Detection of DECT identity spoofing through Radio Frequency fingerprinting

I. Sanchez *, R. Satta†, R. Giuliani‡, G. Baldini§
European Commission – Joint Research Centre (JRC), Institute for the Security and Protection of the Citizen,
Digital Citizen Security, Ispra, Via E. Fermi 2749, 21027, Italy
Emails:* ignacio.sanchez@jrc.ec.europa.eu†riccardo.satta@jrc.ec.europa.eu, ‡raimondo.giuliani@jrc.ec.europa.eu,
§ gianmarco.baldini@jrc.ec.europa.eu

***Abstract*—Digital Enhanced Cordless Telecommunications (DECT) is an European Telecommunications Standards Institute (ETSI) standard for short-range cordless communications with a large worldwide installed customer base, both in residential and enterprise environments. As in other wireless standards, the existence of active attacks against the security and privacy of the communications, involving identity spoofing, is well documented in the literature. Although the detection of spoofing attacks has been extensively investigated in the literature for other wireless protocols, such as Wi-Fi and GSM, very limited research has been conducted on their detection in DECT communications. In this paper, we describe an effective method for the detection of identity spoofing attacks on DECT communications, using a radio frequency fingerprinting technique. Our approach uses intrinsic features of the front end of DECT base stations as device fingerprints and uses them to distinguish between legitimate and spoofing devices. The results of measurement campaigns and the related analysis are presented and discussed.**

I. Introduction

In wireless communication networks, spoofing is a serious attack where a malicious attacker masquerades as a legitimate mobile device and transmits false information. Device identity spoofing is often used as part of larger and more complex active attacks that require sending forged information originated from the identity of a legitimate device of the network.

DECT, Digital Enhanced Cordless Telecommunications [1], is a radio frequency protocol developed by ETSI, widely used in residential and enterprise environments for the transmission of voice in cordless telephony. It is considered by ETSI as its second most successful protocol after GSM, with an estimated install base of almost 820 millions of cordless phones world-wide [2]. DECT is largely widespread in Europe, where it is commonly used by citizens in residential environments as wireless access protocol for fixed telephony. It is also commonly found in enterprise environments, usually integrated into Unified Communication systems.

Despite the security features foreseen in the standard, several attacks against the security and privacy of DECT communications have been described in the literature. In addition to passive attacks against both non-encrypted [3], [4] and encrypted communications [5], [6], a set of active attacks, involving the injection of spoofed DECT packets into the network, has also been described in the literature. In [3], the authors demonstrate how the lack of mutual authentication in some implementations of the standard, can be exploited to perform a Man-In-The-Middle attack able to intercept the voice communications of the victim. In order to do so, the attacker impersonates the identity of the legitimate DECT base station (Fixed Part - FP), spoofing its identity in such a way that the Portable Part (PP) of the victim will eventually connect to it, instead of the legitimate one. In essence, this attack is similar to the one described in the literature [7], [8] for GSM networks, where the identity of the Base Station (BTS) is spoofed by the attacker.

The application of DECT identity spoofing has also been proven to be effective attacking encrypted communications, as part of a more complex active attack. In [9] the authors demonstrated an active attack that sends spoofed DECT packets into the network in order to progressively decrypt an encrypted communication.

The identification of device identity spoofing on DECT networks is an effective way to generically detect a big percentage of active attacks that rely on the injection of spoofed packets into the network. To this end, several approaches can be followed. One approach would be the detection of the spoofed packets based on anomalies in the data and metadata contained in the spoofed packets. This technique could be effective in certain cases where differences between the legitimate and the spoofed packets can be appreciated by looking at their content, as it has been demonstrated in GSM networks for the detection of rogue base stations [10] and in Wi-Fi for the detection of MAC address spoofing on the basis of the analysis of the sequence numbers [11].

In many cases, these detection methods can be circumvented by an attacker, by carefully imitating or jamming the data transmitted by the legitimate station, given the fact that the features used in the detection can be easily modified by the attacker to match the legitimate ones.

In order to tackle this point, the radio frequency (RF) fingerprinting of mobile devices has been proposed as a method for the detection of active attacks in other protocols such as GSM [12] and Wi-Fi [13].

The basic idea behind the RF fingerprinting technique, is that each electronic device has unique features, also called Radio-Frequency Distinctive Native Attributes or (RF-DNA), which can be extracted from its spectral emissions and can be used to uniquely identify the specific model or mobile device. The RF pattern cannot be manipulated at the software level by the attacker, and is therefore hard to forge, even using customisable transceivers, such as those based on Software-defined radio.

In other words, the term RF-DNA is used to embody the coloration of RF emissions (both intentional and unintentional) induced by the intrinsic physical attributes of a unique device and related to components like filters, amplifiers, Integrated Circuits (IC) and so on. While other authors have focused their research efforts in the unintentional emission as in [14], in this paper we focused on the intentional emissions of the DECT base station during transmission and/or signal broadcast.

The use of fingerprinting to detect spoofing has been also proposed in other wireless communication technologies other than DECT. In [15], the authors have applied RF-DNA fingerprints to IEEE 802.16 WiMax-based airport communications by using both Time Domain (TD) and Wavelet Domain (WD) techniques.

Another popular application for fingerprinting is related to Wi-Fi technology. In [16], the authors used unique features extracted from RF-components or from the timing behavior of the MAC-chips to attest the uniqueness of a dedicated wireless station. The authors argue that Wi-Fi Protected Access (WPA) or IEEE 802.11i (WPA2) are not a complete protection against MAC address spoofing because WPA and WPA2 can provide data-frame authentication to prevent clients from being spoofed but unfortunately they do not provide authentication for management frames. The authors applied different approaches for fingerprinting. In one case, Discrete Wavelet Transformation (DWT) was applied to signal phase and signal amplitude to generate features used for the classification process. In another approach, the analysis of the distribution of delay values between 802.11 packets and the corresponding acknowledgment frames was used for fingerprinting as delay values differ in various chipsets.

Still on Wi-Fi technology, Sheng and others [17] applied the analysis of received signal strength (RSS) for fingerprinting on the basis of the RSS patterns (e.g., their Gaussian profile). This approach has the merit to avoid the need for sampling the RF signals, as in [14] and [16], even if this need has become less costly with the latest generations of sampling devices (e.g., the RTL-SDR).

In [18], the authors applied RF-DNA fingerprints to mitigate the risk of impersonation of authorized network devices. The fingerprinting was implemented using Multiple Discriminant Analysis (MDA) for training and authorised device classification and Multivariate Gaussian (MVG) likelihood values to identify rogue devices attempting to gain unauthorized network access by presenting false bit-level credentials. Finally, in a recent paper [19] the authors have applied Support Vector Machine (SVM) to identify GSM phones based on their uplink RF emissions. The analysis in [19] is similar to what done in this paper because the fingerprinting method was based on instant amplitude as in this paper and GSM have some similarities to DECT (e.g., modulation scheme).

As we described above, fingerprinting analysis has been applied to various widespread wireless communication technologies like Wi-Fi, WiMax, GSM and Zigbee but we are not aware of similar analysis for DECT. The purpose of this paper is to cover this gap and provide some preliminary results to mitigate the spoofing of DECT by using a simple, yet effective, RF fingerprinting technique.

The structure of the paper is the following. In section II, we describe the DECT standard. In section III we provide a description of the measurement setup and the definition of the algorithms for classification and identification, which have applied to provide the results in section IV. Finally, V describes the conclusions and potential future developments of this paper.

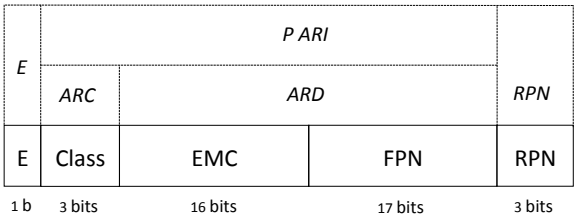

Fig. 1. Radio Fixed Part Identity (RFPI)

II. Digital Enhanced Cordless Telecommunication standard

In Europe, the DECT protocol operates in the range of 1800 Mhz to 1900 Mhz, where a total of 10 physical channels are allocated, using Frequency Division Multiple Access (FDMA), leading to the creation of a total 120 logical channels by dividing each physical channel into 12 logical channels using Time Division Multiple Access (TDMA), with separate time slots for the reception and transmission of data following Time Division Duplexing (TDD). Each DECT device will only transmit in its assigned time slot, producing bursts that will be clearly identifiable in the DECT channel assigned for the transmission.

A typical DECT installation will be composed of one or more cordless phones, denoted as Portable Parts (PP) in the standard, registered to a DECT base, named Fixed Part (FP). In a residential installation, the FP is typically connected to the fixed telephone line and also acts as a battery charger for the portable parts. In enterprise installations, the portable parts are registered to the FP, which is, in many cases, integrated into a Private Automatic Branch eXchange (PABX) system. In recent years, a new generation of residential Unified Communication systems have started to integrate DECT devices for the Smart Home ecosystem. The Generic Access Profile (GAP) of the DECT standard ensures the interoperability of fixed and portable parts from several manufacturers.

Each FP is identified by a RFPI (Radio Fixed Part Identity), which is a 40-bit number mainly composed of a 16-bit Equipment Manufacturer's Code (EMC), a 17-bit Fixed Part Number (FPN) and a 3-bit Radio fixed Part Number (RPN). The first 4 bits of the RFPI, reserved for the E bit and the class type, are set to zeros in residential and small corporate DECT installations (Class A). Figure 1 depicts the composition of the RFPI and the formal relation of each part with the Access Right Class (ARC), Access Right Details (ARD) and Primary Access Rights Identity (PARI) fields.

The EMC code determines the specific manufacturer of the FP. The FPN and FPN codes are assigned by the manufacturer and will uniquely identify a specific FP device. Unless an ECO mode is enforced, a FP will continuously advertise its

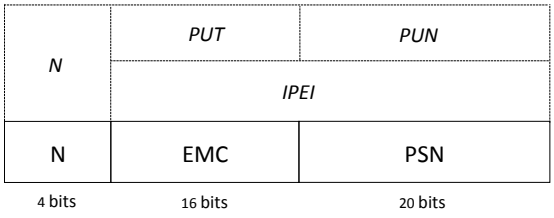

Fig. 2. International Portable User Identity (IPUI)

presence by broadcasting its RFPI, sending 100 DECT frames per second. Due to this fact, a physical channel with a single FP and no active PP communications, will show short bursts in regular intervals of 10 milliseconds. Each burst is a DECT frame that is composed of a preamble, the A field data where the RFPI is located and an optional B field in case there is voice being transmitted in the frame.

On the other end, the PP is uniquely identified by a 40 bit number called IPEI (International Portable Equipment Identity) that is composed of a 4-bit identity type field (type N for residential and small corporate set-ups), a 16-bit EMC and a 20-bit Portable equipment Serial Number (PSN) code. Both EMC and PSN are known as the Portable Part Equipment Identity (IPEI) and uniquely identify the specific PP device, with the EMC uniquely identifying the manufacturer and the PSN the specific device. Figure 2 depicts the composition of the IPEI.

When a PP is registered into a given FP, the RFPI of the FP is known to the PP and it is stored in its permanent memory. Similarly, the IPUI of the PP is registered in the permanent memory of the FP. A PP will monitor the available DECT channels and identify the corresponding FP on the basis of the RFPI code transmitted in the DECT frames.

The DECT standard foresees the usage of authentication, by using the DECT Standard Authentication Algorithm (DSAA), and encryption, by means of the DECT Standard Cipher (DSC). The Generic Access Profile (GAP) part of the standard ensures the interoperability between different DECT models and manufacturers and establishes a pairing process in order to register a DECT handset (PP) into a base station (FP). As part of this process, a long term key, named User Authentication Key (UAK), will be exchanged and permanently stored by both PP and FP.

The DSAA algorithm will use the UAK key for authentication and negotiation of temporal session keys, named Derived Cipher Keys (DSC), which will be used by the DSC algorithm for the encryption of the communications between FP and PP.

It shall be noted that DSC encryption, which protects the confidentiality and up to a certain point the integrity of the data, is only applied against the B-field (voice) and C-channel data (control information). The RFPI and IPUI identities included in the A-field of the FP and PP frames respectively, are not protected.

In that regard, for the purposes of this paper it is sufficient to say that there are several weaknesses on the security of the DECT GAP communications and, as described in section I, various active attacks against DECT communications that involve spoofing of the DECT devices identities have been described in the literature.

III. Fingerprinting analysis

A. Measurement setup

A schema of the measurement setup is provided in Figure 3. The correspondent image of the measurement setup used to collect the radio frequency emissions is provided in Figure 4.

The test-bed is in a shielded semi-anechoic chamber (i.e., absorbers are only partially covering the walls of the chamber). The DECT handset and the base station are separated at a distance of four meters and at a height of one meter from the ground. In the experiments performed, a total of 4 DECT models were analyzed from 2 well known manufacturers of DECT cordless phones.

The receiver used to record the radio frequency samples is an Universal Software Radio Peripheral (USRP) N210 with a configured sampling rate of ten mega samples I/Q per second. The receiver is located in the middle between the DECT handset and the base station (i.e., two meters from each DECT component) and it is also at an height of one meter from the ground. The antenna is a vertical omni-directional full wavelength monopole. The USRP N210 is connected to a desktop computer for the recording and the processing of the samples. To avoid possible biases, the USRP and its antenna inside the shielded semi-anechoic chamber, were the same for all the signal acquisitions.

The experiments were focused on the scenario where the identity of the DECT base station (FP) is spoofed by an attacker, so the recordings of the samples took place with and without PP transmissions. As described in section II, the FP transmits 100 frames per second, even in the absence of a call or PP activity. This was the case for all the DECT models analyzed.

The signals were acquired in 2 rounds for the 4 DECT devices and stored in I/Q format. The signals acquired the first day for all the devices became the training dataset and the set recorded the second day (also for all the devices) was used for testing, as it will be described in the next section.

B. Algorithms for fingerprint verification

Formally, the detection of a spoofing attack can be modeled in the same way of biometric fingerprint *verification* [20], i.e., an one–VS–one comparison of two fingerprints. The first one is the *template* fingerprint of the target DECT base station B, the second one is the fingerprint of the base station who "claims" to be B.

The template fingerprint of a base station is constructed, as follows, from a recorded radio transmission originated from that base station. First, we process in MATLAB the samples recorded by the USRP N210 in I/Q format, in order to identify and process the bursts.

In order to do so, we first calculate the modulus of the I/Q signal. Then we apply a low pass filter to ensure that only the in-band DECT signal is used to fingerprint the DECT device. In our case, we adopted a 2nd order Butterworth filter with a

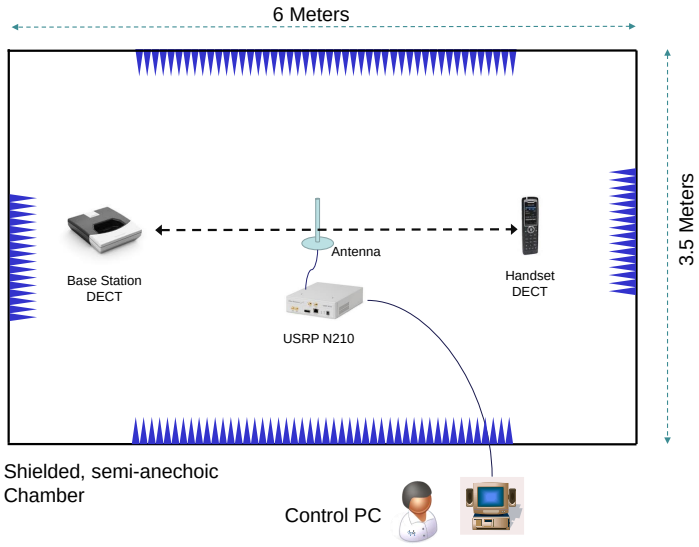

Fig. 3. Schema of the test bed used to collect the radio frequency emissions

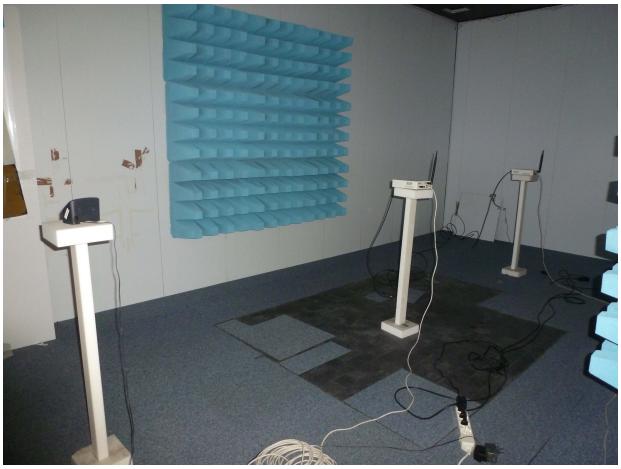

Fig. 4. Image of the test bed used to collect the radio frequency emissions

normalized cutoff frequency of $10e-5\ \pi$ rad per sample in normalized frequency. The Butterworth filter is used because it provides a flat response in the DECT frequency bands. A flat response is more appropriate because we did not know a priori which frequency components of the DECT signal could be more valuable for fingerprinting.

Once the Butterworth filter is applied, the bursts are identified by detecting the ramp-up and ramp-down of the signal. Each burst is normalized to the maximum amplitude of that specific burst and extracted using a fixed thresholding to synchronize it with the others.

We are interested only in the part of the burst which is not related to the content being transmitted (e.g., the voice during the DECT call), in order not to fingerprint content differences rather than the DECT device itself. The content invariant parts in the bursts are the ramp-up and ramp-down sections of a burst plus the preamble. Apart from being content invariant, these sections are appropriate for fingerprinting because they are more related to the physical properties of the front-end of the wireless devices [15].

The ramp-up and ramp-down sections plus the preamble of each burst are then stored in arrays, which are the primary source of data for the fingerprinting algorithms described in the following paragraphs. For simplicity, the combination of ramp-up and ramp-down and preamble are called mini-bursts in the rest of the paper to differentiate them from the initial raw bursts.

The mini-burst of both datasets are normalized into the interval $[0, 1]$, to make their signals comparable. In an initial training phase, a template T_B of the base station B is created by calculating the average of all the mini-bursts stored in the training dataset for that specific DECT device.

Verification of a given mini-bursts b^* of the validation dataset is then performed by computing a *burst similarity score* $S(T_B, b*)$, defined as the Normalized Cross-Correlation between T_B and b^* (both real vectors of the same length):

$$S(T_B, b^*) = \frac{(T_B - \bar{T_B}) \cdot (b^* - \bar{b^*})}{\|T_B - \bar{T_B}\| \cdot \|b^* - \bar{b^*}\|} \quad (1)$$

where $\bar{T_B}$ and $\bar{b^*}$ are the means of T_B and b^*, respectively. The value of $S(T_B, b*)$ measures the likelihood that b^* is a mini-bursts transmitted by the base station B. NCC was chosen as likelihood measure as it evaluates the similarity of the *behaviour* of the two signals (i.e., to which extent the vary in the same way over time) rather than the similarity of their values as it would be done e.g. by the Euclidean distance.

In order to obtain a sharp Yes/No decision, a threshold Th is applied so that b^* is deemed as coming from the base station B only if $S(T_B, b*) \geq Th$. The value of Th impacts on the False Positives (i.e., false alarms triggered by the spoofing detection systems) and of False Negatives (i.e., spoofing attacks not detected). In particular, the higher the threshold, the lesser False Positives, and the more False Negatives. It is worth to point out that False Positives and False Negatives can be reduced by verifying more than one mini-burst, and then decide on a majority vote (provided that the initial number of errors is lower than 50%). In this paper, we measure the accuracy when only one mini-burst is verified.

IV. Results and Discussion

Figure 5 shows the mini-burst templates calculated for each of the four classes, generated by taking the average of all the mini-bursts extracted out of the training data. This is the result of the training phase, where the mini-burst templates of each DECT device are calculated.

Distinct patterns can be appreciated visually in the transient part of the signal, particularly in the ramp-up, possibly generated by front-end components of the DECT device including filters and amplifiers [15].

The verification scenario was carried out with the signals acquired a second day (validation dataset). Figure 6 reports False Positive and False Negative ratios with respect to the selection threshold, as well as the Equal Error Rate (EER), i.e., the point at which the two errors are equal.

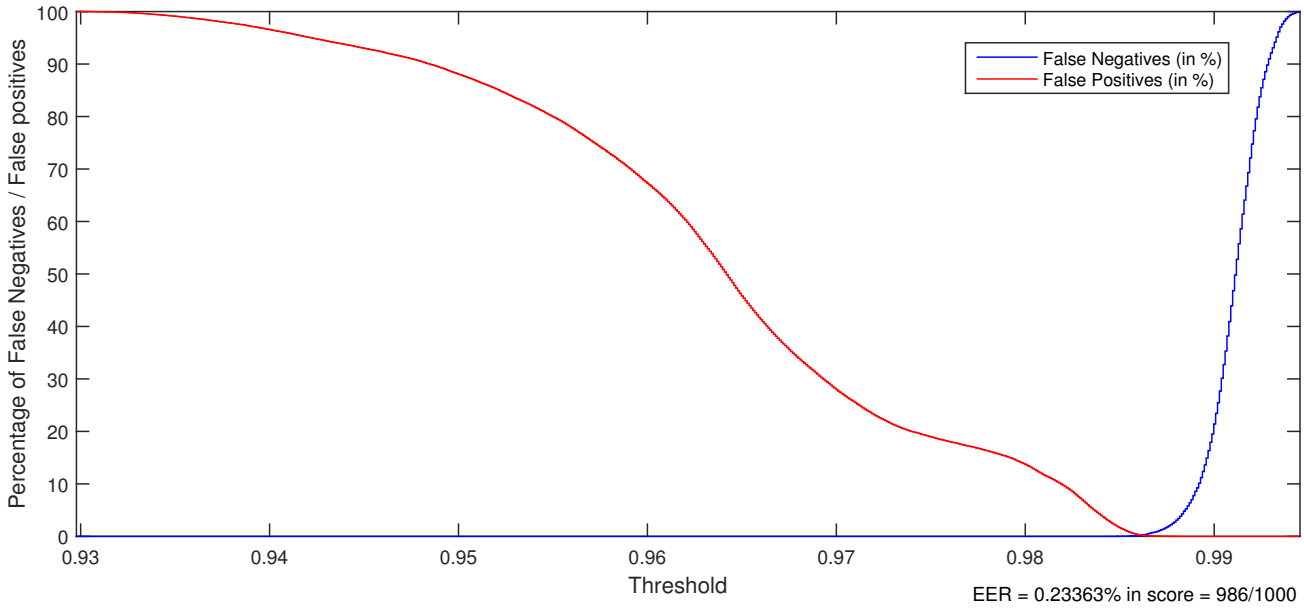

Fig. 6. False Positive and False Negative rates versus decision threshold Th. The Equal Error Rate (EER), i.e., the point where False Positive and False Negative rates are equal, is also reported.

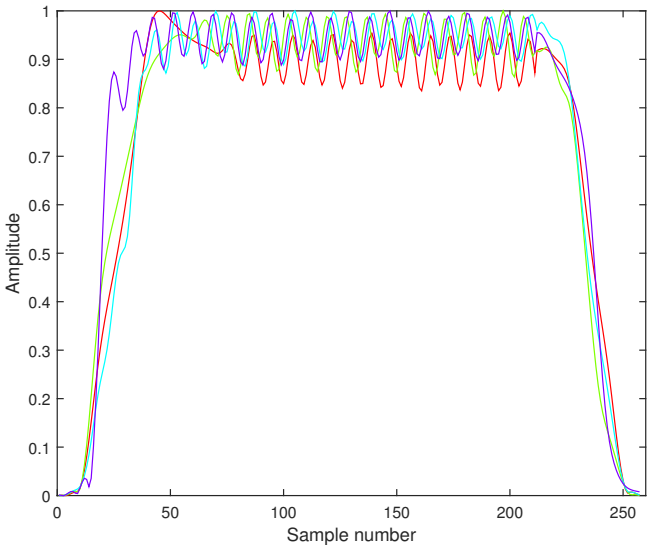

Fig. 5. Averaged Mini-bursts

The results of burst verification clearly show that it is possible to achieve almost 0% Equal Error Rate, i.e. a perfect discrimination between legitimate bursts and attacks. However, it is worth to point out the limited extent of our evaluation, which was limited to a small data set of bursts coming from four base stations. A more fair evaluation should average the results attained with several devices. Nevertheless, as highlighted in III-B if necessary the accuracy can be easily increased by classifying several bursts in place of only one, and then apply a majority voting rule.

In most of the actual spoofing scenarios, the hardware used by the attacker will be sensibly different from the one of the legitimate DECT FP whose identify is being spoofed. This is specially the case where the attacker uses a Software-Defined Radio device as a DECT transmitter and receiver, but also when specific DECT RF chip, completely different than the legitimate FP, is employed to launch the active attack.

The results obtained in the experiments demonstrate that the proposed fingerprinting technique can directly be used to detect such active attacks which involve device identity spoofing, in the probable scenario where the hardware used by the attacker does not perfectly match the one of the spoofed DECT device.

V. Conclusion

In this paper we have described an approach for the detection of device identify spoofing attacks in DECT communications based on the fingerprinting of the radio-frequency signal. We have demonstrated that the proposed RF fingerprinting technique, based on the analysis of the transient parts of the DECT signal, is effective in the detection of active attacks that impersonate the identity of the DECT base station, assuming that the RF hardware use by the attacker is not exactly the one of the legitimate station.

Unlike other techniques usually employed in intrusion detection, the RF signature is intrinsically linked to the RF circuit used by the transmitting device and therefore it is not easily manipulable by an adversary.

On the basis of the results obtained, we think that RF fingerprinting is a promising technique for the detection of active attacks on DECT communications and could be considered, in combination with other approaches, for its practical application by intrusion detection systems specialized in this type of wireless communications.

The proposed approach only takes into account the transient part of the signal and it uses a single burst for the classi-

fication. In order to handle more complex spoofing scenarios, where the same RF hardware than the legitimate DECT station is used to conduct the attack, future work will consider the usage of sequences of bursts in combination with other more complex RF fingerprinting techniques.

REFERENCES

[1] ETSI, Digital Enhanced Cordless Telecommunications (DECT). "Common Interface (CI). Part 1: Overview", ETSI standard EN-300-175-1, 2013.

[2] ETSI, Digital Enhanced Cordless Telecommunications (DECT) official website. Retrieved December 2014. URL: http://www.etsi.org/technologies-clusters/technologies/dect.

[3] S. Lucks, A. Schuler, E. Tews, R.P. Weinmann and M. Wenzel, "Attacks on the DECT authentication mechanisms", *Topics in Cryptology CT-RSA*, San Francisco,CA, USA, 2009, pp. 48-65.

[4] I. Sanchez, G. Baldini, D. Shaw and R. Giuliani , "Experimental passive eavesdropping of Digital Enhanced Cordless Telecommunication voice communications through low cost software defined radios", *Security and Communication Networks*. *8(3)*, 2014, pp. 403-417.

[5] K. Nohl, E. Tews, and R.P. Weinmann, "Cryptanalysis of the DECT Standard Cipher", *Fast Software Encryption*, Springer Berlin Heidelberg, 2010, pp. 1-18.

[6] Coisel, I.; Sanchez, I., "Practical Interception of DECT Encrypted Voice Communication in Unified Communications Environments", *IEEE Joint Conference on Intelligence and Security Informatics Conference JISIC*, The Hague, The Netherlands, 24-26 Sept. 2014, pp. 115-122.

[7] S. Yubo, H. Xili, L. Zhiling, "The GSM/UMTS Phone Number Catcher", *Third International Conference on Multimedia Information Networking and Security (MINES)*, Shanghai, China, 4-6 Nov. 2011, pp. 520-523.

[8] Barkan, Elad, Eli Biham, and Nathan Keller. "Instant ciphertext-only cryptanalysis of GSM encrypted communication", *Advances in Cryptology-CRYPTO 2003*. Santa Barbara, California, USA, 2003. pp. 600-616.

[9] P. McHardy, A. Schuler, and E. Tews, "Interactive decryption of DECT phone calls", *Proceedings of the fourth ACM conference on Wireless network security*, Hamburg, Germany, 2011, pp. 71-78.

[10] K. Nohl. "Mobile self-defense (SnoopSnitch)", *Chaos Computer Congress*, Hamburg, Germany, 2014

[11] F. Guo and T. Chiueh. "Sequence number-based MAC address spoof detection", *Recent Advances in Intrusion Detection*. Springer, 2006. pp. 309-329

[12] A. Chouchane, S. Rekhis and N. Boudriga, "Defending against rogue base station attacks using wavelet based fingerprinting", *IEEE/ACS International Conference on Computer Systems and Applications*, Rabat, Morocco, 2009, pp. 523-530.

[13] Y. Sheng, Tan, G. Chen, D. Kotz, A. Campbell, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength", *27th IEEE Conference on Computer Communications INFOCOM 2008*, Phoenix, AZ, April 2008, pp. 13-18.

[14] W.E. Cobb, E.D. Laspe, R.O. Baldwin, M. A. Temple, Y.C. Kim, "Intrinsic Physical-Layer Authentication of Integrated Circuits", *IEEE Transactions on Information Forensics and Security*, 7(1), Feb. 2012, pp. 14-24.

[15] M. D. Williams, S. A. Munns, M. A. Temple, M. J Mendenhall, "RF-DNA fingerprinting for airport WiMax communications security", *Proceedings of 4th International Conference on Network and System Security, NSS 2010*, Melbourne, Australia, 2010, pp. 32-39.

[16] G. Lackner, U. Payer, P. Teufl, "Combating Wireless LAN MAC-layer Address Spoofing with Fingerprinting Methods", *IJ Network Security*, 9(2), 2009, pp. 164-172.

[17] S. Yong, K. Tan, C. Guanling, D. Kotz, A. Campbell, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength", *27th Conference on Computer Communications INFOCOM 2008*, Phoenix, AZ, USA, April 2008, pp. 13-18.

[18] C.K. Dubendorfer, B.W. Ramsey, M.A Temple, "An RF-DNA verification process for ZigBee networks", *Military Communications Conference, MILCOM 2012*, Orlando, FL, USA, 2012, pp.1-6.

[19] J. Hasse, T. Gloe and M. Beck, "Forensic identification of GSM mobile phones", *Proceedings of the first ACM workshop on Information hiding and multimedia security*, Montpellier, France, 2013, p. 131-140.

[20] Anil K. Jain, P. Flynn and Arun A. Ross, "Handbook of Biometrics", Springer-Verlag New York, Inc., 2007.