also common to provide the FRR for certain benchmark operating points such as FAR of 0.01, 0.1, 1 %.

The ROC and EER are the mostly commonly used metrics for the comparison of identification (verification) systems [13].

We note that physical-layer device identification systems in current state-of-art works (Sect. 3) were often evaluated as classification systems [1]. In a classification system, unknown device fingerprints are classified (correctly or incorrectly) to their respective reference device fingerprints. The error rate is referred to as the classification error rate and shows the ratio of the number of incorrectly classified device fingerprints over all classified fingerprints. The classification error rate does not capture the acceptance of imposters nor the rejection of genuine devices, and therefore is typically not an appropriate metric for the evaluation of the accuracy of identification (verification) systems.

The requirement on computational resources, cost, and exception handling need to be considered as well. In physical-layer identification techniques the complexity of the extracted fingerprints directly relates to the quality and speed of signal acquisition and processing; the higher the quality and speed, the higher the cost. Acquisition setups depend on environmental factors which make exception handling a critical component (e.g., signals may be difficult to acquire from certain locations; alternatively, acquired signals may not have the acceptable quality for feature extraction). Therefore, appropriate procedures need to be devised in order to fulfill given requirements.

Last but not least, the evaluation of a physical-layer device identification system must address related security and privacy issues. Can the device fingerprints be forged and therefore compromise the system? How can one defend against attacks on the integrity of the system? Related works on these systems have largely neglected these issues.

2.8 Improving Physical-Layer Identification Systems

Before enrollment and identification modules can be deployed, the identification system must go through a building phase where design decisions (e.g., features, feature extraction methods, etc.) are tested and, in case, modified to fulfill the requirements on the above-mentioned system properties: accuracy, computational speed, exception handling, and costs.

Although these last three may significantly affect the design decisions, accuracy is usually the most considered property to test and evaluate an identification system. Typically, to improve the accuracy of a (physical-layer) identification system (for wireless devices), i.e., to improve its overall error rates, different strategies can be deployed: (i) acquire signals with multiple acquisition setups, (ii) acquire signals from multiple transmitters on the same device (e.g., when devices are MIMO[2] systems), (iii) consider several acquisitions of the same signals, (iv) consider different signal parts (e.g., both transients and data) and different features, and (v) deploy different approaches for both feature extraction and matching.

So far, neither MIMO systems as devices under identification nor multiple acquisition setups have been considered yet. MIMO systems as devices under identification may offer a wider range of characteristics which the identification process can be based on. This can lead to more robust fingerprints (by analogy with human fingerprints, it is like verifying a human identity by scanning two different fingers). Using multiple acquisition setups may increase the accuracy of the identification, e.g., by acquiring a signal from different location at the same time may lead to more robust fingerprints. The impact of MIMO systems and of multiple acquisition setups is still unexplored.

Considering several acquisitions (samples) of the same signal is the common approach to obtain more reliable fingerprints [5, 17, 33]. Generally, the acquired samples are averaged out into one significant sample, which is then used by the feature extractor module to create fingerprints.

Considering different signal parts, features, and feature extraction methods is often referred to as multi-modal biometrics, where different modalities are combined to increase the identification accuracy and bring more robustness to the identification process [38]. Several works have already considered combining different modalities. For example, different signal properties (e.g., frequency, phase) were used in [3, 17], different signal regions, signal properties and statistics (e.g., skewness, kurtosis) were explored in [25, 35]. Different modalities extracted from device responses to various challenge requests were studied in [6]. The use of more modalities have resulted in significant improvement of the overall device identification accuracy. It should be noted that the above modalities were mostly combined before the feature matching (classification) procedure. Therefore, the combination of different classification techniques remains to be explored [20, 24].

In addition to the above-mentioned strategies to improve the accuracy of an identification system, it is worth to mention *feature selection* and *statistical feature extraction*. Feature selection aims at selecting from a set of features, the sub-set that leads to the best accuracy [19] (that sub-set will then be used in enrollment and identification modules). Statistical feature extraction exploits statistical methods to choose and/or transform features of objects (in our case, devices) such that the similarities

[2]MIMO refers to multiple-input and multiple-output. Such wireless systems use multiple antennas for transmitting and receiving for the purpose of improving communication performance.

between same objects are preserved, while the differences between different objects are enhanced [1]. Statistical feature extraction is a powerful technique to improve the features' discriminant quality.

3 State of the Art

Identification of radio signals gained interest in the early development of radar systems during the World War II [22, 28]. In a number of battlefield scenarios it became critical to distinguish own from enemy radars. This was achieved by visually comparing oscilloscope photos of received signals to previously measured profiles [28]. Such approaches gradually became impractical due to increasing number of transmitters and more consistency in the manufacturing process.

In mid and late 90's a number of research works appeared in the open literature to detect illegally operated radio VHF FM transmitters [4, 18, 45, 46]. Subsequently, physical-layer identification techniques were investigated for device cloning detection [6, 23], defective device detection [49], and access control in wireless personal and local area networks [3, 15, 16, 21, 33]. A variety of physical properties of the transmitted signals were researched and related identification systems proposed.

Here we review the most prominent techniques to physical-layer identification available in the open literature. We structure them in three categories, namely transient-based, modulation-based, and other approaches based on signal part used for feature extraction. For each category, we discuss the works in chronological order. A concise summary is provided in Table 2.

3.1 Transient-Based Approaches

Physical-layer identification techniques that use the turn-on/off transient of a radio signal are usually referred to as transient-based approaches to physical-layer device identification. These approaches require accurate transient detection and separation before feature extraction and matching. The detection and separation of the turn-on transient depend on the channel noise and device hardware and have been shown to be critical to these systems [39, 47].

The open literature on transient-based device identification can be traced back to the early 90s. Toonstra and Kinsner [45, 46] introduced wavelet analysis to characterize the turn-on transients of 7 VHF FM transmitters from 4 different manufacturers. Device fingerprints were composed of wavelet spectra extracted from signal transients captured at the FM discriminator circuit. All extracted fingerprints were correctly classified by means of a genetic algorithm (neural network). Gaussian noise was added to the original transients in order to simulate typical field conditions. Hippenstiel and Payal [18] also explored wavelet analysis by filter banks in order to characterize the turn-on transients of 4 different VHF FM transmitters. They showed

Table 2 Summary of physical-layer device identification techniques

Approach	Signal	Features	Evaluation data			Evaluated factors	Methodology	Error rate
			Device Type	#	Origin[a]			
Toonstra and Kinsner [45]	Transient	Wavelets	Analog VHF txmtr	7	D1	–	Classification	0 %
Ellis and Serinken [10]	Transient	Amplitude, phase	Analog VHF txmtr	28	D1	Fixed distance	Visual inspection	n/a
Tekbas et al. [42]	Transient	Amplitude, phase	Analog VHF txmtr	10	D1	Wide temp. range, voltage and SNR	Classification	5 %
Hall et al. [15]	Transient	Amplitude, phase, power, DWT coeffs.	IEEE 802.11 trx	14	D2	Close proximity and temperature	Classification	8 %
Hall et al. [17]	Transient	Amplitude, phase, power, DWT coeffs.	Bluetooth trx	10	D2	Close proximity	Classification	7 %
Ureten and Serinken [48]	Transient	Amplitude envelope	IEEE 802.11 trx	8	D2	Close proximity	Classification	2 %
Rasmussen and Capkun [33]	Transient	Length, amplitude, DWT coeffs.	UHF trx	10	D3	Close proximity	Classification	30 %
Brik et al. [3]	Data	Frequency, sync, I/Q, magnitude, phase	IEEE 802.11 trx	138	D3	Varied distance and location	Classification	0.34 %

(continued)

Table 2 (continued)

Approach	Signal	Features	Evaluation data			Evaluated factors	Methodology	Error rate
			Device Type	#	Origin[a]			
Jana and Kasera [21]	Data	Clock skew	IEEE 802.11 Access Point	5	D1	Virtual AP, temp. and NTP sync.	Classification, attacks	0 %
Danev and Capkun [5]	Transient	FFT spectra	IEEE 802.15.4 trx	50	D3	Distance, location, voltage, temp.	Verification, attacks	0.24 %
Suski et al. [40]	Preamble	Power spectrum density	IEEE 802.11 trx	3	D3	Proximity, SNR	Classification	13 %
Danev et al. [6]	RF burst	FFT spectra, modulation	ISO 14443 HF RFID txpndr	50	D3	Varied position, distance	Verification	4 %
Periaswamy et al. [31]	Preamble	Minimum power response	EPC C1G2 UHF RFID txpndr	50	D3	fixed position	Verification	5 %
Williams et al. [50]	Data, near transient	Amplitude, frequency, phase, statistics	GSM trx.	16	D1	Fixed position, SNR	Verification	5–20 %

[a]D1: Devices from different manufacturers and some of the same model; D2: Devices from different manufacturers and models; D3: Devices from the same manufacturer and model (identical)

that Euclidean distance was an accurate similarity measure to classify extracted device fingerprints from different manufacturers. Choe et al. [4] presented an automated device identification system based on wavelet and multi-resolution analysis of turn-on transient signals and provided an example of transmitter classification of 3 different transmitters.

Ellis and Serinken [10] studied the properties of turn-on transients exhibited by VHF FM transmitters. They discussed properties of universality, uniqueness, and consistency in 28 VHF FM device profiles characterized by the amplitude and phase of the transients. By visual inspection, the authors showed that there were consistent similarities between device profiles within the same manufacturer and model and device profiles from different models that could not be visually distinguished. Moreover, some devices did not exhibit stable transient profiles during normal operation. The authors suggested that further research is needed to quantify environmental factors (e.g., doppler shift, fading, temperature). Following these recommendations, Tekbas, Serinken and Ureten [42, 43] tested 10 VHF FM transmitters under ambient temperature, voltage, and noise level changes. The device fingerprints were composed of transient amplitude and phase features obtained from the signal complex envelope. A probabilistic neural network (PNN) was used for classifying the fingerprints. The experimental results showed that the system needed to be trained over a wide temperature range and the operational supply-voltage levels in order to achieve low classification error rates of 5 %. Classification accuracy of low-SNR transients could be improved by estimating the SNR and modifying its level in the training phase [43].

Transient-based approaches were also investigated in modern wireless local and personal area networks (WLAN/WPAN), primarily for intrusion detection and access control. Hall et al. [15–17] focused on Bluetooth and IEEE 802.11 transceivers. The authors captured the transient signals of packet transmissions from close proximity (10 cm) with a spectrum analyzer. They extracted the amplitude, phase, in-phase, quadrature, power, and DWT coefficients and combined them in device fingerprints. Classification results on 30 IEEE 802.11 transceivers composed of different models from 6 different manufacturers [14, 16] showed error rates of 0–14 % depending on the model and manufacturer. The average classification error rate was 8 %. The same technique was also applied to a set of 10 Bluetooth transceivers and showed similar classification error rates [17]. The authors also introduced dynamic profiles, i.e., each device fingerprint was updated after some amount of time, in order to compensate internal temperature effects in the considered devices.

Ureten and Serinken [48] proposed extracting the envelope of the instantaneous amplitude of IEEE 802.11 transient signals for device classification. The authors classified signals captured at close proximity from 8 different manufacturers using a probabilistic neural network. The classification error rates fluctuated between 2–4 % depending on the size of the device fingerprints.

In the above works, signal transients were captured at close proximity to the fingerprinting antenna, approximately 10–20 cm. The classification error rates were primarily estimated from a set of different model/manufacturer devices; only a few devices possibly had identical hardware. Physical-layer identification of same model and same manufacturer devices was considered by Rasmussen and Capkun [33]. Each device fingerprint contained the transient length, amplitude variance, number of peaks of the carrier signal, difference between normalized mean and the normalized maximum value of the transient power, and the first DWT coefficient. Experimental results on 10 UHF (Mica2/CC1000) sensor devices with identical hardware showed a classification error rate of 30 % from close proximity. A follow-up work [5] showed that a carefully designed hardware setup with high-end components and statistically selected features can also accurately identify same model and manufacturer sensor devices. The authors built device fingerprints with statistically filtered FFT spectra of transient signals and used Mahalanobis distance as a similarity measure. The system accuracy was evaluated using identity verification on 50 IEEE 802.15.4 (CC2420) Tmote Sky sensor devices from the same model and manufacturer. Low equal error rates (EER) of 0.24 % were achieved with signals captured from distances up to 40 m. The authors also concluded that large fixed distances and variable voltage preserve fingerprint properties, whereas varying distance and antenna polarization distort them enough to significantly decrease the accuracy (EER = 30 %).

3.2 Modulation-Based Approaches

Modulation-based approaches to device identification focus on extracting unique features from the part of the signal that has been modulated, i.e., the data. Such features have only recently being proposed for device identification. More precisely, Brik et al. [3] used five distinctive signal properties of modulated signals, namely the frequency error, SYNC correlation, I/Q origin offset, and magnitude and phase errors as features for physical-layer identification. The latter were extracted from IEEE 802.11b packet frames, previously captured using a high-end vector signal analyzer. Device fingerprints were built using all five features and classified with k-NN and SVM classifiers specifically tuned for the purpose. The system was tested on 138 identical 802.11b NICs and achieved a classification error rate of 3 and 0.34 % for k-NN and SVM classifiers respectively. The signals were captured at distances from 3 to 15 m from the fingerprinting antenna. Preliminary results on varying devices' locations showed that the extracted fingerprints are stable to location changes.

Modulation-based approaches were also applied to classifying RFID devices. Danev et al. [6] showed that the modulation of tag responses of different model ISO 14443 RFID transponders shows distinctive and consistent characteristics when challenged with various out-specification commands. They tested their proposal on RFID transponders from 4 different classes.

3.3 Other Approaches

A number of physical-layer identification techniques have been proposed [6, 21, 40] that could not be directly related to the aforementioned categories. These approaches usually targeted a specific wireless technology and/or exploited additional properties from the signal and logical layer.

Suski et al. [40] proposed using the baseband power spectrum density of the packet preamble to uniquely identify wireless devices. A device fingerprint was created by measuring the power spectrum density (PSD) of the preamble of an IEEE 802.11a (OFDM) packet transmission. Subsequently, device fingerprints were matched by spectral correlation. The authors evaluated the accuracy of their approach on 3 devices and achieved an average classification error rate of 20 % for packet frames with SNR greater than 6 dB. Klein et al. [25, 26] further explored IEEE 802.11a (OFDM) device identification by applying complex wavelet transformations and multiple discriminant analysis (MDA). The classification performance of their technique was evaluated on 4 same model Cisco wireless transceivers. The experimental results showed SNR improvement of approx. 8 dB for a classification error rate of 20 %. Varying SNR and burst detection error were also considered.

Various signal characteristics, signal regions and statistics were recently investigated on GSM devices [34, 35, 50]. The authors used the near-transient and midamble regions of GSM-GMSK burst signals to classify devices from 4 different manufacturers. They observed that the classification error using the midamble is significantly higher than using transient regions. Various factors were identified as potential areas of future work on the identification of GMSK signals. In a follow-up work [35], it has been shown that near-transient RF fingerprinting is suitable for GSM. Additional performance analysis was provided for GSM devices from the same manufacturer in [50]. The analysis revealed that a significant SNR increase (20–25 dB) was required in order to achieve high classification accuracy within same manufacturer devices.

Recently, a number of works investigated physical-layer identification of different classes of RFID [6, 31, 32, 36, 37, 51]. Periaswamy et al. [31, 32] considered fingerprinting of UHF RFID tags. In [31], the authors showed that the minimum power response characteristic can be used to accurately identify large sets of UHF RFID tags. An identification accuracy of 94.4 % (with FAR of 0.1 %) and 90.7 % (with FAR of 0.2 %) was achieved on two independent sets of 50 tags from two manufacturers. Timing properties of UHF RFID tags have been explored in two independent works [32, 51]. The authors showed that the duration of the response can be used to distinguish same manufacturer and type RFID tags independent of the environment. This poses a number of privacy concerns for users holding a number of these tags, e.g., user unauthorized tracking can be achieved by a network of readers with a high accuracy [51].

In the context of HF RFID, Danev et al. [6] explored timing, modulation, and spectral features extracted from device responses to purpose-built in- and out-specification signals. The authors showed that timing and modulation-shape features could only be used to identify between different manufacturers. On the other hand, spectral features would be the preferred choice for identifying same manufacturer and model transponders. Experimental results on 50 identical smart cards and a set of electronic passports showed an EER of 2.43 % from close proximity. Similarly, Romero et al. [36] demonstrated that the magnitude and phase at selected frequencies allow fingerprinting different models of HF RFID tags. The authors validated their technique on 4 models, 10 devices per model. Recently, the same authors extended their technique to enable identification of same model and manufacturer transponders [37]. The above works considered inductive coupled HF RFID tags and the proposed features work from close proximity.

Jana and Kasera [21] proposed an identification technique based on clock skews in order to protect against unauthorized access points (APs) in a wireless local area network. A device fingerprint is built for each AP by computing its clock skew at the client station; this technique has been previously shown to be effective in wired networks [27]. The authors showed that they could distinguish between different APs and therefore detect an intruder AP with high accuracy. The possibility to compute the clock skew relies on the fact that the AP association request contains time-stamps sent in clear.

3.4 Attacking Physical-Layer Device Identification

The large majority of works have focused on exploring feature extraction and matching techniques for physical-layer device identification. Only recently the security of these techniques started being addressed [5, 7, 9]. In these works, attacks on physical-layer identification systems can be divided into *signal replay* and *feature replay* attacks. In the former, the attacker's goal is to observe analog identification signals of a targeted device, capture them in a digital form, and then transmit (replay) these signals towards the identification system by some appropriate means (e.g., through purpose-built devices or more generic ones like software-defined radios [12], high-end signal analyzers, or arbitrary waveform generators). Differently, feature replay attacks aim at creating, modifying, or composing identification signals that reproduce only the features considered by the identification system. Such attacks can be launched by special devices such as arbitrary waveform generators that produce the modified or composed signals, by finding a device that exhibits similar features to the targeted device, or to replicate the entire circuitry of the targeted device or at least the components responsible for the identification features.

Edman and Yener [9] developed impersonation attacks on modulation-based identification techniques [3]. They showed that low-cost software-defined radios [12] could be used to reproduce modulation features (feature replay attacks) and impersonate a target device with a success rate of 50–75 %. Independently, Danev et al. [7] have designed impersonation attacks (both feature and signal replay attacks) on transient and modulation-based approaches using both software-defined radios and high-end arbitrary waveform generators. They showed that modulation-based techniques are vulnerable to impersonation with high accuracy, while transient-based techniques are likely to be compromised only from the location of the target device. The authors pointed out that this is mostly due to presence of wireless channel effects in the considered device fingerprints; therefore the channel needed to be taken into consideration for successful impersonation. In addition, Danev and Capkun [5] showed that their identification system may be vulnerable to hill-climbing attacks if the number of signals used for building the device fingerprint is not carefully chosen. This attack consists of repeatedly sending signals to the device identification system with modifications that gradually improve the similarity score between these signals and a target genuine signal. They also demonstrated that transient-based approaches could easily be disabled by jamming the transient part of the signal while still enabling reliable communication.

3.5 Summary and Conclusion

A detailed look of the state of the art shows a number of observations with respect to the design, properties, and evaluation of physical-layer identification systems.

A broad spectrum of wireless devices (technologies) have been investigated. The devices under identification cover VHF FM transmitters, IEEE 802.11 network access cards (NIC) and access points (AP), IEEE 802.15.4 sensor node devices, Bluetooth mobile phones, and RFID transponders. Identification at the physical layer has been shown to be feasible for all the considered types of devices.

In terms of feature extraction, most works explored inferred features for device identification [5, 10, 15, 40, 42, 45, 48]. Few works used predefined features [3, 21, 33] with only one work [3] exploiting predefined in-specification features. Typically, predefined features would be more controlled by device manufacturers (e.g., standard compliance) and are therefore likely to exhibit less discriminative properties compared to inferred features. The inferred features are however more difficult to discover and study given that purpose-built equipment and tailored analysis techniques are required. Both transient and data parts of the physical-layer communication were used for extracting device fingerprints.

The majority of works used standard classifiers such as Neural Network, Nearest Neighbor, and Support Vector Machines classifiers [1] to classify (match) fingerprints from different devices. Classification error rate was used as a metric of accuracy in [3, 10, 15, 33, 40, 42, 45, 48], while identification (verification) accuracy in terms of FAR, FRR and EER metrics is used in [5, 6]. In Sect. 2.7, we discuss the differences between those metrics and suggest an appropriate usage.

In terms of system evaluation, earlier works mostly considered heterogeneous devices from different manufacturers and models, while recent works focused on the more difficult task of identifying same model and manufacturer devices (see Table 2). In addition to hardware artifacts in the analog circuitry introduced at the manufacturing process, physical-layer identification of devices that present different hardware design, implementation, and were subject to a different manufacturing process may benefit from those differences. Differently, physical-layer identification of devices that present the same hardware design, implementation, and manufacturing process is exclusively based on hardware variability in the analog circuitry introduced at the manufacturing process, which makes the physical-layer identification of those devices a harder task.

Proper investigations on the actual components that make devices uniquely identifiable have been so far neglected. Although in some (few) works these components can be easily identified (e.g., Toonstra and Kinsner [45] based their device identification on signals generated by the local frequency synthesizer), in most of the other works only suggestions were provided (e.g., the device antenna and charge pump [6] or the modulator sub-circuit of the transceiver [3]).

Only few works considered evaluating the robustness of the extracted fingerprints to environment and in-device effects (see Table 2). Although parameters like temperature and voltage (at which the device under identification is powered) were considered, robustness evaluations mainly focused on determine the impact of distance and orientation of the device under identification with respect to the identification system. Obviously, features not (or only minimally) affected by distance and orientation will be easily integrated in real-world applications. Results show that inferred features based on spectral transformations such as Fast Fourier Transform or Discrete Wavelet Transform are particularly sensitive to distance and orientation [5, 6] (i.e., the identification accuracy significantly decreases when considering different distances and orientations), while features less affected by the transmission medium (i.e., the wireless channel) like clock skews or (some) modulation errors [3] are less sensitive.

In general, the proposed system evaluations rarely considered acquisition cost and time, feature extraction overhead and device fingerprint size. For example, some brief notes on feature extraction overhead and fingerprint size can be found in [5, 6] and on signal acquisition time in [3], but they are rather an exception in the reviewed state-of-the-art works.

Security and privacy considerations were largely neglected. Only recently, researchers considered attacks on selected physical-layer techniques [7, 9], but no comprehensive security and privacy analysis has been attempted.

4 Future Research Directions

Although physical-layer identification has been increasingly investigated within the last decade, several questions related to the performance of identification systems, fingerprint robustness, and applicability of physical-layer identification in real-world scenarios are still unanswered. In particular, during the presented work, we highlighted the following aspects:

- The causes of unique identification.
  Identify the components that make devices uniquely identifiable is a difficult task, but have relevant implications on both applications and attacks. Application

systems can benefit from more tailored features and detailed attack analysis, while attackers can use this information for advanced feature replay attacks.

- Robust fingerprints.
  Analyze the robustness of fingerprints with respect to application-related environmental and in-device aspects would help in both understanding the limitations and finding improvements on the considered features. Potential, and currently not-explored areas of improvement include MIMO systems, multiple acquisition setups, and multi-modal fingerprints. Deploying multiple acquisition setups may increase the accuracy of the identification while MIMO systems as devices under identification may offer a wider range of identification features. Considering different signal parts, features, and feature extraction methods and combining them to obtain multi-modal fingerprints may increase the identification accuracy and bring more robustness to the identification process.
- Security and privacy of device identification.
  Attacks on both security and privacy of physical-layer identification entities need to be thoroughly investigated and appropriate countermeasures designed and evaluated. Investigation of data-dependent properties in device fingerprints might be a promising direction to improve the resilience against replay attacks.

5 Conclusion

Physical-layer identification has been investigated on a broad spectrum of wireless technologies, but primarily as a defensive technique in order to enhance wireless security against identity-targeted attacks. The feasibility of physical-layer device identification has been largely neglected in the security analysis of protocols aiming at ensuring device (user) identity and location privacy. Moreover, the proposed techniques often lack proper performance evaluation and their resilience to attacks is rarely analyzed.

By systematizing the main concepts of these systems and analyzing the state-of-the-art approaches in the open literature, we provide a comprehensive overview of physical-layer identification and highlight the different types and origins of fingerprints.

Despite the existence of a number of works on the subject, understanding physical-layer identification in terms of feasibility, accuracy, cost, assumptions, and implications still remains a challenge. Further research is required to address a number of questions such as: what are the exact causes of identification? What is the impact of diversity on the identification accuracy? What are the properties of different physical-layer device fingerprints in terms of robustness and security guarantees? How much information entropy do fingerprints contain? Understanding the exact causes of fingerprinting would enable more tailored pattern analysis techniques and provide insights on how offensive uses could be mitigated. Diversity (e.g., MIMO, multi-modal features) can be exploited for improving the accuracy and increasing the robustness of these systems. Similarly, data-dependent properties could largely enhance the resilience to replay attacks.

References

1. Bishop, C.: Pattern Recognition and Machine Learning. Springer (2006)
2. Bolle, R., Connell, J., Pankanti, S., Ratha, N., Senior, A.: Guide to Biometrics. Springer (2003)
3. Brik, V., Banerjee, S., Gruteser, M., Oh, S.: Wireless device identification with radiometric signatures. In: Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom), pp. 116–127 (2008)
4. Choe, H., Poole, C., Yu, A., Szu, H.: Novel identification of intercepted signals for unknown radio transmitters. Proc. SPIE **2491**, 504–517 (1995)
5. Danev, B., Capkun, S.: Transient-based identification of wireless sensor nodes. In: Proceeding of ACM/IEEE Conference on Information Processing in Sensor Networks (IPSN), pp. 25–36 (2009)
6. Danev, B., Heydt-Benjamin, T.S., Capkun, S.: Physical-layer identification of RFID devices. In: Proceedings of USENIX Security Symposium, pp. 199–214 (2009)
7. Danev, B., Luecken, H., Capkun, S., Defrawy, K.E.: Attacks on physical-layer identification. In: Proceedings of ACM Conference on Wireless Network Security (WiSec), pp. 89–98 (2010)
8. Danev, B., Zanetti, D., Capkun, S.: On physical-layer identification of wireless devices. ACM Comput. Surv. **45**(1), 6:1–6:29 (2012)
9. Edman, M., Yener, B.: Active attacks against modulation-based radiometric identification. Technical report 09-02, Rensselaer Institute of Technology (August 2009)
10. Ellis, K., Serinken, N.: Characteristics of radio transmitter fingerprints. Radio Sci. **36**, 585–597 (2001)
11. EPCglobal: UHF Class 1 Gen 2 standard v. 1.2.0 (2008)
12. Ettus, M.: Universal software defined radio (USRP) (2007). http://www.ettus.com/
13. FVC: Fingerprint Verification Competition FVC (2006). http://bias.csr.uni-bo.it/fvc2006/
14. Hall, J.: Detection of rogue devices in wireless networks. Ph.D. thesis (2006)
15. Hall, J., Barbeau, M., Kranakis, E.: Enhancing intrusion detection in wireless networks using radio frequency fingerprinting. In: Proceedings of Communications, Internet, and Information Technology (CIIT), pp. 201–206 (2004)
16. Hall, J., Barbeau, M., Kranakis, E.: Radio frequency fingerprinting for intrusion detection in wireless networks. Manuscript (2005). http://wiki.uni.lu/secan-lab/Hall2005.html
17. Hall, J., Barbeau, M., Kranakis, E.: Detecting rogue devices in Bluetooth networks using radio frequency fingerprinting. In: Proceedings of IASTED International Conference on Communications and Computer Networks (CCN), pp. 108–113 (2006)
18. Hippenstiel, R., Payal, Y.: Wavelet based transmitter identification. In: Proceedings of International Symposium on Signal Processing and Its Applications (ISSPA), pp. 740–742 (1996)
19. Jain, A., Zongker, D.: Feature selection: evaluation, application, and small sample performance. IEEE Trans. Pattern Anal. Mach. Intell. **19**(2), 153–158 (1997)
20. Jain, A.K., Duin, R.P.W., Mao, J.: Statistical pattern recognition: a review. IEEE Trans. Pattern Anal. Mach. Intell. **22**(1), 4–37 (2000)
21. Jana, S., Kasera, S.K.: On fast and accurate detection of unauthorized wireless access points using clock skews. In: Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom), pp. 104–115 (2008)
22. Jones, R.: Most Secret War: British Scientific Intelligence 1939–1945. Hamish Hamilton (1978)
23. Kaplan, D., Stanhope, D.: Waveform collection for use in wireless telephone identification. US Patent 5999806 (1999)

24. Kittler, J., Hatef, M., Duin, R., Matas, J.: On combining classifiers. IEEE Trans. Pattern Anal. Mach. Intell. **20**(3), 226–239 (1998)
25. Klein, R.W., Temple, A., Mendenhall, M.J.: Application of wavelet-based RF fingerprinting to enhance wireless network security. Secur. Commun. Netw. **11**(6), 544–555 (2009)
26. Klein, R.W., Temple, M.A., Mendenhall, M.J.: Application of wavelet denoising to improve OFDM-based signal detection and classification. Secur. Commun. Netw. **3**(1), 71–82 (2010)
27. Kohno, T., Broido, A., Claffy, K.: Remote physical device fingerprinting. IEEE Trans. Dependable Secure Comput. **2**(2), 93–108 (2005)
28. Margerum, D.: Pinpointing Location Of Hostile Radars. Microwaves (1969)
29. Mitra, M.: Privacy for RFID systems to prevent tracking and cloning. Int. J. Comput. Sci. Netw. Secur. **8**(1), 1–5 (2008)
30. Pang, J., Greenstein, B., Gummadi, R., Seshan, S., Wetherall, D.: 802.11 user fingerprinting. In: Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom), pp. 99–110 (2007)
31. Periaswamy, S.C.G., Thompson, D., Di, J.: Fingerprinting RFID tags. IEEE Trans. Dependable Secure Comput. **8**(6), 938–943 (2011)
32. Periaswamy, S.C.G., Thompson, D.R., Romero, H.P.: Fingerprinting radio frequency identification tags using timing characteristics. In: Proceedings of Workshop on RFID Security (RFIDSec Asia) (2010)
33. Rasmussen, K., Capkun, S.: Implications of radio fingerprinting on the security of sensor networks. In: Proceedings of International ICST Conference on Security and Privacy in Communication Networks (SecureComm) (2007)
34. Reising, D.R., Temple, M.A., Mendenhall, M.J.: Improved wireless security for GMSK-based devices using RF fingerprinting. Int. J. Electron. Secur. Digit. Forensics **3**(1), 41–59 (2010)
35. Reising, D.R., Temple, M.A., Mendenhall, M.J.: Improving intra-cellular security using air monitoring with RF fingerprints. In: Proceedings of IEEE Wireless Communications and Networking Conference (WCNC) (2010)
36. Romero, H.P., Remley, K.A., Williams, D.F., Wang, C.M.: Electromagnetic measurements for counterfeit detection of radio frequency identification cards. IEEE Trans. Microwave Theory Tech. **57**(5), 1383–1387 (2009)
37. Romero, H.P., Remley, K.A., Williams, D.F., Wang, C.M., Brown, T.X.: Identifying RF identification cards from measurements of resonance and carrier harmonics. IEEE Trans. Microw. Theory Tech. **58**(7), 1758–1765 (2010)
38. Ross, A., Jain, A.: Multimodal biometrics: an overview. In: Proceedings of European Signal Processing Conference (EUSIPCO), pp. 1221–1224 (2004)
39. Shaw, D., Kinsner, W.: Multifractal modeling of radio transmitter transients for classification. In: Proceedings of IEEE Conference on Communications, Power and Computing (WESCANEX), pp. 306–312 (1997)
40. Suski, W., Temple, M., Mendenhall, M., Mills, R.: Using spectral fingerprints to improve wireless network security. In: Proceedings of IEEE Global Communications Conference (GLOBECOM), pp. 1–5 (2008)
41. Suski, W.C., Temple, M.A., Mendenhall, M.J., Mills, R.F.: Radio frequency fingerprinting commercial communication devices to enhance electronic security. Int. J. Electron. Secur. Digital Forensics **1**(3), 301–322 (2008)
42. Tekbas, O., Ureten, O., Serinken, N.: An experimental performance evaluation of a novel radio-transmitter identification system under diverse environmental conditions. Can. J. Electr. Comput. Eng. **29**(3), 203–209 (2004)
43. Tekbas, O., Ureten, O., Serinken, N.: Improvement of transmitter identification system for low SNR transients. Electron. Lett. **40**(3), 182–183 (2004)
44. Tippenhauer, N.O., Rasmussen, K.B., Pöpper, C., Capkun, S.: Attacks on public WLAN-based positioning. In: Proceedings of ACM/USENIX International Conference on Mobile Systems, Applications and Services (MobiSys), pp. 29–40 (2009)
45. Toonstra, J., Kinsner, W.: Transient analysis and genetic algorithms for classification. In: Proceedings of IEEE Conference on Communications, Power, and Computing (WESCANEX), pp. 432–437, vol. 2 (1995)

46. Toonstra, J., Kinsner, W.: A radio transmitter fingerprinting system ODO-1. In: Proceedings of Canadian Conference on Electrical and Computer Engineering, pp. 60–63, vol. 1 (1996)
47. Ureten, O., Serinken, N.: Detection of radio transmitter turn-on transients. Electron. Lett. **35**, 1996–1997 (2007)
48. Ureten, O., Serinken, N.: Wireless security through RF fingerprinting. Can. J. Electr. Comput. Eng. **32**(1), 27–33 (2007)
49. Wang, B., Omatu, S., Abe, T.: Identification of the defective transmission devices using the wavelet transform. IEEE Trans. Pattern Anal. Mach. Intell. **27**(6), 696–710 (2005)
50. Williams, M., Temple, M., Reising, D.: Augmenting bit-level network security using physical layer RF-DNA fingerprinting. In: Proceedings of IEEE Global Telecommunications Conference (GLOBECOM), pp. 1–6 (2010)
51. Zanetti, D., Danev, B., Capkun, S.: Physical-layer identification of UHF RFID tags. In: Proceedings of ACM Conference on Mobile Computing and Networking (MOBICOM), pp. 353–364 (2010)
52. Zanetti, D., Sachs, P., Capkun, S.: On the practicality of UHF RFID fingerprinting: how real is the RFID tracking problem? In: Proceedings of Privacy Enhancing Technologies Symposium (PETS), pp. 97–116 (2011)

http://www.springer.com/978-1-4939-6599-1

Digital Fingerprinting
Wang, C.; Gerdes, R.M.; Guan, Y.; Kasera, S.K. (Eds.)
2016, IX, 189 p. 46 illus., Hardcover
ISBN: 978-1-4939-6599-1