# On Physical-Layer Identification of Wireless Devices

BORIS DANEV, DAVIDE ZANETTI, and SRDJAN CAPKUN, ETH Zurich, Switzerland

Physical-layer device identification aims at identifying wireless devices during radio communication by exploiting unique characteristics of their analog (radio) circuitry. This work systematizes the existing knowledge on this topic in order to enable a better understanding of device identification, its implications on the analysis and design of security solutions in wireless networks and possible applications. We therefore present a systematic review of physical-layer identification systems and provide a summary of current state-of-the-art techniques. We further present a classification of attacks and discuss the feasibility, limitations, and implications in selected applications. We also highlight issues that are still open and need to be addressed in future work.

Categories and Subject Descriptors: C.2.0 [**Computer Communication Networks**]: General—*Security and protection (e.g., firewalls)*

General Terms: Security, Design

Additional Key Words and Phrases: Identification, fingerprinting, physical layer, wireless device, security, privacy

**ACM Reference Format:**
Danev, B., Zanetti, D., and Capkun, S. 2011. On physical-layer identification of wireless devices. ACM Comput. Surv. 45, 1, Article 6 (November 2012), 29 pages.
DOI = 10.1145/2379776.2379782 http://doi.acm.org/10.1145/2379776.2379782

## 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*, that is, 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 [Bolle et al. 2003].

In this work, 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

This work was partially supported by the Zurich Information Security Center.
Authors' addresses: B. Danev, D. Zanetti, and S. Capkun, Department of Computer Science, ETH Zurich, Universitätstrasse 6, 8092 Zurich, Switzerland; email: {bdanev, zanettid, capkuns}@inf.ethz.ch.

DOI 10.1145/2379776.2379782 http://doi.acm.org/10.1145/2379776.2379782

measurable. While more precise manufacturing and quality control could minimize such artifacts, it is often impractical due to significantly higher production costs.

The use of physical-layer device identification has been suggested for defensive and offensive purposes. It has been proposed for intrusion detection [Toonstra and Kinsner 1995; Choe et al. 1995; Hall et al. 2004], access control [Ureten and Serinken 2007b; Brik et al. 2008], wormhole detection [Rasmussen and Capkun 2007], cloning detection [Kaplan and Stanhope 1999; Danev et al. 2009], malfunction detection [Wang et al. 2005], secure localization [Tippenhauer et al. 2009], rogue access point detection [Jana and Kasera 2008], etc. It has also been discussed as one of the main hurdles in achieving anonymity and location privacy [Pang et al. 2007; Mitra 2008]. 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 therefore 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 further present a classification of attacks on device identification systems and discuss their feasibility, limitations, and implications in selected applications. We finally summarize issues that are still open and need to be addressed for this topic to be fully understood. To the best of our knowledge, this work is the first to review and analyze the existing knowledge on physical-layer device identification and make explicit its assumptions and implications on the security of wireless networks.

The remainder of this article is organized as follows. In Section 2, we present the main components of a physical-layer device identification system and discuss the system properties and requirements. We summarize the state of the art in Section 3. In Section 4, we classify attacks on physical-layer device identification systems, and in Section 5, we analyze the implications of physical-layer device identification and related attacks in selected applications. Finally, we present alternative approaches to device identification in Section 7 and conclude the article in Section 8.

## 2. PHYSICAL-LAYER DEVICE IDENTIFICATION

### 2.1. General View

Physical-layer device identification involves three entities as shown in Figure 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 from devices during communications with the ultimate aim of identifying (or verifying) devices or their affiliation classes.

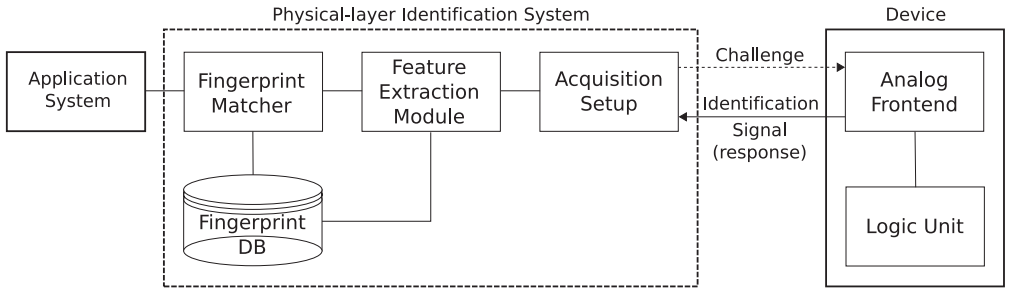


Fig. 1. Entities involved in the physical-layer identification of wireless devices and their main components.

Such an identification system can be viewed as a pattern recognition system typically composed of (Figure 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 (Section 2.6) acquires the signals transmitted (Section 2.3) from the device under identification (Section 2.2), which may be a response to a specific challenge sent by the acquisition setup. Then, the feature extraction module (Section 2.6) extracts features (Section 2.4) from the acquired signals and obtains device fingerprints (Section 2.5). Subsequently, the fingerprint matcher (Section 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 [Bolle et al. 2003]. We detail those aspects, as well as strategies to improve device identification performance in Sections 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 [Toonstra and Kinsner

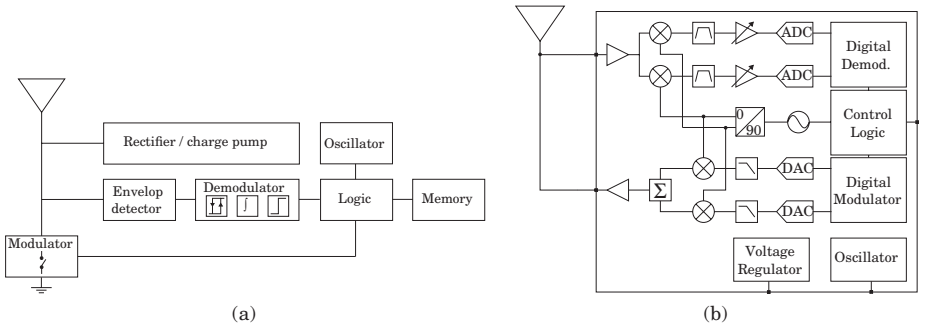


Fig. 2. Block diagrams of two classes of wireless devices. (a) RFID transponder. (b) IEEE 802.11 transceiver.

1995, 1996; Hippenstiel and Payal 1996; Ureten and Serinken 2007a; Tekbas et al. 2004a, 2004b], IEEE 802.11 transceivers [Hall et al. 2004, 2005; Hall 2006; Ureten and Serinken 2007b; Brik et al. 2008; Suski et al. 2008a; Klein et al. 2009], IEEE 802.15.4 transceivers [Danev and Capkun 2009], Bluetooth transceivers [Hall et al. 2006], UHF sensor nodes [Rasmussen and Capkun 2007], HF RFID [Danev et al. 2009; Romero et al. 2010] and UHF RFID [Periaswamy et al. 2010a; Zanetti et al. 2010] transponders. All these devices are composed of antennas, analog frontends, and logic units, but have different levels of complexity, for example, IEEE 802.11 transceivers (Figure 2(b)) are complex whereas RFID transponders are relatively simple (Figure 2(a)).

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 [1995, 1996] based their identification system on the uniqueness of VHF transmitter's frequency synthesizers (local oscillators), while Danev et al. [2009] 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. [2008] identified IEEE 802.11 transceivers considering modulation-related features; the cause of hardware artifacts can be then located in the modulator subcircuit of the transceivers. Table I shows a nonexhaustive 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 (Sections 4 and 5), which makes the investigation on such components an important open problem and research direction.

### 2.3. Identification Signals

Considering devices communicating through radio signals, that is, 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 nondata related parts. The data

Table I. Nonexhaustive List of Reported Identification Experiments Together with Feature-Related Information

| Device | Signal Part | Feature | Type | Cause of Imperfections | Reference |
|---|---|---|---|---|---|
| Analog VHF txmtr | Transient | Wavelets | Inferred | Frequency synthesizer | [Toonstra and Kinsner 1995] |
| Bluetooth trx | Transient | Wavelets | Inferred | - | [Hall et al. 2006] |
| IEEE 802.15.4 trx | Transient | FFT spectra | Inferred | - | [Danev and Capkun 2009] |
| IEEE 802.11 trx | Data | Modulation errors | Predefined (in-spec) | Modulator circuitry | [Brik et al. 2008] |
| ISO 14443 RFID txpndr | RF burst | FFT spectra | Inferred | Antenna, charge pump | [Danev et al. 2009] |
| IEEE 802.11 trx | Data | Clock skew | Predefined (out-spec) | Trx analog circuitry | [Jana and Kasera 2008] |
| UHF trx | Transient | Transient length | Predefined (out-spec) | - | [Rasmussen and Capkun 2007] |
| IEEE 802.11 trx | Data (preamble) | Wavelets | Inferred | - | [Klein et al. 2009] |
| EPC C1G2 RFID txpndr | Data | Timing errors | Predefined (out-spec) | Oscillator | [Zanetti et al. 2010] |
| GSM trx | Near-transient, Data | Amp., freq., phase | Predefined | - | [Williams et al. 2010] |

Device: class of considered devices; Signal Part: the signal part used to extract fingerprints; Feature: basic signal characteristic; Type: type of the considered features. *predefined* - well-understood signal characteristics. *inferred* - various signal transformations; Cause of Imperfections: device component likely to be the cause of exploited hardware variations.

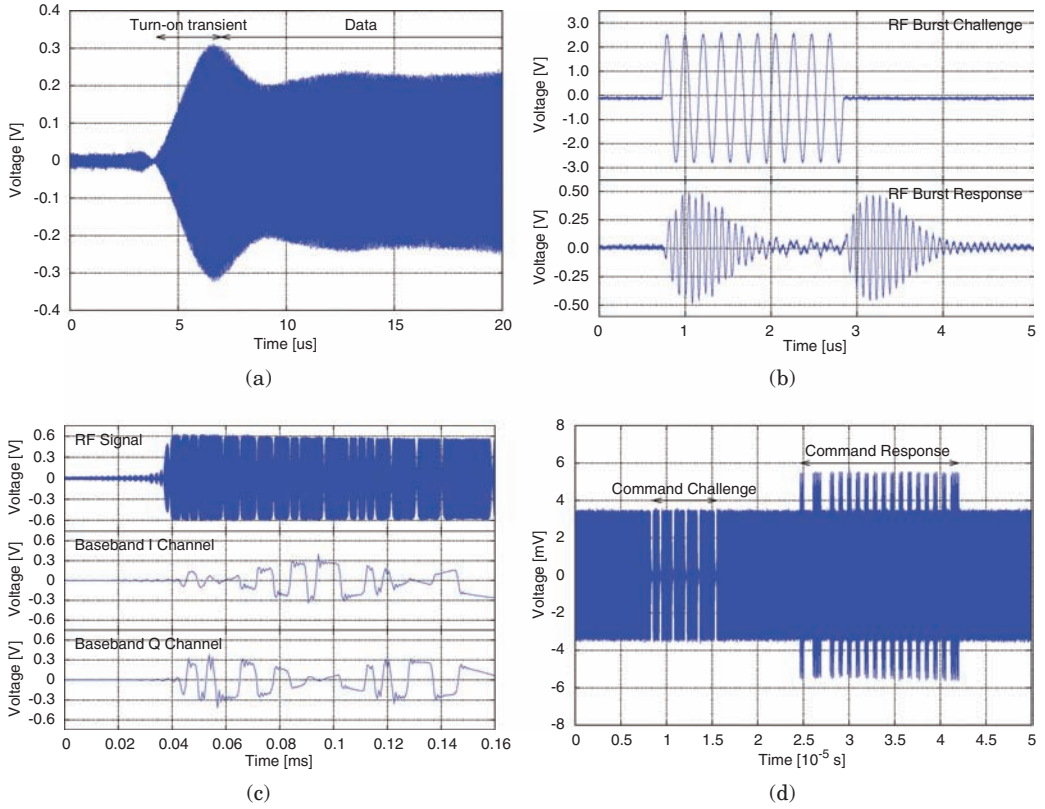


Fig. 3. Several signal parts (regions) commonly used for identification: (a) Turn-on transient of a IEEE 802.15.4 (CC2420) transceiver. (b) ISO 14443 HF RFID tag response to an out-of-specification RF burst signal. (c) Preamble and data modulated regions in IEEE 802.11 transceivers. Signal parts can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

parts of signals directly relate to data (e.g., preamble, midamble, payload) transmission, which leads to considered data-related properties such as modulation errors [Brik et al. 2008], preamble (midamble) amplitude, frequency and phase [Klein et al. 2009; Reising et al. 2010a], spectral transformations [Hall et al. 2006; Klein et al. 2009]. Non-data-related parts of signals are not associated with data transmission. Examples include the turn-on transients [Toonstra and Kinsner 1995, 1996], near-transient regions [Reising et al. 2010b; Williams et al. 2010], RF burst signals [Danev et al. 2009]. Figure 3 shows an nonexhaustive 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 I shows a nonexhaustive 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 [Brik et al. 2008], as well as time-related parameters such as the duration

of the response [Periaswamy et al. 2010b]. Examples of out-specification characteristics include clock skew [Jana and Kasera 2008] and the duration of the turn-on transient [Rasmussen and Capkun 2007].

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, for example, 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 [Hippenstiel and Payal 1996; Hall et al. 2006] and different data-related signal regions [Klein et al. 2009, 2010]. The Fourier transformation has also been used to extract features from the turn-on transient [Danev and Capkun 2009] and other technology-specific device responses [Danev et al. 2009].

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 Section 2.8.

### 2.5. Device Fingerprints

Fingerprints are sets of features (or combinations of features, Section 2.8) that are used to identify devices. The properties that fingerprints need to present in order to achieve practical implementations (adapted from Bolle et al. [2003]) 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 (detailed in Section 5) 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 (Figure 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, for example, 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 [Hall et al. 2006] and baseband signals [Brik et al. 2008].

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, for example, 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 Danev et al. [2009] and Zanetti et al. [2010].

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 (Section 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 [Ureten and Serinken 2007b], but also to find more discriminant subspaces [Suski et al. 2008b]. 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) [Bishop 2006]. The choice of the matching technique highly depends on the extracted device fingerprints and the requirements of the application system. (Section 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 [Bolle et al. 2003].

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 [Bolle et al. 2003]. 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 [FVC 2006].

We note that physical-layer device identification systems in current state-of-art works (Section 3) were often evaluated as classification systems [Bishop 2006]. 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. In Section 4, we classify the attacks on physical-layer identification systems and in Section 5, we discuss their implications on selected applications.

### 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 previously 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), that is, 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[1] 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, for example, 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 [Hall et al. 2006; Rasmussen and Capkun 2007; Danev and Capkun 2009]. 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 [Ross and Jain 2004]. Several works have already considered combining different modalities. For example, different signal properties (e.g., frequency, phase) were used in Hall et al. [2006] and Brik et al. [2008], different signal regions, signal properties and statistics (e.g., skewness, kurtosis) were explored in Klein et al. [2009] and Reising et al. [2010b]. Different modalities extracted from device responses to various challenge requests were studied in Danev et al. [2009]. The use of more modalities have resulted in significant improvement of the overall device identification accuracy. It should be noted that these modalities were mostly combined before the feature matching (classification) procedure. Therefore, the combination of different classification techniques remains to be explored [Kittler et al. 1998; Jain et al. 2000].

In addition to the previously mentioned strategies to improve the accuracy of an identification system, it is worth to mention *feature selection* and *statistic feature extraction*. Feature selection aims at selecting from a set of features, the subset that leads to the best accuracy [Jain and Zongker 1997] (that subset 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 between same objects are preserved, while the differences between different objects are enhanced [Bishop 2006]. 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 [Margerum 1969; Jones 1978]. In a number of battlefield scenarios it became critical to distinguish own from enemy radars. This was achieved by visualy comparing oscilloscope photos of received signals to previously measured

[1]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.

profiles [Margerum 1969]. Such approaches gradually became impractical due to increasing number of transmitters and more consistency in the manufacturing process.

In mid- and late-90s a number of research works appeared in the open literature to detect illegally operated radio VHF FM transmitters [Toonstra and Kinsner 1995, 1996; Hippenstiel and Payal 1996; Choe et al. 1995]. Subsequently, physical-layer identification techniques were investigated for device cloning detection [Kaplan and Stanhope 1999; Danev et al. 2009], defective device detection [Wang et al. 2005], and access control in wireless personal and local area networks [Hall et al. 2004, 2005; Rasmussen and Capkun 2007; Jana and Kasera 2008; Brik et al. 2008]. 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 II.

### 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 [Shaw and Kinsner 1997; Ureten and Serinken 2007a].

The open literature on transient-based device identification can be traced back to the early 90s. Toonstra and Kinsner [1995, 1996] 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 [1996] also explored wavelet analysis by filter banks in order to characterize the turn-on transients of 4 different VHF FM transmitters. They showed that Euclidean distance was an accurate similarity measure to classify extracted device fingerprints from different manufacturers. Choe et al. [1995] presented an automated device identification system based on wavelet and multiresolution analysis of turn-on transient signals and provided an example of transmitter classification of 3 different transmitters.

Ellis and Serinken [2001] 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 [2004a, 2004b] 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

Table II. Summary of Physical-Layer Device Identification Techniques

| Approach | Signal | Features | Evaluation Data | | | Evaluated Factors | Methodology | Error rate |
|---|---|---|---|---|---|---|---|---|
| | | | Device Type | # | Origin[1] | | | |
| [Toonstra and Kinsner 1995] | Transient | Wavelets | Analog VHF txmtr | 7 | D1 | - | classification | 0% |
| [Ellis and Serinken 2001] | Transient | Amplitude, phase | Analog VHF txmtr | 28 | D1 | fixed distance | visual inspection | n/a |
| [Tekbas et al. 2004a] | Transient | Amplitude, phase | Analog VHF txmtr | 10 | D1 | wide temp. range, voltage and SNR | classification | 5% |
| [Hall et al. 2004] | Transient | Amplitude, phase, power, DWT coeffs. | IEEE 802.11 trx | 14 | D2 | close proximity and temp. | classification | 8% |
| [Hall et al. 2006] | Transient | Amplitude, phase, power, DWT coeffs. | Bluetooth trx | 10 | D2 | close proximity | classification | 7% |
| [Ureten and Serinken 2007b] | Transient | Amplitude envelope | IEEE 802.11 trx | 8 | D2 | close proximity | classification | 2% |
| [Rasmussen and Capkun 2007] | Transient | length, amplitude, DWT coeffs. | UHF trx | 10 | D3 | close proximity | classification | 30% |
| [Brik et al. 2008] | Data | Freq., sync, I/Q, magnitude, phase | IEEE 802.11 trx | 138 | D3 | varied distance and location | classification | 0.34% |
| [Jana and Kasera 2008] | Data | Clock skew | IEEE 802.11 Access Point | 5 | D1 | virtual AP, temp. and NTP sync. | classification, attacks | 0% |
| [Danev and Capkun 2009] | Transient | FFT spectra | IEEE 802.15.4 trx | 50 | D3 | distance, location, voltage, temp. | verification, attacks | 0.24% |
| [Suski et al. 2008a] | Preamble | Power spec. density | IEEE 802.11 trx | 3 | D3 | proximity, SNR | classification | 13% |
| [Danev et al. 2009] | RF burst | FFT spectra, modulation | ISO 14443 HF RFID txpndr | 50 | D3 | varied position, distance | verification | 4% |
| [Periaswamy et al. 2010a] | Preamble | Minimum power response | EPC C1G2 UHF RFID txpndr | 50 | D3 | fixed position | verification | 5% |
| [Williams et al. 2010] | Near transient, Data | Amp., freq., phase, statistics | GSM trx. | 16 | D1 | fixed position, SNR | verification | 5–20% |

[1]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).

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 [Tekbas et al. 2004b].

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. [2004, 2005, 2006] 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 [Hall et al. 2005; Hall 2006] showed error rates of 0% to 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 [Hall et al. 2006]. The authors also introduced dynamic profiles, that is, each device fingerprint was updated after some amount of time, in order to compensate internal temperature effects in the considered devices.

Ureten and Serinken [2007b] 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 these works, signal transients were captured at close proximity to the fingerprinting antenna, approximately 10 to 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 [2007]. 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 [Danev and Capkun 2009] 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, that is, the data. Such features have only recently being proposed for device identification. More precisely, Brik et al. [2008] 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. [2009] 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 [Suski et al. 2008a; Jana and Kasera 2008; Danev et al. 2009] 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. [2008a] 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 three devices and achieved an average classification error rate of 20% for packet frames with SNR greater than 6 dB. Klein et al. [2009, 2010] 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 four 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 [Reising et al. 2010a, 2010b; Williams et al. 2010]. 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 [Reising et al. 2010b], 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 Williams et al. [2010]. 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 [Danev et al. 2009; Romero et al. 2009, 2010; Zanetti et al. 2010; Periaswamy et al. 2010a, 2010b]. Periaswamy et al. [2010a, 2010b] considered fingerprinting of UHF RFID tags. Periaswamy et al. [2010a] 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 [Periaswamy et al. 2010b; Zanetti et al. 2010]. 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, for example, user unauthorized tracking can be achieved by a network of readers with a high accuracy [Zanetti et al. 2010].

In the context of HF RFID, Danev et al. [2009] 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. [2009] 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 [Romero et al. 2010]. These works considered inductive coupled HF RFID tags and the proposed features work from close proximity.

Jana and Kasera [2008] 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 [Kohno et al. 2005]. 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 [Danev and Capkun 2009; Edman and Yener 2009; Danev et al. 2010]. Danev and Capkun [2009] 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. Edman and Yener [2009] developed impersonation attacks on modulation-based identification techniques [Brik et al. 2008]. They showed that low-cost software-defined radios [Ettus 2007] could be used to reproduce modulation features and impersonate a target device with a success rate of 50–75%. Independently, Danev et al. [2010] have designed impersonation 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.

### 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 (Section 2).

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 [Toonstra and Kinsner 1995; Ellis and Serinken 2001; Tekbas et al. 2004a; Hall et al. 2004; Ureten and Serinken 2007b; Danev and Capkun 2009; Suski et al. 2008a]. Few works used predefined features [Brik et al. 2008; Jana and Kasera 2008; Rasmussen and Capkun 2007] with only one work [Brik et al. 2008] exploiting predefined in-specification features. Typically, any 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 [Bishop 2006] to classify (match) fingerprints from different devices. Classification error rate was used as a metric of accuracy in Toonstra and Kinsner [1995], Ellis and Serinken [2001], Tekbas et al. [2004a], Hall et al. [2004], Rasmussen and Capkun [2007], Ureten and Serinken [2007b], Brik et al. [2008], and Suski et al. [2008a], while identification (verification) accuracy in terms of FAR, FRR and EER metrics is used in Danev and Capkun [2009] and Danev et al. [2009]. In Section 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 II). 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 [1995] 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 [Danev et al. 2009] or the modulator subcircuit of the transceiver [Brik et al. 2008]).

Only few works considered evaluating the robustness of the extracted fingerprints to environment and in-device effects (see Table II). 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 [Danev and Capkun 2009; Danev et al. 2009] (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 [Brik et al. 2008] are less sensitive.

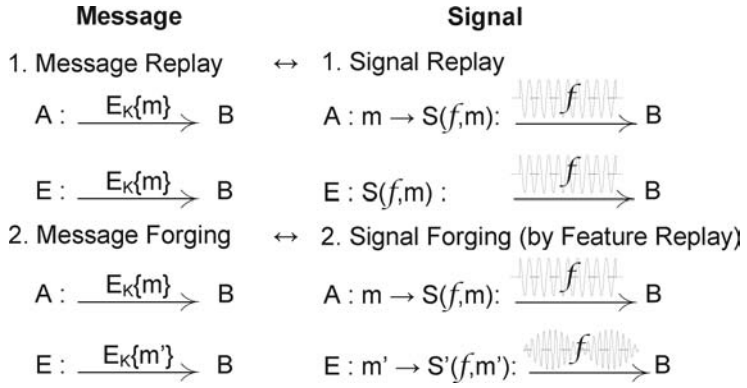


Fig. 4. Relation between message and signal attacks. A and B are genuine parties. E is a Dolev-Yao attacker that can observe, capture, modify, and compose messages or signals. A signal replay attack aims at preserving the digital sampling S($f$,m) of the signal carrying message $m$ and features $f$ as opposed to a message replay attack that preserves the bits of information within the message. In signal replay, the features do not need to be known to the attacker. In a feature replay attack, the attacker needs to know the features $f$ and then can compose signals that reproduce $f$. The difficulty for the attacker resides in composing the signal S'($f$,m') that preserves $f$.

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 Danev and Capkun [2009] and Danev et al. [2009], on signal acquisition time in Brik et al. [2008], 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 [Edman and Yener 2009; Danev et al. 2010], but no comprehensive security and privacy analysis has been attempted.

## 4. CLASSIFICATION OF ATTACKS WITHIN PHYSICAL-LAYER DEVICE IDENTIFICATION

In this section, we present a classification of attacks within physical-layer device identification. We distinguish between attacks on the system that aim at subverting the decision of an application (e.g., grant or not grant access) and attacks on the anonymity of wireless devices that aim at identifying them disregarding their will to be identified. We do not discuss attacks that could be performed by an attacker that controls internal system components. The latter and related countermeasures are classical to biometric identification systems and have been already extensively discussed [Bolle et al. 2003].

We assume a Dolev-Yao style attacker [Dolev and Yao 1983], that is, the attacker may have the capability of observing, capturing, modifying, composing, and (re)playing identification signals transmitted by authorized devices. The relation between message and signal attacks is shown in Figure 4. To observe and capture identification signals, the attacker needs to have access to the identification area or may directly acquire identification signals from the target device. This implies a temporal possession or proximity to the target device and possibly knowledge of the challenges used to acquire the identification signals. The attacker can arbitrarily modify and compose identification signals. To (re)play identification signals, the attacker needs to access the identification area. In Section 5 we discuss restrictions of these capabilities and contextualize them in selected applications.

### 4.1. Signal Replay Attack

In a signal replay attack, the attacker's goal is to observe analog identification signals of a target device, capture them in a digital form (digital sampling), and then transmit (replay) these signals towards the identification system by some appropriate means. The attacker does not modify the captured identification signals, that is, the analog signal and the data payload are preserved. This attack is similar to message replay in the Dolev-Yao model and it is illustrated in Figure 4. The difference resides in the level of replayed information. The message replay attack preserves the bits of information within the message (e.g., 01101), while a signal replay aims at preserving the digital sampling (usually in 8-bit precision) of the signal. The message replay is therefore subsumed by the signal replay. It should be noted that the replay of digital signal samples can never be exact as opposed to information bits. This is due to inherent randomness in hardware components and the wireless medium. Improvement of replay accuracy could be achieved by high-end hardware and controlled wireless medium.

The signal replay attack does not assume attacker's knowledge on the feature extraction and matching procedures used by the identification system. However, knowledge on how to observe, capture, and submit identification signals to the system is required.

Given the requirement of digitizing analog signals and subsequent analog conversion for radio transmission, the attacker needs appropriate devices for capturing and rendering the analog identification signals. Some knowledge on the features used (e.g., baseband or RF) would narrow the choice of an impersonation device. The range of devices includes low-cost hardware [Ettus 2007], high-end signal analyzers [Agilent 2008], and arbitrary waveform generators [Tektronix 2008].

It should be noted that analog identification signals could also be relayed without being previously stored in a digital form. A few components such as amplifiers and antennas are needed to perform the task.

### 4.2. Feature Replay Attack

Unlike in signal replay attacks, where the goal of the attack is to reproduce the captured identification signals in their integrity, feature replay attack creates, modifies or composes identification signals that reproduce only the features considered by the identification system. The analog representation of the forged signals may be different, but the features should be the same (similar) as illustrated in Figure 4.

The feature replay attack is related to message forging in the Dolev-Yao model where the attacker can arbitrarily modify and compose messages. The difference is that forging involves analog and/or digital signal samples and data payload (information bits) as opposed to only information bits in the Dolev-Yao model. The difficulty of this attack resides in the ability to compose signals while preserving the identification features. In order to impersonate a device, the attacker needs to know the features that the identification system extracts to identify a device and needs to be able to forge signals while preserving their distinctive features. This corresponds to attacks on message authentication, where the attacker typically needs to know the secret key in order to create an authentic message or needs to be able to modify/forge existing messages such that they appear authentic to the receiver.

The feature replay attacks could be launched in a number of ways. Similar to a signal replay attack, special devices such as arbitrary waveform generators could be used to produce the modified or composed signals. The attack could also be launched by finding a device that exhibits similar features to a target device, which is then used during the identification procedure. This scenario is relevant in applications where a large set of possibly same model and manufacturer devices could be obtained by the attacker (Section 5).

A third means for launching feature replay attacks is to replicate the entire circuitry of the target device or at least the components responsible for the identification features. This is probably the hardest means as it assumes precise knowledge of the hardware component(s) affecting/causing the features. It is unclear if that is feasible in practice.

### 4.3. Coercion Attack

For completeness, we should mention the coercion attacks. In this attack, an attacker needs to come into (temporal) possession of an authorized device, and use it during the identification procedure. While straightforward, such an attack has relevant implications in some applications (Section 5).

## 5. IMPLICATIONS OF PHYSICAL-LAYER IDENTIFICATION

In this section, we discuss the implications of physical-layer device identification on selected applications. For each application, we first describe the considered scenarios and discuss the system requirements. We then analyze the security threats on the system based on the attacker models described in Section 4.

### 5.1. Intrusion Detection in WLAN Networks

Physical-layer device identification could be used to enhance the security of wireless local area networks (WLAN) in different scenarios. In a first scenario, it can be used to provide an additional layer of access control to prevent unauthorized devices (users) of using the resources of the network. The primary layer of access control could be some cryptographic mechanism that authenticates user devices with an authentication server. In these settings, physical-layer identification could be deployed in the wireless access points (APs) to defend against cryptographic key compromise. It also provides means to quicker detect compromised key material by WLAN administrators. More precisely, physical-layer identification can determine that multiple MAC addresses or cryptographic keys belong to the same wireless device or that multiple devices share a common MAC or cryptographic key. An attacker who holds the cryptographic keys will not be able to authenticate to the network with her own device unless she is able to subvert the physical-layer identification.

In a second scenario, physical-layer identification techniques can be used by the users to detect rogue access points, that is, unauthorized access points that aim at redirecting communication through them instead of the authorized AP and stealing sensitive information (e.g., passwords). While the 802.11i standard addresses this vulnerability by means of strong authentication [IEEE Standards Association 2004], a rogue AP can still fool user devices by using higher signal strength or operate on a different channel [Jana and Kasera 2008]. Therefore, rogue access point detection is a common feature in WLAN intrusion detection systems.

*System Property Requirements*. The aforementioned applications in WLAN networks pose specific requirements to the physical-layer identification system. These networks typically have wireless APs at fixed locations, while mobile devices (clients) communicate with the APs from random locations in the proximity of a given AP. This implies that the physical-layer device fingerprints need to be resilient to distance and location. Recent investigations on transient-based approaches [Danev and Capkun 2009; Danev et al. 2010] suggest that fingerprints extracted from the transient signal do not only contain device specific information, but also wireless channel characteristics that may vary in different locations. It is an open question how the channel characteristics can be compensated. Therefore, using transient-based techniques may introduce severe restrictions on the usability (e.g., authentication must be performed only from a particular location). On the other hand, modulation-based fingerprints are much less

location sensitive [Brik et al. 2008] and clock-related fingerprints such as clock skew would be wireless channel independent [Kohno et al. 2005; Jana and Kasera 2008].

*Security Requirements*. In terms of security requirements, the identification system must be resilient to remote impersonation attacks. In particular, given the large distances in these networks, attacks by signal and feature replay are of a particular concern. Two recent works [Edman and Yener 2009; Danev et al. 2010] show at least that some modulation-based physical-layer fingerprints [Brik et al. 2008] would be inherently insecure for WLAN access control due to high probability of feature reproduction by signal replay. Physical-layer device fingerprints that contain data-dependent characteristics could provide (if they exist) protection against signal replay attacks.

### 5.2. Device Cloning Detection

Recently, Radio Frequency Identification (RFID) technology has becoming the more and more deployed for identification and inventory applications in many different scenarios like libraries, transportation payments, and animal identification. Two promising, and (partially) already in-place applications are identity documents, where biometric data are stored in a RFID device embedded in the document, and RFID-enabled supply chains, where products and/or product-aggregations (e.g., pallets) are equipped with RFID tags.

*5.2.1. Identity Documents.* Physical-layer identification techniques could be used for cloning detection of RFID-enabled identity documents. Despite a number of protective measures, it has been recently shown [Zetter 2006; Grunwald 2006; Witteman 2005; Boggan 2006; van Beek 2008] that RFID transponders in electronic identity documents can be successfully cloned even if the protective measures specified by the ICAO standard [ICAO] are in place.

Physical-layer device identification can be applied to document cloning detection in two different ways. In the first, the fingerprints are measured before RFID deployment and are stored in a back-end database, indexed with the unique document identifier. When the authenticity of the document with identifier ID is verified, the fingerprint of the document transponder is measured and then compared with the corresponding transponder fingerprint of document ID stored in the database. In the second way, the physical-layer fingerprints are again measured before their deployment, but are stored in the transponders memory, digitally signed by the document-issuing authority and protected from unauthorized remote access. When the document authenticity is validated, the binding between the document ID and the fingerprint stored on the transponder is ensured through cryptographic verification of the authority's signature. If the signature is valid, the stored fingerprint is compared to the measured fingerprint of the document transponder. The main advantage in this use case is that the document authenticity can be verified offline. The main drawback is that the fingerprint is now stored on the transponder and requires appropriate access protection [ICAO]. Additionally, the fingerprints need to be compact enough to fit in the transponder's memory. The cloning detection accuracy will depend on the allowable error rates.

*System Property Requirements*. The requirements on the properties of the physical-layer fingerprints are significantly different compared to the intrusion detection scenario. Given that the anti-cloning verification must be achievable in multiple locations (e.g., country border controls), special purpose-built devices need to be devised. This relaxes the requirement on the fingerprints to be robust to environmental factors and channel-specific effects as these can be controlled in the purpose-built device. However, the purpose-built devices should be of a (high) quality in order to preserve the fingerprint from unpredictable (undesirable) distortions.

*Security Requirements*. Now we analyze the security implications with respect to the attacker models in Section 4. For all the attack strategies, the attacker needs to obtain the fingerprint of the transponder in the original document. If this could not be done remotely, physical possession of the target document is required. Attacks by signal replay and feature replay would require a generator device that has similar external appearance as the one that is being cloned; in the case of an ePassport, replay attacks require introducing a special device within a passport. It is not clear if and how this is feasible. Such attacks would not be possible if the fingerprints contain data-dependent characteristics.

Given that building a cloned device is considered a hard task (Section 4), a more realistic strategy would be to find a transponder that exhibits similar fingerprints to these of the target for cloning transponder. Such a task also requires knowledge on the feature extraction process. To realize this attack, the attacker needs to test a given quantity of RFID transponders from the same manufacturer and model. The quantity of tags that need to be tested would depend on the system error rates.

*5.2.2. RFID-Enabled Supply Chains.* Within RFID-enabled supply chains, each product and/or product-aggregation is equipped with an RFID tag containing a unique identifier. Through an RFID infrastructure (e.g., the EPCglobal network [EPCglobal 2009]), supply chain partners can record, store, and share information associated with those unique identifiers, and use it to automate and speed-up processes. Tag cloning in RFID-enabled supply chains may facilitate the injection into legal supply chains of tag-cloned counterfeit products, which, carrying identifiers of genuine products, will be recognized as those genuine products by the RFID infrastructure (unless human inspection is performed).

Current solutions for RFID-enabled supply chains, like the afore-mentioned EPCglobal architecture, do not provide effective anti-cloning measures [Juels 2005]. In the past years, several works have been proposed [Juels 2005; Dimitriou 2005; Nguyen Duc et al. 2006; Bolotnyy and Robins 2007; Lehtonen et al. 2009], but due to the limited resources and cost constraints of RFID tag for supply chain applications, a standardizable anti-cloning mechanism is still under investigation. Physical-layer identification provides means to detect counterfeit products by creating physical-layer device fingerprints that bind the RFID tag to the claimed identity. Differently from ePassport applications, where fingerprints may be directly stored on the ePassports [Danev et al. 2009], due to the limited resources of RFID tags, fingerprints need to be stored in a database (e.g., maintained by tag manufacturer) for later comparisons with those obtained from the RFID tag.

*System Property Requirements*. Specific requirements for both system performance and fingerprint properties should be considered to enable physical-layer device identification within RFID-enabled supply chains. Considering a scenario where pallets of tagged products pass through a gate for identification, the large amount of products that need to be identified in a short time would require a high computational speed. Additionally, tagged products can be placed anywhere on a pallet and interfere to each others during wireless communication (e.g., by signal superposition or signal diffraction due to product packaging); fingerprints would then be required to be particularly robust and the identification system conceived to handle exceptions. Moreover, system accuracy should be particularly high; differently from ePassports control, where a false positive can be easily and quickly checked by human inspection, verifying falses may slow down supply chain processes.

*Security Requirements*. An attacker may be easily able to acquire identification signals from target tags (EPC RFID tags have relatively large read range up to 8 meters [Koscher et al. 2009]) and to extract relevant features (which may be public

information to allow supply chain partners to verify tags' identity). Even considering both signal and feature replay attacks feasible, an attacker needs to consider the cost of replaying devices with respect to the gain of counterfeit injection. Equip each counterfeit product with a replaying device might be too expensive. Differently, equip counterfeit products with RFID tags that present similar features to tags on genuine products will not only fulfill identification requirements, but, considering the low cost of RFID tags for supply chain applications, be an optimal solution in terms of costs. As mentioned in Section 4, building devices that present similar signal features to target devices is a hard task. Considering the high number of similar (same model, same manufacturer) RFID tags available on the market and their relative low unit cost, finding devices that present similar signal features to target devices may be feasible (also depending on the identification accuracy). Coercive attacks may also be considered within RFID-enabled supply chain: an attacker could remove a tag from a genuine product and attach it to a counterfeit product.

### 5.3. Other Related Applications

We briefly discuss applications of physical-layer identification on securing all-wireless multi-hop networks. Wireless multi-hop networks rely on the correct execution of neighborhood discovery, localization and time synchronization protocols. A number of attacks such as wormhole, node replication, and Sybil attacks have been shown to be particularly harmful to these networks [Hu et al. 2003; Parno et al. 2005; Poovendran and Lazos 2007] and therefore their detection/prevention is critical to ensure normal operations.

In a wormhole attack, the attacker creates a tunnel (wired or wireless) that connects two points (multiple hops away to each other) in the network and relays messages from one point to the other. She is then in a position to filter out unwanted packets or refuse to forward traffic [Hu et al. 2003]. Several methods have been suggested to counter this attack [Hu et al. 2003; Poovendran and Lazos 2007; Buttyán et al. 2005]. Physical-layer identification techniques could be used to verify the origin (device) of the transmitted signal [Rasmussen and Capkun 2007]. The system and security requirements are similar to the scenarios in Section 5.1.

In a Sybil attack [Douceur 2002], an attacker assigns several identities to the same network node. These identities can be fake, but they might also be true identities of nodes that the attacker compromised. Similarly, in a replication attack [Parno et al. 2005], the attacker assigns the same (legitimate) identity to several nodes that she controls. Although several methods have been suggested to prevent these attacks [Newsome et al. 2004; Parno et al. 2005], as for wormhole attacks, physical-layer identification techniques could detect the presence of multiple device identities.

In addition, in scenarios where power consumption plays a relevant role (e.g., wireless sensor networks), physical-layer identification can be used alone for device authentication saving power compared to cryptography-based solutions [Wander et al. 2005].

### 5.4. Anonymity and Location Privacy

In the previous applications, we focused on the defensive usage of device identification techniques. We now consider scenarios in which physical-layer device identification techniques can be employed to compromise systems designed to preserve the anonymity and/or location privacy of devices (users). We argue that such systems would not be secure solutions unless the privacy preserving properties are ensured on all communication layers, that is, including the physical layer.

The security of WLAN networks have been largely improved in the IEEE 802.11i standard [IEEE Standards Association 2004] with MAC security enhancements

including key distribution management and strong encryption techniques. However, it is considered trivial to track 802.11 devices as they have globally unique MAC addresses. Although various techniques have been proposed to hide identifying information in the packet transmissions [Gruteser and Grunwald 2005] and to guarantee anonymous routing [Kong and Hong 2003; Zhu et al. 2004], attacks based on profiling the traffic patterns of users have been demonstrated to compromise such techniques [Pang et al. 2007]. Through physical-layer device identification, such techniques may easily be compromised: while the accuracy of the mentioned profiling attacks is dependable on a number of factors (e.g., consistency in user behavior), physical-layer device identification techniques would require few packets to identify the number of devices in the vicinity and classify individual packets to the corresponding transmitting devices [Brik et al. 2008].

RFID technologies raised a number of privacy concerns in many different applications [Juels 2006]. Several solutions to guarantee privacy (i.e., tag untraceability) have been proposed [Spiekermann and Evdokimov 2009], but, as for WLAN networks, physical-layer device identification techniques may invalidate the privacy guarantees of these solutions.

Although most physical-layer device identification targeting HF and UHF RFID transponders [Danev et al. 2009; Romero et al. 2010; Periaswamy et al. 2010a] are able to accurately distinguish same manufacturer and type tags, these techniques only work from close proximity (e.g., $\leq$10 cm) and at fixed positions. Recently, it has been shown that even same manufacturer and type UHF RFID leak distinguishable information which is independent of the position [Periaswamy et al. 2010b; Zanetti et al. 2010]. If a user holds a number of UHF tags, a network of readers can track him with high accuracy, irrespective of the location and distance to the reader of up to 6 meters (tested) [Zanetti et al. 2010]. For example, a user who holds 5 tags can be uniquely identified among $6 \times 10^6$ users. Given this and related results on the ability to read UHF RFID from larger distances [Koscher et al. 2009], it is clear that tag holder privacy can be compromised and lead to unauthorized tracking of people.

In summary, we note that the possibility of identifying wireless devices at the physical-layer has been so far largely underestimated in the design of privacy-preserving communication protocols. Similarly, countermeasures against unauthorized identifications is an open issue that needs to be addressed.

## 6. 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 multimodal 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 multimodal 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.

## 7. RELATED WORK

The present work considered identification of wireless devices based on imperfections in their analog circuitry that can be measured at the physical-layer during radio communication. Physical fingerprints for device identification can also be extracted from the internals of the device circuitry. Examples include measuring the MOSFET threshold voltages [Lofstrom et al. 2000], threshold voltage mismatch in NOR cells [Su et al. 2007], and the power-up of the SRAM [Holcomb et al. 2009] for RFID identification. The main drawback of these approaches is that they require special access to the device circuitry as opposed to the techniques considered in this work.

Identification using physical properties of devices can also be achieved with Physically Unclonable Functions (PUFs) [Gassend et al. 2004; Devadas et al. 2008]. Processors in PUF-enabled RFID devices contain a special circuit that maps input challenges to output responses using a function (PUF) determined by the inherent variations of that circuit. The difficulty of controlling these variations prevents an adversary from duplicating the PUF-enabled chips given some assumptions on its capabilities. The main limitation of PUF-based identification is that it requires PUF-enabled devices. However, it presents the advantage of relying on "controlled" variability as opposed to unintentionally introduced manufacturing variability that physical-layer device identification exploits. Additionally, PUF-based solutions provide robustness to replay attacks due to their challenge-response nature.

Another field of research, related to physical-layer device identification, is integrated circuit (IC) watermarking. The goal is to build digital watermarks inside ICs in order to prevent illegal copies of the hardware and protect intellectual property. An overview of digital watermarking techniques is provided in Abdel-Hamid et al. [2003]. Watermarking has been proposed at many different hardware levels (e.g., ASIC, FPGA) [Torunoglu and Charbon 2000]. Recently, they have been also hidden into special side-channels [Becker et al. 2010; Koushanfar and Alkabani 2010]. In comparison to physical-layer identification, watermarking presents a similar objective, that is, uniquely distinguish devices in an unforgeable manner. The difference is that watermarks are intentionally included in the hardware (like PUFs) and may require specialized procedures to be verified.

We note that additional physical properties of the wireless communication could be used for security applications such as access control, device location distinction, etc. In particular, a number of researchers have explored the physical properties of the wireless channel for wireless device authentication [Faria and Cheriton 2006; Xiao et al. 2007] and device location distinction [Patwari and Kasera 2007]. While the channel characteristics are believed to be unique within a given location due to specific multipath effects, these characteristics are not inherent to the device and therefore cannot be used for device identification unless the device is bound to its location.

We conclude this section by mentioning that the present work covers the physical-layer subset of techniques on device identification. In general, device identification

spans all communication layers of the OSI architecture [ITU 1994] and a variety of network devices. Device identification (fingerprinting) has been explored on both wired and wireless devices at the link, transport, and application layers. Prominent works include Nmap Security Scanner, Xprobe, Kohno et al. [2005], Gerdes et al. [2006], Murdoch [2006], Franklin et al. [2006], Loh et al. [2008], and Bratus et al. [2008].

## 8. CONCLUSION

Physical-layer device identification aims at identifying wireless devices by some unique features that they exhibit and that can be observed during radio communication. It can benefit a number of applications such as access control, device cloning detection and at the same time provide means for compromising the device identity (location) privacy. The properties and requirements on physical-layer device identification are inherently different from those on the related biometric identification systems due to the shared medium and broadcast nature of wireless devices.

Our literature analysis revealed that 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, analyzing the state-of-art approaches in the open literature, classifying related attacks, and discussing the system and security issues in selected applications, we provide a comprehensive overview of physical-layer identification and its implications on the security of wireless networks and protocols.

Despite the existence of a number of works on the subject, understanding physical-layer identification in terms of feasibility, accuracy, cost, assumptions, and implications is still a remaining 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, multimodal 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.

Last, but not least, the feasibility or nonfeasibility of identifying devices remotely at the physical-layer needs to be carefully considered in the design of privacy-preserving wireless protocols. This could only be achieved by further investigations.

## REFERENCES

Abdel-Hamid, A. T., Tahar, S., and Aboulhamid, E. M. 2003. IP watermarking techniques: Survey and comparison. In *Proceedings of the IEEE International Workshop on System-on-Chip for Real-Time Applications*. 60.

Agilent. 2008. Digital Signal Analyzer (DSA) 90804A. http://www.home.agilent.com/.

Becker, G., Kasper, M., Moradi, A., and Paar, C. 2010. Side-channel based watermarks for integrated circuits. In *Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. 30–35.

Bishop, C. 2006. *Pattern Recognition and Machine Learning*. Springer.

Boggan, S. 2006. Cracked it! http://www.guardian.co.uk/technology/2006/nov/17/news.homeaffairs/. (Last accessed 6/11)

Bolle, R., Connell, J., Pankanti, S., Ratha, N., and Senior, A. 2003. *Guide to Biometrics*. Springer.

Bolotnyy, L., and Robins, G. 2007. Physically unclonable function-based security and privacy in RFID systems. In *Proceedings of the IEEE International Conference on Pervasive Computing and Communications (PER-COM)*. 211–220.

Bratus, S., Cornelius, C., Peebles, D., and Kotz, D. 2008. Active behavioral fingerprinting of wireless devices. In *Proceedings of the ACM Conference on Wireless Network Security (WiSec)*. 56–61.

Brik, V., Banerjee, S., Gruteser, M., and Oh, S. 2008. Wireless device identification with radiometric signatures. In *Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom)*. 116–127.

Buttyá N. L., Dóra, L., and Vajda, I. 2005. Statistical wormhole detection in sensor networks. In *Proceedings of the 2nd European Workshop on Security and Privacy in Ad-hoc and Sensor Networks*. 128–141.

Choe, H., Poole, C., Yu, A., and Szu, H. 1995. Novel identification of intercepted signals for unknown radio transmitters. *Proc. SPIE 2491*, 504–517.

Danev, B. and Capkun, S. 2009. Transient-based identification of wireless sensor nodes. In *Proceedings of the ACM/IEEE Conference on Information Processing in Sensor Networks (IPSN)*. 25–36.

Danev, B., Heydt-Benjamin, T. S., and Capkun, S. 2009. Physical-layer identification of RFID devices. In *Proceedings of the USENIX Security Symposium*. 199–214.

Danev, B., Luecken, H., Capkun, S., and Defrawy, K. E. 2010. Attacks on physical-layer identification. In *Proceedings of the ACM Conference on Wireless Network Security (WiSec)*. 89–98.

Devadas, S., Suh, E., Paral, S., Sowell, R., Ziola, T., and Khandelwal, V. 2008. Design and implementation of PUF-based "unclonable" RFID ICs for anti-counterfeiting and security applications. In *Proeeedings of the IEEE International Conference on RFID*. 58–64.

Dimitriou, T. 2005. A lightweight RFID protocol to protect against traceability and cloning attacks. In *Proceedings of the International ICST Conference on Security and Privacy in Communication Networks (SecureComm)*. 59–66.

Dolev, D. and Yao, A. C. 1983. On the security of public key protocols. *IEEE Trans. Info. Theory 2*, 29, 198–208.

Douceur, J. R. 2002. The sybil attack. In *Proceedings of the International Workshop on Peer-to-Peer Systems (IPTPS)*. 251–260.

Edman, M. and Yener, B. 2009. Active attacks against modulation-based radiometric identification. Tech. rep. 09-02, Rensselaer Institute of Technology.

Ellis, K. and Serinken, N. 2001. Characteristics of radio transmitter fingerprints. *Radio Science 36*, 585–597.

EPCglobal 2009. The EPCglobal Architecture Framework v. 1.3. EPCglobal.

Ettus, M. 2007. Universal software defined radio (USRP). http://www.ettus.com/.

Faria, D. B. and Cheriton, D. R. 2006. Detecting identity-based attacks in wireless networks using signalprints. In *Proceedings of the ACM Workshop on Wireless Security (WiSe)*. 43–52.

Franklin, J., McCoy, D., Tabriz, P., Neagoe, V., Randwyk, J., and Sicker, D. 2006. Passive data link layer 802.11 wireless device driver fingerprinting. In *Proceedings of the USENIX Security Symposium*.

FVC. 2006. Fingerprint Verification Competition FVC. http://bias.csr.uni-bo.it/fvc2006/.

Gassend, B., Lim, D., Clarke, D., Devadas, S., and van Dijk, M. 2004. Identification and authentication of integrated circuits. *Concurr. Computat.: Pract. Exper. 16*, 11, 1077–1098.

Gerdes, R., Daniels, T., Mina, M., and Russell, S. 2006. Device identification via analog signal fingerprinting: A matched filter approach. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*.

Grunwald, L. 2006. New attack to RFID-systems and their middleware and backends. In *Black Hat Briefings USA*.

Gruteser, M. and Grunwald, D. 2005. Enhancing location privacy in wireless LAN through disposable interface identifiers: A quantitative analysis. *Mobile Netw. Appl. 10*, 3, 315–325.

Hall, J. 2006. Detection of rogue devices in wireless networks. Carleton Univ., Ph.D. dissertation.

Hall, J., Barbeau, M., and Kranakis, E. 2004. Enhancing intrusion detection in wireless networks using radio frequency fingerprinting. In *Proceedings of the Conference on Communications, Internet, and Information Technology (CIIT)*. 201–206.

Hall, J., Barbeau, M., and Kranakis, E. 2005. Radio frequency fingerprinting for intrusion detection in wireless networks. Manuscript. http://wiki.uni.lu/secan-lab/Hall2005.html.

HALL, J., BARBEAU, M., AND KRANAKIS, E. 2006. Detecting rogue devices in Bluetooth networks using radio frequency fingerprinting. In *Proceedings of the IASTED International Conference on Communications and Computer Networks (CCN)*. 108–113.

HIPPENSTIEL, R. AND PAYAL, Y. 1996. Wavelet based transmitter identification. In *Proceedings of the International Symposium on Signal Processing and Its Applications (ISSPA)*. 740–742.

HOLCOMB, D. E., BURLESON, W. P., AND FU, K. 2009. Power-up SRAM state as an identifying fingerprint and source of true random numbers. *IEEE Trans. Comput. 58*, 9, 1198–1210.

HU, Y., PERRIG, A., AND JOHNSON, D. 2003. Packet leashes: A defense against wormhole attacks in wireless networks. In *Proceedings of the IEEE Conference on Computer Communications (INFOCOM)*. 1976–1986.

ICAO. http://www.icao.int/.

IEEE STANDARDS ASSOCIATION 2004. IEEE 802.11i-2004: MAC Security Enhancements. IEEE Standards Association.

ITU 1994. ITU-T Recommendation X.200: Information technology—Open Systems Interconnection—Basic Reference Model: The basic model. ITU.

JAIN, A. AND ZONGKER, D. 1997. Feature selection: Evaluation, application, and small sample performance. *IEEE Trans. Patt. Anal. Mach. Intell. 19*, 2, 153–158.

JAIN, A. K., DUIN, R. P. W., AND MAO, J. 2000. Statistical pattern recognition: A review. *IEEE Trans. Patt. Anal. Mach. Intell. 22*, 1, 4–37.

JANA, S. AND KASERA, S. K. 2008. On fast and accurate detection of unauthorized wireless access points using clock skews. In *Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom)*. 104–115.

JONES, R. 1978. *Most Secret War: British Scientific Intelligence 1939–1945*. Hamish Hamilton.

JUELS, A. 2005. Strengthening EPC tags against cloning. In *Proceedings of the ACM Workshop on Wireless Security (WiSe)*. 67–76.

JUELS, A. 2006. RFID security and privacy: A research survey. *IEEE J. Select. Areas Commun. 24*, 2, 381–394.

KAPLAN, D. AND STANHOPE, D. 1999. Waveform collection for use in wireless telephone identification. US Patent 5999806.

KITTLER, J., HATEF, M., DUIN, R., AND MATAS, J. 1998. On combining classifiers. *IEEE Trans. Patt. Anal. Mach. Intell. 20*, 3, 226–239.

KLEIN, R. W., TEMPLE, A. M., AND MENDENHALL, M. J. 2009. Application of wavelet-based RF fingerprinting to enhance wireless network security. *Secur. Commun. Netw. 11*, 6, 544–555.

KLEIN, R. W., TEMPLE, M. A., AND MENDENHALL, M. J. 2010. Application of wavelet denoising to improve OFDM-based signal detection and classification. *Secur. Commun. Netw. 3*, 1, 71–82.

KOHNO, T., BROIDO, A., AND CLAFFY, K. 2005. Remote physical device fingerprinting. *IEEE Trans. Depend. Sec. Computi. 2*, 2, 93–108.

KONG, J. AND HONG, X. 2003. ANODR: Anonymous on demand routing with untraceable routes for mobile ad-hoc networks. In *Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc)*. 291–302.

KOSCHER, K., JUELS, A., KOHNO, T., AND BRAJKOVIC, V. 2009. EPC RFID tag security weaknesses and defenses: Passport cards, enhanced drivers licenses, and beyond. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*. 33–42.

KOUSHANFAR, F. AND ALKABANI, Y. 2010. Provably secure obfuscation of diverse watermarks for sequential circuits. In *Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. 42–47.

LEHTONEN, M., MICHAHELLES, F., AND FLEISCH, E. 2009. How to detect cloned tags in a reliable way from incomplete RFID traces. In *Proceedings of the IEEE International Conference on RFID*. 257–264.

LOFSTROM, K., DAASCH, W., AND TAYLOR, D. 2000. IC identification circuit using device mismatch. In *Proceedings of the IEEE International Solid-State Circuits Conference (ISSCC)*. 372–373.

LOH, D., CHO, C., TAN, C., AND LEE, R. 2008. Identifying unique devices through wireless fingerprinting. In *Proceedings of the ACM Workshop on Wireless Security (WiSe)*. 46–55.

MARGERUM, D. 1969. *Pinpointing Location of Hostile Radars*. Microwaves.

MITRA, M. 2008. Privacy for RFID systems to prevent tracking and cloning. *Int. J. Comput. Sci. Netw. Sec. 8*, 1, 1–5.

MURDOCH, S. J. 2006. Hot or not: Revealing hidden services by their clock skew. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*. 27–36.

NEWSOME, J., SHI, E., SONG, D., AND PERRIG, A. 2004. The sybil attack in sensor networks: analysis and defenses. In *Proceedings of the ACM/IEEE Conference on Information Processing in Sensor Networks (IPSN)*. 259–268.

NGUYEN DUC, D., PARK, J., LEE, H., AND KIM, K. 2006. Enhancing security of EPCglobal Gen-2 RFID tag against traceability and cloning. In *Proceedings of the Symposium on Cryptography and Information Security (SCIS)*.

NMAP SECURITY SCANNER. http://www.insecure.org/nmap/2004/.

PANG, J., GREENSTEIN, B., GUMMADI, R., SESHAN, S., AND WETHERALL, D. 2007. 802.11 user fingerprinting. In *Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom)*. 99–110.

PARNO, B., PERRIG, A., AND GLIGOR, V. 2005. Distributed detection of node replication attacks in sensor networks. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*. 49–63.

PATWARI, N. AND KASERA, S. 2007. Robust location distinction using temporal link signatures. In *Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom)*. 111–122.

PERIASWAMY, S. C. G., THOMPSON, D., AND DI, J. 2010a. Fingerprinting RFID tags. Dependable and secure computing. *IEEE Trans. PP, 99,* 1.

PERIASWAMY, S. C. G., THOMPSON, D. R., AND ROMERO, H. P. 2010b. Fingerprinting radio frequency identification tags using timing characteristics. In *Proceedings of the Workshop on RFID Security (RFIDSec, Asia)*.

POOVENDRAN, R. AND LAZOS, L. 2007. A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. *Wire. Netw. 13*, 1, 27–59.

RASMUSSEN, K. AND CAPKUN, S. 2007. Implications of radio fingerprinting on the security of sensor networks. In *Proceedings of the International ICST Conference on Security and Privacy in Communication Networks (SecureComm)*.

REISING, D. R., TEMPLE, M. A., AND MENDENHALL, M. J. 2010a. Improved wireless security for GMSK-based devices using RF fingerprinting. *Int. J. Electron. Secur. Digit. Forensic 3*, 1, 41–59.

REISING, D. R., TEMPLE, M. A., AND MENDENHALL, M. J. 2010b. Improving intra-cellular security using air monitoring with RF fingerprints. In *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC)*.

ROMERO, H. P., REMLEY, K. A., WILLIAMS, D. F., AND WANG, C.-M. 2009. Electromagnetic measurements for counterfeit detection of radio frequency identification cards. *IEEE Trans. Microwave Theory Tech. 57*, 5, 1383–1387.

ROMERO, H. P., REMLEY, K. A., WILLIAMS, D. F., WANG, C.-M., AND BROWN, T. X. 2010. Identifying RF identification cards from measurements of resonance and carrier harmonics. *IEEE Trans. Microwave Theory Tech* 58, 7, 1758–1765.

ROSS, A. AND JAIN, A. 2004. Multimodal biometrics: An overview. In *Proceedings of the European Signal Processing Conference (EUSIPCO)*.

SHAW, D. AND KINSNER, W. 1997. Multifractal modeling of radio transmitter transients for classification. In *Proceedings of the IEEE Conference on Communications, Power and Computing (WESCANEX)*. 306–312.

SPIEKERMANN, S. AND EVDOKIMOV, S. 2009. Critical RFID privacy-enhancing technologies. *IEEE Secur. Priv. 7*, 2, 56–62.

SU, Y., HOLLEMAN, J., AND OTIS, B. 2007. A 1.6pJ/bit 96%-stable chip ID generating circuit using process variation. In *Proceedings of the IEEE International Solid-State Circuits Conference (ISSCC)*. 406–611.

SUSKI, W., TEMPLE, M., MENDENHALL, M., AND MILLS, R. 2008a. Using spectral fingerprints to improve wireless network security. In *Proceedings of the IEEE Global Communications Conference (GLOBECOM)*. 1–5.

SUSKI, W. C., TEMPLE, M. A., MENDENHALL, M. J., AND MILLS, R. F. 2008b. Radio frequency fingerprinting commercial communication devices to enhance electronic security. *Int. J. Electron. Secur. Digit. Forensic 1*, 3, 301–322.

TEKBAS, O., URETEN, O., AND SERINKEN, N. 2004a. An experimental performance evaluation of a novel radio-transmitter identification system under diverse environmental conditions. *Canad. J. Elect. Comput. Eng. 29*, 3, 203–209.

TEKBAS, O., URETEN, O., AND SERINKEN, N. 2004b. Improvement of transmitter identification system for low SNR transients. *Electron. Lett. 40*, 3, 182–183.

TEKTRONIX. 2008. Arbitrary Waveform Generator 7000 Series. Tektronix. http://www.tek.com/products/signal\sources/awg7000/.

TIPPENHAUER, N. O., RASMUSSEN, K. B., PÖPPER, C., AND CAPKUN, S. 2009. Attacks on public WLAN-based positioning. In *Proceedings of the ACM/USENIX International Conference on Mobile Systems, Applications and Services (MobiSys)*. 29–40.

TOONSTRA, J. AND KINSNER, W. 1995. Transient analysis and genetic algorithms for classification. In *Proceedings of the IEEE Conference on Communications, Power, and Computing (WESCANEX)*. Vol. 2, 432–437.

TOONSTRA, J. AND KINSNER, W. 1996. A radio transmitter fingerprinting system ODO-1. In *Proceedings of the Canadian Conference on Electrical and Computer Engineering*. Vol. 1, 60–63.

TORUNOGLU, I. AND CHARBON, E. 2000. Watermarking-based copyright protection of sequential functions. *IEEE J. Solid-State Circ. 35*, 3, 434–440.

URETEN, O. AND SERINKEN, N. 2007a. Detection of radio transmitter turn-on transients. In *Elect. Lett. 35*, 1996–1997.

URETEN, O. AND SERINKEN, N. 2007b. Wireless security through RF fingerprinting. *Canad. J. Elect. Comput. Eng. 32*, 1, 27–33.

VAN BEEK, J. 2008. ePassports reloaded. In *Black Hat Briefings USA*.

WANDER, A. S., GURA, N., EBERLE, H., GUPTA, V., AND SHANTZ, S. C. 2005. Energy analysis of public-key cryptography for wireless sensor networks. In *Proceedings of the IEEE International Conference on Pervasive Computing and Communications (PERCOM)*. 324–328.

WANG, B., OMATU, S., AND ABE, T. 2005. Identification of the defective transmission devices using the wavelet transform. *IEEE Trans. Patt. Anal. Mach. Intell. 27*, 6, 696–710.

WILLIAMS, M., TEMPLE, M., AND REISING, D. 2010. Augmenting bit-level network security using physical layer RF-DNA fingerprinting. In *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM)*. 1–6.

WITTEMAN, M. 2005. Attacks on digital passports. In *What The Hack*. (http://en.wikipedia.org/wiki/What_the_Hack)

XIAO, L., GREENSTEIN, L., MANDAYAM, N., AND TRAPPE, W. 2007. Fingerprints in the ether: Using the physical layer for wireless authentication. In *Proceedings of the IEEE International Conference on Communications (ICC)*. 4646–4651.

XPROBE. http://www.sys-security.com/.

ZANETTI, D., DANEV, B., AND CAPKUN, S. 2010. Physical-layer identification of UHF RFID tags. In *Proceedings of the 16th ACM Conference on Mobile Computing and Networking (MOBICOM)*.

ZETTER, K. 2006. Hackers clone e-passports. Online publication. Last access: 14.06.2011, http://www.wired.com/science/discoveries/news/2006/08/71521/.

ZHU, B., WAN, Z., KANKANHALLI, M., BAO, F., AND DENG, R. 2004. Anonymous secure routing in mobile ad-hoc networks. In *Proceedings of the IEEE International Conference on Local Computer Networks*. 102–108.

Received June 2010; revised March 2011 and June 2011; accepted July 2011