Attacks on Physical-layer Identification

Boris Danev
Dept. of Comp. Science
ETH Zurich
8092 Zurich, Switzerland
bdanev@inf.ethz.ch

Heinrich Luecken
Comm. Tech. Laboratory
ETH Zurich
8092 Zurich, Switzerland
lueckenh@nari.ee.ethz.ch

Srdjan Capkun
Dept. of Comp. Science
ETH Zurich
8092 Zurich, Switzerland
capkuns@inf.ethz.ch

Karim El Defrawy
School of ICS
UC Irvine
Irvine, CA USA
keldefra@uci.edu

ABSTRACT

Physical-layer identification of wireless devices, commonly referred to as Radio Frequency (RF) fingerprinting, is the process of identifying a device based on transmission imperfections exhibited by its radio transceiver. It can be used to improve access control in wireless networks, prevent device cloning and complement message authentication protocols. This paper studies the feasibility of performing impersonation attacks on the modulation-based and transient-based fingerprinting techniques. Both techniques are vulnerable to impersonation attacks; however, transient-based techniques are more difficult to reproduce due to the effects of the wireless channel and antenna in their recording process. We assess the feasibility of performing impersonation attacks by extensive measurements as well as simulations using collected data from wireless devices. We discuss the implications of our findings and how they affect current device identification techniques and related applications.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design —*Distributed networks, Wireless communication*; C.3 [**Computer Systems Organization**]: Special-Purpose And Application-Based Systems—*Signal processing systems*

General Terms

Security, Experimentation, Measurement, Design

Keywords

Wireless Security, Attacks, Physical Layer, Identification

1. INTRODUCTION

Physical-layer identification of wireless devices, also referred to as radio frequency (RF) fingerprinting, aims to identify a wireless device based on distinctive physical layer characteristics exhibited by the device (or class of devices). These distinctive characteristics are mainly due to manufacturing imperfections in the hardware of a device's radio transceiver. In a typical scenario, the fingerprinter observes traffic to and from a targeted device (fingerprintee) in order to find characteristics that (uniquely) distinguish that device. Physical-layer based identification can benefit a number of wireless applications such as access control [10, 13, 22, 26], device cloning [7] and malfunction detection [28].

Two main approaches were proposed in the open literature for accurate physical-layer identification of wireless transceivers, namely transient and modulation-based techniques. Transient-based techniques consist of observing unique features during the transient phase when the radio is turned on. These features appear at the beginning of each packet transmission as shown in Figure 3a. It is primarily used for distinguishing classes (e.g., model or manufacturer) of wireless devices [13–15] and was recently improved to distinguish individual devices of the same model and manufacturer [8, 22]. Modulation-based techniques rely on imperfections in the modulator of the radio transceiver such as frequency and constellation symbol deviations (Figure 3b). It has been experimentally demonstrated that modulation-based features can accurately identify not only classes but also identical devices [6]. Both techniques achieve high identification accuracy over 99%.

While the accuracy of the above techniques was validated, little is known about the degree of security that these techniques provide to the applications using it. It is generally believed that hardware imperfections and thus the resulting signals are hard to reproduce.

In this paper, we investigate if and under which conditions this is true: we study the robustness of physical-layer identification techniques to impersonation attacks. More precisely, we explore impersonation attacks on modulation and transient-based identification techniques by feature and signal replay. In feature replay, we modify radio signals to match the targeted identification features, while in signal replay we capture and replay radio signals in radio frequency (RF). Our findings show that modulation-based identification can be impersonated with an accuracy close to 100% by simply modifying and replaying the used features. We further show that transient-based features can also be accurately reproduced using a high-end arbitrary waveform generator over a wire; however, these features are hard to record by an external attacker since they can be channel- and antenna-dependent. We validate the impersonation perfor-

WiSec'10, March 22–24, 2010, Hoboken, New Jersey, USA.

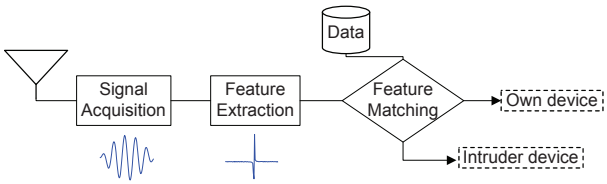

Figure 1: Physical-layer Identification System: The system consists of three major processes, namely signal acquisition, feature extraction/matching and decision making.

mance using software-defined radios [4, 11] and high-end arbitrary waveform generators [2, 25] both in threshold-based identification and classification scenarios. Finally, we analyze the security implications of these findings to applications that make use of device identification.

To the best of our knowledge, this is the first work that shows the feasibility of impersonation attacks on current physical-layer identification techniques.

The remainder of this paper is organized as follows. In Section 2, we provide an overview of physical-layer identification and present our system and attacker model. In Section 3 and Section 4 we present the details of the design and implementation of two impersonation attacks. The performance of the attacks is analyzed in Section 5. We discuss the implications in Section 6, provide related work in Section 7 and conclude the paper in Section 8.

2. SYSTEM AND ATTACKER MODEL

We first present an overview of physical-layer identification and then describe our system and attack model.

2.1 Physical-layer Identification

Physical-layer identification of wireless devices consists of a number of techniques that aim at uniquely identifying a given device and/or a class of devices. Figure 1 shows the main components of a typical physical-layer identification system: signal acquisition, feature extraction/matching, and decision making processes.

The signal acquisition process consists of high-end hardware components that capture the radio signals of wireless devices with sufficient precision. This is an important requirement given that devices' fingerprints at the physical layer are due to small impairments/variations in the device's radio circuitry that could be easily lost if captured with inappropriate hardware [8].

The feature extraction process consists of extracting and selecting features from the radio signal that have sufficient discriminative capabilities to distinguish a device and/or a class of devices. The combination of all the extracted features forms the device's fingerprint template, also referred to as fingerprint. In the feature matching and decision processes, an appropriate measure of similarity is applied between the extracted fingerprints in order to yield a decision depending on the application requirements.

In this work, we show impersonation attacks on some physical-layer identification techniques. More precisely, we consider the two most prominent instances of a modulation and transient-based identification techniques that have demonstrated the highest identification accuracy in the open literature. The background of the techniques and proposed attacks are detailed in Section 3.1 and 4.1 respectively.

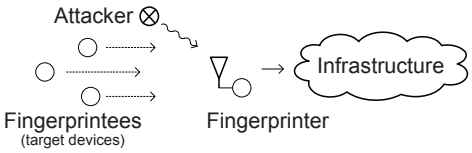

Figure 2: Our system consists of a wireless network with a number of wireless devices (fingerprintees) and a fingerprinting device (fingerprinter). We assume that in the system initialization phase the fingerprints of the devices are registered with the fingerprinter. The fingerprints are extracted from the packets sent by the devices and verified by the fingerprinter. The goal of the attacker is to impersonate a target device by generating packets that contain the fingerprints of that device.

2.2 System and Attacker Model

We consider the following setting: a wireless network is deployed in an area $\mathcal{A}$. The network consists of N wireless devices and a fingerprinting device. A physical-layer identification mechanism is used in the network. During the initialization phase, the fingerprinting device (e.g., wireless access point) extracts a physical-layer fingerprint of each wireless device in its network and stores it in a back-end database. At a later stage, during network operation, the fingerprinter records each packet radio transmission of wireless devices, extracts their fingerprints (according to the specified fingerprinting methodology) and verifies if the extracted fingerprints match one of the reference fingerprints in the back-end database.

The attacker's goal is to break this physical-layer identification mechanism. In Section 5 we define more precisely what constitutes a break in the identification systems that we consider in this paper. We consider the following two impersonation methods and related assumptions:

- *Impersonation by Feature Replay*: In this attack, we modify the radio signal characteristics of an attacker device to closely match all or part of the features used to identify the device targeted for impersonation. We assume that the attacker knows the features used by the identification system and the exact feature extraction, matching and decision making processes as shown in Figure 1.

- *Impersonation by Signal Replay*: In this attack, we record signals from a device targeted for impersonation and retransmit those signals without modification at RF with high-end arbitrary waveform generators. We do not assume any knowledge of the features used for identification.

For both impersonation methods, the attacker is in possession of all necessary hardware equipment to measure and reproduce radio communication signals at any location. He can also build a second fingerprinting device for emulating the entire identification process. The attacker does not have access to the true reference fingerprints captured by the fingerprinter F and the only feedback he can get from F is

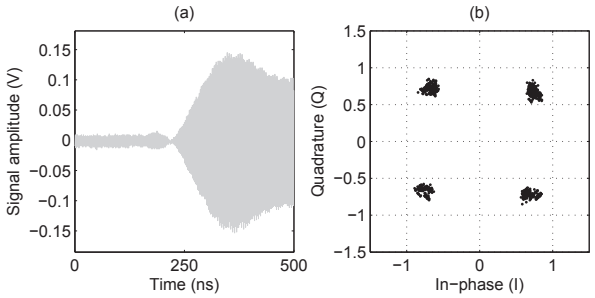

Figure 3: (a) Transient-based techniques extract unique features for device identification from the radio signal transient shape at the start of each new packet transmission. (b) Modulation-based techniques extract frequency and constellation symbol imperfections (i.e., modulation errors).

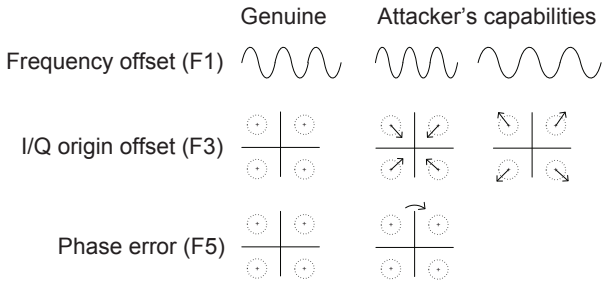

Figure 4: Attacks on modulation-based identification. We are able to modify the signal frequency offset (F1) by changing its carrier frequency in the analog domain, the I/Q origin offset (F3), magnitude (F4) and phase (F5) errors by modifying its original constellation in the digital domain.

an Accept/Reject response. However, in some application scenarios the attacker might have access to the location of the fingerprinter in order to collect the signals from it.

As an instance of the above system and attacker models, we considered a network with 3 wireless devices (Universal Software Radio Peripheral - USRP [11]) and the fingerprinting device is a high-end Agilent Digital Signal Analyzer (DSA) [2]. The attacker is in possession of two devices for the proposed impersonation attacks: a 4-th USRP device and a high-end 20 GS/s arbitrary waveform generator (Tektronix AWG 7000B [25]). These two types of devices allow evaluating an attacker with different strengths: low-cost USRP versus high-quality, but costly signal generator.

3. IMPERSONATION OF MODULATION-BASED FEATURES BY FEATURE REPLAY

In this section, we present an impersonation attack on the modulation-based RF identification proposed in [6]. We first provide background on the identification technique and then detail the attack design, implementation and test scenarios.

3.1 Modulation-based Identification

Modulation-based identification was proposed in [6] as an alternative to transient-based techniques to uniquely identify same model and manufacturer wireless devices. This class of techniques focuses on extracting unique features from the modulated signal. More precisely, the authors in [6] extracted five distinctive signal properties of IEEE 802.11b modulated signals, namely the Frame frequency offset (F1), Frame SYNC correlation (F2), Frame I/Q origin offset (F3), Frame magnitude error (F4) and Frame phase error (F5). These five features together formed a fingerprint of the wireless device, subsequently used for device identification. They were extracted from each packet frame by means of a high-end vector signal analyzer at 70 MHz intermediate frequency (IF) for high precision. The accuracy of the fingerprints for device identification was tested with a k-NN classifier with L1 distance similarity and an SVM classifier with maximum-margin separation [3]. The experimental results from over 100 IEEE 802.11 Network Interface Cards (NIC) demonstrated an identification (classification) accuracy of over 99%.

3.2 Attack Overview and Design

In this attack, we use the capabilities of a USRP with the GNU radio software library [4] to modify parameters in the radio transmission of individual 802.11 packets. In particular, we find that a combination of digital and analog techniques can be applied to modify F1, F3, F4 and F5 detailed below. The basic ideas are summarized in Figure 4.

Frame frequency offset (F1) is the most discriminative feature [6] in the considered modulation-based technique. It represents the difference (offset) between the carrier frequency of the fingerprintee and the fingerprinter. In order to pretend being a given device with respect to F1, we need to adjust the carrier frequency of our attacking device to the carrier frequency of the targeted for impersonation device. We achieved this by using the analog circuit of the USRP which allows arbitrary changes of the carrier frequency with the precision of 0.01 Hz.

Frame SYNC correlation (F2) is the second most discriminative feature. It measures the modulation quality of the frame synchronization preamble by normalized cross-correlation with the ideal synchronization sequence. We found that this feature is difficult to modify in a deterministic way unlike the other features. In Section 5, we demonstrate that it is not necessary to modify this feature in order to impersonate a targeted device with high accuracy. We also show that an attack including impersonation of this feature improves the impersonation accuracy (Section 4).

Frame I/Q origin offset (F3) is the third most discriminative feature in the modulation-based identification. It shows the distance of the ideal I/Q plane centered at (0,0) and the average of all measured I/Q values (symbols in an I/Q constellation) within a packet frame. The Frame I/Q origin offset is usually specific to a given transceiver under the assumption that the analog circuit is provided with the ideal fixed constellation symbols (e.g., $\pm 0.707 \pm 0.707i$ in a Gray-coded constellation). The latter are generated digitally in the digital signal processing (DSP) module of the radio transceiver. In our attack, we digitally shrink or expand the ideal constellation symbols' position in order to change the Frame I/Q origin offset.

Frame Magnitude (F4) and *Phase* (F5) errors are the least discriminative features in the modulation-based identification. The frame magnitude error is the average difference

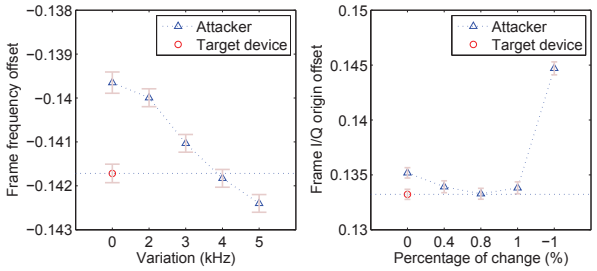

Figure 5: Experimental results on incremental modification of the frame frequency offset (F1) and frame I/Q origin offset (F3). The results show that we can deterministically change feature values of one device in order to match those of a targeted device.

in the scalar magnitude between all ideal and measured I/Q symbol values, while the frame phase error is the average difference in phase (i.e., angle in degrees) between the ideal and all measured I/Q symbol values in the frame. We modify these values in the digital domain by shrinking/expanding the I/Q symbols in order to impersonate these features.

It is important to note that the digital modifications of F3, F4 and F5 must take into consideration the analog circuit deviations that occur in processing the signal from the D/A converter to the antenna and compensate them. In addition, any modifications must also not go beyond the standard tolerances of the impersonated technology [17].

In Figure 5 we show some experimental results from deterministically decreasing the features F1 and F3 of the attacker's device to the values exhibited by the target device (Device 2). In particular, the frame frequency offset is closely equalized at $f = f_C + 4.7$ kHz where f_C is the original carrier frequency of the attacker's device. The Frame I/Q origin offset exhibited by the target device was closely equalized by shrinking the attacker's QPSK constellation points by a factor of 0.7%.

3.3 Implementation details and attack procedure

For the purpose of performing and evaluating the attack, we used four USRPs (3 genuine devices and 1 attacker device). For close matching of the signals used in [6], we developed an 802.11-style QPSK digital baseband modulator. The frame is constructed according to the IEEE 802.11 specification [17] with a preamble (used for coarse frequency offset estimation), followed by a longer preamble for fine frequency offset and channel estimation and the actual data payload. The frequency estimation algorithms were implemented according to [23] which are well established algorithms for that purpose. It should be noted that more sophisticated algorithms will only improve the computation of the errors. The data payload was modulated using QPSK modulation [19]. All packet frames contained the same content transmitted at a data rate of 1Mb/s.

The design of the fingerprinter is shown in Figure 6. Each signal was captured with a standard 2 dB dipole antenna and subsequently amplified by an ultra low-noise and low-power amplifier (NF=0.15 dB) and filtered by a low insertion loss bandpass filter to eliminate radio frequencies outside the industrial, scientific and medical (ISM) band. The received

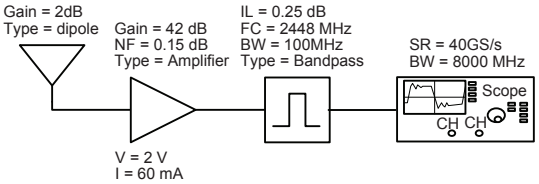

Figure 6: Radio hardware setup of the fingerprinter.

signal was digitized by an Agilent Digital Signal Analyzer [2] and processed by our 802.11-style QPSK digital demodulator for feature extraction. Feature matching and classification was performed offline with Matlab. The genuine devices were positioned at fixed locations to the fingerprinter's antenna. We note that for the modulation-based features the distance should not have an effect on the classification accuracy as outlined in [6].

We started the impersonation attack by modifying the carrier frequency in order to reach the one of the targeted genuine device. We determined the carrier frequency of the targeted device by analyzing the power spectrum density of the radio transmission. Subsequently, we adjusted the frame I/Q origin offset, magnitude and phase of the attacking device by digitally modifying its ideal QPSK constellation symbols (Figure 4) to closely reproduce the feature values of the targeted device after the entire analog processing at the attacking device. Here, we chose to measure the targeted device communication, compute the corresponding features and then adjust them appropriately. There is a second possible approach that consists of launching a hill-climbing attack [5] by repeatedly sending signals with modified features until they are identified as the targeted device.

4. IMPERSONATION OF MODULATION- AND TRANSIENT-BASED FEATURES BY SIGNAL REPLAY

In this section, we demonstrate a device impersonation attack by radio signal replay on modulation and transient-based identification. As opposed to the previous attack, we do not modify the signal characteristics, but retransmit the entire radio packet frame in its integrity at the RF frequency. For the impersonation attacks, we considered the same modulation-based identification technique (Section 3.1) and the transient-based technique described in [8]. We first provide some background on transient-based identification and then the details of the attack design and implementation.

4.1 Transient-based Identification

Transient-based techniques extract unique features for device identification from the radio signal transient occurring at the start of each new packet transmission. The signal transient is the period during which the radio signal amplitude raises to full power. An example transient signal is shown on Figure 3. Data transmission starts immediately after it. A number of characteristics in the signal transient have been explored and shown to be primarily effective in distinguishing classes of wireless devices (model and/or manufacturer). Prominent examples include [13,15,16,20,24,26].

These techniques are of less interest from an impersonation point of view as the attacker can easily choose a de-

vice from the same model and pretend to be a genuine device. Recently, it has been shown in [8] that a carefully designed hardware setup with high-end components complemented with statistical analysis can also accurately distinguish between same model and manufacturer devices using the transient signal. More precisely, the authors proposed filtered FFT-based spectra extracted by means of Linear Discriminant Analysis (LDA) to form device fingerprints of Tmote Sky (CC2420) sensor nodes. The similarity measure between fingerprints for device identification was based on Mahalanobis distance [3]. The accuracy of the technique was estimated by threshold-based operation which is common for biometric systems [5]. Experimental results on 50 identical (same model and manufacturer) sensor nodes demonstrated a very low error rate (EER = 0.24%).

4.2 Attack overview and design

In this attack, we use the capabilities of the 20 GS/s arbitrary waveform generator Tektronix AWG 7000 Series [25]. Due to its fast digital to analog converter, this generator can output any 802.11 signals directly at the required radio frequency of 2.4 GHz. Unlike in the previous attack, where the attacker tries to match as close as possible the features of a device targeted for impersonation, in this attack, we captured the signals of the target device at the RF frequency and replayed them without any modification. This attack is more powerful than feature replay attacks since it does not require knowledge of the features that are extracted by the fingerprinter. It simply requires that the attacker records the transmissions of the targeted device.

A more sophisticated attack based on signal replay would be to produce crafted signals by replaying parts of the message. In the case of modulation-based identification, the attacker can replay the preamble part of the message to reproduce F1 and F2 and craft its own payload. Furthermore, the attacker can also craft his own payload and at the same time reproduce all F3, F4 and F5 features. This is due to the fact that he has full control over the features in the digital domain and relies on the arbitrary waveform generator to directly output the crafted signal in RF thanks to the 20GS/s digital-to-analog (D/A) converter.

In transient-based identification only the transient part of the signal is used for identification [10]. Therefore, the attacker can create a message with the transient part in its integrity concatenated with the actual payload. In this case, the replay attack becomes an impersonation attack. We point out however that such an attack can only be mounted with a high-end arbitrary waveform generator which has the available bandwidth to output the crafted transient signals (e.g., the transient signals in [8] require at least 4 GS/s D/A converter). Such fast conversion is usually way below the capabilities of off-the-shelf software-defined radios (e.g., for the GNU USRP, the D/A converter is 128 MS/s).

4.3 Measurement Setup

To evaluate the impersonation attack by signal replay, we built an experimental setup in a lab environment. The setup consisted of two tripods: the first was used to hold the device to be impersonated; the second holds two identical 2 dB dipole antennas, connected to the fingerprinter and the attacker respectively. Both antennas were fixed on the platform separated by a distance of 30 cm in order to avoid near-field effects, but still get a high signal-to-noise ratio (SNR). The design of the fingerprinter was the same as shown in Figure 6 with an additional implementation of the transient-based feature extraction and matching procedures that were proposed in [8].

We first collected frames from the targeted device. Subsequently, we replayed the recorded frames to the fingerprinter. The evaluation criteria of the attack performance are described in Section 5.

5. PERFORMANCE EVALUATION

In this section, we present the performance results of the impersonation attacks. We first review the metrics and propose definitions for evaluating the performance of such attacks.

5.1 Evaluation criteria

Identification systems are typically evaluated by using a threshold-based approach [5]. The threshold-based approach allows dimensioning the system according to the desired False Accept Rate (FAR) and False Reject Rate (FRR). The Equal Error Rate(EER), i.e. the error where FAR=FRR, is the most common evaluation measure for accuracy. The rate of False Accepts/Rejects is determined by an application specific operating threshold T that serves as an Accept/Reject decision boundary for determining if a given fingerprint is genuine (belonging to the set of genuine fingerprints) or if it is an imposter. All scores from matching two fingerprints coming from the same device form the genuine distribution of matching scores. All scores from matching two fingerprints coming from two different devices form the imposter distribution. We assume that similarity values close to 0 indicate better matching between 2 fingerprints, i.e., the genuine distribution is the one closer to the origin. We used histograms to visualize the two distributions. For threshold-based identification, we use the following definition for a successful impersonation attack:

DEFINITION 1. *We say that an impersonation attack is successful if the matching score between fingerprints of a device targeted for impersonation (D) and that of the attacker (A) is below the application specific threshold T.*

Given that the considered modulation-based approach was evaluated in related work using a classification procedure, we also tested our impersonation attack on classification in Section 5.3.

5.2 Impersonation performance

5.2.1 Impersonation of modulation-based features by feature replay

In this evaluation, we used the capabilities of a software-defined radio for feature replay and followed the design described in Section 3. For data collection, feature extraction and matching, we followed the procedures in [6]. We briefly summarize them: we used 80 valid frames [1] per genuine device and computed the corresponding F1, F2, F3, F4 and F5 features. A device reference fingerprint was built from a total of 20 frames and the remaining 60 frames were used to build testing fingerprints. All presented results were validated using 4-fold cross validation [3]. The similarity score

[1]We consider as valid the frames that comply with the standard [17].

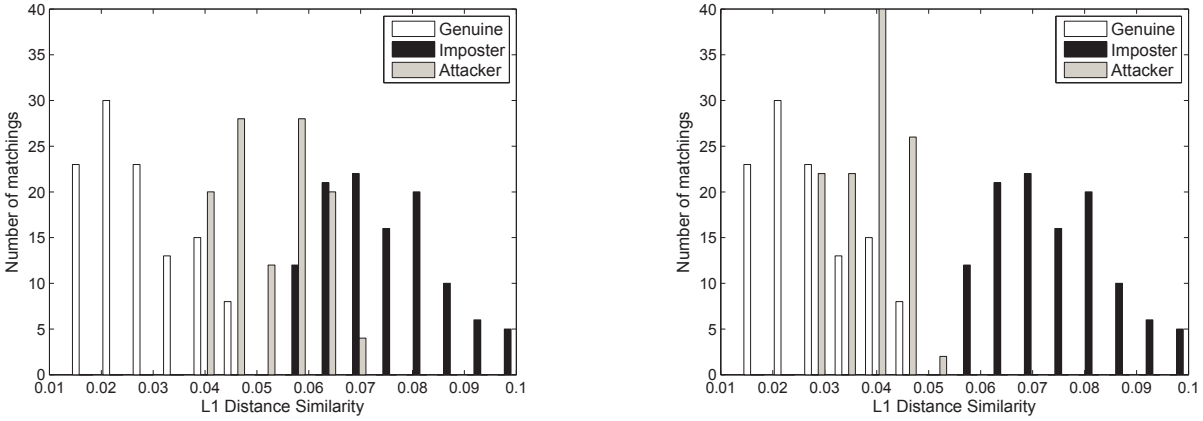

Figure 7: Modulation-based identification: genuine, imposter and attacker matching score histograms: a) Impersonation attack by feature replay of F1 and F3. b) Impersonation attack by feature replay of F1, F3 and F5. The device fingerprints were computed by averaging the features over 5 packet frames. The application specific operating threshold was fixed to $T = 0.05$.

between reference and testing device fingerprints was computed with L1 distance as proposed in [6].

For evaluation with respect to Definition 1, we had to fix the application specific threshold T. We chose to set T to the threshold of the EER operation point which is the mostly used threshold for evaluation [1,5]. In our particular case, EER = 0% and the corresponding $T_{EER} = 0.05$. It should be noted that if one would like to have a realistic estimate of the EER and corresponding T, a much larger amount of devices must be considered [5]. Therefore, the above results, should only be used to assess the attacker's ability to go below the system's operating point T.

To visualize the impersonation attack performance, we computed the genuine, imposter and attacker scores in all folds and show them in the form of histograms. The genuine matching scores were computed by matching the testing frames from the devices to their respective reference fingerprints. The imposter matching scores were computed in the same way, but using the reference fingerprints of the other devices. The attacker scores were computed by matching the impersonating (attacker) frames to the reference fingerprint of the targeted device. We used an average of 5 frames to compute the overall matching score. This is consistent with [6] where it was shown that averaging over more than 4 frames is needed to achieve the highest accuracy.

Figure 7 shows the matching scores of the impersonating (attacker's) frames against the target device (Device 2). If we reproduce only F1 and F3 features, the impersonating frames will be rejected by the system in approx. 60% of the cases according to Definition 1 with $T = T_{EER}$. This is shown in Figure 7a. If we lower the operating point, the system can reject 80% of the impersonating frames while only slightly increasing its FRR. On the other hand, if we reproduce F1, F3 and F5 features, we successfully place 98% of the impersonating frames below T_{EER}, i.e., the impersonation success rate is 98% (Figure 7b).

It should be noted that if the system can tolerate some false rejects, it can reduce the attack success rate, however annihilating the attack without significantly increasing the FRR cannot be achieved (e.g., at $T = 0.025$ the system will reject all impersonating frames, but also 50% of its genuine frames).

In Figure 7b, we also observe that the attacker matching scores are still shifted towards the imposter histogram scores. This is due to the fact that our attack did not modify the F2 and F4 characteristics of the attacking device. We found that F2 was hard to change digitally and F4 could not be independently modified without influencing F3 due to computational dependence. Therefore, we chose to modify the most discriminative of the two, F3. We now show that the impersonation attack by signal replay sufficiently preserves all the features and places all impersonating frames in the genuine matching score space.

5.2.2 *Impersonation of modulation-based features by signal replay*

In this evaluation, we used our high-end 20 GS/s arbitrary waveform generator to retransmit device packet frames in their integrity at RF. Following the procedures in Section 4, we collected 20 frames from the target device (Device 2) at the attacker's position. Subsequently, we retransmitted those frames towards the fingerprinter twice, resulting in 40 impersonating frames. It should be noted that the device signals were captured at RF = 2.4 GHz and sampling rate of 20 GS/s in order to preserve as much as possible the radio signal (e.g., no downconversion to intermediate frequency). The genuine and replayed matching score histograms are shown in Figure 8.

We observe that all the genuine score bins are filled with the scores resulted from matching with the impersonating (replayed) frames. The results demonstrate that signal replay at RF is a powerful attack that makes the impersonating (attacker's) frames very difficult to distinguish from the genuine device frames.

In summary, the modulation-based features and L1 distance similarity measure proposed in [6] are vulnerable to impersonation attacks by feature and signal replay. Impersonation by signal replay at RF makes the impersonating (attacker) frames almost indistinguishable from the genuine frames of the targeted for impersonation device.

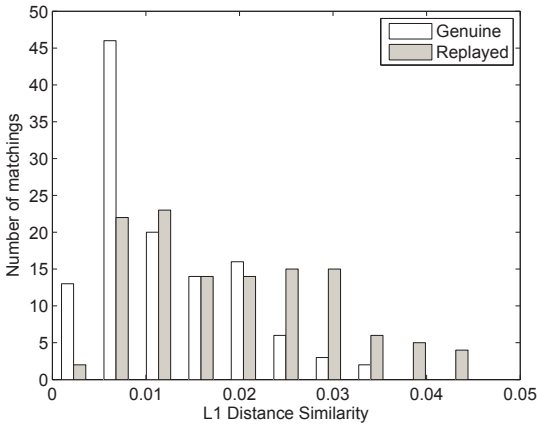

Figure 8: Modulation-based identification: genuine and replayed (attacker) matching score histograms obtained by signal replay at RF with a 20 GS/s arbitrary waveform generator. The two histograms are overlapping making it very difficult to distinguish a genuine device from the attacking device.

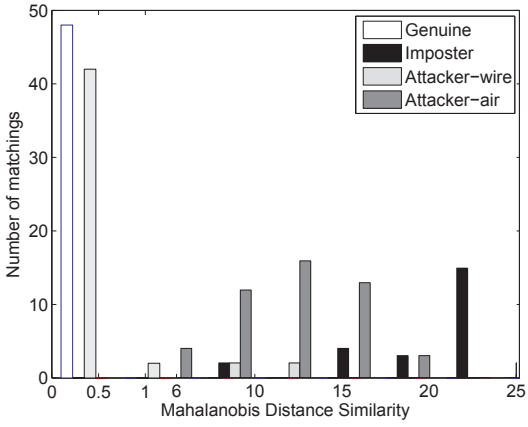

Figure 9: Transient-based identification: genuine and imposter matching scores are from the genuine fingerprinting system; attacker matching scores with fingerprints of the device targeted for impersonation over a wire and over the air. The attacker transient signals over cable are indistinguishable from those of the genuine device.

5.2.3 *Impersonation of transient-based features by signal replay*

As in the previous section, we used the high-end arbitrary waveform generator to retransmit transient signals. We implemented the transient-based identification technique in [8] and followed the proposed procedure in Section 4. We collected transient signals from 3 Tmote Sky sensor nodes in order to fully match the conditions in [8]. We present our results for replaying these signals both using a cable and air interface to better assess the limitations of our attack.

Figure 9 shows the genuine and imposter histograms from matching transient-based features from the original devices captured with our setup as well as the histograms of matching original and replayed transients by arbitrary waveform generator over a cable and over the air. The results clearly show that the replayed signals over the cable closely match the original signals. This is an important result as it shows that the arbitrary waveform generator can retransmit transient signals with high accuracy.

On the other hand, replaying the same signals over the air altered the signals, so that the replayed signals were recognized as imposter signals and the impersonation attack failed. We further investigated the issue and discovered that in addition to the device fingerprint in the transient-based features, there is also the presence of the wireless channel characteristics. In order to confirm the channel effect on the transient, we simulated a frequency selective channel to estimate the degree of modification of the original transient signals under channel changes. The results showed that different channels modify the transient features and the system rejects all attacker's replayed transient signals at the threshold $T = 3.01$ [8].

Impersonation of transient-based spectral features [8] is inherently more difficult due to channel and antenna effects on the transient part of the signal as shown in our analysis. While our high-end signal generator can accurately reproduce it as well over a cable (i.e., fixed channel), replaying over the air from a different location is not likely to be successful to impersonate a device. However, we could impersonate the targeted device from its location. There are two possible scenarios that could achieve this depending on the attacker model. In the first scenario, if we are allowed to measure the transient signal of the targeted device before actual transmission through the antenna (e.g., capture the device and measure over a cable with an oscilloscope), we can then replay it with the arbitrary waveform generator from the same location. In the second scenario, a possible compromise of the fingerprinter would reveal the transient signal received at the fingerprinter. Subsequently, we need to estimate the wireless channel response between the targeted device location and the fingerprinter, compensate the transient signal accordingly and replay it with the arbitrary waveform generator. This second scenario can also be applied if the attacker is allowed to collect frames at the location of the fingerprinter.

5.3 Impersonation in classification

Given that the considered modulation-based identification was evaluated using classification [6], we also evaluated our modulation-based feature impersonation by feature replay in terms of classification accuracy. In standard classification, unlike in threshold-based identification, there is no notion of rejection based on threshold, i.e., the classifier assigns an unknown device fingerprint to the device that has the highest similarity in the entire set of devices. Therefore, we need to adopt a different definition as follows:

Definition 2. *We say that an impersonation attack is successful with probability p if the classification process assigns the fingerprints of attacker (A) to the class of fingerprints of the device targeted for impersonation (D) with probability p.*

We considered the k-Nearest Neighbor (k-NN) and Support Vector Machine (SVM) classifiers trained and executed as in the related work [6]. The data collection and feature

Table 1: Classif. success rates on genuine devices

1-NN	3-NN	5-NN	SVM
87.65%	97.78%	100%	100%

extraction are the same as in Section 5.2. For complete compliance with [6], in the k-NN [2] classifier half of the training frames (10) were discarded from the reference device fingerprint by removing the frames whose features deviated the most from the overall mean. No frames were removed from the testing set. The similarity measure was L1 distance.

The classification success rates using k-NN and SVM classifiers for distinguishing the 3 genuine devices are shown in Table 1. Both k-NN and SVM classifiers successfully classify the fingerprints of the genuine devices. Inline with [6], the k-NN classifier requires averaging over a number of frames ($k \geq 4$) to reach its highest accuracy. In our case, a success rate of 100% was reached for $k = 5$.

After tuning our attacking software-defined radio device in order to match the feature F1, F3 and F5 of the target device (Device 2) as well as possible (see Figure 5), we injected the attacker's collected frames in the k-NN and SVM classifiers by replacing all Device 3 frames and computed again the classification success rates.

The results in Table 2 show the success rate of classifying genuine frames and impersonating frames with feature replay of F1 and F3. The impersonation attack success rate is 62% for the 5-NN classifier, while for the SVM classifier it tops 100%. On the other hand, if the attacker performs a feature replay with F1, F3 and F5, it will impersonate both classifiers in 100% of the cases (Table 3). An impersonation attack by signal replay also succeeds in 100% inline with the results in Section 5.2.

It should be noted that the above results on classification are highly dependent on the number of classes (devices) and the separability between different device fingerprints. It is interesting to observe that a system with highly discriminative classifier such as SVM was easier to impersonate ($p = 100\%$ with 2 reproduced features). In our case, this is due to the fact that SVM builds large decision boundaries well separating the three devices. Therefore, few modifications of the features towards the features of one of the 3 devices make the impersonating frames cross the decision boundary of that device. However, if the number of classes is larger, this might not be sufficient and more impersonated features would be required. This finding suggests that if the attacker can modify only some of the features of an identification technique, a good strategy would consist of identifying a device in the network that differs the most from all other devices and try impersonating that device. We also point out that a general problem of standard classification is that without a rejection criterion, the attacker would be always assigned to one of the genuine devices.

6. IMPLICATIONS AND FUTURE WORK

This work demonstrates that impersonation attacks on modulation and transient-based physical-layer identification are feasible and realistic. Our findings show that in a number of application scenarios, where their use has been suggested, these techniques cannot be safely used. A prominent example is access control where access is granted based on the recorded device fingerprint. From the results of this work it is clear that the use of physical-layer identification for access control is inherently insecure, unless this identification is combined with additional measures (e.g., physical device inspection). Our results also have implications on other applications of physical-layer identification such as device tracking and device cloning detection. Assuming that a device that is tracked can impersonate other devices, as we have demonstrated to be feasible, it could hide its identity by pretending to be a known or unknown device (i.e., the one with a fingerprint that has not appeared before). On the other hand, if an attacker wants to clone a device (e.g., an e-passport), he would need to be able to generate genuine fingerprints by a device that has similar external appearance as the one that is being cloned; in the case of an e-passport cloning the chip within a cloned passport would need to reproduce a fingerprint of a genuine passport. It is not clear if this is feasible; our results only show that impersonation can succeed with specific software-defined radios (SDR) or arbitrary waveform generators (AWG).

[2]We complied to the definition of parameter k and notation k-NN in [6]. We note that these definitions are different from the commonly accepted ones in pattern recognition [3].

Table 2: Genuine and attacker classification success rate on Device 2 by feature replay of F1 & F3

	1-NN	3-NN	5-NN	SVM
Input	Device 2	Device 2	Device 2	Device 2
Device 2	73.33%	98.33%	100%	100%
Attacker	50%	50%	62.33%	100%

Table 3: Genuine and attacker classification success rate on Device 2 by feature replay of F1, F3 & F5

	1-NN	3-NN	5-NN	SVM
Input	Device 2	Device 2	Device 2	Device 2
Device 2	73.33%	98.33%	100%	100%
Attacker	63.33%	98.33%	100%	100%

We also note that further research is needed to validate if the SDRs used in our work are also able to impersonate by feature replay commercial off-the-shelf IEEE 802.11 NICs. Given that SDR hardware is rather different (e.g., noise figures), additional enhancements may be required in order to perform such an attack.

Our results further motivate the investigation of techniques that would detect impersonation by signal or feature replay. These techniques would typically have to either make sure that the signals or features are not known to the attacker such that he cannot replay them or would have to detect from the replayed signals that they have been replayed (e.g., by looking for features specific to SDRs or AWGs). Whether such impersonation detection is feasible, is an open question that motivates future work.

7. RELATED WORK

Parallel to our investigation, the authors in [9] independently explored attacks on modulation-based identification. Our work differs in a number of aspects. First, in our work, we investigate feature- and signal-replay based impersonation of both modulation and transient fingerprints using both software-defined radios (SDR) and high-end arbitrary waveform generators; the work in [9] investigates only impersonation of modulation-based features using SDRs. Sec-

ond, the work in [9] achieves lower impersonation rates of 55-75%. This is due to significant differences in our feature- and signal-replay attack semantics and measurement setup and feature extraction as follows: we used 8 GHz oscilloscope to measure the signal imperfections with high precision; our modulation-based feature extraction followed [6], while in [9] some of the most discriminative features (e.g., F2) were not computed, and therefore altered the original design; we used a high-end arbitrary waveform generator for signal replay at RF as opposed to an SDR in [9]; finally, we evaluated the effectiveness of the attacks using both threshold-based identification and two classifiers (k-NN and SVM), whereas the work in [9] evaluates only using SVM.

Transient techniques for RF identification was initially explored to detect illegally operating radio transmitters [16, 26, 27], device cloning [18] and defective devices [28]. Subsequently, various physical characteristics [10] were explored on Bluetooth and 802.11 devices [13, 15, 20, 22, 24] showing the ability to classify different classes of devices (e.g., manufacturer). In particular, Hall et al. [13, 14] explored a combination of features such as amplitude, phase, in-phase, quadrature, power and DWT of the transient signal. The authors tested 30 IEEE 802.11b transceivers from 6 different manufacturers and achieved a classification error rate of 5.5%. Further work on 10 Bluetooth transceivers from 3 manufacturers recorded a classification error rate of 7% [15]. Ureten et al. [20] extracted the envelope of the instantaneous amplitude and classified the signals using a Probabilistic Neural Network (PNN). The method was tested on 8 IEEE 802.11 transceivers from 8 different manufacturers and registered a classification error rate of 2 - 4%.

Recently, a transient-based technique was proposed for identifying identical IEEE 802.15.4 (CC2420) sensor node devices [8]. The authors experimentally demonstrated the ability to identify such devices with an EER of 0.24%. Modulation-based identification was proposed by Brik et al. [6]. The technique accurately captures the variance of frequency and modulation errors. The authors achieved a classification error rate of 3% and 0.34% for k-NN and SVM classifiers respectively on IEEE 802.11 NICs. We consider both of the above techniques in our work.

Physical-layer identification was recently demonstrated for RFID transponders [7] as well. Physical-layer techniques based on the wireless channel characteristics were explored for location distinction [12, 21, 29]. The latter two uses are out of the scope of this work.

8. CONCLUSION

In this paper, we investigated the feasibility of performing impersonation attacks on physical-layer identification techniques. We designed and implemented a number of impersonation attacks by feature and signal replay on the two most prominent techniques, namely modulation and transient-based identification. We analyzed their efficiency in threshold-based identification and classification. Our results showed that modulation-based features are vulnerable to feature and signal replay, whereas transient-based identification is vulnerable to signal replay attacks. We further showed that transient-based features can be accurately replayed over a wire, however due to presence of wireless channel and antenna characteristics in the recorded transients, actual replay over the air is likely to succeed only from the location of the device targeted for impersonation.

Acknowledgments

The authors thank Marc Kuhn and Armin Wittneben for their suggestions and assistance during the project. This work was partially supported by the Zurich Information Security Center. It represents the views of the authors.

9. REFERENCES

[1] Fingeprint verification competitions (FVC). http://bias.csr.uni-bo.it/fvc2006/.

[2] Agilent. *Digital Signal Analyzer (DSA) 90804A*, 2008. http://www.home.agilent.com/.

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

[4] Blossom, E. GNU software radio. http://www.gnu.org/software/gnuradio/.

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

[6] Brik, V., Banerjee, S., Gruteser, M., and Oh, S. Wireless device identification with radiometric signatures. In *Proc. ACM International Conference on Mobile Computing and Networking (MobiCom)* (2008).

[7] Danev, B., Heydt-Benjamin, T. S., and Čapkun, S. Physical-layer identification of RFID devices. In *Proc. USENIX Security Symposium* (2009).

[8] Danev, B., and Čapkun, S. Transient-based identification of wireless sensor nodes. In *Proc. ACM/IEEE Conference on Information Processing in Sensor Networks (IPSN)* (2009).

[9] Edman, M., and Yener, B. Active attacks against modulation-based radiometric identification. TR 09-02, Rensselaer Institute of Technology, Aug. 2009.

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

[11] Ettus, M. Universal software radio peripheral (USRP). http://www.ettus.com/.

[12] Faria, D. B., and Cheriton, D. R. Detecting identity-based attacks in wireless networks using signalprints. In *Proc. ACM Workshop on Wireless Security (WiSe)* (2006).

[13] Hall, J., Barbeau, M., and Kranakis, E. Enhancing intrusion detection in wireless networks using radio frequency fingerprinting. In *Proc. Communications, Internet, and Information Technology (CIIT)* (2004).

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

[15] Hall, J., Barbeau, M., and Kranakis, E. Detecting rogue devices in Bluetooth networks using radio frequency fingerprinting. In *Proc. IASTED International Conference on Communications and Computer Networks (CCN)* (2006).

[16] Hippenstiel, R., and Payal, Y. Wavelet based transmitter identification. In *Proc. International Symposium on Signal Processing and Its Applications (ISSPA)* (1996).

[17] IEEE Standards Association. *IEEE Standard 802.11b-1999: Wireless LAN MAC and PHY Specifications*, 1999.

[18] Kaplan, D., and Stanhope, D. Waveform collection for use in wireless telephone identification. US Patent 5999806, 1999.

[19] Oppenheim, A., Schafer, R., and Buck, J. *Discrete-Time Signal Processing*. Prentice-Hall Signal Processing Series, 1998.

[20] O.Ureten, and N.Serinken. Wireless security through RF fingerprinting. *Canadian Journal of Electrical and Computer Engineering 32*, 1 (Winter 2007).

[21] Patwari, N., and Kasera, S. Robust location distinction using temporal link signatures. In *Proc. ACM International Conference on Mobile Computing and Networking (MobiCom)* (2007).

[22] Rassmussen, K., and Capkun, S. Implications of radio fingerprinting on the security of sensor networks. In *Proc. International ICST Conference on Security and Privacy in Communication Networks (SecureComm)* (2007).

[23] Schmidl, T., and Cox, D. Robust frequency and timing synchronization for OFDM. *IEEE Transactions on Communications 45*, 12 (1997).

[24] Tekbas, O., Ureten, O., and Serinken, N. Improvement of transmitter identification system for low SNR transients. In *Elec. Letters* (2004), vol. 40.

[25] Tektronix. *Arbitrary Waveform Generator 7000*. http://www.tek.com/products/signal_sources/awg7000/.

[26] Toonstra, J., and Kinsner, W. Transient analysis and genetic algorithms for classification. In *Proc. IEEE Conference on Communications, Power, and Computing (WESCANEX)* (1995).

[27] Toonstra, J., and Kinsner, W. A radio transmitter fingerprinting system ODO-1. In *Proc. Canadian Conference on Electrical and Computer Engineering* (1996).

[28] Wang, B., Omatu, S., and Abe, T. Identification of the defective transmission devices using the wavelet transform. *IEEE Transactions on Pattern Analysis and Machine Intelligence 27*, 6 (2005), 696–710.

[29] Xiao, L., Greenstein, L., Mandayam, N., and Trappe, W. Fingerprints in the ether: Using the physical layer for wireless authentication. In *Proc. IEEE International Conference on Communications (ICC)* (2007).